AIR FORCE SPACE COMMAND

Volume 7, Number 1

# HIGH FRONTIER

THE JOURNAL FOR SPACE AND CYBERSPACE PROFESSIONALS

## SCHRIEVER WARGAME 2010

INSIDE:



# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **NOV 2010** | | **00-00-2010 to 00-00-2010** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **High Frontier. The Journal for Space & Missile Professionals. Volume 7, Number 1, November 2010** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br>**Air Force Space Command (AFSPC/PAI),150 Vandenberg St Ste 1105,Peterson AFB,CO,80914** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | |
| **unclassified** | **unclassified** | **unclassified** | **Same as Report (SAR)** | **56** | |

Headquarters
**Air Force**
**Space Command**
Peterson Air Force Base, Colorado

**Commander**
General C. Robert Kehler

**Vice Commander**
Maj Gen Michael J. Basla

**Director of Public Affairs**
Col Dewey Ford

**Creative Editor**
Ms. Nadine Sage

**High Frontier Staff**

Mr. Steve Tindell
Dr. Rick Sturdevant
Maj Catherine Barrington
Maj Bradley Brewington
Maj Vanessa Hillman
Maj April Wimmer
Mr. Gregory V. Williams

Published by a private firm in no way connected with the US Air Force, under exclusive written contract with Air Force Space Command. This command funded Air Force journal is an authorized publication for members of the United States military Services. The views and opinions expressed in this journal are those of the authors alone and do not necessarily reflect those of the United States Department of Defense, the United States Air Force, or any other government agency.

Editorial content is edited, prepared, and provided by the *High Frontier* staff. All photographs are Air Force photographs unless otherwise indicated.

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

AFSPC/PA
150 Vandenberg St. Ste 1105
Peterson AFB, CO 80914
Telephone: (719) 554-3731
Fax: (719) 554-6013

For more information on space professional development please visit:
http://www.afspc.af.mil

To subscribe:
Hard copy: nsage@sgis.com
Digital copy: http://www.af.mil/subscribe

Cover: Schriever Wargame 2010: US, Australia, Canada, and United Kingdom. Cover designed by Daniel Santistevan.
Back Cover: Blue binary code, digital background, psdGraphics.

# HIGH FRONTIER

The Journal for Space and Cyberspace Professionals

November 2010 Volume 7, Number 1

## Contents



**Next Issue:** ***Implications of the New National Space Policy***

# *Introduction*

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

The Schriever Wargame series has been an incredible success for Air Force Space Command and the National Security Space community, to include our allied and commercial space partners. The series has evolved from the first game in 2001, and has grown both in sophistication and participation. This year, 550 military and civilian experts from more than 30 government agencies and the countries of Australia, Canada, and Great Britain participated in the wargame. The Title 10 wargame series provides an opportunity to examine issues surrounding space policy and rules of engagement and to explore organizational alternatives. As a result, we have a greater understanding of the issues related to conflicts that involve space and cyberspace and we are developing a cadre of military and civilian members who are fluent in these issues in relation to the needs of combatant commanders.

The value of the series is due largely to the high caliber of the participants. I extend my heartfelt gratitude to the advisors and participants who made Schriever Wargame 2010 (SW 10) a rewarding and beneficial experience. The team assembled at Nellis AFB, Nevada included our allies, commercial and industry partners, policy experts, and senior statesmen. Their perspectives and insights increased the sophistication of gameplay and exposed key policy questions; many are examined in this issue of the *High Frontier Journal*. The articles in this edition provide a multi-dimensional view of major lessons learned during the wargame.

It is important to note that the Schriever Wargame series is more expansive than the gameplay at Nellis AFB. The initial interaction for SW 10 began in February 2010 with the Senior Leadership Seminar. This gathering of key government, allied, and industry leaders provided a venue to discuss the SW 10 scenario and to illuminate the key space and cyberspace issues that could influence policy and decision-making in a future conflict. For the first time, we aligned the Schriever Wargame with the chief of staff of the Air Force's Title 10 wargame, Unified Engagement, in order to complement the Air Force-wide wargame effort.


*Figure 1. General C. Robert Kehler and General Lance W. Lord, retired, at the Senior Leadership Seminar in Washington, DC for Schriever Wargame 2010.*

The robustness of the wargame has produced valuable insights and has influenced current policy debates and decision-making. As many of our authors in this issue note, there may be inherent value in evolving the Joint Space Operations Center to a Combined Space Operations Center. Others note that conflict involving space is not isolated to one domain. And we found the Cold War era deterrence theories may not be well suited for application in the space and cyberspace domains.

This issue of the *High Frontier Journal* is a natural precursor to our next issue which will examine strategic space policy. The release of the National Space Policy in June 2010 provides the president's direction for the nation's space activities. As we have found with the Schriever Wargame series, our strategic space policy is vital to freedom of action in and through space. I look forward to the dynamic discussion this topic will generate in the next journal.

**General C. Robert "Bob" Kehler** (BS, Education, Pennsylvania State University; MS, Public Administration, University of Oklahoma; MA, National Security and Strategic Studies, Naval War College, Newport, Rhode Island) is commander, Air Force Space Command (AFSPC), Peterson AFB, Colorado. He is responsible for organizing, equipping, training and maintaining mission-ready space and cyberspace capabilities for North American Aerospace Defense Command, US Strategic Command (USSTRATCOM), and other combatant commands around the world. General Kehler oversees Air Force network operations; manages a global network of satellite command and control, communications, missile warning and space launch facilities; and is responsible for space system development and acquisition. He leads more than 46,000 professionals, assigned to 88 locations worldwide and deployed to an additional 35 global locations.

General Kehler has commanded at the squadron, group and wing levels, and has a broad range of operational and command tours in ICBM operations, space launch, space operations, missile warning, and space control. The general has served on the AFSPC staff, Air Staff, and Joint Staff and served as the director of the National Security Space Office. Prior to assuming his current position, General Kehler was the deputy commander, USSTRATCOM, where he helped provide the president and secretary of defense with a broad range of strategic capabilities and options for the joint warfighter through several diverse mission areas, including space operations, integrated missile defense, computer network operations, and global strike.

# Schriever Wargame 2010, A Political Perspective

**Hon. Thomas M. Davis**
**Director of Federal Relations**
**Delloitte**
**Arlington, Virginia**

In May of this year, the Air Force held the Schriever Wargames 2010 (SW 10), a major exercise focused on space and cyber warfare issues. As in previous years, an international array of players was assembled to provide political, diplomatic, and military perspectives around an evolving geopolitical and military scenario.

Based on my tenure as a member of Congress, I was invited to play the role of the president of US. In this capacity, I tried to bring a realistic political perspective to the games. While the details of the wargame are classified, I can describe what I found to be the most interesting lessons learned from the exercise.

A politician's currency is credit and blame, which is ultimately measured in their ability to either win reelection themselves or to elect/reelect their allies. Public opinion is the key barometer, which is most affected by the public's sense of security—be it physical security or economic security. This point was on vivid display in the mid-term elections in November. The anemic economic recovery and attending high unemployment figures are leading most political pundits to the conclusion that the Democratic Party, which currently controls both bodies of Congress and the White House, is likely to suffer at the polls.

In the role of president at SW 10, I was therefore highly attuned, not just to the political, but to the economic consequences when considering potential courses of action. Indeed, it was fascinating to observe the dominant role economics played in influencing the game.

It is often said that government's main responsibility is the security of the people. Thus, when confronted with an attack of any sort, the expectation is a swift, decisive response. As is so frequently the case in the modern world, however, such a response might not be an option. In the specific case of a cyber attack, there are several key considerations with which a commander-in-chief will have to deal. The most immediate of these is the fact he likely will not initially know who is initiating the assault. Scientific, third party validation of an attack's origin does not always exist. The world would recognize a direct attack against a country's soil or military forces as an invasion of sovereignty, and would likely expect, if not assist, retaliation. What would global reaction be to retaliation if the identity of the aggressor was in doubt? It is safe to say it would be unpredictable, at best. While some might argue international acceptance would be unnecessary, it is reality that political leaders would seek it when weighing a response. The matter would be further clouded by the lack of protocols and agreements pertaining to cyber attacks. Treaties between countries offer support and deterrence in case of attacks on land, sea, or in the air, but if an ally were attacked in cyberspace, would we feel an obligation to attack the aggressor? Would they be compelled to help us? I suspect aversion to economic damage would certainly give pause.

A second and more significant consideration would be the economic ramifications of a retaliation, cyber or otherwise, to a cyber attack. The Internet over which a cyber attack would come has given rise to the global economy in which we now live, an economy in which the fortunes of developed and developing nations are increasingly intertwined. This paradigm of international corporations, interlocking contractual agreements, cross-purchases of national debt, global supply chains, and the expectation of goods and services provided through international trade have created a web of international interdependence that diminishes a purely nationalistic approach to world conflict. Choosing to initiate an attack, cyber or otherwise, would disrupt this web with inevitable—and potentially significant—adverse effects to both aggressor and victim. From a military perspective, a new form of mutually assured destruction—or at least mutually assured disruption—has evolved.

Author and columnist Tom L. Friedman describes this dynamic with his "McDonald's Theory of Warfare," which postulates that no two countries with McDonald's Restaurants have ever gone to war with each other. Why? Because they are too busy making burgers, eating burgers, and selling burgers. They are making money. They have an elevated living standard worth preserving. They have much to lose by going to war. The presence of a McDonald's in a country denotes a certain level of development in their economy and an integration and economic interdependence with the rest of the world.

One would hope thoughts of two all-beef patties, special sauce, lettuce, cheese, pickles, onions on a sesame seed bun would enter into the decision matrix of any developed state contemplating a cyber attack on another member of the global economy.

*Figure 1. Hon. Thomas M. Davis acting as president of the US during Move 0 (wargame kickoff) of Schriever Wargame 2010.*

In the confused aftermath of a coordinated cyber attack, elected officials would have to weigh these economic considerations, especially if they were working on suspicion, but it would be the case even if we were certain of the culprit. As the debate as to how to respond played out, one can be sure multinational corporations would be active participants.

Regardless of what one's opinion towards them might be, multinational corporations have evolved into a true fifth estate, and as our experience at the war games bore out, are extremely averse to disruptions in the business cycle. By law, businesses owe their allegiance to shareholders from around the world, and global customers and offices around the globe will be subject to different pressure points than we have witnessed in the past. To some extent this is an uncharted area of 21st century military conflicts. In the past, businesses traditionally exerted influence to resolve these conflicts or show loyalty to their home nation. In the future, national interests become more difficult to discern and could well be secondary to business interests. In any event, we can be sure they will not hesitate to exert unprecedented pressure on political leaders to end a conflict or limit a response.

As a result, countries that rely on economic growth to sustain their political model will, understandably, show hesitancy toward overt conflict and will influence their response to provocations and attacks. Understanding the likely corporate reaction in advance to likely scenarios should be a priority of military and political leaders, specifically how it would translate into political decision-making. A related component would be an understanding of the global supply chain.

That is not to say mutual assured anything is reason enough to assume another nation-state would not initiate a cyber attack. First, the potential consequences are far too great. There is no end to the mayhem and chaos a cyber "Pearl Harbor" would unleash; the thought that the perpetrator is also suffering would not provide much comfort.

Second, we already know the US is subject to thousands of cyber attacks every day. While the scope of these attacks is limited—often involving industrial espionage, intellectual property theft, or cyber vandalism—the ramifications are still significant in terms of keeping our military and commercial advantage. This is reason enough to develop a robust defense in cyberspace.

Third, potential cyber attackers come in many shapes and sizes. The considerations discussed above assume a country and government interested in remaining a part of the global economy. A rogue nation like North Korea, on the other hand, displays interests that are exactly the opposite. The government of Kim Jong Il has been determined to do anything but interconnect with the rest of the world. As satellite imagery has shown, it seeks to literally keep its citizens in the dark as to the advancements implemented by modern societies. Nevertheless, such despotic regimes understand the importance of cyberspace and can inflict large scale damage through cyber attacks. After all, it is not so painful to disrupt the information superhighway if you are riding a mule. Moreover, the low barrier to entry for a cyber attack—no need for a standing army, no massive logistical capability, relatively inexpensive training opens the door to a host of bad actors beyond nation-states. Teenage punks, organized crime, or terrorist organizations are all potential aggressors capable of doing significant harm.

A final point—command and control is a significant challenge for any military in response to conventional challenges. A cyber attack adds an additional layer of complexity to the task. In the wake of any kind of attack or disaster, the public—and politicians—want to know who is in charge. A cyber attack will affect many different segments of the economy and society, and a mélange of federal, state, and local officials will be involved in the response. In order to avoid confusion, it is vital that a cross-governmental chain of command be established.

In closing, SW 10 illustrated that cyber warfare continues the march towards unconventional warfare. Indeed, conflicts between nations are seldom the cut-and-dry affairs of blue versus red, with tanks and airplanes boldly proclaiming their owner's flags. Increasingly, a no-holds-barred approach is simply not an option. Just as counterinsurgencies in Iraq and Afghanistan have displayed the political difficulties of fighting a limited engagement, so too will conflicts in cyberspace present political and military leaders with a complex array of considerations. The games were an important reminder that military, political, and economic leaders must work in concert to adapt to this evolving battle space.

**Hon. Thomas M. Davis** (BA Political Science and Economics, Amherst College; JD, University of Virginia) joined Deloitte in November 2008 after serving 14 years in the US House of Representatives. In his current capacity as director of federal relations, he serves as a subject matter expert on political, policy, and procurement matters for Deloitte practitioners and clients.

During his tenure in Congress, which included six years as the chair and ranking Republican member of the House Committee on Oversight and Government Reform, Mr. Davis compiled an impressive record of legislative accomplishments. Among these were the Federal Information Security Management Act, which established an information security framework for the federal government; the District of Columbia Control Board Act, which is credited with restoring DC's financial credibility; the National Capital Transportation Amendments, which authorized $1.5 billion for the Washington Metro system; the Family Smoking Prevention and Tobacco Control Act, which authorized the Food and Drug Administration to regulate tobacco products; and the Postal Accountability and Enhancement Act of 2006, which marked the first comprehensive overhaul of the Postal Service since 1971.

Mr. Davis also led a number of key oversight efforts, most notably the investigation into the use of performance enhancing drugs in professional sports. He also chaired the committee to investigate the Bush administration's response to Hurricane Katrina.

Before coming to Congress in 1995, Mr. Davis served as a supervisor on the Fairfax County Board for 15 years, rising to chairman in 1993. Simultaneously, he served as the general counsel of Litton PRC, specializing in federal procurement law and policy.

*Senior Leader Perspective*

# The Complexities of America's National Security: Enabling A New Generation of Leadership

**Hon. George W. Foresman**
**Former Under Secretary**
**US Department of Homeland Security**

America's strategic national security environment continues to evolve in both its breadth and complexity. This evolution demands that current and future generations of civilian and military leaders expand their understanding of the range of global risks facing the US and the interdependencies that exist between what can harm our nation and the steps we must be capable of taking to defend our interests. Developing the integrated capabilities that will be required to ensure America's security today and in the future requires 21st century leadership.

The National Security Strategy for the US, released on 27 May 2010, underscores the overarching obligation for America, and to be enabled through current and future generations of civilian and military leaders.

> At the dawn of the 21st century, the United States of America faces a broad and complex array of challenges to our national security. Just as America helped to determine the course of the 20th century, we must now build the sources of American strength and influence, and shape an international order capable of overcoming the challenges of the 21st century.…
>
> Our national security strategy is, therefore, focused on renewing American leadership so that we can more effectively advance our interests in the 21st century.

While the National Security Strategy defines America's goals, we must also provide the tools to transform the words into accomplishments. Key to this transformation is delivering the right leadership at home and abroad. Clearly national leadership depends on ideas and vision. Most importantly it requires individuals who transform words into action.

Thus a dilemma facing current civilian and military leaders—adapting to a generation of challenges far different from those they faced during their own formative years of education, service and growth. In many respects, in the context of the individual, the institutions they represent and the processes that enable their efforts, America is in the midst of a generational transition of its national security apparatus and its underpinning strategies. Generational transition does not simply mean "out with the old and in with the new." Rather it implies preserving the foundational approaches that have served the US well during countless domestic and international crises in the 20th century, but must now be adapted to current requirements and conditions.

## Appreciating the Global Interdependencies

During the height of the Cold War there was no mistaking the most likely adversary and the highest probability scenarios that could potentially undermine America's national security and even conceivably threaten our national survival. A generation of civilian and military leaders grappled to both understand the nature of the threats confronting the US and to develop strategies to deter potential conflicts and if necessary, to prevail.

In our 20th century environment civilian and military leaders benefited from a degree of certainty and stability. America was more able to readily identify potential adversaries and possessed an appreciation of their "ultimate red lines," and we also had confidence that they knew ours. In number and capabilities, potential adversaries were fewer and less menacing. The speed by which information flow and most crises erupted was, by comparison to today, much slower. Military and economic actions taken by the US or others in one part of the world could be exquisitely targeted and isolated. Together these did not eliminate the threats confronting America. But they did provide America's leaders with a more stable environment in terms of time, simplicity, and mutual understanding to formulate strategies and make decisions about the actions they needed to undertake.

Today many of external global influencers have changed—economically, geopolitically, and societally. These, along with others, must be contemplated in new ways by leaders in the 21st century. Individually and collectively these factors impact the national security decisions our leaders make and the actions they choose to pursue. The US and our civilian and military leaders are neither isolated from the remainder of the world, nor can we afford to be. Present and future leadership decisions and strategic direction must adjust for these dynamic changes.

The US is inextricably linked to the trillions of dollars of global financial transactions occurring daily. More than ever before, transactions at home and abroad directly and immediately affect our overall national wealth, debt, and economic stability. This means that economic considerations have greater influence than in the past. Super-powers have been replaced by a myriad of competing nations possessing heightened levels of global political, military, and economic influence. This challenges our interests abroad—both in the context of our existing partnerships and our ability to create new alliances to help resolve future conflicts. The internet and resulting capacity to connect previously isolated societies have resulted in new dimensions of engagement—with positive and negative consequences. Instant communications and hundreds of billions of daily e-mail messages not only connect the global populations, promoting enlightenment, but can also spread misinformation and foster conflict. More than ever before information technology tools have evolved to be capable, with lightening speed, of also being used as weapons of mass disruption and destruction.

## A Useful Paradigm for Today's Leaders?

America's current national security environment is demand-

ing—by the speed in which situations occur, the greater interdependencies that exist between problems and their solutions and the growing ambiguities created by the added reliance on a proliferation of information. Today's civilian and military leaders must be adaptable to these new dynamics while retaining sage lessons of America's past. To some degree the challenges we face in our space and cyberspace domains provide useful illustrations of the complexities that leaders will increasingly face in today's other global commons.

The US maintained a dominating and, to some degree, solitary presence in space and cyberspace during the last century. This is no longer the case. America shares both physical and virtual presence in these domains with other countries, groups, and individuals, including a large contingent of commercial operators, many of each category with capabilities on par with those of the US.

Today, virtually every human being and government on Earth depends on some aspect of global space and cyberspace domains to ensure their safety, security, or prosperity. The activities they enable are interwoven into the very fabric of our daily lives. America's military, public safety, transportation, and other essential crisis response organizations are supported by global satellite communications, precision navigation, and wide area weather patterns and predictions to name a few. The military specifically depends on space and cyber systems to provide targeting information for units and individual weapons, global and regional missile warning, and a wide range of computing capabilities essential to modern warfare.

These same space and cyberspace systems enhance our national wellbeing by providing crucial information that informs civilian and military leaders. They enable America's ability to determine the extent of a potential adversary's strategic capabilities and their readiness. They allow us to monitor an adversary's operational activities and preparations, verify arms control agreements, assess force activities, and in near real-time, the intentions of an adversary's leadership, among others. Together space and cyberspace are significant components of the US intelligence and military operations and capabilities.

Yet space and cyberspace are no longer domains solely dedicated to science and national defense. They also underpin our national economy in critically important ways. Precise timing signals provided by the GPS satellites regulate global and national financial institution transactions, individual automated teller machines and automated credit card validation services like those that support gasoline sales at the pump. Space and cyberspace capabilities enhance environmental monitoring, agricultural forecasting, real-time weather forecasting, and support disaster relief operations following catastrophes. They enable the provision of a wide array of life-saving medical and health care, from urban centers to the most remote reaches of the globe. Quite literally space and cyberspace have transitioned during the past four decades from being unique tools of the US government to become essential backbones of global life.

Given these factors it is no surprise that the potential global consequences of even a minor conflict in space and cyberspace domains have evolved to become far-reaching. In the same manner, the implications of civilian and military leadership decisions about the steps to take to deter conflicts in these domains, and if necessary defeat adversaries, are equally far-reaching. The leadership decisions necessary to preserve and protect America's interests in space and cyberspace require both an understanding of the interdependencies between these and other domains and an appreciation of the intricacies required in pursuing viable courses of action. Just as the space and cyberspace domains are interwoven so too are the strategies to protect and defend them—crossing both public and private sectors and international boundaries.

To be clear there has always been mutual dependency between the military and civil government and to a lesser degree the private sector in addressing America's national security contingencies. However, 19th and 20th century conflicts allowed for clearer lines between the roles and actions of the military, civil government, international partners, and the private sector. Accordingly, responding to a crisis was often unilateral—with little interaction and coordination required between the various elements of the US government.

Today's global condition is characterized by a proliferation of other nations and the private sector engagement across both the space and cyberspace domains and a much more interdependent and interconnected world. The absence of distinct geographic and political boundaries in space and cyberspace coupled with our nascent understanding of second and third order effects arising from defensive or offensive operations in these domains create greater potential for unintended collateral disruption and destruction that extend well beyond the intended target and can encircle the globe in seconds.

Strategies of the past—predominately leveraging the forces of the military to advance national security objectives, while the ultimate fail-safe, is not necessarily the optimal approach for defending America's interests in space and cyberspace. Interdependencies in these domains, both in terms of cause and effect, by their very nature transcend America's military and incorporate a broad range of civilian, private sector, and international equities. The ability of civilian and military leaders to understand these equities and make better informed decisions is critical.

Accomplishing improvements in civilian and military leadership decision making will require enhancements in the supporting structures and strategies for protecting space and cyberspace. These enhancements are not unlike the advances being implemented under the concept of "smart power," where national security objectives and leadership direction are advanced by mixing a range of the right instruments of national power, in a manner best structured for addressing a given scenario and with a full understanding of the interdependencies among cause and effect—implementing the so called comprehensive approach.

These changing dynamics and characteristics necessitate military and civilian leaders and operational capabilities enabled by a new generation of technology, policy, and organizational structures. These capabilities must be agile in order to continuously adapt to the constant state of evolution and must allow for integration of efforts that transcend all domains, including space and cyberspace. In many respects these are the same characteristics that drive us in all of our global interactions.

## A Laboratory for 21st Century Leadership Learning in Space and Cyberspace

The US Air Force began the Schriever Wargame series in 2001 with the goal of developing a deliberate approach to strengthening America's capabilities for preserving its national security interests in space. More recently, in light of interdependencies it has added the cyberspace dimension. Key to Schriever's success has been the building block approach. Rather than attempting to "boil the ocean" in its first few games, there has been a steady progression in both the scenario and corresponding education required to create a common level of knowledge across the range of participants—from tactical operators to strategic leaders and decision makers. Consequently, the deliberate approach has allowed transition from the tactical to the strategic and from the military centric to the whole of nation(s), that is, comprehensive approach. The Schriever series has provided a critical lens by which to view and assess the new dynamics of America's national security leadership and decision making.

The first four Schriever Wargames series (I-IV) were almost exclusively dedicated to exploring issues of space and to a lesser degree focused only on the US government—both military and civilian. The initial narrow focus was dictated by two key factors. The complexity of the space domain with regard to America's national security objectives necessitated that military and civilian leaders have an improved understanding of the space domain as a foundation for exploring alternative national security operational concepts and approaches. Secondly, given the evolving nature of the space domain—access by a multitude of other nation's and commercial providers and the corresponding impacts on America's vital national security interests, the range of government centric issues that requiring attention was significant. Treating the space domain separately provided a manageable starting approach for what would become a broader combined effort involving cyberspace.

Building on the first four wargames, both Schriever V Wargame (2009) and Schriever Wargame 2010 (SW 10) added levels of complexity, reflecting the current and future global necessities that increasingly drive how the US and its civilian and military leaders understand and organize to addresses national security requirements—leveraging "whole of government" capabilities, additional cyberspace focus, stronger engagement of international partners and more commercial sector integration.

Key to understanding the integrating value of this war-game series and most recently SW 10, is that backdrop to each scenario has been a conventional national security crisis. They are conventional because they are premised on US military operations in some region of the world, involving employment of traditional and generally better understood land, sea, or air military capabilities, supported by other functional areas of the US government that are either supported or inhibited by actions occurring in the space and cyberspace domains.

The Schriever Wargame series contemplates space and cyberspace as domains that provide capabilities that enable national security actions in the more traditional land, sea, and air "domains," but simultaneously they are also potential battlefields unto themselves. Strengthening both the military's and the "whole of government" ability to better understand and protect America's increasingly complex interests in space and cyberspace and their corresponding effects on our vital national, homeland, and economic security imperatives and civilian and military leadership requirements is a primary Schriever objective. Accomplishing this objective—because of the significant interdependencies both between space and cyberspace coupled with their relevance to national military, intelligence, economic, and diplomatic activities has been in many respects a groundbreaking experience.

The overarching challenge facing civilian and military leaders as they seek to strengthen the national security of the US in space and cyberspace is illustrative of a poignant and equally applicable fact to the other global domains. Future conflicts will not be as in the past—easily constrained to clearly delineated battlefields on land, sea, or in the air, with distinct national boundaries and perpetrated by easily recognizable adversaries with whom we have the optimal level of understanding of their strategic intents. Rather we will face potential adversaries capable of cloaking their actions in the darkness of space, the complexity of the internet, or hidden among innocent civilians, countryside, and in the name of religious beliefs, transcending traditional geopolitical boundaries.

The Schriever Wargame series is grounded in an evolving understanding of the realities of these and other current and future national security strategies and leadership requirements. The wargame recognizes that workable operational approaches to support America's national security objectives cannot occur in a vacuum. Understanding the national and international dimensions, political influences, and other external conditions such as business imperatives that drive international corporate decisions about alliances and customers, and how these and other factors influence the decisions of civilian leaders and military leaders is paramount to developing operationally viable approaches in advance of a conflict. They are also essential to better crisis decision making in the midst of an event, especially given the speed by which events occur.

The overarching benefits derived from the series and especially the most recent SW 10 is three fold. First, it provided a venue for the US to further explore "whole of government" integration of diplomatic, informational, military, and economic capabilities as a means for addressing a national security crisis. In this vein it has helped to highlight approaches for military and civilian leaders to more effectively integrate their decision making.

Secondly, it provided the US military a realistic backdrop for assessing the nexus between its traditional doctrines for land, sea, and air domain military operations and parallel but lesser developed approaches for addressing space and cyberspace, from both the tactical and strategic levels. SW 10 also created an opportunity to more accurately define our national security capabilities and vulnerabilities in space and cyberspace, as a precursor to reducing future risk by enhancing our resiliency in these domains.

Most critically SW 10 allowed for improved understanding of many of the challenges America's civilian and military leaders will face in addressing 21st century crises. These included the full range of potential strategy and structural challenges facing the US national security apparatus—land, sea, air, space, and cyberspace domain conflicts, requiring a range of diplomatic,

informational, military, economic solutions, orchestrated across the military and civilian government, and engaging international partners and the private sector.

National security requirements and strategic influences for US space and cyberspace operations are rapidly evolving. The Schriever Wargame series has underscored the need to evolve America's corresponding operational approaches as well.

Several overarching themes have emerged from the SW 10 and the series as a whole.

- America's capabilities to secure our national, economic, and homeland security interests are inextricably dependent on highly resilient space and cyberspace enterprises; civilian and military leaders across the national security enterprise must comprehend the resiliency required to ensure that America maintains the needed levels of security demanded by current and projected conditions.
- The implications of space and cyberspace on America's overall security environment are inadequately understood across the full range of military and civilian leaders with responsibilities dependent on these domains; accordingly our national vulnerabilities are higher because of the lack of sufficient information available to leaders to make well informed routine and crisis management decisions.
- The implications of space and cyberspace to our potential adversary's security environments are also inadequately understood by civilian and military leaders; accordingly this impedes opportunities for America leaders to select the best options for deterring a potential crisis and if necessary, wining conflicts.
- Preserving space and cyberspace for peaceful purposes and defending national interests requires clearly defined and functioning integrated strategies, organizational structures, and situational awareness/intelligence sharing capabilities across the US government and with international and selected private sector entities that do not exist today; the absence of a fully developed, implemented, and regimented approach increases the possibility of confusion, ineffective response to a potential or actual crisis, and may result in unnecessary escalation of a conflict.

The proliferation of non-US lead capabilities in both the space and cyberspace domains is producing demonstrable global advances. Simultaneously, these circumstances are creating new operational imperatives for America's civilian and military leaders to enhance both their individual knowledge of and America's capabilities required to protect our national interests linked to space and cyberspace. The Schriever Wargame series reflects this modern national security challenge emanating from the increasing intersect between the civilian and military functions of government, public and private sector interaction, and with the international community, in protecting America's and increasingly, global vital interests for security and stability in space and cyberspace.

The Schriever Wargame series contributes to the US understanding of the challenges to preserving America's national security in space and cyberspace. Concurrently it provides a practical laboratory for pursuing alternative concepts for whole of nation(s) comprehensive approach to addressing America's current and future national security contingencies, whether in space, cyberspace, or elsewhere. Its conduct reflects the broad engagement beyond the US government, especially our military that is necessary to effectively understand, explore, and prepare contingencies—taking into account the range of possible scenarios and interdependencies arising from the space and cyber domains. SW 10 is the first US military sponsored strategic wargame to examine space and cyberspace concurrently.

The value from SW 10 cannot simply be measured in the conduct of a wargame. Its ultimate benefit will be derived when the steps taken to translate the lessons of the wargame into tangible improvements to support current and future generations of civilian and military leaders. Implementing a more robust capacity to deal with future national security conflicts in the space and cyberspace domains has the dual benefit of strengthening our readiness in those domains while simultaneously allowing us to improve our capabilities for more other traditional, albeit, increasing complex land, sea, and air domains.

The lessons identified by the Schriever Wargame series are not futuristic concepts. They are imperatives that confront of the US and our allies today. SW 10 provided the tangible evidence that we must give more attention to our national security capabilities, including developing the understanding of civilian and military leaders relating to space and cyberspace operations. The potential risks from these domains to our national, economic, and homeland security are significant. SW 10 and the series as a whole have made a compelling case that immediately addressing space and cyberspace related operational capabilities is a national imperative. So too is our ability to prepare a broader array of current and future generations of civilian and military leaders to operate in a complex, fast paced, and increasingly ambiguous 21st century national security environment, including space and cyberspace. The potential consequences to America's national security and economic well being of failing to accomplish either, could be grave.

**Hon. George W. Foresman** (Virginia Military Institute) is currently president of Highland Risk and Crisis Solutions, Ltd. Mr. Foresman also serves as a senior advisor and facilitator for the Schriever War-game. Previously, Mr. Foresman was confirmed by the US Senate in 2005 as America's first under secretary of preparedness at the US Department of Homeland Security and subsequently became the first under secretary for national protection and programs. He vice-chaired the Congressionally established Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (1998-2003) and served in Virginia state government for two decades, including as a Cabinet official.

# The Challenge of Integration: Lessons from Schriever Wargame 2010

**Lt Gen Larry D. James, USAF**
**Commander, 14th Air Force and**
**Commander**
**Joint Functional Component Command for Space**
**US Strategic Command**
**Vandenberg AFB, California**

The 2010 edition of Air Force Space Command's Schriever Wargame (SW 10) explored the complex world of 2022 … a world comprised of peer space and cyberspace competitors; a world where reliance on coalition space and cyber capabilities would be key to warfighting success; and a world where space and cyberspace capabilities would be challenged both kinetically and non-kinetically in the air, sea, land, space, and cyber domains.

## The SW 10 Wargame

For nearly a week, almost 600 participants and supporting staff worked through the 2022 scenario. Similar to the 2009 Schriever V Wargame, SW 10 was designed to evaluate leveraging all national government instruments of power in a strategic-level engagement. However, SW 10 also sought to expand on Schriever V by exploring how the US could leverage capabilities provided by commercial and coalition partnerships. More specifically, the wargame's objectives were to:

1. Investigate space and cyberspace alternative concepts, capabilities, and force postures to meet requirements.

2. Examine the contributions of space and cyberspace to future deterrent strategies.

3. Explore integrated planning processes that employ a whole of government approach to protect and execute operations in space and cyberspace domains.

As the scenario unfolded, participants gained a number of significant insights regarding the employment of space capabilities in future conflicts between space powers. Key among these insights was the realization that space force organization, military-industry integration, entanglement with cyberspace and the reconstitution of space forces would be fundamentally important concepts.

Certainly, SW 10 was too brief for the participants to appreciate the full implications of these insights. That will require deliberate and comprehensive study over the coming months. The concepts outlined here are intended to contribute towards that effort.

## Space Organization and Construct

The SW 10 scenario validated the importance of coalition space capabilities. It illustrated the need for mechanisms to employ those capabilities in a way that is consistent with national objectives while being value-added to the coalition. The game explored three related organizations to achieve this: a Combined Space Operations Center (CSpOC), a Combined Joint Task Force-Space (CJTF-Space), and a Space Council.

The CSpOC provided a means to direct the full range of coalition space capabilities at the operational level of war. The CSpOC concept, exercised in Schriever V, was matured considerably for SW 10. Its responsibilities were expanded and more fully developed, its size was increased considerably and coalition personnel were added to its membership. These changes enabled improved communications across the coalition, facilitated more rapid deployment and employment of coalition capabilities, and allowed coalition partners to be fully integrated in strategy, planning, and execution. The CSpOC was one of the clear successes of SW 10 and, as such, it is as an excellent model upon which to base a real-world combined operations center. If the adage that we must train as we expect to fight is true, then the lesson of SW 10 is clear: we must work to establish a CSpOC today if it is to be employed successfully in a future time of crisis.

In keeping with US Joint Doctrine, the CSpOC reported to a CJTF-Space, which served as the single, integrated military structure to direct the employment of coalition space forces. SW 10 was the first use of a CJTF-Space in the Schriever Wargame series. As a result, the roles and responsibilities of the CJTF were not sufficiently developed to allow full concept development. Still, the CJTF filled an important gap identified during Schriever V—that the CSpOC needed a higher level military organization to guide its efforts.

Similarly, to ensure the CJTF employed each coalition member's space capabilities in accordance with its national constraints and in pursuit of its national objectives, SW 10 employed a Space Council. This council brought together high-level policy representatives of each coalition nation to develop strategic guidance. Like the CJTF-Space, this construct needs further development. In particular, SW 10 highlighted the need to examine the authorities that a Space Council requires, the relationship of the Space Council to the combatant commander and his/her staff,

*As the scenario unfolded, participants gained a number of significant insights regarding the employment of space capabilities in future conflicts between space powers.*

*Subject matter experts from industry are uniquely qualified to understand how best to employ their space systems; thus they are ideally suited to develop employment strategies and identify how their assets fit in broader strategy-to-task planning.*

and lines of authority from the Space Council to the CJTF and participating nations.

While it was clearly valuable to explore strategic-level organizations at the SW 10, the CJTF-Space and Space Council concepts, as employed, were relatively new and immature concepts. Still, both organizations showed promise. As such, policies and operating concepts for a CJTF-Space should be further developed and re-evaluated in future wargames and exercises. One of the primary recommendations stemming from SW 10 is to create an International Space Cooperation Working Group, with appropriate sub-working groups focused in particular functional areas, to work through the task of establishing a CSpOC and CJTF-Space. US Strategic Command has begun discussions with key coalition partners to develop the way ahead for establishing a CSpOC. These early discussions suggest the initial iteration of the CSpOC will likely be based on virtual connections and data sharing between coalition nations' space operations centers and the US Joint Space Operations Center.

## Industry Integration

Much as SW 10 built on the lessons of Schriever V regarding coalition space capabilities, SW 10 also sought to expand the role of the space commercial sector by improving on the limited industry integration experienced in Schriever V. The intent was to tighten linkages between industry and CJTF-Space. Representatives from key space industry organizations were attached to the CSpOC to participate in operations planning and execution. With these representatives, the CSpOC was able to rapidly identify and leverage industry capabilities to meet operational needs. By all accounts, the inclusion of industry representatives in the CSpOC was a clear success. However, the game highlighted two challenges we must overcome to realize the full potential of a partnership between industry and CJTF-Space.

First, CSpOC planners need a better understanding of how to leverage the industry "order of battle." That is, planners need to be familiar with the assets industry has available for use, capabilities they provide, costs for using those assets, and how long the assets might be available. Gathering this information from companies and consortiums in multiple countries will require considerable time. We need to begin compiling this "order of battle" information now.

The second challenge is the need to involve industry in CJTF-Space deliberate planning processes so that the information identified above is included in concept of operations, concept plans, and operational plans (OPLAN). Subject matter experts from industry are uniquely qualified to understand how best to employ their space systems; thus they are ideally suited to develop employment strategies and identify how their assets fit in broader strategy-to-task planning.

Finally, as demonstrated in SW 10, once open conflict extends to space, protection and liability become primary concerns for industry. These concerns must be addressed explicitly during deliberate planning. There are several hurdles that must be overcome before industry representatives can become a routine part of military deliberate planning—for example, ensuring proper security clearances, determining the best and most appropriate representatives to represent industry, constructing a legal framework that governs the government-industry collaboration, and so forth.

Despite these challenges, SW 10 was a pivotal event in ongoing efforts to explore how best to integrate industry capabilities with government and coalition space capabilities. Certainly, there is more work to do, but the lessons of SW 10 suggest that the outcome will be worth the effort.

## Space and Cyber Entanglement

SW 10 offered an important revision to what was, perhaps, the central lesson of Schriever V; namely that conflict in space would most likely begin in cyberspace (e.g., cyber attacks on networks, links, command and control systems, etc.). As the SW 10 scenario unfolded, however, it became clear that space and cyber are "entangled" across the entire spectrum of conflict. In other words, space and cyber systems are so intertwined, that the opening actions of a conflict could take place in either medium—and, more than likely, the effects would be felt across both domains. This suggests a critical need to understand linkages between the mediums and employ a fully integrated strategy.

Although SW 10 participants understood the need for fully integrated space and cyber operations, the coalition executed a campaign whose space and cyber courses of action were often developed independently and were more often than not disconnected. This was a result of the speed of space and cyber engagements, the inability to accurately assess and attribute adversary space and cyber engagements, the lack of doctrinal integration processes, the lack of joint integration tools, and a relative void of personnel steeped in the integration of space and cyber activities. There were certainly exceptions to this general observation, but most participants recognized that, in the aggregate, there is much to do before space and cyber are truly integrated.

The team identified two specific recommendations to improve space-cyber integration. First, space and cyber planners should develop standing integrated space-cyber branch plans to anticipate plausible or probable events. For example, an antisatellite launch from an adversary, jamming of communication downlinks, or a launch of a critical allied resource offer opportunities to develop standing branch plans codifying how space and cyber communities will react. Much like standing OPLANs, these branch plans should be exercised regularly to ensure a robust, integrated, and ready capability.

The second recommendation is to develop processes and tools enabling continuous integration between space and cyber. Planners and operators need tools that provide an understanding of

friendly space and cyber systems, real time situational awareness of those systems, the ability to rapidly defend systems under attack and the ability to deny/degrade the adversary's ability. These requirements are not unique to space; they are essential to operations in every domain. These tools must be supported by processes that enable integrated planning, joint targeting, and cross-domain mutually reinforcing operations. Significant work is being done in this area, but, as demonstrated in SW 10, there is considerable work yet to do.

## Ability to Protect and Reconstitute Space Forces

Space capabilities are an asymmetric advantage for US military operations. They provide the ability to see with clarity, communicate with certainty, navigate with accuracy, and operate with assurance.[1] Current and future adversaries recognize this and will almost certainly seek to deny those capabilities to us and our allies in times of conflict. This was definitely the case in SW 10, where the adversary attacked aggressively, deliberately and decisively on a variety of vectors to deny US and coalition forces access to space capabilities. As a result, a fundamental lesson from SW 10 is the need for the US and its coalition partners to be able to protect space capabilities and be able to reconstitute them should their efforts to protect fail.

During the game, adversary forces had a significant offensive advantage against US space capabilities. They executed counterspace operations at the time and place of their choosing, with little warning. This situation was exacerbated by the limited ability of the US and coalition to reconstitute their space forces. The combination of these realities ensured the coalition suffered from significantly degraded space capabilities during the conflict and well into the post conflict period.

The lesson drawn from this situation is the US needs an effective mix of capabilities allowing it to protect assets, operate through hostilities, and reconstitute when necessary. Pursuing these capabilities will require increased collaboration with coalition and industry partners. It will also demand continued progress in domestic military capabilities such as the Space Protection Program initiative and the responsive reconstitution options being developed by the Operationally Responsive Space program. Producing an ability to counter the type of determined adversary presented in SW 10 will take considerable time. However, implementing a broadly integrated strategy utilizing the above capabilities will ultimately ensure our ability to maintain the high ground of space in any future conflicts.

## Conclusion

The recently-signed National Space Policy states:[2]

> The US will employ a variety of measures to help assure the use of space for all responsible parties, and, consistent with the inherent right of self-defense, deter others from interference and attack, defend our space systems and contribute to the defense of allied space systems, and, if deterrence fails, defeat efforts to attack them.

SW 10 provided an invaluable opportunity to explore these concepts during a time of conflict with a notional peer adversary. It also greatly illuminated the challenges we are likely to have in defending our space systems, integrating with allied and commercial capabilities, operating in a contested environment, and conducting operations at the speed of light in both the space and cyber domains. In SW 10, as in Schriever V, the power of the coalition was evident, and the need for integrated planning and operations across all domains and all coalition nations was unambiguous. However, the necessities were equally obvious—new space organizations, integration with industry, the ability to integrate space and cyber mission areas; and the ability to protect and reconstitute space forces are all needed, so we are prepared to move forward. The lessons have been clearly identified … now we must implement specific actions to translate the lessons of SW 10 into reality.

*Notes:*

[1] General C. Robert Kehler, "Military Space Programs in Review of the Defense Authorization Request for Fiscal Year 2011 and the Future Years Defense Program," Statement before Congress, Washington, DC, 21 April 2010, http://www.afspc.af.mil/library/speeches/speech.asp?id=548.

[2] *National Space Policy of the United States of America*, President of the United States, Principles (28 June 2010) 3, http://www.whitehouse.gov/the-press-office/fact-sheet-national-space-policy.

**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, and commander, Joint Functional Component Command for Space (JFCC SPACE), US Strategic Command (USSTRATCOM), 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 entered the Air Force as a distinguished graduate of the US Air Force Academy in 1978. His 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 Air Force Space Command. 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.

At the time of publication, General James has been confirmed by the Senate for assignment as deputy chief of staff, intelligence, surveillance, and reconnaissance, Headquarters US Air Force, Washington, DC.

# Schriever Wargame 2010: Thoughts on Deterrence in the Non-Kinetic Domain

**Maj Gen Susan J. Helms, USAF**
**Director of Plans and Policy**
**US Strategic Command**
**Offutt AFB, Nebraska**

In May, a large team from US Strategic Command (USSTRATCOM) participated in Schriever Wargame 2010 (SW 10), hosted by Air Force Space Command (AFSPC) at Nellis AFB, Nevada.

The Schriever Wargame series is the AFSPC commander's game, designed to examine space and cyberspace operations in depth. The wargame allows participants to consider the diplomatic, economic, informational, and military influences that will shape deterrent strategy and defensive operations for space and cyberspace. It provides information for future requirements, examines organization constructs, and provides a venue for advancement of space and cyberspace policy and rules of engagement. Although SW 10 was a service wargame, USSTRATCOM has been a key mission partner of the series since its inception 10 years ago.

An important conclusion we have drawn through the experience of the Schriever series is that some lessons about deterrence from the Cold War era do not necessarily translate to the space and cyber realm.

A critical objective of SW 10 was to examine how to wage deterrence in space and cyberspace, and to explore integrated planning processes that employ a comprehensive, "whole of nations" approach to execute operations across multiple domains. Other objectives of the wargame were to demonstrate strategic posture and resolve, and to effectively conduct strong coalition operations to, if necessary, recapture the initiative in space and cyberspace.

Building upon previous wargames of the Schriever series, this year's wargame provided the opportunity to expand on previous lessons, test new concepts, and importantly, to incorporate new elements of integration across space and cyber, functional and geographic combatant commands, government and industry, Department of Defense and interagency, and the US and her allies and partners.

From the very first move of the wargame, the entire scenario served to remind us all how difficult it can be to think through and implement an effective deterrence strategy to forestall a crisis.

The year was 2022 and, in response to a perceived provocation, a regional adversary disabled the cyber and space assets of a key US ally. Over the course of the next four days of the wargame, the crisis escalated to the senior executive level, and soon encompassed us all, including partners beyond our own government and nation. Interagency leadership gathered to weigh in on how to counter and deter future conflict—and how to coordinate actions among multiple nations to achieve the best effect.

Throughout the process, as we and our allies debated about what to do to deter the adversary from threatening our space and cyberspace capabilities, it became clear that the enemy was not deterred from further escalation. As we came to learn, the leaders of this provocative regional state had defined their objectives (although those objectives were not obvious to us) and had already thought through the overall costs and benefits of their plan. In other words, they had assessed our likely behavior in the context of the scenario at hand, determined that, for them, the benefits of action outweighed the risks and they made their decision to "move out." At that point, options for deterrence by the US and her allies were "late to need."

As a coalition, what *were* the options?

Could we take some actions that would de-escalate the conflict and return to status quo? Was there a way to encourage restraint, such that the flashpoint scenario that began the wargame could dissipate? What did the adversary actually want, and what were they willing to incur as a cost to get it? Had they analyzed in advance the most likely responses of the coalition once they "kicked over the anthill"—and did we behave just as they had assessed we would? If so, then we were unwittingly and obediently following a script that the adversary had already written for the campaign, and our military actions to deter would have no effect on their decision calculus. The predictability of our response—and their accounting for it—was a part of their cost/benefit trade space well before they made their first move.

## Principles of Deterrence

Effective deterrence is extremely difficult to plan for and execute after hostilities appear imminent. An effective deterrence strategy is not one that is defined by actions within one domain, or one area of responsibility, or one nation. Deterrence cannot be an invisible strategy, for a core premise is that an enemy is influenced by actions and messages that can be perceived—and

*Over the course of the next four days of the wargame, the crisis escalated to the senior executive level, and soon encompassed us all, including partners beyond our own government and nation.*

conveyed in advance.

To be effective at the strategic level, deterrence must be viewed through the lens of how your adversary views the geopolitical world, and that can be a very complex thing to comprehend. Deterrence is not static; effective deterrence strategies will morph under conditions of crisis, and the level of uncertainty about your adversary's decision process must be actively tracked and accounted for, or else you risk serious miscalculation and unexpected deterrence failure.

## The Challenge of Space and Cyber Deterrence Objectives

In the decades-old nuclear framework, deterrence objectives are geared toward influencing the political perceptions and military choices of your adversary. The objective of *nuclear* deterrence is to deter an adversary from using nuclear weapons. Having a confident comprehension about the beliefs, goals, values, politics, and motivations—on both sides—is a daunting challenge, yet highly important to develop an effective deterrence strategy. It is also a high stakes endeavor, due to the risks of miscalculation.

However, in spite of all of the complexities that make up the equation of a national leadership's decision calculus, there is one simple point of clarity about nuclear deterrence that transcends all of the variables: your deterrence objective is to convince your adversary that his least bad option is to exercise restraint.

In other words, in the nuclear framework, the complicated questions are not about *what* to deter, but *how* to deter. The strategy to deter a decision to cross the nuclear threshold will be scenario-specific and highly complex, especially in crisis, but there is really no ambiguity surrounding the goal of your deterrence objective.

An additional simplicity is that the nuclear threshold serves as a universal "pass/fail standard" for deterrence that any political leader can understand. Given the scale and scope of the consequence, it would not be difficult to recognize that your adversary has made his decision.

Beyond the relatively obvious kinetic thresholds, the discussions to date on space and cyber deterrence objectives do not have similar clarity. What exactly are the deterrence objectives on a non-kinetic battleground? Is the objective to deter "use" of space and cyber "weapons," to deter "attacks" in the space and cyber domains, or to deter notable disruptions of our space and cyber networks? Or is it really all about deterring any type of attack, kinetic and non-kinetic, on the US and her allies?

In essence, a deterrence strategy has to be built on a common understanding of what decision you are explicitly attempting to influence. Until you can put clarity on *what* to deter, there will be no clear or effective strategy on *how* to do it.

Let's say that our objective is to deter use of a kinetic antisatellite weapon against space-based platforms: that objective is generally easy to measure for success or failure, as the debris cloud that would ensue will catch everyone's attention and serve as a focal point of righteous global outrage. However, what if the satellite just quits working? The effect is the same, in that you cannot use the satellite for its intended purpose, but the means by which the satellite is no longer available changes the entire context of your deterrence objective.

In fact, your objective is really to deter *any* attack on a US satellite, kinetic or non-kinetic. Assuming you can prove to yourself that an adversary actually has a hand in this issue, then you need to broaden the scope of your deterrence strategy. That is, rather than defining the deterrence context to a narrow dimension—kinetic antisatellite threats and the associated costs to an adversary of space debris—your deterrence strategy should include other significant influencing factors in order to deter a potential adversary effectively.

## Attribution and Other Factors

The challenge of attribution faced by the cyber forces in SW 10 was indicative of the significant "grey areas" involved with deterrence objectives in the non-kinetic domain. The deterrence objective was to generally deter "disruption of the network," but "disruption" is not a "binary" situation in the space and cyber realms.

*Figure 1. Schriever Wargame 2010: Senior Leadership Seminar involving military, civil, and industry leaders.*

Given the spectrum of effects achievable by non-kinetic means—from massive disruption to unnoticeable—the attribution and assessment challenge varies from trivial to likely impossible. Having the situational awareness to fully characterize disruption is not a certainty, depending on both the disruption effects and the means to monitor the situation. And if the effects were fully intentional, then who was behind it?

We are all aware of the challenges of attribution, and yet the measure of your deterrence campaign's success or failure depends on it. Without confidence of attribution, how do you credibly assure an adversary in a pre-crisis environment that you intend to respond? How do you mitigate the risk of a third party exploiting the ambiguity to create or escalate the crisis? How can you assess the success of meeting your deterrence objectives and adjust your adversary-focused campaign accordingly, if you are not confident about attribution?

To further complicate the situation, our tolerance for disruption will adjust depending on both the crisis environment and the scope and duration of the outages, which could undermine the credibility of the resolve we intend to communicate well ahead of the crisis. There are an infinite number of scenarios that are neither indicative of a minor harassing incident of jamming nor strategic attack. For non-kinetic activity, we have yet to articulate a well understood threshold for a space and cyber deterrence objective set.

Unfortunately, we are not helped by a culture that passively accepts occasional disruption of our networks as a way of life. However, the incredible complexity of the operating environment does not alleviate the imperative to think through clear geopolitical deterrence objectives and effective strategies to implement them.

## The Challenge of Space and Cyber Deterrence Strategies

There is a pervasive assumption that the strategy lessons learned from nuclear deterrence in the Cold War can be directly imported to space and cyber mission areas for implementation. The relative simplicity of the Cold War, with its glacial standoff between just two primary actors, enjoyed the advantage of a shared understanding about mutual cost imposition, and a nuclear force structure that was designed to ensure stability in the balance of power.

## The Nuclear Scenario

Consider the premise of the nuclear cost/benefit trade space. Nuclear weapons have prompt, massive destruction effects, and the general point of using them first is as a last resort weapon to achieve strategic political objectives, most notably in situations of an existential threat.

However, using nuclear weapons comes with an incredibly high bar for "benefits of action," generally because the costs of your decision will likely provoke nuclear retaliation by your enemy or their allies. In a conflict that has not escalated to the nuclear threshold, a nation would be strongly motivated to exercise self-restraint, thereby preserving nuclear deterrence.

Even in this relatively simple deterrence strategy example of "costs of using nuclear weapons outweigh the benefits of using nuclear weapons," the strategy analysis required to avoid miscalculation in both the Soviet times and in today's geopolitical environment is immensely complex and has always required a deep intellectual investment.

## The Cyber and Space Scenario

In developing strategies for space and cyber deterrence, the entire context in these domains is different from the nuclear balance equation. Space and cyber capabilities are generally new means of technology to perform the age old function of command and control and situational awareness, not to create prompt destruction and horrific effects. This warrants a thorough, deliberate, nationally important discussion, for there are many strategy lessons that will not necessarily translate to space and cyber applications without careful consideration and adjustment.

As was mentioned often during the wargame, the space and cyber attacks and the motivations behind them were more about disruption than mass destruction. As such, they could easily be perceived as attempts to create an environment of disruption for information flow and imposing the "fog of war" in an asymmetric manner. Confusing your adversary, if you have the means, is not only a highly intuitive benefit, but also a sound element of traditional military strategy to achieve strategic objectives. Because of the lack of precedence and the wide variance amongst nations on space and cyber dependence, the costs you could possibly incur along with the supposed benefits of disruption are not nearly as intuitive as they are with nuclear weaponry.

It is a calculation that depends on a complex web of scenario-specific factors: the resilience of operations to a non-kinetic attack, the scale of the effects created, the state of declaratory policy, the credibility of a threat of escalation, and so on. It is both more complex and more uncertain due to a lack of precedents, compounded by issues such as attribution.

Ambiguity can have a role in the achievement of our deterrence objectives, but the strategy must be maturely formed, effectively influential in reference to your opponent's perceptions, and implemented well ahead of the adversary's decision cycle.

Implementing a deterrence strategy after the fight has already begun is utterly "late to need." To be effective, a deterrence strategy for the space and cyber domains must somehow relate to enduring standards that are understood by all sides before crisis.

*Space and cyber capabilities are generally new means of technology to perform the age old function of command and control and situational awareness, not to create prompt destruction and horrific effects.*

Depending on the adversary, the deterrence strategy may or **may not** include cost imposition options that are delivered by space and cyber forces. It will depend on whether those options have any deterrent value in the mind of your adversary—and whether he believes you would actually use them in the scenarios that he has laid out in his campaign. It is a critically important point: unlike the mature strategies developed over the years in the nuclear paradigm, the threat of sophisticated space and cyber options does not necessarily deter your adversary from using the same type of military capabilities.

Creating disruptive effects by leveraging space and cyber capabilities will certainly have military value, but whether it forms the basis of a viable deterrence strategy is an entirely separate question. The most effective strategy to deter crippling non-kinetic effects may not be to deter the use of space and cyber capabilities, but to deter the entire conflict before it begins, because the benefits of utilizing such capabilities in conflict may not be counterbalanced with costs meaningful to the adversary.

## Conclusion

Thanks to our long history of deterrence thought and our national energy to make the necessary cultural adjustments, space and cyber deterrence concepts are clearly evolving in positive ways. However, nuclear deterrence concepts that worked very well during the Cold War and still work extremely well today do not always translate in practice to the space and cyber domains.

At the same time, the fundamental behavioral principles on which classical deterrence theory is based are still valid when applied to the nuclear as well as cyber and space domains:

- The need to know and inform in advance;
- Motivation of an adversary—what the adversary values, and what would be unacceptable costs;
- The importance of making deterrence effective with other means, such as strategic communication, to communicate a clear message of intentions and limits. Strategic communication can play a reinforcing role in communicating our intentions to the adversary as well as broader publics. In the information age, enlisting broader popular support may play as great a role in affecting an adversary's behavior as flexing military muscle.

Finally, areas of increased complexity in the space and cyber domains—attribution is the most salient example—are becoming potentially more complex than in the nuclear age, where we had grown accustomed to a single clearly defined adversary and threat. The challenge of asymmetric threats posed by rogue groups and non-state actors that may acquire weapons of mass destruction is a sobering adjustment to classical deterrence study.

Based on observations during the SW 10, this article has attempted to highlight some initial thoughts on where the differences lie. The discussion here has noted where it might be necessary to make some modifications in our approach to objectives and the strategies to implement them, while posing additional questions that will be fertile ground for future wargames.

The Schriever Wargames provide an opportunity for space and cyber professionals to experiment with "lessons observed" from previous games and real world scenarios in a penalty-free environment where "out of the box" problem-solving methods can be used. Many of these methods, if successful, can translate directly into real world policies and practices as "lessons implemented."

And that is the ultimate objective of conducting these wargames—to prepare our leadership and our warfighters for the day when the game may no longer be just a game. The invaluable opportunity of SW 10 enables us all to become a more agile, adaptable, and effective force in today's high technology global environment.

**Maj Gen Susan J. Helms** (BS, Aeronautical Engineering, US Air Force Academy; MS, Aeronautics/Astronautics, Stanford University, California) is director of plans and policy, US Strategic Command (USSTRATCOM), Offutt AFB, Nebraska. She is directly responsible to the USSTRATCOM commander for the development and implementation of national security policy and guidance; military strategy and guidance; space and weapons employment concepts and policy; and joint doctrine as they apply to the command and the execution of its missions. She is also responsible for the development of the nation's strategic war plan, strategic support plans for theater combatant commanders, and contingency planning for the global strike mission.

General Helms was commissioned from the US Air Force Academy in 1980. She has served as an F-15 and F-16 weapons separation engineer and a flight test engineer. As a flight test engineer, General Helms has flown in 30 types of US and Canadian military aircraft. She has also served as project officer on the CF-18 aircraft as a US Air Force exchange officer to the Canadian Aerospace Engineering Test Establishment.

Selected by NASA in January 1990, General Helms became an astronaut in July 1991. On 13 January 1993, then an Air Force major and a member of the space shuttle Endeavour crew, she became the first US military woman in space. She flew on STS-54 (1993), STS-64 (1994), STS-78 (1996), and STS-101 (2000), and served aboard the International Space Station as a member of the Expedition-2 crew (2001). A veteran of five space flights, General Helms has logged 211 days in space, including a spacewalk of eight hours and 56 minutes, a world record.

General Helms commanded the 45th Space Wing at Patrick AFB, Florida. Her staff assignments include tours at Headquarters Air Force Space Command and Air Education and Training Command.

*Senior Leader Perspective*

# Schriever Wargame 2010 – A Coming of Age

**Brig Gen Robert J. Chekan, CF**
**Deputy Director, Strategy, Policy and Plans Directorate**
**North American Aerospace Defense Command and**
**US Northern Command**
**Peterson AFB, Colorado**

It was my privilege to lead the North American Aerospace Defense Command (NORAD) and US North Command (USNORTHCOM) team that played in the Schriever Wargame 2010 (SW 10), but my experience with the game dates back to Schriever II Wargame. In 2003, it would have been outrageous to send a team of 25 from NORAD and USNORTHCOM to the game venue—but in 2010 it would have been foolish not to. Schriever has matured into an extraordinary opportunity to think through global security and defense challenges. We came away with awareness and insights that are changing how we operate today, and how we are thinking about our collective security in the future.

Schriever has come a long way in just a few years. The early games were more or less running tutorials for many of us. In truth we had very little idea of how space supported us in our daily endeavors, and less understanding of what we should be doing to prepare for space as a contested arena. Our tool kits included some fanciful capabilities and at times seemed bottomless. We were to explore the policy dimensions arising from the use of those fanciful weapons. We made a lot of assumptions about grey space and sprinkled in commercial capabilities if we had the foresight to get our contracts in place before the bad guys did. We worked hard during our stay at Nellis AFB, Nevada, but honestly took very little home with us when we left. The game design, the capabilities, the time frame all were so different from what we encountered every day that there were few take-aways of real significance to the supporting players. It was great that the players outside of Air Force Space Command were getting smarter about space, but in many ways we were the supporting players of a space wargame.

To be fair to all the men and women who worked hard to put the early games together they were very much in the walking before running stage of the game evolution, and the players definitely needed to be educated in the ways of space. And absolutely to their credit they remained sufficiently disconnected from their first initiatives so that they could objectively learn and drive the evolution of the game to what it is today.

The game today, SW 10, is an example of a good idea driven to become really good by honest self-appraisal. What's different? Just about everything.

SW 10 looked into the near future, with capabilities either available today or already under development. Close allies were all present, bringing complexity for sure, but also bringing capabilities and ideas. Both industry and the interagency pieces were fully developed. The combatant commands fielded strong teams. The game ran at the strategic level and the policy dimensions explored not only the *what*, but also the *how*.

And a big part of this was that the players were all far more space savvy than they were even a few years ago—due in part to the education accomplished by previous Schriever Wargames.

The cumulative effect of all of these changes was that the combatant commands all fed more realistic inputs into the game. We did not have to suspend disbelief to engage in the game, rather we had to overlay our understanding of our roles and missions onto the template of the game scenario. We spent a lot of time thinking about what we would really do in the situation, and almost no time trying to break the code on the game tool kits or basic rules of play. We gained insight to real issues that we confront now and will likely confront in the future.

So what did we learn at NORAD and USNORTHCOM?

First, the whole idea of a home and away game needs to be challenged. It's a no-brainer that degradation of a space system has global effect, but what of cyber degradation? The World Wide Web is just that, and significant degradation anywhere is unlikely to remain geographically localized. Also, conventional, kinetic assets are a diminishing resource—if they are spent at home to protect the homeland, the number one mission for every military, they are not available to respond to a security or defense issue anywhere else. The home and away games are connected by space systems, in the cyber domain, and in the resource dimension. They are not independent.

Second, we really need to understand how much of what we do everyday—our six missions assigned in the case of these commands—flows in and through space systems and the cyber domain. During the game play it became increasingly obvious that we had a definite dependence on both space and cyber systems. And this makes sense. The NORAD area of operation is global, so global capabilities only available from space and running on the backbones of computer networks fit, but there is more here than meets the eye.

Our networks are constantly changing, and many of our mission partners are not resident on Department of Defense systems. Take the Federal Aviation Administration (FAA) for example. What information flowing from the FAA is critical to our mission accomplishment, and how can this be assured in a contested cyber environment?

*We came away with awareness and insights that are changing how we operate today, and how we are thinking about our collective security in the future.*

*We really need to understand how quickly cyber defense support of civil authorities might be required, whether there is a physical dimension to that response, and who can add value to the situation. We need to understand the interaction of things going wrong in cyber and the physical consequence management aspects of the situation.*

It was a clear sign of progress that we felt comfortable in our knowledge of space systems and how they support our missions—but it was equally clear that we lacked a fundamental understanding of our digital lifelines.

So naturally I turned to the Cyber Command players, fully expecting to deliver to them the insightful "request for information" that would shift the responsibility for cyber dependency awareness into their capable hands. But I was wrong. It turns out I did not know enough to either ask the right question, or to respond to their requests for clarification. What systems were critical to my mission accomplishment? How did they map out?

It was game play—and I am not the cyber expert in NORAD and USNORTHCOM, but here is my take-away: answering the questions about networks and critical information flow is a shared responsibility between ourselves and Cyber Command.

And now life is imitating art. We have just spent the last two days working with Strategic Command and Cyber Command staff talking about these exact issues. These talks have been underway for a little while, but SW 10 was definitely a catalyst for progress, and it established both connections and even friendships that will help us sort this out.

Third, during SW 10 we spoke often about how cyber might play out with respect to defense support of civil authorities (DSCA). At that time I was fairly dogmatic on the subject, "nothing in the establishment of Cyber Command has changed the DSCA mission assigned to USNORTHCOM. It was ours. Title 10 forces assigned in a cyber DSCA role would work for commander USNORTHCOM."

On my way home from the staff talks yesterday I gave this a lot more thought, and I think I am a little wiser. It is not so clear, and certainly not black and white. Depending on the scenario, and there are many you can imagine, USNORTHCOM could be supported, supporting, or working in parallel with our colleagues in Cyber Command. We really need to understand how quickly cyber DSCA might be required, whether there is a physical dimension to that response, and who can add value to the situation. We need to understand the interaction of things going wrong in cyber and the physical consequence management aspects of the situation.

The answer is to think this through now and develop the working relationships and responsibilities together.

Fourth, I cannot in good conscious end this short article without mentioning a few observations from a Canadian perspective.

As I mentioned earlier, I have had the good fortune of playing in Schriever Wargames for a number of years—the first few as a result of my duties as the director of space development for the Canadian military.

The notional space resources available from the US Air Force during the early Schriever Wargames were virtually limitless. There was a polite and respectful interaction with the Canadians, Australians, and Brits that participated, and an attempt to consider what value allied space resources might provide. But given the tool kits available our potential contribution was insignificant. The intent to engage the closest allies was genuine enough—but the game by its early design reinforced a "go it alone" approach for the US.

It is much different today. The game's foundation nearer to today's reality has facilitated more substantive discussions of

*Figure 1. Move 0 (wargame kickoff) of Schriever Wargame 2010: Deputy commander of the North American Aerospace Defense Command, Lt Gen Marcel Duval.*

*It takes far more intellectual horsepower to put together an alliance than it does to set up a coalition. But where there is common interest alliances are possible, and they are far more agile and powerful than coalitions.*

the finite resources available to all of us, including for investment in space capabilities. We are a lot smarter about developing complementary space capabilities, and we are well into the discussion of how we work together in space and well past whether we should work together in space. The understanding that none of us can do it alone is now widely held, and I believe a real outcome of the game.

I bring this forward mostly to compliment the leadership and developers of the game. Adding allies, even the three closest that the US works with all the time, adds complexity and big challenges. We are a lot alike in many ways, and then frustratingly different in others. Every relationship, alliances included, works because of common interest and then compromise. I applaud the intellectual and actual owners of Schriever for their professionalism, and at times patience, as they have worked hard to stitch in Canada, Australia, and Great Britain. I believe all of our nations are profiting from this, and will for many years to come.

And lastly, a short word on the differences between alliances and coalitions, a subject I brought up during the game play and which is worth thinking about. We all sometimes use the terms "alliance" and "coalition" interchangeably, and that is a mistake.

What follows is not the doctrinal definitions of these terms, but how I see things.

A coalition is a group of like-minded nations that agree to work together to accomplish a specific task or combined effect—and the coalition, by design, is bounded by both space and time. Coalitions get things done—no argument there—but often because the actions are de-conflicted more so than designed as interdependent. It is sometimes more important to be present in a coalition than it is to bring real contributions to that coalition.

In contrast an alliance is developed because of common needs, and those needs are most often enduring. Actions are designed to be inter-dependent. Allies have to bring something important to the alliance, and the effect generated is more important than the perception of participation.

It takes far more intellectual horsepower to put together an alliance than it does to set up a coalition. But where there is common interest alliances are possible, and they are far more agile and powerful than coalitions. In space, I believe an alliance is the gold standard we should be striving to achieve.

NORAD and USNORTHCOM invested significantly in SW 10, and we received a valuable return on our investment. We are smarter about things we are already challenged by, and we have opened new lines of communication and collaboration that are helping us to better protect and defend these homelands we hold so dear. I am thankful to my great team—let's start thinking about Schriever Wargame 2012 now. And I am thankful to the SW 10 team for all of their insight and hard work, they have developed a world-class wargame. In a word it was … unforgettable.

**Brig Gen Robert "Bob" J. Chekan,** Canadian Forces (BS, Biology, Carleton University, Ottawa; MS, Space Operations,US Air Force Institute of Technology, Ohio) is the deputy director of the strategy, Policy and Plans Directorate North American Aerospace Defense Command (NORAD) and US Northern Command (USNORTHCOM), Peterson AFB, Colorado. USNORTHCOM conducts homeland defense, civil support, and security cooperation to defend and secure the US and its interests. NORAD conducts persistent aerospace warning, aerospace control, and maritime warning in the defense of North America. General Chekan joined the Canadian Forces in September 1977. Among his assignments the general has commanded and served in operations and staff appointments in Canada and Europe as part of Canada's contribution to NATO, and in the US as part of Canada's participation in NORAD. The general commanded the 51st Aerospace Control and Warning Squadron in North Bay, Ontario, and the Canadian Forces Experimentation Centre in Ottawa. His operational experience includes the 22nd NORAD Region in North Bay, 42nd Radar Squadron in Cold Lake, and the NATO Airborne Early Warning component in Geilenkirchen, Germany. General Chekan served at the National Defence Headquarters, the US Air Force Space Command Headquarters and Fighter Group Headquarters. Most notable among these duties, he served as the director of space development for the Department of National Defence for three years and as special assistant to the vice-chief of the defense staff for two years. In 2008 General Chekan joined NORAD and USNORTHCOM Headquarters as a command center director. Upon his promotion to brigadier general in June 2009 the general was assigned to his current position as deputy director, strategy, policy, and plans.

General Chekan is a distinguished graduate of the Canadian Forces Command and Staff College, an ancien of the NATO Staff College in Rome, and a graduate of the National Security Studies Course.

# Schriever – An Australian Perspective

**Air Cdre Andrew Dowse, RAAF**
**Director General**
**Integrated Capability Development**
**Canberra, Australia**

## Introduction

Schriever Wargame 2010 (SW 10) had the largest commitment by Australia in a Schriever Wargame to date, with 20 Australians in attendance. They came from a range of areas, agencies, and specializations. All were very keen to be involved with the premier space wargame.

The increased Australian interest was driven by a number of factors: including our recognition of the importance of space in the planning and conduct of operations; the appeal of a cooperative approach to space operations; the challenges and uncertainty that we face in developing and operating space-related assets effectively and efficiently; and the fact that Schriever Wargame is so well placed to shape future space capabilities.

These factors form a reasonable framework to describe the Australian perspective on SW 10.

## Recognition

Australia was one of a handful of nations involved in early space activities, with the Weapons Research Establishment Satellite program in 1967 making it the fourth nation to successfully launch a satellite. However, Australia effectively went into a period of space 'hibernation' through the latter part of the 20th century. For economic and strategic reasons, Australia's priorities became more regional and little priority was given to national space programs. Although a low level of experimentation continued, as well as a modest investment in satellite communications and cooperation with the US through Australia-based joint facilities, it has not been until recent times that Australia's interest in space has been reinvigorated.

The agreement between Australia and the US in 2007 in relation to the Wideband Global Satellite (WGS) Communications system seems a pivotal moment. By essentially funding a sixth satellite in the WGS constellation, this agreement provided Australia with assured access through the entire constellation.

Before this agreement, Australia's commitments to military operations around the world over the past decade brought the value of space related capabilities into sharp focus. Sensors, beyond line of sight communications, and position, navigation, and timing are all critical to the effectiveness of modern military operations. The recognition of space as a high priority for Australia originated within the Department of Defense but was quickly acknowledged by the government in its priorities. As a simple indicator, the current 2009 Defense White Paper cites space 32 times, whereas it was mentioned only twice in the preceding 2007 Defense Update policy document.

Such defense policy typically establishes the need for investment in associated capabilities commensurate with the value they might confer. The policy's focus on space thus translates into higher priorities for projects that may deliver space-related capabilities.

The not-so-obvious implication is that our increased dependency on such systems creates vulnerabilities. This demands we consider contingency requirements for resilience and redundancy, such as the need for hardened or protected systems, alternative means, procedures to deal with degradation, and operationally responsive arrangements. This aspect of strategic planning is not as mature in Australia in the development of space capabilities.

Space and cyber are domains that are not easily contained within national borders. An important element of our recognition of them is that they are different in terms of the strategic nature of their global reach, as well as their rapid application and effect. This is also reflected in the growing international recognition of the need to put in place measures that strengthen stability in space, and provide a set of 'rules of the road' under which nations may conduct space activities. SW 10 recognized this and its utility of a hypothetical Code of Conduct helped frame valuable policy discussions that will support future real world dialogue on greater space regulation.

## Cooperation

Relationships with our close allies underpin Australia's national security and we have maintained these relationships throughout our history. In terms of space, operational-level cooperation may range from ensuring interoperability, to technical and acquisition collaboration, to provision of operationally important information, to exchange of capacity and mutual support through tasking of each others' assets. A more advanced approach to cooperation might encompass burden sharing, joint systems, and coalition command and control of such systems. Such cooperation is supported by open and growing dialogue on a range of space-related issues.

As with any shared system arrangement, there are potential benefits for space capabilities of economies of scale, administrative efficiency, and improved flexibility. In the example of the WGS partnership or Australia's desire to acquire a sensing satellite capability, the choice of joining a constellation rather than a national-only capability is more likely to achieve a greater capability at a lower cost.

Such shared constellations should mean greater coverage or revisit rates, as well as lower non-recurring expenses, which adds up to a clear advantage. Moreover, the ability for our space systems to adapt to changing circumstances and priorities may be enhanced under a cooperative approach.

Technical cooperation introduces the prospect of innovative synergies (i.e., two heads are better than one), in which the outcome may be leading edge capabilities of mutual benefit. However, this needs to be tempered with the possibility that heterogeneous capabilities inherently may be more survivable than a homogenous environment.

A factor related to economies of scale is the consideration of economies of geography. A global constellation, whether low Earth orbital or geostationary, will provide coverage of broad areas that may or may not align with the geographical interests of its user base. Economies of geography may relate to the capacity of space assets being optimized in all of their geographic areas of operation, and may extend to the provision of anchor station services from one partner to another. It would be fair to say that a global constellation that serves a group of European partners might not achieve such economies of geography (with some areas of operation being highly contended and others being underutilized); whereas a group of users whose interests are spread across the areas of coverage may take far better advantage of the full extent of the space capability.

Cooperation tends to be more effective when there is some level of convergence of the strategic interests of the partner nations. Such convergence may mean that there is greater responsiveness to changing requirements. Real partnerships in space need to be based around a model of trust and mutual support, in which the burden of ownership is shared but is not simply contractual and inflexible. Whereas convergence of interest may at times create situations in which there is competition for scarce assets (i.e., when these similar interests bring the partners to the same location at the same time in response to a situation), a partnership based upon trust and strategic convergence should facilitate a reasonable outcome in the management of priorities.

Another advantage of cooperation in space, as in cyber, is that such arrangements mean that multiple nations are dependent upon shared systems, are responsive to other partners' needs, and comply with uniform codes of behavior. Whereas space is often referred to as the 'commons,' in such cooperative situations these shared systems truly are a commons. Together with more incidental situations of entanglement (e.g., when services are shared on a commercial bearer), these common systems create a real potential for deterrence and stability.

Having said that, with each nation having different approaches to how it manages its dependencies upon space capabilities in contingencies, there is the real possibility that the impact of degradation, contention, or unavailability of space assets may be different for each partner. This may then lead to a level of 'disentanglement,' in which the partners have different positions or desired responses to a common problem.

As space capabilities typically represent segments in end-to-end systems, the benefits of a space partnership in isolation may be limited. There are considerable benefits and synergies that may be exploited with broader existing arrangements in areas such as information exchange, cyber defense, communications, and interoperability.

Australia currently is involved in space-related cooperation with our allies across a number of lines, including the WGS partnership and exchange of narrowband satellite communications, as well as access to the products of other satellite systems. Additionally, the 2009 Defence White Paper recognized Australia's need for a synthetic aperture radar satellite capability, as well as improved space situational awareness. Given the benefits I have described, there is a strong presumption that new capabilities in these areas should be developed within a cooperative framework.

## Challenges

In developing the future space arrangements, our levels of cooperation could exist along a continuum from sharing information to shared systems. There is a high level of uncertainty about how shared systems should be managed; nevertheless there seems to be a general agreement between the close allies on a concept in which the space partnership starts with modest steps, but on a path that leads towards an objective situation that might offer far greater benefits.

Given the sort of discussions and mutually beneficial activities we already undertake at the Schriever Wargames, it could be said that we are already on this path. However there are substantial further steps we could be taking, such as the creation of the Combined Space Operations Center (CSpOC). The CSpOC might begin as a virtual center, enabling greater integration of our national space operations centers to share situational awareness and other mutually beneficial data, whilst maintaining protection of national information.

Building upon this framework could include improvements in the way space assets are utilized in terms of mutual support and tasking. An ultimate objective may be the standing up of an allied task force commander for space, who either manages coalition space assets or is assigned them as required by national authorities.

If we assume the existence of an allied space task force commander in future, as indeed is integral to the Schriever Wargame, we experience the real challenges that we need to address to make such an approach work. Each nation has policies, laws, interpretations of laws, and rules of engagement. Their differentiation across the allied partners can be managed if we are in a predictable environment.

However, they become problematic in situations that involve unexpected events and a highly dynamic environment. In such situations, each nation's interests and equities cannot be resolved as quickly as decisions need to be made.

Additionally, there is the possibility that in certain contingencies, the partner nations might not have consensus and there then becomes a difference between the steady state coalition and the coalition in a particular contingency. There has been some discussion that the steady state arrangement should be an alliance, although the term alliance can have specific implications or interpretations that need to be considered. Whether it is called an alliance or some other term, the partnership may evolve with an understanding by the member nations of the respective standing commitments to mutual support as they relate to space. Coalitions might be a better reference to temporal arrangements, including the invitation of additional nations into partnership arrangements as circumstances arise.

Our biggest challenge will be for national equities and interests to support the timely and appropriate decisions made by an allied space commander, rather than being an obstacle to such decision-making. I expect that we can overcome this quandary through comprehensive deliberate planning that effectively provides some level of national pre-clearance of decisions under certain conditions. It is too late to embark on the planning journey as events unfold.

As there is the very real prospect of hasty decisions leading to

unintended consequences, it is critical to have considerable depth and analysis to this planning. The planning function needs to be resourced and undertaken, and then rules of engagement aligned with these plans.

A related and similarly daunting challenge is that of attribution of interference or attacks on our space, and for that matter cyber, systems. Suffice to say that this challenge is understood and there is much to be done technologically and in planning in this area.

In terms of achieving a vision of allied space assets, there is more work to be done on developing concepts for the prioritization of scarce assets in a contingency. Additionally, we need to consider how we might best fund joint space assets, as well as to maintain/replace such capabilities on an operationally responsive basis. The burden sharing of such costs and the programming of future commitments are fundamental considerations for a future alliance arrangement.

Finally, there would be mutual advantage if we collaborate more not only on the use of our space assets, but also on our contingency arrangements in situations in which these assets are degraded or unavailable. As with all good planning, our partnership arrangements should cover the breadth of possibilities, so that we don't simply fall into a state of disentanglement.

## Schriever

Rather than Australia participating as a standalone team, the overall structure of the wargame allowed allied team members to integrate with the cells that suited their specialization. Not only did this reinforce the future vision of allied partnerships in space, it was also highly rewarding as a training opportunity by allowing specialists to interact with others in their respective areas of expertise.

The structure of the wargame was well developed, as it presented a good balance between broader considerations and the need to focus on space issues. The opportunities to highlight policy issues, and to start dealing with the 'so what' matters concurrent with the wargame, was a key advantage.

A notable part of SW 10 was the experience, insights, and skills of the members of the executive cell and the various people who acted as mentors and advisors to the wargame. The Australian participants found interaction with these leaders and other SW 10 participants to be immensely rewarding.

SW 10 facilitated interactions between the allies on various issues that helped the Australian participants consider real world issues. While there will continue to be national perspectives, there was common ground and the commonwealth nations operated well as a team.

The wargame seemed to gravitate, to some extent, around the activities of the executive cell. Possibly this was in some part due to the wealth of experience and seniority present in that cell or the need for national strategic guidance in the scenarios. This left the role of the Space Council somewhat uncertain and underutilized at times, and there may be value for future wargames in considering the respective roles and membership of the executive cell and Space Council.

In the absence of mature partnership arrangements for allied space and the underlying planning needed to support those arrangements, the national strategic level was pivotal and there was an assumption that allied policies would be resolved at this level. As mentioned previously, in order to keep up with the high tempo, we may need better clarity of policies and plans at the operational level, and focus more of the decision-making at that level.

The only suggestion for improvement of an already well organized wargame therefore is to consider shifting the focus more onto the Joint Space Operations Center and CSpOC activities. To do so may require a substantial effort by all involved to develop the CSpOC framework between now and the next wargame, however such preparation would be rewarded.

## Conclusion

The members of the Australian Defence Force and the broader Australian Defence Organisation appreciate the strength of our relationship with our allies. We also recognize the value of space capabilities to our mutual security and are beginning to understand that we cannot take them for granted.

The experiences of the Schriever Wargame are very important as we continue to develop these capabilities. We look forward to the next wargame, while continuing the good liaison and evolution of our partnership.

*I would like to take the opportunity to thank General C. Robert Kehler and his team for making the allies so welcome, and for the efforts that go into the preparation of the wargame, which reflect the high level of professionalism that we consistently see from the US services and especially from Air Force Space Command.*

**Air Cdre Andrew Dowse** (BS, Electronic Engineering; Graduate Diploma, Legal Studies; MS; and PhD) joined the Royal Australian Air Force as an engineer cadet in 1981 and graduated as an electronics officer, working in areas of air defence and communications. In 1989 he was posted to Tinker AFB, Oklahoma on exchange with the US Air Force in the development of command and control systems. Subsequently he had postings as the Air Force Headquarters staff officer for communications systems and the senior engineer at 114 Mobile Control and Reporting Unit.

Following completion of Command and Staff Course, Dowse served as the deputy director for information operations at Strategic Command Division before a posting in 1999 to the Australian Defence Staff Washington to liaise on aircraft systems, command, control, communications, computers, intelligence, surveillance, and reconnaissance and information operations matters. In 2002 he was promoted to group captain and posted to be the director of information operations and electronic warfare in Defence Headquarters, followed by director of information technology services in the Defence Chief Information Officer Group. He was Air Force director of enabling capability from 2006 to 2008.

Air Commodore Dowse was promoted and posted to his current role as director general integrated capability development in November 2008. He will take on the role of director general capability and plans from November 2010.

Air Commodore Dowse is a graduate of the Australian Institute of Company Directors.

*Senior Leader Perspective*

# Beyond Schriever Wargame 2010

**Brig Gen Perry Matte, CF**
**Director General Integrated Force Development**
**National Defence Headquarters**
**Ottawa, Ontario, Canada**

## Canadian Space Development

Canada, like all developed countries today, is dependant on support from space-derived capabilities for critical public services ranging from financial transactions synchronized via GPS timing signals to weather forecasting using satellite imaging. Further to those basic public and commercial demands for satellite services, Canada has a vested interest in developing space capabilities to address the sovereignty and security challenges presented by its unique geographic and demographic characteristics. By area, Canada is the second largest country in the world and has the world's longest coastline bordered by three ocean approaches,[1] yet 80 percent of its population of 35 million is within 100 miles of the nearly 4,000 mile southern border with the US.[2] This vast country, including its Arctic archipelago, presents a significant challenge for providing wide-area surveillance of its air and maritime approaches as well as connecting its people through communication links across great distances. It is, therefore, not surprising that space-based capabilities have become critical to all elements of our national power.

In addition to addressing the challenges inherent in national sovereignty and security, space systems provide essential support to a myriad of Canadian military operations and global deployments. As is the case for other modern militaries, space is no longer viewed as merely a force multiplier for the Canadian Forces (CF), but rather as a critical force enabler for operations. This is especially true for applications that enhance a commander's situational awareness and provide for assured command and control (C2) functions.

This combination of demanding national and global operational requirements has led to Canadian initiatives across the full spectrum of civil and military space capabilities, including partnering agreements with key allies where there is a common, shared interest. Most notably, Canada has developed the Sapphire satellite as a contribution to shared space situational awareness; has partnered with the US in the advanced extremely high frequency satellite program; has invested in space based synthetic aperture radar technology as evidenced by RADARSAT 1 and 2; and the next generation of Canadian space based radars, the RADARSAT Constellation Mission.

In concert with this growing reliance on space capabilities, space is becoming relatively more affordable and accessible especially with the advances being made in micro and nano satellites. While this trend supports expansion of Canada's space presence, it also opens the door for an increasing number of new state and non-state actors. The result, of course, is the expression that space has become a congested, contested, and competitive environment that is no longer a sanctuary. It is also clear that no single country has the capacity to develop and sustain all of its space-based needs, not only leading to the recognition that partnerships are required but also forming one of the underlying principles behind allied participation in recent Schriever Wargames.

To provide a cohesive framework for addressing the increasing importance and use of space in light of the increased risks faced, the Canadian Department of National Defence and the Canadian Forces (DND/CF) is drafting a new national defense space policy and a national defense space strategy. Our draft space policy has identified three strategic DND/CF goals: assured access to space and its unhampered exploitation; effectively integrate the unique capabilities that are attainable from space to fulfill Canada's defense commitments; and protect national space systems and allied space assets critical to national defense from all threats, including those located in or passing through space. Together our space policy and space strategy documents will guide, define, and inform future investment decisions for space capabilities as part of a more comprehensive and sustainable Canadian National Defence Space Program. Central to this program will remain the need for strong collaboration with other Canadian government departments and agencies, industry, and allies.

## Canada in Schriever Wargame 2010

Since 2003, a key element of our DND/CF international involvement in shaping our requirements for space development has been our participation in the Schriever Wargame series.

Wargames provide a controlled forum to investigate, modify, and validate capabilities, constructs, concepts, and strategies by playing them against "what if" scenarios designed to provide gauged but often uncertain outcomes based on decisions made or actions taken. The outcomes can then be assessed for further exploration or "real-world" application. By providing such a forum for game playing, the Schriever Wargames have presented Canada with a unique opportunity to work with, and leverage, a broad military space community in gaining insight

*Together our space policy and space strategy documents will guide, define, and inform future investment decisions for space capabilities as part of a more comprehensive and sustainable Canadian National Defence Space Program.*

on key issues impacting our nascent defense space program.

Beginning with three observers for the Schriever II Wargame in 2003, Canada's participation has continued to grow. For Schriever Wargame 2010 (SW 10), our 20 person team consisted of representatives from a broad range of defense and civil organizations. The intent was to have the appropriate representation across all game cells to capture the breadth of issues and requirements associated with military-to-military collaboration and government-to-government interaction. Our ongoing involvement in these games has provided the DND/CF with critical insight and renewed appreciation of the challenges and potential vulnerabilities associated with space operations, which have been effectively used to inform the development of our new draft space policy and plan for future investments in our space capability development strategy. Several Air Force Space Command commander's objectives for SW 10 had previously been briefed, including one to explore integrated planning processes that employed a whole of nations approach to the protection of assets and execution of operations in both space and cyberspace. In line with these objectives, Canada also established the following national objectives: to further develop and exercise the combined joint task force (CJTF) Space and Combined Space Operations Center (CSpOC) constructs; to gain a better understanding of the synergies and related vulnerabilities of the space-cyberspace linkages; and to assess the direction articulated in our draft national defense space policy against issues and events that arose during the conduct of game play. I will therefore provide both my comments and perspectives on SW 10 as a reflection of these objectives.

## Game Play

From a Canadian perspective, the game's overall success was due, in no small part, to the changes made very early to the Executive Decision Cell (EDC) and Space Council (SC). Expanding the EDC membership to include the senior SC members effectively closed the seams between military and political gaming authorities and resulted in a more responsive structure in terms of game options analysis, inject of coalition perspectives, and game direction for execution. This, in turn, allowed a much improved strategic approach to the game focused on policies, evolving geopolitical dynamics, and measured responses. More importantly, SW 10 allowed the senior leadership to actively challenge "what-if" scenarios with the red team in advance of game play, providing the unique opportunity to better understand the complexity and uncertainties of an issue; an adversary's underlying intent or ambition; an adversary's interpretation of and likely response to actions; and finally the potential collateral or 2nd and 3rd order effects of a conflict that escalates into the global commons. I would at this stage encourage that this EDC/SC structure be retained for the development of future Schriever Wargames.

Notwithstanding the benefits derived from a restructured EDC, it was evident that elements of the CJTF-Space and CSpOC construct require further attention to ensure that they are fully enabled to take a more active and deliberate role in the actual command, control, and management of apportioned national space assets in response to dynamic day-to-day events in space. The doctrinal intent of a CJTF is to ensure the effective and efficient employment of assigned forces through unified command and control. In SW 10, the CJTF-Space was to provide assured space capabilities support to a regional CJTF, utilizing the CSpOC's centralized command and control of apportioned national US/coalition space assets. The CSpOC was to support the planning, coordination, and employment optimization of these space assets to provide maximum effect while concurrently protecting those assets and, when applicable, mitigating their exposure to either interference or attack. The CSpOC construct would enable increased space capabilities and capacity, employment flexibility, and enhanced redundancy if/when some of these assets were lost. Unfortunately, from my perspective, much of the SW 10 game play resulted in strategic level direction and tactical level engagement. Consequently, the CSpOC was not "operationalized" to adeptly manage the employment of apportioned space assets, nor was it able to be responsive to interference or attack on its apportioned space assets. The CSpOC and its operators, including analysts, should have been working issues of attribution by ascertaining the cause and effect of satellite losses or degradation, subsequently determining the impacts on the capabilities available to the users, and developing plans to mitigate the effects. The commander CJTF-Space, through the CSpOC, should have been actively managing and dynamically repositioning space assets, as applicable, in direct response to perceived threats to, and inherent vulnerabilities of, US/coalition satellites.

While I firmly believe in the intrinsic value of the CJTF-Space/CSpOC construct, its basic ability to influence and react to unfolding space events in SW 10 was, unfortunately, artificially constrained by game moves which spanned several days' activities. While these game moves greatly enhanced the game play at the strategic level and enabled a comprehensive assessment of the consequences of the previous day's direction, they unfortunately inhibited the CSpOC from taking more deliberate and timely action to address the unfolding dynamics of a conflict in the space commons. Specifically, when a week or several days of events are compressed into a single day for a game move, the result could be a significant loss of key space capabilities that could have been potentially avoided or mitigated if the CJTF-Space and CSpOC had been able to engage when the actual events were occurring. Timely engagement and management of space capabilities could have significantly altered some of the strategic decisions that the EDC may have had to contend with, from deterrent efforts to managing escalating activities that at times artificially pushed the game to red lines.

I fully appreciate and value the necessary controls and mechanisms required to move scenarios along to generate strategic decision making. There may now be an opportunity, if not a fundamental requirement, to consider adopting a more operational focus for Schriever Wargame 12 (SW 12) that would enable the CJTF-Space/CSpOC construct to specifically be gamed. If this is not possible, then we should consider running the CJTF-Space/CSpOC constructs in an exercise, maybe similar to the US Strategic Command sponsored Global Thunder or

*While we did introduce cyberspace into Schriever Wargame 2010, it appeared to materialize more in the form of activities and events against national assets and networks such as power and electrical grids vice against space segments themselves.*

Global Lightening exercises, wherein the C2 constructs could be better tested, assessed, and refined without the artificial time compression of events, thereby providing more opportunities to plan and respond to dynamic space events. The Schriever Wargame series has made it clear that the CJTF-Space/CSpOC construct has the potential to be a significant force enabler, but it is now time to fully exercise and "operationalize" this construct to formally address any underlying issues or requirements that we may expose.

## Space-Cyberspace Convergence

Cyberspace is ubiquitous by nature, impacting all operational, environmental, and global domains. The global reach and compressed timelines inherent in space operations has tightly bound space with cyberspace and it's that strong "convergence between space and cyberspace domains and operations" that was to be explored in SW 10.[3] Essentially the guidance received was to focus cyberspace activity on the common area in the notional space-cyberspace Venn diagram. To that end, a cyber collaborative cell referred to as the "CAFÉ" was established to explore innovative solutions to cyber threats. While I understand that there was a great exchange of ideas, and discussion of potential cyber tools or capabilities that could be used to influence or exploit areas of cyberspace, the inject and impact of the potential effects of cyber network operations (CNO) between the space and cyberspace domains was limited. Based on the intent of SW 10 to explore the convergence between space and cyberspace domains, there was an inherent expectation that this would result in direct cyber influence, exploitation, or attack activities targeted against our space infrastructure (satellite, control, or user segments). This would have certainly challenged our collective abilities to fully assess and understand the cause and extent of a cyber event, as well as determine whether we still had assured use of, as well as trusted data from, our affected space systems. While we did introduce cyberspace into SW 10, it appeared to materialize more in the form of activities and events against national assets and networks such as power and electrical grids vice against space segments themselves. This limitation to being able to effectively play the space-cyberspace convergence was another result of game moves, wherein the cyber events would have only been seen after the fact as an accumulation or summary of activities, having provided little to no opportunity for the CJTF-Space/CSpOC to have been able to assess and react as they occurred.

While the fundamental space-cyberspace linkages and potential vulnerabilities are evident, we must ensure that SW 12 is designed to fully explore the consequences of cyber exploitation or attacks against any or all segments of space infrastructure and operating architecture. This is the only way to effectively test and assess our space-cyberspace vulnerabilities, and to further test and assess the effect of our own capabilities and redundancies to ensure we can continue to provide assured and trusted space effects. The CF is currently standing up a cyber task force to address CNO, and we intend to bring forward many of our own lessons learned as well as cyber tools or capabilities as part of our play in SW 12.

## National Defence Space Policy

The SW 10 game play allowed our team representatives from national defence and foreign affairs to fully explore the robustness and limits of our draft National Defence Space Policy, as well as a proposed international code of conduct, and the ability to leverage extant treaties, agreements, and legal instruments. While we did not encounter any unmanageable restraints inherent in the draft Canadian National Defence Space Policy, it was apparent that any new international agreements introduced for game play need to be widely coordinated during the planning workshops to ensure concurrence of all participant nations. That said, it is clear that the Schriever environment continues to foster a well informed base for collaborative space operations across all the participating nations.

SW 10 was the first game in the Schriever series to conduct a post-game Mission Assurance and Reconstitution Seminar. This upper management level seminar provided an ideal forum for putting the game results into a real world context and exploring the way ahead. A recurring theme during this event was the limits of ad hoc or informal coalitions. However, it is clear that there exist a number of international treaties, alliances, and legal instruments that can be more effectively utilized to further strengthen the CJTF-Space/CSpOC construct. Ultimately, the level of integration, coordinated force development and burden sharing required to realize the full benefit of space collaboration dictates the need for strong enduring commitments from the participating nations and may be another area we can further explore in seminar in preparations for SW 12.

## Conclusion

I recognize that some readers may interpret my comments or perspectives as being critical of either the construct or the play of SW 10. Let me state unequivocally that was not my intent, for I fully support the Schriever Wargame series and feel very fortunate that Canada has repeatedly been invited to participate. My intent in this article is to provide my perspectives to highlight some key lessons learned, specifically regarding the CJTF-Space/CSpOC construct and space-cyberspace convergence, which I hope will serve to generate informed debate and discussion to determine how best to functionally enable and exploit the knowledge and insights gleaned from SW 10.

I appreciate the strategic value that our participation in the Schriever Wargame series has afforded us, not only in shaping many of our own Canadian space and cyberspace requirements, but in developing strong, trusting relationships with key allies over common interests and shared values as we collectively address the new challenges evolving in the global domains. We look forward to our continued active participation in Schriever Wargames as we now turn our immediate attention to preparing for the SW 12.

*Notes:*

[1] Natural Resources Canada, The Atlas of Canada, August 2010, http://atlas.nrcan.gc.ca/site/english/index.html.

[2] Royal Canadian Mounted Police, Border Integrity Program Fact Sheet, 2010, http://www.rcmp-grc.gc.ca/bi-if/index-eng.htm

[3] Schriever Wargame series, *Eye in the Sky Newsletter*, 3 March 2010.

*I would like to thank General C. Robert Kehler for the opportunity he provided to Canada to participate in SW 10 and for allowing me to share some of my thoughts and perspectives through this article. I would also like to express my appreciation on behalf of the Canadian team, to Col Roger Vincent and his Space Innovation and Development Center SW 10 team for an excellent effort. Canada is looking forward to working with our Schriever partners in progressing our collective requirements to eventually achieve real world results.*

*Also I would like to thank Mr. Frank Pinkney for his participation in writing this article.*

**Brig Gen Perry Matte, OMM, CD** (BS, Computer Science, Acadia University) is the director general integrated force development for the Canadian Forces (CF), working for the chief of force development at National Defence Headquarters (HQ), Ottawa. He is responsible for the development and integration of CF joint capabilities with a principal focus on C4ISR. His three functional directors are responsible for joint capability development in command and control; space; and chemical, biological, radiological, and nuclear, and the new Canadian Forces Warfare Centre has recently been assigned to his area of responsibility.

He earned his Air Navigator wings in 1981, and has flown over 2,500 flying hours on the CP140 (P3) with three tours at 405 Maritime Patrol (MP) Squadron. His staff tours have included: the Aurora Software Development Unit as an operational liaison and analysis officer; Wright-Patterson AFB, Dayton, Ohio, on exchange as the senior avionics engineer on the US Air Force's ring-laser gyro and embedded GPS/Inertial Navigation Systems programme; Maritime Air Group HQ in Halifax as the director of air operations Atlantic and then as chief of staff and director of operations in the Maritime Air Component (Atlantic); 1 Canadian Air Division/ Canadian NORAD Region (CANR) HQ in Winnipeg as A3 Force Employment/A3 Force Generation and as a director of operations for the CANR. He participated in Rim of the Pacific Exercise in 2006 as the MNF MPA TG commander, and more recently as the senior CF officer for the Executive Decision Cell/Senior Council in the Schriever V Wargame and Schriever Wargame 2010.

General Matte is a graduate of the Aerospace Systems Course, the CF Command and Staff College and the National Security Studies Programme. He was appointed as an Officer of the Order of Military Merit in June 2006. His command appointments include commanding officer 405 MP Squadron, 14 Wing operations officer, and 14 Wing commander.

Following his tour as wing commander, General Matte served as the special assistant to the chief of the defence staff. He was promoted to his current rank in July 2008 and assigned to his current position.

**Mr. Frank Pinkney, CD** (BS, Computer Science, University of Victoria) is a consultant supporting space strategic planning and concept development for the Directorate for Space Development within the Canadian Department of National Defence. Mr. Pinkney's career in the Canadian Forces spanned 35 years beginning as a private in the 3rd Battalion Princess Patricia's Canadian Light Infantry where he also served as a peace keeper in Cyprus. While a corporal he was selected for officer training and upon graduation was commissioned as an Air Force Communications Electronics Engineering (CELE) officer. As a CELE officer Mr. Pinkney accrued 20 years of military space experience in planning, project management, and research and development beginning with an assignment, via NORAD, in Air Force Space Command. Following that initial space exposure in Colorado Springs, Mr. Pinkney was assigned to National Defence Headquarters where he was responsible for space-based surveillance and reconnaissance engineering and development. From this position he served as the defence representative on the RADARSAT 1 Project Implementation Committee and was a member of the Defence Space Development Working Group that defined the way ahead for Canadian Defence Space. Following that first headquarters assignment he served as an exchange officer in the US Army Communications Research and Development Center at Fort Monmouth, New Jersey; where his accomplishments included the first demo of full duplex video via SATCOM-on-the-move and tactical radio range extension using NASA's Advanced Communications Technology Satellite. After New Jersey he took over as the leader of the Space Systems Group in Defence Research and Development Canada in Ottawa where he initiated the department's microsatellite research and development program and directly supported the RADARSAT GMTI development. Mr. Pinkney's military career culminated in the Directorate for Space Development where amongst other responsibilities he became the National Coordinator for Canadian participation in the Schreiver Wargame Series. SW10 was Mr. Pinkney's fourth Schriever Wargame.

# Flight Suits and Sport Coats: The Role of Industry in Military Space Operations

**Air Cdre Mark L. Roberts, RAF**
**Air Commodore Air Staff**
**United Kingdom Ministry of Defence**
**Whitehall, London**

*There exist limitless opportunities in every industry. Where there is an open mind, there will always be a frontier.*
~ Charles Kettering, american inventor

For the United Kingdom (UK), the Schriever Wargame series represents a unique opportunity for us to strengthen our long-standing relationship with the US and the wider allied space community. This year, we fielded a team of 20 personnel from across a range of policy, strategy, operational, legal, and scientific disciplines, which included among their number representatives from both the Royal Navy and the British Army. Also included this year, for the first time, were two cyber specialists in recognition of the emerging synergies between the space and cyberspace domains; and two industry representatives, which reflected the shifting emphasis of SW 10 towards a 'whole of nations approach' ['comprehensive approach' in UK parlance].

*The pace of globalization has surpassed the capacity of the system to adjust to new realities of a more interdependent and integrated world.* ~ Anna Lindh, swedish politician

Language is just one aspect of the human condition that connects one person with another, although our perception of any interconnectedness is often blurred by the geographical, political, societal, ethnic, or religious divides that we have imposed upon ourselves. As military personnel, we are often the worst offenders when it comes to imposing divisions upon ourselves and the wider world. Armed forces are often divided into distinct services, each with their own hierarchical organizations, rank structures, and professional specializations; and our military understanding of the outside world (broken down by region) is often viewed through the lens of the intelligence community. However, the advent of globalization (enabled by human exploitation of the ubiquitous air, space, and cyberspace domains) is slowly bringing our interconnectedness back into focus—bringing with it both opportunity and potential threat.

As the SW 10 scenario highlighted, the globalized world is a complex 'matrix' of inter-relationships that often transcends sovereign borders. Within this 'matrix' we will need to use every available avenue of influence in pursuit of our national or shared multi-national objectives; this is where industry (in all its forms) may provide a conduit for the military into our interconnected world.

In the UK, our thriving space industry contributes over £5.6 ($8.8) billion to the national economy, supports over 68,000 jobs,[1] and last year saw over £1 ($1.58) billion worth of satellite systems shipped from UK shores to countries around the globe. Our civil space industry is also supported by a cutting-edge scientific research community and an engaging academia. But how does this enable industry to contribute to military space operations within a whole of nations approach?

The first and most significant contribution that industry could make pertains to its global links, which often have fewer constraints than those placed on military forces acting overseas. For example, military forces never (intentionally) cross the sovereign borders of another country without explicit government approval; the same is not true of industry. Industry continuously looks to overseas markets to attract new customers and to create new outposts for their commercial activities. Company representatives are able to move freely amongst the global community, developing relationships as they go—and with relationships comes *influence*. With the right mechanisms in place, industry could act as a vehicle for the military to apply influence across international borders more subtly, and perhaps more anonymously, than conventional weapon effects. Similarly, industry may be able to provide warfighters with an extended range of options in their development of courses of action.

The utility of this industrial *'Six Degrees of Kevin Bacon'* was dramatically but simply demonstrated during the gameplay. A group of military officers hatched a detailed plan to gain insight into the activities of a particular foreign commercial entity. As the developing plan was proudly briefed to the assembled masses, one of the industry representatives interjected 'I could always phone and ask them.' While there may be some poetic license in my recounting of this incident, the point is clear: industry is able to influence across international boundaries in ways that would be inconceivable for the military. These valuable industrial linkages may not only be with foreign companies but perhaps also with foreign governments. Where an overseas outpost of a company is contributing to the local economy or employing the indigenous population, that company may be able to apply both economic and political influence, and may even be able to shape public opinion. Similarly, where companies have multiple capability-based divisions, these relationships with governments and commercial partners may run deeper than just space-related applications. For example, many aerospace companies span a number of technical disciplines ranging from satellites, to airframes, to avionics, to information systems, and may support a number of downstream services that result from these activities. However, influence is a two-way street so we will need to be mindful that foreign

powers may also seek to exploit the economic or technical advantage offered by their commercial space sector.

*Attitude is a little thing that makes a big difference.*
~ Sir Winston Churchill, british politician and wartime prime minister

Harnessing the full potential of industry's global influence will require new a *modus operandi* [or 'MO' as they say in popular crime dramas], in which military personnel will have to work side-by-side with their industrial counterparts as equal partners—something that is not normally in their DNA. Such a change may require a little 'attitude re-adjustment' on both sides in order to progress the relationship beyond that of 'customer and supplier' and into a new era of collaboration. However, if industry influence is to become an integrated part of our military campaigns there is a balance to be struck. Firstly, the industry relationships we may wish to exploit are built upon a mutual trust that may have been nurtured over many years. As military practitioners, we will need to respect this trust and ensure that we only seek to apply pressure when absolutely necessary in order to preserve the relationship. Secondly, our industry partners would probably not wish to be seen as acting directly in support of a military objective for fear of being ostracized from the international industrial community or, during times of conflict, being labelled as a combatant. The onus, therefore, is on the military to protect the commercial integrity of its industry partners.

As alluded to earlier, the traditional interface between the military and industry has principally been concerned with the provision of military equipment. In this regard, the nature of the relationship is one of customer and supplier and is focused on the delivery of project milestones; this engenders a somewhat formal (or even adversarial) relationship between the participants. So, outside these formal contractual obligations, what could industry do to enhance the effectiveness of our military operations?

When one considers that every military capability is developed or manufactured by a commercial company, no-one knows more about the internal workings of these systems than the industry technicians that built them. In a high-tech manufacturing community, the industry technician is the master of his domain and we cannot presume to understand his world any more than the industry technician can presume to be proficient in military operations. Therefore, it follows that industry may be able to help us to derive maximum utility from our current equipment—not just as individual systems but as networked capabilities spanning multiple physical, electronic, and informational domains. This approach would be analogous to an industrial version of the 'Tier One' solutions that form part of the operationally responsive space concept.[2] These solutions aim to implement more effective ways of employing current space power capabilities to meet joint commanders' needs within operationally relevant time scales. Such an approach would not only require a military mindset change but commercial companies would also have to find new ways of 'playing nicely' with potential competitors in order to provide holistic technical solutions to military problems.

As technology marches on, the military tends to focus on an adversary's use of technology rather than the technology itself. Industry, on the other hand, usually has a better understanding of what may be technologically feasible and how new technologies could present both opportunities and threats. Therefore, there could be a greater role for industry (working closely with the defense scientific community) in the technological assessment of developmental systems; both ours and those of our potential adversaries. Of equal importance, industry could also assist in scanning the horizon for emerging technologies, particularly those that could change the balance of power (so called disruptive technologies).

*Procurement programs that take decades may be obsolesced in an afternoon by new technological innovations.*[3]

The military is a big machine in which some wheels turn comparatively slower than their commercial equivalents, many would say that one such wheel is defense acquisition. In deference to any readers from the defense acquisition community, I will not attempt to justify this popular UK perception, instead I will simply ask what more could we do collectively to capitalize on new technologies before they become obsolete?

Much of the UK defense acquisition life cycle is concerned with conceptualizing, assessing and demonstrating technologies before manufacturing can begin; we have yet to embrace the spiral development process. Future developments in space technology will likely have both civil and military applications; so by the time that defense decides to proceed with an acquisition program, the chances are that industry has already done much of the necessary de-risking activity. Therefore, perhaps commercial off-the-shelf solutions or service-based provision of capability would enable the military to keep pace with, and exploit, technological advancements while avoiding much of the initial development costs. The UK's SKYNET Private Finance Initiative has successfully demonstrated the utility of this 'contracting for capability' methodology.[4] Under this arrangement, industry will continue to provide 'assured' military satellite communications (including commercial bandwidth) out to 2022.[5] Equally, one could apply this model to the provision of intelligence, surveillance, target acquisition, and reconnaissance or even global navigation services.

Although 'dual-use' (civil/military) systems are not uncommon, the SKYNET model has resulted in a new form of integrated partnership with the commercial provider, in which military personnel work side-by-side with company representatives to deliver an operational capability. This close relationship with industry has resulted in the fielding of critical communications with a flexibility rarely seen in other contractual arrangements. The mutual trust is such that the company often assumes financial risk in order to ensure that we have <u>what</u> we want, <u>where</u> we want it, and <u>when</u> we want it. Of course, the administrative processes (and any outstanding payments) will always catch-up eventually.

*Successful people are always looking for opportunities to help others. Unsuccessful people are always asking, "What's in it for me?* ~ Brian Tracy, American business author

As military practitioners, the defense applications of space are usually foremost in our minds; however, we should not forget the panoply of civil and commercial space assets that support our critical national infrastructure and influence the way in which we go about our daily lives. With this in mind, industry also has a stake in ensuring that users of the space domain adhere to generally accepted norms of responsible behavior, in order to preserve the environment for future generations. Such behavior could include minimizing the creation of orbital debris, preventing interference within the electromagnetic spectrum and reducing the risk of collisions in space. Monitoring (or even policing) these behaviors throughout the global space medium is a mammoth task and one which the military cannot achieve alone. The integration of industry into our efforts to sense, warn, and attribute actions in space (collectively termed space situational awareness [SSA]) would alleviate some of the resource burden and potentially open up new streams of vital SSA information.

Today commercial owners and operators of space assets far outnumber government users of space (including defense). By building strong relationships with our indigenous civil space companies, and those of our allies, we may gain access to orbital data which previously would have only been available by tasking military space surveillance networks. So instead of wasting valuable sensor resources tracking friendly satellites, we should set the conditions for industry to be able to share data with us to improve our collective space security. After all, improved space security further protects the revenue streams that industry derives from its space products and services.

But the contribution that industry could make to SSA extends far beyond providing accurate positional data on their satellites. As experts in the finer technical details of satellite design, manufacture, and operation, industry could help us achieve another level of granularity in our surveillance of space—turning 'awareness' into 'understanding.' Industry's knowledge in these areas could provide a greater insight into the operating parameters of foreign satellite systems, assess the potency of foreign counter-space systems and help to develop effective mission assurance, reconstitution, and deterrent strategies. Moreover, with more permissive International Traffic in Arms Regulations fast-becoming a reality, it is conceivable that our space industry could soon be building or launching the space systems of our future adversaries.

Operations in the 'global theatre' of space are usually planned and executed in our national space operations centers. If industry is to become an effective force multiplier, we must incorporate industry into our space Joint Air, Space, and Information Operations/Joint Plans and Requirements processes from the strategic through to the tactical levels. While the thought of industry representatives working within the heart of our military space organizations may be unnerving to some, we will need to move beyond any historical biases if we are to capitalize upon industry's full potential. Industry may also have to adopt new ways of working in which individuals are able to put aside their company's commercial interests and concentrate on national imperatives. Seconding industry representatives into our national space operations centers would be a relatively easy process; ensuring that these secondees represent the united industry view may prove more difficult. Therefore, if we are seeking to mobilise the space industry as a single entity in support of military objectives, who should we approach? Should it be the governing trade association, a civil space agency, or perhaps the government department charged with promoting business growth?[6] This raises wider issues in terms of how we then synchronize our space effects with those of other industrial sectors; in other words how do we achieve industrial cross-domain integration?

What was made clear during SW 10 was that an unprecedented speed of response will be required in order to react dynamically to events in space; this will necessitate pre-agreed processes with both national and allied industrial sectors in order to capitalize on their contributions in a timely manner. Such arrangements are already in place with commercial satellite imagery providers for support to global disaster relief efforts,[7] perhaps similarly flexible arrangements could be developed to bolster our response to emerging national and international security crises.

*There has been a shift in culture to one that emphasizes openness, sharing of information, and ready access. Establishing the risk balance will be an enduring challenge for defense.*[8]

As a 'valued international partner' [formerly foreign national], I would be remiss not to mention something about information sharing. However, in this instance, I will limit my comments to information sharing with our commercial counterparts. Clearly, those industry representatives working within our military space organizations would have to be security cleared to an appropriate level. The question is how they would discuss issues with their wider industry colleagues without revealing classified or commercially sensitive information. While maintaining a list of authorized defense contractors is common practice, we will need to widen this net to compass the entire civil space sector. This could become particularly problematic where a company has commercial links with countries outside the traditional group of space allies. As mitigation, companies

*While the thought of industry representatives working within the heart of our military space organizations may be unnerving to some, we will need to move beyond any historical biases if we are to capitalize upon industry's full potential.*

could be categorized within a tiered security sharing framework according to their 'trustworthiness' and only be granted access to appropriately releasable information. In concept, this would be similar to the tiered approach we currently use for the release of information to military personnel according to their security clearance; the only difference is that the industrial version would be by company, rather than individual. Once we have bridged the informational divide between our national defense and national industrial organizations, the next challenge will be to make the model work within an alliance of nations. Our success in this task will be pivotal to the development of a Combined Space Operations Center in which allied militaries would work with allied industry partners; this approach was showcased in the last two Schriever Wargames.

One should not forget that people too are a military capability and continued engagement with industry could be a way to develop a broader cadre of technically astute military operators. Creating collaborative training opportunities, and expanding our personnel placement schemes within industry, would help military and industry to have a better understanding of the other's activities, outputs, and aspirations.

*If you're walking down the right path and you're willing to keep walking, eventually you'll make progress.*

~ US President Barack H. Obama II

SW 10 offered a glimpse of the future challenges of operating within the air, space, and cyberspace domains but the lessons that we identified are firmly rooted in the present. The wargame confirmed that, in a globalized world in which the pace of technology is unlikely to abate, the military instrument will rarely, if ever, be able to deliver decisive strategic effect alone. Moreover, our traditional understanding of war as 'armed hostilities between nations' is being eroded as war is increasingly neither armed nor between nation states. It follows that enduring success will invariably require the careful integration of all levers of national power—including industry.

From an operational perspective, industry is currently an untapped resource that will need to become part of our 'toolbox' and reflected in our operational plans and estimates. The challenge for industry is to work out how the military can best harness their collective horsepower to amplify strategic effect and retain the capacity to shape events, seize the initiative, and respond to the unexpected. Such an endeavour will require a mutual trust and understanding such that the phrase 'without prejudice, without commitment' will no longer have to feature at start of each conversation.[9] What is clear is that, no matter what we wear—be it a flight suit or a sport coat, our collective professionalism and ingenuity could generate a combined force that is greater than the sum of its parts.

*Notes:*

[1] UK Space Directory 2010/11 (although figures quoted are circa 2007).

[2] Plan for Operationally Responsive Space: A Report to Congressional Defence Committees, dated 17 April 2007.

[3] John M. Richardson, "The Joint Narrative: Describing the Future Environment and Joint Operations," extract, National Defense University, Washington, DC.

[4] A private finance initiative is a means of bringing private sector funding and expertise into the running of public services. The underlying principle is the government customer receives an assured service but the risks and responsibilities (financial or otherwise) associated with running the service remain with the private sector supplier.

[5] While private finance initiatives may provide a cost-effective solution, there is often a high premium to pay for 'assuring' space capabilities through hardening, electronic protection and other resilience measures.

[6] For the UK, this is the Department for Business, Innovation, and Skills.

[7] The European Space Agency initiated the International Charter: Space and Major Disasters in 1999, there are now 18 commercial and governmental signatories to the charter.

[8] UK Ministry of Defence, MOD Information Strategy 2009.

[9] This term is used as the industrial equivalent of 'off the record' and denotes that the ensuing discussion will not constitute a formally binding agreement.

**Air Cdre Mark L. 'Roberto' Roberts** (MA, Defence Studies, Joint Service Staff College; MBA, Open University) is Air Commodore Air Staff within the United Kingdom's (UK) Ministry of Defence (MOD). He is responsible for providing specialist support to the assistant chief of the Air Staff and ministers in all policy and parliamentary aspects of the Royal Air Force's non-operational activities both at home and overseas.

Air Commodore Roberts was commissioned into the Royal Air Force in 1984. On completion of flying training, his first assignment was to Royal Air Force Laarbruch in Germany where he flew the Tornado GR1. During this tour he was deployed to Operation GRANBY (British military operations in the Persian Gulf region 1990 - 1991), flying 26 combat missions over Iraq. He returned to the UK in 1992 for an instructional tour on the Tornado Operational Conversion Unit (XV [Reserve] Squadron), during which time he became a qualified weapons instructor and completed a season as a display pilot. Following a staff tour in the Personnel Management Agency, where he was responsible for Junior Officer Fast Jet manning, he was appointed officer commanding No 12 (Bomber) Squadron, flying the Tornado GR4. During this tour he participated in Operation Resinate (South) (the UK component of Operation Southern Watch); and deployed to Al Udeid AB as the Tornado force element commander for Operation TELIC (British military operations in Iraq 2003 - 2009), during which he flew 13 combat missions. Air Commodore Roberts was assigned to the MOD, London in 2003 where he was responsible for future combat air capabilities within the Deep Target Attack Directorate. Later that year he took command of Royal Air Force Lossiemouth in Scotland and was deployed on Operation Herrick (the UK contribution to International Security Assistance Force operations in Afghanistan) as the deputy commander British Forces (Air) and the air component commander's Afghanistan liaison officer. He was assigned to his current position as Air Commodore Air Staff, UK MOD in 2007.

Air Commodore Roberts received the Queen's Commendation for Valuable Service for his part in Operation Resinate (South) and is a graduate of the Joint Service Advanced Command and Staff Course.

# Effects Felt Around the World: The Growing Complexities of the Interaction Between Geographic and Functional Combatant Commanders

**Brig Gen Terrence J. O'Shaughnessy, USAF**
**Commander, 57th Wing**
**Nellis AFB, Nevada**

**Lt Col Baron V. Greenhouse, USAF**
**Chief, Special Technical Operations**
**613th Air and Space Operations Center**
**Hickam AFB, Hawaii**

**Lt Col Kurt M. Schendzielos, USAF**
**Director, Commander's Action Group, 13th Air Force**
**Hickam AFB, Hawaii**

The geographic combatant commander (GCC) in US Pacific Command (USPACOM), like other GCCs, faces a variety of challenges. The Pacific Theater is immense, encompassing nearly half of the Earth's surface divided by 13 time zones. The boundaries extend to both poles, involve over half the world's population and are the locale of over 40 percent of the world's gross domestic product. The actors within the designated area of responsibility (AOR) range from fledgling democracies to entrenched dictatorships, constitutional monarchies to theocratic republics, altruistic non-government organizations to state-sponsored violent extremist organizations. Potential adversaries range from near-peer/peer competitors to techno-peasants, from the financially sound to the economically destitute. The terrain is challenging, including glaciers, cave-ridden mountains, expansive deserts, triple-canopy jungle, and open oceans spanning thousands of square miles.

These challenges complicate the way in which USPACOM operates, whether it is providing active deterrence to potential conflagrations; maintaining a stable presence to provide trust and confidence in allies and coalition partners; or responding to humanitarian assistance and disaster relief, in preparation of, during, and recovering from natural disasters or unforeseen events.

As little as two decades ago, we relied primarily on airborne, maritime, and terrestrial capabilities to provide the lion's share of information and support structure to expeditionary activities. The US gained a greater appreciation of the value of space capabilities and services during Operation Desert Storm, and more recently is gaining the same appreciation concerning cyberspace. These services and capabilities provide significant advantages in most of the challenge areas that combatant commands (COCOM) face.

In Schriever Wargame 2010 (SW 10), we were afforded a valuable opportunity to represent the theater perspective in the role of the GCC with a joint team comprised of USPACOM, Pacific Air Forces, and Thirteenth Air Force representatives with the wargame's charter to:

- Investigate space and cyberspace alternative concepts, capabilities, and force postures for future requirements;
- Consider space and cyberspace contributions to deterrent strategies; and
- Explore a whole of nations approach to planning in order to protect and execute space and cyberspace operations.

To put that in context, the space and cyberspace community requested Pacific-warfighters provide *theater-specific, joint and operational perspectives* to an Air Force Space Command sponsored wargame focused on using current technological, cultural, economic, and political trends to inform future strategic/operational planning and programming decisions championed by organizations responsible for space/cyber capabilities and services.

Conducting and synchronizing missions across the Pacific necessitates a heavy reliance upon space and cyberspace enablers. American combat forces are accustomed to space and cyber enablers 'being there,' and often take for granted the myriad of space and cyberspace capabilities that are relied upon on a regular basis. For many years, US space and cyberspace capabilities enjoyed a seemingly unassailable sanctuary—so much so, that few of our follow-on capabilities were built to withstand the array of non-kinetic weapons that are emerging and proliferating throughout the world. Based on a perceived minimal threat, our acquisition process consistently accepted risk decisions trading protection for increased capability—

*American combat forces are accustomed to space and cyber enablers 'being there,' and often take for granted the myriad of space and cyberspace capabilities that are relied upon on a regular basis.*

*An effective plan cannot be executed if operational planners lack an understanding of the ends, ways, and means in order to evaluate and estimate the potential strategic implications.*

choices that made sense given the US superiority and unchallenged domains at the time. However, we failed to predict the aptitude with which our near-peer competitors (most of which are located in/near seams along the Pacific AOR) would learn from our historical successes, or the energy with which they would pursue countering our space and cyberspace enablers. It is readily apparent how reliant we have become, how complacent we have been, and what objectives we must now establish for future capabilities.

## Geographic Bias

The SW 10 training audience learned a number of lessons in how we, as a nation, must approach future efforts in support of national objectives when challenged in the space and cyberspace dimensions. Historically, a conflict initiated in South-East Asia did not produce a significant threat to livelihood in North America, nor in the US' ability to project power in additional AORs. This is indicative of the geographical bias we have been able to enjoy when discussing adversary power projection. During SW 10, USPACOM planners quickly discovered that actions taken with a regional perspective in the Pacific often had significant unintended effects within other AORs to include the continental US. Likewise, actions with a global perspective taken by a functional combatant commander (FCC) such as a US Strategic Command commander may produce desynchronized effects within the AOR where the crisis originated.

These lessons were realized against forecasted Pacific-based near-peers, which developed capabilities to affect space and cyber nodes globally, therefore becoming a concern for additional GCCs. Unfortunately, the capacity to develop counter space and counter cyber weapons is not limited to large nation-state militaries and is increasingly proliferated. The ability to trigger cyber mass effects anywhere in the world against an informationalized society such as the US is reasonably obtainable by determined non-state-sponsored adversaries who can no longer be easily contained to a relatively small geographic region. This causes a relatively new conundrum for GCCs and FCCs as they consider the actions to take in a given crisis highlighting the need for increased integration and synchronization across GCC seams and diplomatic, information, military, and economic (DIME) instruments of power.

## Global Integration

The need to synchronize planning efforts and actions between a GCC and FCC is not new. It is widely recognized that the GCC in whose AOR the crisis originates should be the primary supported commander. The challenge lies in properly balancing the areas in which the GCC has principle responsibility (i.e., military assessment of a dispute over contested islands) with areas where the FCC has the resources and expertise (i.e., global deterrent actions in space). This results in a latticework of supporting-supported relationships. What often results is the development of two differently focused strategies (one regional, one global) which are ultimately fused together with varying degrees of success. The danger, and unfortunately often the reality, is that functional actions (i.e., space and cyber) can fall out of sync with the regional actions (i.e., posturing and strike operations).

It is important to remember that integration and synchronization of kinetic capabilities did not come quickly or easily. It took decades to effectively synchronize air and ground conventional and non-conventional kinetic operations. Unfortunately we are finding that space and cyberspace capabilities today are being added in an ad hoc fashion—overlays to what briefs well as a cohesive plan, but ultimately executes in a piecemeal fashion, failing to create the desired level of synergistic effect.

A senior mentor envisioned the concept during a mentor session at SW 10, remarking that space and cyber are not just icing to be thrown on a pre-made kinetic cake. This analogy can be taken one step further where space and cyber are more like baking powder … if it is not a part of the recipe from day one, then no amount of icing will produce something usable. While the cake/baking powder analogy is a simplification of a very complex challenge, it articulates the importance of the relationship between the GCC and the FCC. Deliberate planning is a continuous process that cannot be accomplished simply through touch-point events like conferences, exercises, or even wargames. It requires more than simply 'tacking on' liaison officers. Integration is a robust, continuous process, through established, habitual relationships. Without it, duplicative planning efforts for the same scenario will continue and desired effects best provided by other COCOMs or agencies outside the theater of operations will never be realized.

An additional integration issue lies with many of our compartmentalized capabilities. Operational planning staffs still lack adequate awareness of capabilities available to effectively integrate those capabilities and services into GCC crisis operations. It is a significant challenge to correctly incorporate compartmentalized capabilities when the operational planners are only provided PowerPoint deep information from multiple agencies around the world. An effective plan cannot be executed if operational planners lack an understanding of the ends, ways, and means in order to evaluate and estimate the potential strategic implications.

Significant progress to demystify integration has been made through Joint Operation Planning and Execution System and special technical operations, but these processes are still inherently stove-piped. This was true during SW 10 as the high cell and allied high cell found it challenging to synchronize with the rapidly shifting planning occurring on the main game floor. This occurred with multiple GCCs and planning staffs enjoy-

ing the luxury of being located together under the same roof. This challenge will be exacerbated tenfold when trying to accomplish it virtually from remote geographic locations in what could be a communications denied environment. Focusing dissemination on an effects-based discussion, vice specific ends, ways and means can significantly improve the process. The intelligence community and special operations forces models of stripping sources to increase releasability are a good starting point.

### Whole of Nation Challenges

SW 10 bore out how integral space and cyberspace capabilities are to the 'whole-of-nation' strategy across the DIME spectrum. However, they bring unique problem sets that complicate their role. Senior leadership, both civilian and military, are conversant and comfortable with conventional air, land, and sea actions and reactions—much like a chess game, the adversary reaction to such moves are relatively predictable for an experienced player. However, the same leadership does not share the same level of knowledge and comfort with space and cyberspace actions—consequently adversary reactions are not as predictable or understood.

Add to the fact that the multi-use nature of space and cyberspace capabilities can rapidly complicate decisions by denying communication paths that carry both military command and control (C2) and civil emergency broadcast services; this multi use nature can give rise to law of armed conflict quandaries. The multi-use non-kinetic target sets require the same attention and assessment required for kinetic targeting such as targeting insurgents hiding in a mosque.

One of the most critical lessons we learned in SW 10 was that actions in space and cyberspace are inherently global, and cannot (or will not) remain constrained to the theater of operations. Effects generated against commercial services being used for military purposes had a palpable impact on the global economy, and often expanded the conflict to neutral third-party players.

However, the complexity of the problem does not abrogate our responsibility to consider the use of space and cyberspace actions. Many of the capabilities available provide a reversible and hard-hitting impact that is not as easily achievable through conventional forces. They simply carry with them the caution that miscalculating outside perceptions and reactions to our own efforts and activities may have a stronger 'whole-of-nation' impact than desired or anticipated.

### Core Enablers

Our reliance on space and cyberspace is well understood by anyone watching US operations evolve over the past twenty years, and it has been identified as a lucrative pressure point in potential adversary's military doctrine. During SW 10, the adversary immediately focused on exploiting and denying US and allied access to space and cyber enablers as a preemptive action shaping the operational environment.

USPACOM understands the trials and tribulations of war, and we train to operate with losses to conventional forces, but there remains minimum and essential resources required to achieve objectives in a given campaign. Within space and cyberspace, we found an analogous set of core enablers the GCCs must have access to, with clear certainty, in order to operate through the contested environments of tomorrow. Core enablers are the basis of a GCC's tipping point—that critical juncture where the risk to accomplishing the assigned mission is too high to guarantee success with any degree of confidence.

These enablers include capabilities and services that support: strategic and tactical communications; intelligence, surveillance, and reconnaissance; position, navigation, and timing; missile warning and integrated air and missile defense; space situational awareness; and network operations. These enablers clearly support the ability to achieve primary mission sets (i.e., protecting the homeland, defending US/allied/coalition forces, etc.), as well as supporting tasks (e.g., neutralizing adversary power projection, posturing for full combat operations, supporting other joint operations areas, etc.). It is critical that the GCC articulates these requirements clearly to the FCC to ensure the proper level of priority is given to maintaining their capability.

### Command and Control of Command and Control

As the adversary challenged our access to space and cyber critical enablers during SW 10, it was difficult for military leadership and the National Security Council to appreciate and predict the full impact of those actions. There was no robust common understanding or methodology to fall back on in their experience or "toolbox" that aided them in making well informed judgments and decisions.

In our theater, Adm Robert F. Willard, USN (as commander, Pacific Fleet and now as commander, USPACOM) has propagated a concept known as C2 of C2. It is a concept whereby commanders and their staffs are educated and trained to recognize and understand the impact of denied, degraded, exploited, or disrupted C2 capabilities in the same way that they recognize the effects of attrition and hindered operating environments on a traditional conventional force. However, situational awareness alone, while valuable, is not the only requirement. Commanders and staffs must maintain the capability to quickly and proactively mitigate the operational consequence of space and cyberspace losses. The commanders are empowered to direct C2 mitigation efforts that are truly synchronized with maintaining appropriate military capability and operations.

*One of the most critical lessons we learned in Schriever Wargame 2010 was that actions in space and cyberspace are inherently global, and cannot (or will not) remain constrained to the theater of operations.*

Simple in concept, it is a fairly complex requirement to levy on the commanders and engineers of the world—to provide true understanding of the full spectrum, global C2 architecture. Not just the tools and services used, but the actual systems on which they reside. At one point during SW 10, it became clear that we had better intelligence and understanding of the state of red's C2 than we had of our own systems. This clearly highlighted the need to better understand the impact of blue system degradations with a mindset of active management of blue systems to mitigate the impact to operations. This requires savvy operators trained and equipped to deal with both intentional and unintentional effects, as well as capabilities that are available via alternate paths, in multiple domains, and multiple platforms.

The world is changing; the face of future warfare will most likely start in the realm of bits and bytes. Freedom of action in space, as well as in cyberspace, clearly enables a more efficient and more successful way to do business. However, these freedoms come with a price—their value and vulnerability mark them as targets and as asymmetric leverage points against the US, and they no longer reside in a sanctuary. We, too, must change and shape the future to our needs—operating in and through the contested environments of tomorrow will require cooperative planning, close integration, and a methodology to assure access and freedom of action at the places and times of our choosing. In this environment, we must ensure our core enablers still function.

As we think of ways to protect the space and cyberspace enterprise, we must consider alternatives—communication paths across multiple domains and multiple platforms. If we cannot complicate and obfuscate the vulnerable chokepoints on our information highways, we may be handing future adversaries a Google map that could potentially cripple any US-involved operation.

The AOR of the GCCs and FCCs are explicitly linked and the complex environment which we now operate demands continuous deliberate planning. Habitual relationships must be formed between GCC and FCC planning staffs to clarify and coordinate the lattice of supporting and supported roles while creating a single synchronized plan developed with the capabilities and perspective of both the GCC and FCC. A geographically isolated event can quickly become a global crisis that demands a whole of nation approach. This makes continued exercises and forums like SW 10 with robust participation from multiple COCOMs and the entire DIME community absolutely critical to promote dialog so our civilian and military leadership are better prepared for those very difficult decisions with global impact that they will inevitably face in the future.

**Brig Gen Terrence J. O'Shaughnessy** (BS, Aeronautical Engineering, US Air Force Academy; MS, Aeronautical Science, Embry-Riddle Aeronautical University) is the commander, 57th Wing, Nellis AFB, Nevada. He is responsible for 38 squadrons at 12 installations comprising the Air Force's most diverse flying wing. General O'Shaughnessy is a 1986 distinguished graduate of the US Air Force Academy. He earned his wings at Sheppard AFB, Texas, and is a command pilot with more than 2,900 hours in the F-16 Fighting Falcon. He has had numerous operational F-16 assignments and served as an instructor in the F-16 Division of the US Air Force Fighter Weapons School. He has commanded the 510th Fighter Squadron, Aviano AB, Italy; 57th Adversary Tactics Group, Nellis AFB; 35th Fighter Wing, Misawa AB, Japan; and 613th Air and Space Operations Center, Hickam AFB, Hawaii. His staff assignments include duty as chief, fighter programs, in the Secretary of the Air Force Legislative Liaison office, and chief, Air Superiority Weapons Branch in the Secretary of the Air Force Global Power Directorate. He also served as the senior special assistant to the supreme allied commander Europe and commander, US European Command, Mons, Belgium. General O'Shaughnessy is a graduate of Air Command and Staff College, National Defense University, and NATO Defense College. Prior to his current assignment, the general served as vice commander of 13th Air Force, Hickam AFB, Hawaii.

**Lt Col Baron V. Greenhouse** (BS, History, US Air Force Academy; MS, Aeronautic Science, Embry-Riddle Aeronautical University) is the chief, special technical operations for the 613 Air and Space Operations Center, Hickam AFB, Hawaii. He is responsible for integration of specialized activities into joint air and space operations. Colonel Greenhouse is a career space and missile operator who has served with distinction as a missile instructor, within the operations directorate at Air Force Space Command, and as the space control requirements lead at US Strategic Command.

**Lt Col Kurt M. Schendzielos** (BS, Political Science, US Air Force Academy; MA, Military Space Application, Army Command and General Staff College; MA, Theater Operations, Army School of Advanced Military Studies) is director, Commander's Action Group for 13th Air Force, and is a senior navigator with over 1,400 hours and 270 combat hours. A distinguished graduate of Undergraduate Space Training, he served as an evaluator space control analyst and orbital analyst for US Space Command. After completing Specialized Undergraduate Navigator Training Colonel Schendzielos graduated from the US Air Force Weapons School and served as a weapons officer instructor, evaluator electronic warfare officer, and assistant director of operations. Colonel Schendzielos holds multiple advanced academic degrees and is a graduate of Army Command and General Staff College and the School of Advanced Military Studies. Prior to his current assignment, Colonel Schendzielos served as the chief of strategy plans team and deputy chief of the strategy division for 613th Air and Space Operations Center.

# National Security Fundamentals in the Space and Cyber Domains

**Ambassador Lincoln P. Bloomfield, Jr.**
**Chairman, Stimson Center**
**Washington, DC**

Schriever Wargame 2010 (SW 10) stimulated the participants' thinking on how the operational toolkit and authorities being developed or contemplated for US military commanders can best serve national security purposes in an unfolding crisis. Potent offensive or defensive capabilities, and accurate knowledge of an adversary's actions and their effects, are keys to tactical success. Being able to use those tools to deter war, or to manage and resolve a conflict at an acceptable cost in lives, treasure, and national reputation, is the strategic measure of success. Following are some policy-level insights gained from the exercise.

## From Marquis of Queensberry Rules to the Law of the Jungle

Picture the White House Situation Room a generation ago at the height of an escalating crisis between the US and a major nuclear-armed adversary. The president has directed a series of specific actions to position our strategic nuclear forces for higher alert; the secretary of defense, joined by the chairman of the Joint Chiefs of Staff, has conveyed the president's directions to the commander of US Strategic Command (STRATCOM), who will implement them. US nuclear policy experts, analysts, and planners have long since developed courses of action to maintain crisis control and prevail at every level of escalation, their certitude based on the existence of nuclear plans, policies, and procedures in the adversary camp. Thousands of miles away, the adversary's senior civilian and military leaders undertake a similar process as the geopolitical conflict between the US and its nuclear rival is played out.

Back in the situation room, a US advisor with deep expertise on the adversary's nuclear doctrine and posture is describing the adversary's actions for the president and the assembled national security senior leadership. The advisor refers to intelligence and warning indicators that both the US and its adversary understand to be departures from normal readiness conditions, some of these codified in bilateral arms control agreements as a way of maintaining strategic stability. "Look at what they haven't done," the US advisor explains. "They have not flushed their bombers or boomers (nuclear weapons-capable submarines); key airfields and facility parking lots are no busier than usual; and certain leadership figures remain on travel around the country or overseas, and do not appear to have been recalled to the capital." With the benefit of such context—weighing what has occurred against what would be expected to occur in a more aggressive scenario—the US president is able to tailor the US response so as to assert US interests and, at the same time, avoid escalating the crisis and risking catastrophic consequences.

Now, jump ahead to a future 21st century scene in the White House Situation Room as a crisis breaks out with a powerful adversary known to have sophisticated offensive capabilities in the space and cyber domains. Reports are coming in about anomalies affecting the supervisory control and data acquisition systems that run certain power, telecom, and transportation networks within the US. Benefiting from upgraded space situational awareness capabilities, STRATCOM is reporting a space event involving the sudden failure of systems on one or more militarily important US satellites, effects which it is able to attribute with strong circumstantial evidence if not absolute certainty, to actions by the adversary.

Security advisors, in the new space and cyber age as in the longstanding nuclear age, are able to compose for the president a compelling all-source summary of these apparent hostile acts against the US. However, in contrast to the nuclear standoff of an earlier era, there are no bilateral negotiations between Washington and the adversary government aimed at maintaining crisis stability—nothing to curb the dangers of hostilities in space or destructive actions against the information systems on which the civil and military sectors of each country has come to depend. The good news is that there has never been a destructive conflict waged in either the space or cyber domains. The bad news is that no one around the situation room table can cite any history from previous wars, or common bilateral understandings with the adversary, relating to space and cyber conflict as a guide to what the incoming reports mean, and what may or may not happen next.

This is the big difference between the space-cyber domains, and the nuclear domain. There is, in this future scenario, no credible basis for anyone around the president to attribute restraint to the adversary, no track record from which to interpret the actions by the adversary. There is no crisis management history: the president has no bilateral understandings or guide-

*There is, in this future scenario, no credible basis for anyone around the president to attribute restraint to the adversary, no track record from which to interpret the actions by the adversary.*

*So long as we live in a world where no country including the US has well-documented experience with either war in space or 'cyber conflict' with an adversary, the potential for error, misunderstanding, miscalculation, overreaction, and escalation will remain high.*

lines from past diplomatic discussions, and no operational protocols from previous incidents where space and cyber moves and counter-moves created precedents. Perhaps the adversary intended to make a point with one series of limited attacks, and hoped for talks with Washington and a compromise; but for all the president knows, sitting in the situation room, the hostile actions taken against America's space assets and information systems are nothing less than early stages of an all-out assault on US interests.

In 2009, at the Schriever V Wargame, players had discussed the potential utility of internationally agreed protocols and confidence building measures such as a Space Code of Conduct.[1] However, at that time the general perception among the assembled military and defense experts was that any proposition to trade away freedom of action in space as the price of an international arms control agreement was at best a questionable bargain for the US. Particularly given that in a future confrontation, the US could not trust its adversary to live up to its obligations in an arms control agreement, the advantage of such a trade was not apparent.

The SW 10 exercise changed that perception precisely because tactical freedom of action was not the only asset worth having in a future crisis. Equally important was having some basis to judge the intent and aims of the adversary. If left only to interpret operational reports from military commanders—or, in the case of cyber networks, incident reports from state and local authorities, and industry—about anomalies and disruptions that are reasonably attributable to the deliberate actions of an adversary, a future president has but one conclusion to draw: the US is under attack. If war, as Clausewitz said, is the continuation of politics by other means, space and cyber war with no precedent or protocols emerged in the SW 10 exercise as a highly problematic channel through which to prosecute "politics," and thereby serve the national interest, in a crisis.

One take-away, therefore, is the advisability of exploring specific protocols and norms relating to possible military actions in the space and cyber domains. While proposals already exist for a space Code of Conduct, the US warfighting community would do well to examine potential protocols in detail to identify those that conform to its mission objectives. The Schriever franchise is well suited to the task. Absent specific norms for space-cyber conflict, our political leaders will likely be compelled to "talk" as they "shoot"—communicating very plainly their aims and intentions. Otherwise, not knowing what the US intends, the adversary may well anticipate the worst and act accordingly. While adversaries in wartime will be very slow to believe each other's words, this is a lesser concern than leaving it to the adversary to figure out American intentions.

Related to this is the possibility that the adversary's sites or systems targeted by the US may have different or secondary purposes than those presumed by US intelligence. These alternative purposes may be deemed far more vital and strategic than the US side had thought—a misunderstanding that could immediately escalate the conflict. There is no assurance that clear messaging at the leadership level between the US and the adversary would serve as a brake on escalation in such a situation; but the absence of such communication would leave each side with no incentive or excuse for restraint. So long as we live in a world where no country including the US has well-documented experience with either war in space or 'cyber conflict' with an adversary, the potential for error, misunderstanding, miscalculation, overreaction, and escalation will remain high.

*Figure 1. Brig Gen Robert J. Chekan and Ambassador Lincoln P. Bloomfield, Jr. at Senior Leadership Seminar in Washington, DC for Schriever Wargame 2010.*

## Offensive Measures with Unpredictable Effects in Domains Without Boundaries

The nature of both space-based and terrestrial information systems raise new challenges for the US and its allies in preserving the peace and defending their shared interests if threatened. Space assets

are costly and scarce; dependent on terrestrial facilities, they may fail if disruption occurs at a single node anywhere in the system.[2] Because space systems are both costly and (for most countries) scarce, they may carry secondary and tertiary functions, servicing government or private sector interests. The US may have imperfect knowledge of what purposes and end-users are served by a foreign space system. Taking deliberate offensive action to disrupt or disable a foreign system, therefore, can bring unpredicted and unintended consequences, even when it achieves the first-order tactical purpose of degrading a known military capability relevant to the adversary's prosecution of the conflict.

Terrestrial information systems, unlike space systems, may be robust, redundant, and defended. While space systems are comparatively scarce, costly, and vulnerable, terrestrial information networks are widespread and constantly proliferating, becoming ever more accessible to the world's population and enabling ever more aspects of daily life. The result is the same: these cyber-networks not only support military capabilities, but they serve multiple users and end-uses. If intelligence analysts and military planners are less than certain of what uses and end-users are tied to a particular foreign satellite or space system, they are surely far less able to predict the second, third, and fourth-order effects of disrupting a foreign cyber network.

Two liabilities emerge from the prospect of defending national interests militarily in the space and cyber domains. The first, mentioned above, is the possibility of targeting an adversary asset with one known purpose, only to find that it has far more sensitive purposes and becomes a trigger for unintended escalation of the conflict. The second is that the physics of space and cyber systems frustrate the military planner's ethical quest for 'surgical' strikes: by the very nature of these geographically unbounded systems and their capacity to serve multiple purposes, as military targets they carry high risks of collateral damage. Moreover, unlike probably any circumstance yet encountered in conventional warfare, with space and cyber systems the negative collateral impacts could be located anywhere, and harm anyone; the unintended damage incurred could exceed the importance of the tactical objective. Most challenging of all, the president and US military commanders would likely have little if any ability to predict who, where, and how collateral effects will impact, or the severity of the harm.

In a world where governments are finding their sensitive activities ever more vulnerable to public exposure and scrutiny, the US should expect, and plan, to be held accountable for all of the impacts caused by its use of military force, including technological tools suited to the space and cyber domains. The moral and ethical heritage underpinning US security policy that gave rise, in recent decades, to the exhaustive preparation of "no-strike" lists in advance of major combat operations such as the removal of Saddam Hussein's regime in Baghdad in 2003, do not cease to exist when geopolitical conflict migrates into the space and cyber domains. The task for US security policy is to conform operational concepts to a world increasingly dependent on these new, geographically unbounded systems, so that no adversary can gain undue advantage by degrading or holding them at risk.

## Early Insights on Space Allies: the Good News

In at least one important aspect, this exercise reflected the clear direction of the 2010 Quadrennial Defense Review and National Security Strategy: certain allies participated as full stakeholders. No information was denied to them; their national assets were combined with US systems; and presidential decisions were deliberated in their presence, with the benefit of their counsel.

Traditional benefits to US security from alliances have included the geographic access they afford to areas of possible conflict; deterrence derived from multinational solidarity; and sharing of burdens among multiple armed forces and national budgets. As significant as these advantages are, in the post-Cold War era there has been a fractured US consensus on the subject of alliances, with a school of thought questioning whether the US may at times be better off acting unilaterally and preserving maximum political-military freedom of action. When allies do not substantially encumber US policy decisions, when their presence in the battlespace adds materially to the conduct of the mission through compatible (if not identical) rules of engagement and a level of self-support that does not require a significant diversion of US resources, the political and military benefits can be substantial.

Based on the SW 10 wargaming experience, in a conflict potentially involving space and cyber networks, the US appears to gain more than it gives up by making common cause with close allies. Here are five prospective benefits of such alliance relationships:

1. Allies have assets such as satellites and ground stations providing communications and intelligence. An adversary hoping to compel the US to concede to its demands by threatening US space assets will have reduced grounds for optimism if allied systems are also functioning and available to support the US side in the confrontation. This enlarged network of space systems creates a measure of deterrence.

2. Allies have geopolitical standing and interests of their own. An adversary hoping to isolate the US in a confrontation will be frustrated by the realization that the price of escalating to hostilities against the US in space is likely

*An adversary hoping to compel the US to concede to its demands by threatening US space assets will have reduced grounds for optimism if allied systems are also functioning and available to support the US side in the confrontation.*

*Just as public disagreement with our allies might invite adventurism by an adversary, political and legal solidarity between the US and its allies can contribute to deterrence.*

to be a state of belligerency with additional governments and trading partners. This expanded political and economic profile on the US side similarly creates deterrence.

3. Allies have tactical value-added based on their own competencies. Having allied teammates who can bring to the table separate intelligence information, analytical perspectives, planning concepts, and specialized language and technical skills can enrich the quality of the options available to US decision makers and field commanders. This enhanced operational capability, if appreciated by the adversary, affords a further increment of deterrence.

4. Allies have their own national policies and interpretations of international laws and norms. This aspect of alliance management has sometimes been perceived in the US as an inconvenience or even a liability. However, a lesson of recent history for civilian policy makers is that in making the decision to use military force, the US will do well not only to assert the legitimacy and legality of its actions, but to make a case that is credible to and accepted by other countries, allies above all. By including close allies in the deliberative process aimed at maintaining the security of space and cyber systems against hostile threats, US decision makers can forestall dissension among friendly capitals once military action is taken, and hopefully receive strong public backing from allied governments. Just as public disagreement with our allies might invite adventurism by an adversary, political and legal solidarity between the US and its allies can contribute to deterrence.

5. Finally, allies have authorities that may prove useful to the war effort. Government activities in the space and (particularly) cyber arenas have the potential to intersect with fundamental American rights involving privacy and private property. Allied legal systems and government policies, while similar to the US are not identical, and allied governments may have authorities relevant to countering these new threats that US officials do not have. In such instances, of course, US officials can have no involvement of any kind with an action by a foreign government that would not be permissible under US law. However, allied governments are free, indeed expected, to protect their national interests according to their own laws. Separate but sympathetic action by allies in facing a threat to shared interests is yet another potential advantage of alliance relationships contributing to space and cyber security, and thus deterrence.

As the US deepens its national security dependence on space and cyber systems, potential adversaries continue to press ahead with the development of capabilities to hold these systems at risk. The Schriever wargaming franchise, by simulating future space and cyber conflict, is helping civilian and military practitioners to recognize what tools, procedures, and thought processes from the past may be relevant to securing our interests in these new domains. More importantly, it is offering a glimpse at challenges of future conflict that are most likely to require fresh thinking and new solutions.

*Notes:*

[1] See, for example, work on space security being conducted at the Henry L. Stimson Center in Washington, http://www.stimson.org/space/programhome.cfm.

[2] The author credits fellow SW 10 participant Lt Gen (USAF, retired) Robert Elder, for the useful insight that the term "circuit" may better describe the functioning of a space system than "network" which implies robustness that may not exist.

**Ambassador Lincoln P. Bloomfield, Jr.** (Harvard, a.b, cum laude, Government, 1974; Fletcher School, M.A.L.D., 1980) is chairman of the Henry L. Stimson Center in Washington, DC. He was the president's special envoy for Man-Portable Air Defense System Threat Reduction from 2008-09, and assistant secretary of state for political military affairs as well as special representative of the president and secretary of state for Humanitarian Mine Action from 2001-2005. He previously served as deputy assistant secretary of state for Near Eastern Affairs (1992-93), deputy assistant to the vice president for National Security Affairs (1991-02), member, US Delegation to Philippine Bases Negotiations (1990-91), member, US Water Mediation in the Middle East (1989-90), and principal deputy assistant secretary of defense for International Security Affairs (1988-89), among other positions in the Department of Defense (OSD/ISA) beginning in 1981. He is president of Palmer Coates LLC, senior advisor at Akin Gump Strauss Hauer & Feld LLP, operating advisor at Pegasus Capital Advisors L. P., senior advisor at ZeroBase Energy LLC, and chairman of the board of Bell Pottinger Communications USA LLC.

# Science Supporting Space and Cyber: Insights From Schriever Wargame 2010

**Dr. Werner J. A. Dahm**
**Chief Scientist of the US Air Force, HQ Air Force**
**Pentagon, Washington, DC**

**Col Eric Silkowski, USAF**
**Office of the Air Force Chief Scientist, HQ Air Force**
**Pentagon, Washington, DC**

Early Schriever Wargames were conducted to understand the value of advanced space technologies in various conflict scenarios, and later evolved to address the cyber domain as well. More importantly, over time the games broadened their scope to increasingly address factors such as strategy and policy dimensions, diplomatic and economic considerations, integration with joint and allied partner operations, and even whole of government approaches for escalation control and coalition warfighting. Today, the primary focus of Schriever Wargames is no longer just on understanding the value of advanced technologies. This is appropriate given the intense interdependences that the space and cyber domains have created among nearly all elements of the military, political, and diplomatic spheres of conflict. It is in these broader challenges where the Schriever Wargames seek to derive some of their most valuable insights.

Yet ultimately it is still science that will provide the advanced technologies for addressing many of these broader challenges of space and cyber domain conflicts. Indeed, space and cyberspace are inherently technical domains, and continued innovation in them is essential to provide our own forces with the greatest freedom to operate while denying adversaries the ability to interfere with our use of these domains or their use by others for peaceful means. Each Schriever Wargame has examined potential future capabilities derived from science and technology, and these have been increasingly informed by the policy and decision-making insights from previous games. Indeed, for Schriever Wargame 2010 (SW 10) it was recognized that the wargame provides an opportunity—and a particularly valuable one—in which scientists and technologists can gain further insights into space and cyberspace operational needs as driven by contemporary thinking about these broader challenges. These insights in turn enable the science and technology (S&T) leadership of the Air Force, and of our international partners, to more clearly understand where investments in technology development should be focused to maximize their value for meeting these challenges.

SW 10 thus for the first time included a S&T cell as an integral part of the wargame to ensure that these key insights would be obtained firsthand and in their proper context. This was additionally motivated by the value seen from having an S&T cell in the previous year's Air Force Strategic Plans and Programs-led Future Capabilities Game. It was also recognized that addition of an S&T cell in Schriever Wargames could further increase the technical fidelity of understanding the future environment that the wargame is presumed to occur in. Such a cell also helps inform and support technical aspects of decisions being made by other cells in the wargame as they formulate their moves. This latter role is provided on a non-interference basis, observing and offering support to other cells as needed. In so doing, the S&T cell obtains additional important insights that collectively provide a clearer understanding of the science investments that will most effectively support our broader space and cyber needs. Those insights, together with major efforts such as the recent Air Force "Technology Horizons" vision for S&T over the next decade and beyond,[1] are essential for guiding the Air Force's technology development efforts and those of our international partners.

The Air Force chief scientist thus assembled a team of a dozen scientists and technologists for this purpose and led the S&T cell in SW 10. The team included representatives from the Air Force Research Laboratory, Air Force Space Command, Air Force Plans and Programs, the Defense Advanced Research Projects Agency, and others, as well as science and technology representatives from Australia, Canada, and the United Kingdom. On each day of the wargame, cell members attended the game brief and then met to discuss key challenges being faced in the game and potential technologies for addressing these. They then spread out across the game floor to interact with other cells as the next move was developed, observing and engaging in discussions to identify issues being addressed by these cells and providing information to support their decision making. Cell members later reconvened to discuss their observations of key issues and corresponding technical implications, and then attended the end-of-day game move brief. This cycle was effective in providing support to the wargame while enabling the insights needed to inform future S&T investments in space and cyberspace capabilities. The S&T cell also interacted with and briefed the senior leadership cell to ensure that these insights would inform their decision making during the wargame.

## Key Insights

SW 10 revealed a clear need for developing cyber posturing tools and methods for signaling to an adversary our changing perceptions of the level of tension during periods of approaching conflict. Such tools are essential ingredients for an effective ability to control conflict escalation. Today, there are few sufficiently nuanced tools available in the cyber domain for expressing varying degrees of satisfaction or dissatisfaction with changes in an adversary's posture or actions in the cyber domain and elsewhere. Information operations conditions do not serve this purpose. They are a relatively coarse threat level system to

enable appropriate internal defense of information systems and networks, but are not meant for disclosure to an adversary as a way of "cyber signaling" to express changes in our posture and enable conflict escalation control. To be effective in managing escalation during the period leading up to a potential conflict, cyber posturing tools must be inherently disclosable to an adversary without increasing the risk of compromise to our own cyber systems. They must also be sufficiently rich in nuance to allow accurate messaging and to express relatively subtle changes in the perceived level of tension. The need for entirely new S&T efforts that can enable such effective cyber posturing tools is one of the key insights from the SW 10

SW 10 also reinforced the need for methods that can provide significantly increased "cyber resilience," as opposed to the traditional focus on cyber defense. Technologies that enable resilience permit cyber systems to fight through attacks to maximize mission effectiveness even in large-scale conflicts. For instance, as noted in "Technology Horizons,"[2] highly virtualized computing environments controlled by hypervisors that are inherently agile by design could enable massive network polymorphism as a new means for achieving cyber resilience. In effect, the topology of critical networks within such an environment could be made to change continually, perhaps hundreds of times each second in a pseudorandom fashion. Such inherently dynamic networks would be fundamentally different from today's static networks, which give cyber adversaries as much time as they need to observe how we operate within the network, to plan attacks against it, and to emplace the tools needed to enable their attacks. In contrast, massive network polymorphism causes a cyber adversary to have almost no time after gaining entry into the network to observe and plan such attacks, thereby negating much of the benefit from gaining access in the first place. Moreover, the quick steps that cyber adversaries must take to be effective in such a highly polymorphic network also increase the likelihood that they will leave behind forensic evidence of their activity. That, in turn, addresses another of the cyber domain's most difficult challenges, again revealed in SW 10, namely the need for improved means of attribution in the cyber domain. Note that many of the key technologies to support massive virtualization and agile hypervisors are already being developed commercially for cloud computing applications. Air Force S&T efforts will focus on those additional technologies that can enable massive network polymorphism to provide greater cyber resilience and improved cyber attribution.

The S&T cell considered various small, micro, and nanosatellites during SW 10, with particular emphasis on adversary use of "grappler" satellites that can attach themselves to a target satellite to change its momentum and shift its center of mass. The former induces drift and tumble in the target satellite, while the latter causes the target satellite's control system to be unable to correctly control its orientation and motion. Conceivably, even very small and remarkably simple satellites of this type can render a large and extremely expensive target satellite essentially uncontrollable. Small satellites could also be designed to provide an on-demand kinetic kill capability, or with microwave-based directed-energy capabilities to degrade or destroy the target satellite. Co-orbiting satellites can also provide non-destructive counterspace options, for instance by interfering at relatively close ranges with satellite uplink transmissions. Such small, maneuvering, co-orbiting satellites might also provide an adversary with other options for lethal and non-lethal proximity operations in support of counterspace efforts. Increased satellite self-awareness of the surrounding space environment will become increasingly important to warn of the approach of such objects.

SW 10 further showed the need for S&T to support better characterization of the capabilities of orbiting space objects. It is technically feasible to achieve such characterization, at least in part, by inferring potential capabilities of space objects based on spectral reflectances and emissivities of various parts of their exterior surface. Factors such as total photovoltaic cell area could be obtained in this manner and then used to infer operating power levels. Radiative surfaces can similarly provide information on thermal management within the object. While such approaches based on external characterization would provide valuable information, they leave room for substantial uncertainties in the real capabilities of an object. In the longer term, interior characterization could potentially be achievable with an inspection satellite pair positioned on either side of the object being inspected, one emitting as an x-ray source and the other as an imager. Corotation of the pair around the object could even allow for three-dimensional tomographic reconstruction of interior components in the object.

During SW 10 the need for substantially greater space situational awareness was again reaffirmed, both for determining potentially hostile space actions and for avoiding orbital debris. Current ground-based radars and telescopes as well as space-based space surveillance assets that together comprise the space surveillance network can, in principle, be augmented to provide birth-to-death detection, tracking and characterization of every object in orbit, from large satellites to picosatellites and orbital debris at low Earth orbit, medium Earth orbit, and geosynchronous Earth orbit altitudes. This can be done through a combination of new ground-based and space-based assets, with appropriate fusion of data from other satellites, ships, and other sources into an integrated database. Augmenting radars and optical telescopes in the space surveillance network with a 3.5-m Space Surveillance Telescope, the Space Based Space Surveillance system, and the S-band Space Fence would greatly improve detection and tracking. As noted above however, determining the contents of a satellite or its potential capabilities and intent will remain challenging. By including whole-chain intelligence as part of birth-to-death tracking, critical "missing pieces" can be provided that allow a clearer picture of an object's true nature to be formed. Bringing together data from active and passive radar frequency and electro optic/infrared sources can provide a true "space situational awareness (SSA) network" with capabilities far beyond those of its individual elements. In principle, all satellites in orbit could contribute various types of information that, when fused and analyzed, provides a far more complete SSA picture, including space weather effects to allow discrimination of hostile actions from natural causes. Commercial satellites

may be willing to host such sensors as the need to avoid space debris continues to grow in importance.

Returning to the cyber domain, SW 10 also reaffirmed that the "speed of light" time scales inherently needed for effective responses in cyberspace will demand increasingly autonomous capabilities. This stands in contrast to the air and space domains, where well-founded policy imperatives do not permit fully autonomous strike for the foreseeable future, even though technology can in large part already provide such a capability. Yet in cyberspace it is not an option to forego fully autonomous response as a necessary means of defense when our cybersystems are attacked. Autonomous response is an essential capability in the cyber domain. However, as these autonomous responses become increasingly nuanced and make use of increasingly greater amounts of data for situational awareness to decide an appropriate action, the underlying autonomous decision systems become increasingly difficult to verify and validate. Highly adaptable autonomous systems are today essentially unverifiable by existing verification and validation (V&V) methods. Their potentially large number of inputs and their inherently high levels of adaptability create a near-infinite number of possible system states that each need to be tested. "Technology Horizons" noted that development of entirely new approaches to V&V for such highly adaptive autonomous systems—not only in cyberspace but in the air and space domains as well—is one of the greatest technical challenges facing the Air Force.[3] S&T efforts to develop such approaches will be essential, and it is precisely in the cyber domain where the need for these will be among the most urgent.

## Way Forward

Having an S&T cell in SW 10 indeed proved to be a valuable addition to the wargame. Beyond supporting technical fidelity in the capabilities postulated for both sides in the 2022 environment, the cell provided technical insights to others as they considered various courses of action during the wargame. Most importantly, the cell gained essential insights into science-based efforts that will be needed for addressing key issues in space and cyber conflicts in the 2022 time frame. While the focus of the SW 10 was largely on strategy, policy, economic, diplomatic, and other broader considerations, all of these have technical dimensions. Observing how they played out in the wargame provided additional perspectives on "disproportionately valuable" technologies that could enable greater freedom of operations for US joint and coalition forces in space and cyberspace.

Numerous insights from SW 10 reaffirmed many of the findings that can be found in the Air Force's recent "Technology Horizons" vision for S&T focus areas during 2010-2030,[4] particularly with regard to the space and cyberspace domains and the interdependences that result from them. These insights will help guide Air Force S&T investments over the coming decade, and potentially those of our allies as well. As the world continues to "flatten" from a technology perspective and we face adversaries having capabilities more nearly equal to ours, it will become increasingly important to retain an S&T cell as an integral participant in future Schriever Wargames, allowing science to more effectively support our broader space and cyber needs.

*Notes:*

[1] US Air Force Chief Scientist, "Technology Horizons: A Vision for Air Force Science & Technology During 2010-2030," report, volume 1 (public releasable), AF/ST-TR-10-01-PR, Headquarters Air Force (AF/ST), Washington, DC, 15 May 2010.

[2] Ibid.

[3] Ibid.

[4] Ibid.

**Dr. Werner J.A. Dahm** (BS, Mechanical Engineering, University of Alabama Huntsville; MS, Mechanical Engineering, University of Tennessee Space Institute; PhD, Aeronautical Engineering, California Institute of Technology) is the chief scientist of the US Air Force, Air Force Pentagon, Washington, DC. He is the principal advisor for science and technology to the Air Force chief of staff and the secretary of the Air Force, and led development of the "Technology Horizons" vision for Air Force science and technology for 2010-2030. While serving as the Air Force chief scientist he is on leave from the University of Michigan, where he has served as a professor of aerospace engineering for the past 25 years. He is an author of over 180 journal articles, conference papers, and technical publications, a holder of several patents, and has given over 130 invited, plenary, and keynote lectures worldwide on topics dealing with various aspects of aerospace engineering.

He has served on the Air Force Scientific Advisory Board and on numerous task forces for the Defense Science Board and as a member of the Defense Science Study Group. He is a Fellow of the American Institute of Aeronautics and Astronautics and the American Physical Society, and a recipient of the William F. Ballhaus Aeronautics Prize from Caltech and the Air Force Meritorious Civilian Service Award, as well as major research awards from the University of Michigan. He has also served widely in advisory and organizational roles in aerospace engineering, and as a consultant to industry.

**Col Eric Silkowski** (BA, Physics, University of Chicago, MS/PhD, Engineering Physics, Air Force Institute of Technology) is the military assistant to the chief scientist of the US Air Force in the Pentagon. He supports the chief scientist in providing independent, objective, and timely scientific and technical advice to the Air Force chief of staff and the secretary of the Air Force, and in evaluating technical issues of relevance to the Air Force mission. He also supports the chief scientist in his contributions to supporting and maintaining the technical quality of the research being conducted across the Air Force.

Previously he led the Air Force Technical Applications Center's Applied Physics Laboratory and ran worldwide operations for nuclear event detection and global atmospheric monitoring. Other technical assignments include high explosive testing, ballistic reentry vehicle acquisition, and conceptual design of directed energy weapons systems. He has also served as executive officer to the J8 for NATO Allied Command Operations at Supreme Headquarters Allied Powers Europe.

# The Schriever Challenge – Keep the Walls Down

**Maj Sam Baxter, USAF, Reservist**
**Special Programs Division**
**Commander's Action Group, Air Force Space Command**
**Peterson AFB, Colorado**

**Capt Nicole O'Neal, USAF**
**Special Programs Division, Air Force Space Command**
**Peterson AFB, Colorado**

"Tear down this wall!" The declaration by former President Ronald Reagan foretold the end of the Cold War—a war impacted by the foresight of General Bernard Schriever in space's ability to influence the fight. At Schriever Wargame 2010 (SW 10), a game named after the "space game-changer," one could not escape the organizational walls that came crashing down. For a drop in the budget bucket, approximately 550 military and civilian space and cyber experts representing more than 30 agencies across the Department of Defense (DoD), intelligence community (IC) and civil sectors, as well as, the countries of Australia, Canada, and Great Britain came together in the unified pursuit of getting a glimpse of *future* warfare in unchartered domains.[1] Within the historic halls of the Red Flag building at Nellis AFB, Nevada, ideas were shared, thoughts generated and insights garnered in a non-attribution environment—the original objectives Col Richard "Moody" Suter sought after when this "air game-changer" sold the idea of Red Flag to Air Force brass.[2] Unfortunately, this unencumbered union of space and cyber brainpower is only gathered together for one week, every two years.

What if instead a new Schriever series is born, not just the wargame series, but a "Schriever Challenge" series in which the coalition of space and cyber willing are brought together to focus on the toughest of *today's* problems? What if bureaucratic walls were to fall to make into reality what is found to be game-changing in a wargame? What if government fiefdoms were set aside and synergies were created between organizations to solve these challenges?

## The Challenge Concept

The concept of posing challenging questions to expand the realm of the possible is not new. Charles Lindberg crossed the Atlantic Ocean in 1927 for a $25,000 Orteig Prize and in 2004, Burt Rutan's SpaceShipOne crossed the boundary of space for a $10 million X-Prize win that may prove him to be the "modern space game-changer."[3, 4] Nor is the concept unfamiliar to government. In line with challenging people and technology, the Defense Advanced Research Projects Agency (DARPA) has brought the brightest minds together for their Grand Challenges for driverless vehicles. Recently DARPA expanded the idea to the 2009 Network Challenge in which a Massachusetts Institute of Technology team was rewarded for the fastest location discovery of 10 balloons simultaneously released across the US—in an amazing nine hours.[5] Even the US Air Force's chief scientist recently issued a series of "grand challenge" problems, not competition based, but technologically game-changing, to drive the research community in "Technology Horizons - A Vision for Air Force Science and Technology During 2010-2030."[6]

What is new with this concept is the unleashing of wargame intellect normally focused on strategic quandaries onto problems that keep senior leaders across the government awake at night—taking a cue from William Shakespeare to "let slip the dogs of war" on today's challenges.[7] Imagine taking the impressive Rolodex the Space Innovation and Development Center (SIDC) uses to gather wargame participants and employing this talent pool towards our nation's toughest space and cyber challenges. Let's modify the wargame to address issues currently facing our Airmen, Soldiers, Sailors, and Marines that could potentially cut research and development time, save money, and ultimately American and coalition lives.

As the Schriever Wargame is held every two years, we propose bringing together the Schriever talent on a regular basis by using the "off-year" to focus on a Schriever Challenge. Similar to the preparation sessions used to put together the wargame, the same could be done for a challenge, in which participants regularly gather together to research for the main event. Similar to the Air Force Space Command issuance of wargame objectives for participants to work through, challenges can be issued to be labored on. The beauty of the Schriever Wargame is the SIDC creates an environment by which the 500+ professionals can come together and make an immediate impact without the need for a formal process. The typical ways by which organizations come together is void in Schriever vocabulary: tiger team, working group, steering group, board, council, committee, commission, and so forth. Instead the SIDC's address book is intertwined to address the wargame crisis of the day, unencumbered by bureaucracy, and challenged to find a way to integrate interweaving organizational capabilities and knowledge to create the ultimate synergistic effects.

## The Schriever Challenge

*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 operation will become an even more powerful force multiplier.*[8]

~ Lt Gen Larry D. James, Schriever V Wargame: The Boundaries of Space and Cyberspace

The Schriever Challenge needs to cut across government agencies by tackling problems in large enough scale that people from multiple agencies and nations cannot wait to start making a difference. Space protection and cyber defense are great examples in which no agency or nation wants to imagine a day without space or cyberspace's influence—GPS, DirecTV, or free navigation of the Internet. But, these issues are not going to be solved in a short time span, so a challenge needs to be a subset to the larger problem. Akin to the wargame, the problem is broken into individual cells to be worked on and periodically the cells come together to look at the problem holistically in a continuous feedback loop. Also, the Schriever Challenge needs to force imagination use and be willing to look at problems differently than current and past efforts.

***An example Schriever Challenge:*** One issue many organizations have studied is how the nation can move from object tracking to true space situational awareness (SSA)—including the sharing of disparate data between the IC, DoD, allies, and industry. The problem is partly looked at as a sensor problem, or the lack thereof, as well as a sharing problem between those with the sensors. The challenge could be to study the problem from an information technology (IT) or cyber perspective. For example, can the government take an IT lesson from industry in how business information is openly shared securely among different competing companies, like in supply chain management, to find better ways to share satellite data for improved situation awareness in space? So, one cell would be composed of supply chain management experts, like Dell and FedEx, with government experts who understand how SSA data currently flows on the space surveillance network to come up with a hybrid way of moving SSA data. Another cell could leverage the financial market IT experts for a lesson in security and open architectures. From one's laptop an individual can use their Internet browser to access their financial account to buy or sell a stock, executed by their institution's corporate network that has access to the larger market clearinghouse networks—all in seconds, securely, yet in an open environment in which all parties have complete trust, otherwise money would not be risked. Could insights be garnered into ways satellite information can be similarly shared in an open, secure, trusted environment?

An industry cell composed of fellow satellite flyers like DirecTV, Iridium, Sirius Radio, and others, could discuss how to facilitate such a "satellite information clearinghouse" with the government. A higher classification cell could be composed of the IC, DoD, and cleared industry companies to discuss ways to more effectively share data—both within current architecture schemes and by transforming old government ways of doing business to embrace the latest lessons from industry. For example, a data-mining lesson from Amazon in how they automatically recommend books could be used to potentially recommend ways to more effectively sift databases to better predict potential future collisions. An allied cell could discuss better ways to share data with our partners, while a legislative/policy cell could investigate what needs to be altered to enable the change. When it comes to preventing future satellite collisions, can the nation afford not to try ideas outside established thinking, such as leveraging supply chain management, financial markets, or buying books? Insights garnered can be used to feed current programs of record (POR), a new POR, a future Joint Capability Technology Demonstration (JCTD), a Tactical Exploitation of National Capabilities Program (TENCAP), or inspire a company's independent research and development.

***The Cyber Challenge:*** In the 50+ years since the launching of Sputnik, the space domain is characterized as "congested, competitive, and contested."[9] This description is even more fitting for cyberspace, the recent game-changer. Where a limited number of nations operate in space, the world operates in cyberspace. Where a handful of government agencies operate satellites, anyone can operate a keyboard. And anyone can use that keyboard to attack the US—nation, non-state actor, and hacker alike. The job of the cyber warrior is to battle back, not with brawn or bombs, but with intellect. And when every agency needs a legion of cyber warriors to defend networks and data, efficiencies must be found.

Cyber has every government fiefdom contending for resources and until lately, had no consolidated voice. The standup of US Cyber Command (USCYBERCOM) and the unification of cyber efforts across the services is a first step in wrapping arms around this interconnected domain. Cyber's interrelationship with intelligence is signified by having the USCYBERCOM commander dual-hatted as the director of the National Security Agency, which could potentially yield a symphony of concerted efforts for the military and intelligence cyberspace warriors. Maybe from this environment of interagency cooperation, future Schriever Challenges can be used to further break down cyber walls—not just within the military, but in civil and industry sectors as well.

USCYBERCOM is charged with only defending the cyber domain, although its impact can be felt in all domains—air, land, sea, and space. To understand the nth order cyber effects to other domains, such as when network defense is broken, conversations need to occur by people who speak different "domain languages," such as found during the wargame. A Schriever Challenge can be used to integrate these domains even closer—ever more important in today's joint fight. To enable this, cells should be a matrix of thinking warriors from the various communities: space, cyber, air, intelligence, acquisition, and so forth, to confront tough problems in nimble ways by employing their domain knowledge and capabilities to create synergistic effects previously unimaginable.

## The Schriever Challenge Rules

As the wargame comes with a basic set of rules on how the game is to be played, so should a Schriever Challenge. First, participants should be required to leave behind their organizational affiliations, their agendas, their rank, and titles as they work on a Schriever Challenge—similar to the ideals of the Schriever Wargame. If Uncle Sam is to take any lesson and turn it into a solution, he needs an open mind to glean insights not just from other government agencies, but industry as well, especially in the cyber arena where industry is continually pushing into new frontiers. A similar second rule is the nation

is dependent on our allies in today and tomorrow's joint fight—we face many of the same problems and need to include our partners in as many Schriever Challenges as possible.

Third, a subset of individuals needs to be permanently cross-cleared to special programs across agencies and across DoD/IC boundaries. To foster the flow of ideas, empowered individuals need complete knowledge of what is in the capability toolkit in order to turn seemingly unrelated components into solutions that provide synergistic effects for the warfighter. GPS is a great example by which the Air Force provides a position and timing capability from which the rest of the world develops unique effects that could never have been imagined if it was locked in a closet accessible by a limited few who only wanted it for precision guided munitions.

Fourth, the challenge needs to be results oriented. The Schriever Wargame's success is partially due to 500 people knowing it's worth taking a break from their normal workloads to be part of the noble cause of the game and the resulting impact it has on senior leader thinking. In the case of the Schriever Challenge, senior leadership is presented potential game-changing solutions that could impact not just thinking, but reality. The best solutions are given to a commander to implement, further develop, or refine in the form of a JCTD, TENCAP, new program, and so forth. Ownership by a commander is essential, otherwise potential solutions will be shelved in a "Raiders of the Lost Ark"-type warehouse. Challenge participants could still work with the solution "owner" to facilitate progress, well after the challenge's main event bell has rung, because of the relationships born out of the cells. Senior leadership can keep tabs on progress through a Schriever Challenge follow-up session in which the owner/commander presents an update on the good, bad, and ugly, that is advances, challenges, and administrative walls that need to be brought down to facilitate development.

## The Real Challenge

The Schriever Challenge series is a potential idea for the real challenge—getting bureaucracy to be more responsive in a world that moves faster than the speed of government. From Ronald Reagan's first inaugural address the following words seem as relevant today as they were in 1981:

> Government can and must provide opportunity, not smother it; foster productivity, not stifle it. If we look to the answer as to why for so many years we achieved so much, prospered as no other people on Earth, it was because here in this land we unleashed the energy and individual genius of man to a greater extent than has ever been done before.[10]

A Schriever Challenge will not answer all of government's conundrums and there will always be a need for in-depth study on the toughest of problems. The hope is a Schriever Challenge can build better relationships, build creative thinking and build potential solutions for the joint warfighter, so much so, that together we passionately declare "Keep the walls down!".

*Notes:*

[1] Air Force Space Command, "Schriever Wargame concludes," 27 May 2010, http://www.afspc.af.mil/news/story.asp?id=123206668

[2] Walter J. Boyne, "Red Flag," *Air Force Magazine* 83, no. 11 (November 2000): 44-52, http://www.airforce-magazine.com/MagazineArchive/Documents/2000/November%202000/1100redflag.pdf.

[3] Charles Lindbergh Website, "The Spirit of St. Louis Story," written in association with the Lindbergh Foundation and the Hall Aviation Foundation, http://www.charleslindbergh.com/hall/spirit.asp.

[4] X Prize Foundation, "Ansari X Prize," http://space.xprize.org/ansari-x-prize

[5] DARPA, "MIT Red Balloon Team Wins DARPA Network Challenge," news release, 5 December 2009, https://networkchallenge.darpa.mil/darpanetworkchallengewinner2009.pdf.

[6] US Air Force official Website, US Air Force Chief Scientist (AF/ST), "Technology Horizons - A Vision for Air Force Science & Technology During 2010-2030," http://www.af.mil/information/technologyhorizons.asp.

[7] Michael Macrone, "The dogs of war," Brush Up Your Shakespeare, Cader Company, 1990, eNotes.com. 2007, 17 August 2010, http://www.enotes.com/shakespeare-quotes/dogs-war.

[8] Lt Gen Larry D. James, "Schriever V Wargame: The Boundaries of Space and Cyberspace," *High Frontier* 5, no. 4 (August 2009): 12-13.

[9] William J. Lynn, remarks at the National Space Symposium, US Department of Defense, 14 April 2010, http://www.defense.gov/speeches/speech.aspx?speechid=1448.

[10] American Rhetoric, Ronald Reagan, inaugural address, 20 January 1981, http://www.americanrhetoric.com/speeches/ronaldreagandfirstinaugural.html.


**Maj Sam Baxter** (BS, Operations Research, US Air Force Academy; MBA, Finance, University of Colorado at Colorado Springs) is a reservist assigned to the special programs division at Air Force Space Command with duty in the Commander's Action Group. Maj Baxter's military experience includes space control, science and technology, strategic planning, wargames, as well as a satellite and intercontinental ballistic missile crew commander, flight commander, instructor, and evaluator. His civilian experience is in information technology (IT)—a web application programmer and IT sales manager.

**Capt Nicole O'Neal** (BS, Applied Mathematics, North Carolina State University; MS, Information Technology, University of Maryland, University College at Adelphi, MD) is an active duty service member assigned to the Special Programs Division at AFSPC. Capt O'Neal's military experience includes strategic and operational planning, test and evaluation, education with industry, and wargames.

*Industry Perspective*

# A Comprehensive Approach to Space and Cyberspace Operations

**Mr. Marc J. Berkowitz***
**Vice President**
**Lockheed Martin Corporation**
**Herndon, Virginia**

The global security environment of the 21st century is dynamic, complex, and dangerous. In part, this is because of the emergence of outer space and cyberspace as new dimensions of competition and potential armed conflict. In an era of hybrid, multi-modal warfare involving nation-states and transnational actors, the US must be prepared to address the challenges to international security in the space and cyber domains.

Schriever Wargame 2010 (SW 10) was part of a series of US Air Force Space Command-sponsored war games designed to address these new security challenges. The series has effectively evolved into a national-level game. It involved over 550 representatives from nearly all of the Department of Defense (DoD) components—the Office of the Secretary of Defense, Joint Staff, combatant commands, military departments, and defense agencies—as well as the intelligence community, other federal departments and agencies, industry, and allies.

The game focused on how to address space and cyber issues across the conflict spectrum. SW 10 involved a complicated, global scenario set in 2022 that evolved from a political crisis through major combat operations. It served as a laboratory to learn about the impact of space and cyber activities on deterrence, escalation control, and warfighting.

The objectives of SW 10 were to: (1) examine the contributions of space and cyberspace to future deterrent strategies; (2) investigate alternative space and cyber concepts, capabilities, and force postures to meet future requirements; and (3) explore integrated planning processes that employ a comprehensive, whole of nations approach to protect and execute operations in the space and cyber domains. This article focuses on the third objective. It addresses both context and considerations for integrated planning.

## Space and Cyberspace Interdependencies

The US economy, society, and way of life are reliant upon access to and use of space and cyberspace. America is reliant and, in some cases, dependent upon space and cyber capabilities for national decision-making, diplomacy, law enforcement, emergency services, homeland security, intelligence activities, and national defense. Consequently, unimpeded access to and freedom of operations in the space and cyber domains are vital national interests.

Space and cyberspace are global commons used for commerce, trade, and other purposes for the benefit of humanity. Similar to the high seas or international airspace, they are a shared resource typically outside the sovereignty or jurisdiction of any state. The commons are part of the underlying foundation of the international system of commerce, communications, and governance.

Space and cyberspace are separate and distinct operating domains with their own unique geophysical characteristics. However, they are interdependent domains. The nexus is information. Space and cyberspace are important conduits for the flow of information, finance, commerce, and trade around the world. The functioning of the global economy depends upon the information lines of communication through space and cyberspace.

Space and cyberspace are integral to the global information infrastructure. Space and cyber capabilities collect, generate, and relay information as well as control physical assets integrated into critical infrastructures. The lines of communications through space and cyberspace are extensions of the US homeland linked to our centers of gravity. Moreover, space and cyber assets enable all elements of national power—they are part of the glue that holds together our grand strategy.

Indeed, space and cyber capabilities provide the US with a comparative military advantage. Command, control, communications, intelligence, surveillance, and reconnaissance (C3ISR) assets operating in space and cyberspace support the execution of our defense strategy and joint warfighting doctrine. They are advanced technology force multipliers that increase the operational effectiveness of our armed forces.

The global access, speed, and precision delivered by space and cyber C3ISR capabilities enable information and decision superiority. The ability to create such effects is a foundation of American military operational style. Smaller formations of dispersed forces can maneuver, synchronize and mass power, and conduct non-linear operations in large part because of space and cyber capabilities.

## Space and Cyber Threats

The space and cyber domains are increasingly congested, competitive, and contested. The number of Internet Protocol

*America is reliant and, in some cases, dependent upon space and cyber capabilities for national decision-making, diplomacy, law enforcement, emergency services, homeland security, intelligence activities, and national defense.*

addresses in cyberspace as well as actors capable of launching payloads into space and/or operating satellite systems has increased significantly. Concurrently, the amount of spacecraft and debris on-orbit has created congestion around Earth that increases the risks of collisions.

While nations compete for prestige and power through space and cyber activities, commercial enterprises compete to generate wealth. There is growing competition over scarce space and cyber resources. This includes positions in geosynchronous orbit as well as allocations of radio-frequency spectrum.

Moreover, foreign nations and sub-national entities are pursuing counter-space and computer network attack capabilities to deceive, disrupt, deny, degrade, and destroy space and cyber systems. Such weapons are proliferating around the world. They are spreading through indigenous development, transfers of goods and services, and transnational collaboration.

Space and cyber assets are held at risk. They are targets of purposeful interference by both nation-state and non-state actors. Satellite communications as well as positioning, navigation, and timing signals have been jammed in peacetime and wartime. Computers and networks are constantly being probed, exploited, and infected with malicious data and software.

Hostile acts against space and cyber assets have the potential to influence our perceptions, corrupt, disrupt, or usurp our decision-making, and create intended and unintended effects on a cascading, global scale. Such effects may occur at an exponentially faster pace than ever experienced, endure for very long periods of time, and generate large-scale collateral damage on non-belligerents. In today's globally interconnected world, an attack on one nation's space or cyber networks can be an attack on all nations.

US dependence upon space and cyber capabilities creates an asymmetry of value compared to potential adversaries. In particular, dependence on vulnerable space and cyber assets is provocative. It may lead to miscalculations about our political will as well as provide incentives for adversaries to threaten or attack such capabilities in crisis or conflict.

Counter-space and computer network attack capabilities pose serious threats to our national interests in space and cyberspace. An adversary may attack US space or cyber assets as part of an anti-access/area denial strategy involving either traditional or hybrid modes of warfare. The objective of such aggression may be to: undermine our political will, societal cohesion, and morale; harm our economic vitality; counter our intelligence capabilities; and reduce the combat effectiveness of our military forces.

## Comprehensive Approach

The nature of the space and cyber domains demands that the US take a holistic approach to address space and cyber security challenges. This approach should utilize all elements—diplomatic, informational, military, and economic—of national power to create "whole of government" solutions to protect space and cyber systems, supporting infrastructure, and operations.

Military or hard power will, of course, be an essential tool for protecting and defending the space and cyber domains. But military power alone may be too blunt an instrument to deal with all of the threats to space and cyber security. The US must be able to blend the right mix of soft and hard power into smart power solutions tailored for the problems endangering the space and cyber commons.

The ability to leverage and synchronize all instruments of statecraft would improve our ability to shape the space and cyber environments, enhance deterrence, and, if deterrence fails or fails to apply, control escalation, and terminate conflict on favorable terms. A "whole of government" approach should generate greater versatility and agility to deal with the complexity and speed of crisis and conflict in the space and cyber domains. It will empower all of the pertinent government departments and agencies to ready resources, deter or withstand attack, and provide consequence management, reconstitution, and recovery.

The US government should work in concert with the private sector, its allies, coalition partners, and friends in the international community when it can, or independently when it must, to advance and protect our interests in the global commons of space and cyberspace. Consequently, the US "whole of government" approach should be extended to a "whole of nations" approach. This would bring the power of many nations and international partners to bear on the challenges of space and cyber security.

Such a comprehensive approach will require America to pursue cooperation and partnerships with allies and friends based on tangible, mutual benefit to achieve shared objectives. Purposeful interference or hostile acts against space and cyber systems demand a coordinated response from governments, the private sector, and the international community. The US should be positioned to ensure such a response by taking the lead in creating an international security framework for space and cyberspace.

Shaping the space and cyber environments and creating such a framework will require a velvet glove covering a steel fist. America and its allies should establish international norms of acceptable space fairing and cyberspace behaviors. Such norms should encourage respect, safety, and order for the global, networked commons of space and cyberspace. Norms should facilitate information sharing and increase transparency to reduce the risk of misperceptions arising from provocative or ambiguous behaviors in space and cyberspace. Nations, sub-national entities, and individuals who engage in space or cyber attacks should face condemnation and other unacceptable consequences.

Even after the onset of hostilities, diplomacy and strategic communications must be employed and synchronized with other lines of operations to sustain the political cohesion of a US-led alliance or coalition and win the battle for world opinion that is a pre-condition for overall success. In a space and cyber conflict where global effects can directly impact the lives of people around the world, public international diplomacy and strategic communications will be equally important to information operations and other military arrows in the nation's quiver.

## Dynamic, Multi-Layered, Defense-in-Depth

A dynamic, multi-layered, defense-in-depth strategy is a key aspect of the comprehensive approach. The US must be willing to take all appropriate collective, mutual, or individual self-defense measures to ensure that hostile actions by nation-states, sub-national entities, or individuals cannot prevent our access to or use of space or cyberspace. Self-defense measures should seek to deny an adversary the benefit of hostile acts and/or inflict punishment for aggression.

The strategy should be based on a theory of victory (and war termination) for conflict involving the space and cyber domains. It should link ends, ways, and means. It should address the relationship among passive and active defenses as well as offensive measures to protect the space and cyber assets the US and its allies own, operate, or employ.

The strategy should recognize that America must be able to deal with surprise attack and absorb an aggressor's first blow. It must take into account the consequences of loss or disruption of space and cyber capabilities and services. This includes understanding their secondary and tertiary implications. We must be able to operate through an attack and the resulting degraded environment. Subsequently seizing the initiative and reasserting at least working control of the operating mediums will be essential to defend successfully the freedom of space and cyberspace.

The strategy should establish clear defense priorities. It should direct actions for mission assurance, resilience, protection, security, reconstitution, and recovery. This should encompass all space and cyber system segments and functions end-to-end. We should seek to channel threats into costly and unproductive areas. While avoiding the imposition of unaffordable costs on us, the strategy should ensure that US space and cyber mission capabilities will be sufficiently ready, secure, resilient, and survivable to meet national and homeland security needs. Indeed, such resilience and survivability are directly tied to issues of self-deterrence and reassurance.

Establishing alliance or coalition arrangements to protect against threats to international security in space and cyberspace will be an important component of the strategy. This includes new public-private sector partnerships in recognition that much of the pertinent assets and infrastructure are privately owned and operated. The US should reorient extant relationships and expand its engagement with new international partners to establish a space and cyber security framework based upon mutual security and economic interests.

In the process, regional security architectures will have to be squared with the global nature of the space and cyber domains. Such arrangements will contribute to deterrence by sharing the defense burden and complicating a potential adversary's risk calculus. They will also contribute to escalation control and warfighting by increasing the resources and options that can be brought to bear in response to aggression.

## Centralized Planning, Decentralized Execution

Preparations for crisis management, conflict prevention, and warfighting should recognize that policies, processes, and structures established for the Cold War may not have caught up with this century's threats to space and cyber security. They may need to be altered or replaced. A comprehensive approach cannot be undertaken on an ad hoc, disjointed basis. It will require comprehensive strategic planning.

Implementing a comprehensive approach will require new policy and guidance, intra- and inter-governmental planning mechanisms and processes, and organizational constructs. The DoD's Joint Operation Planning and Execution System has provided a solid foundation for military planning. But the US will need a new paradigm and broader system to accomplish the holistic planning necessary for a comprehensive, whole of nations approach. The National Security Council system provides a potential mechanism for comprehensive planning at the strategic level. Similarly, the Combined Joint Task Force, Joint Interagency Task Force, and Combined Operations Center constructs could provide a basis for orchestrating integrated planning and execution at the operational levels.

Deliberate, whole of nations, pre-crisis planning for plausible space and cyber contingencies is an essential basis for concerted action. Such centralized planning is necessary to coordinate, de-conflict, synchronize and, as appropriate, integrate decentralized execution of lines of operations. It should produce a rich menu of carefully thought out courses of action, ranging from flexible deterrent to major attack options, similar to what the Joint Strategic Target Planning Staff generated for the Single Integrated Operations Plan. In addition, it should align conditions, postures, rules of engagement, and authorities to enable those alternative courses of action.

The options should encompass all phases of operations and involve all available instruments. Military options should range from conditioning and signaling to preemptive and preventative actions. Response options may range from demarches and sanctions to a response-in-kind to asymmetric (horizontal or vertical) cross-domain, escalation.

Planning should clarify our red lines (or zones), thresholds, and triggers. We should recognize that unintended or unanticipated effects may contribute to inadvertent escalation. Consequently, our red lines/zones must be clearly articulated through communications of declaratory policy, conditioned by operational behavior, and understood by both allies and adversaries alike.

While no plan can be expected to endure beyond contact with the enemy, the process of comprehensive, whole of nations planning will enrich strategy formulation and its operational execution. Given the dynamism and complexity of the space and cyber mediums, the intellectual engagement of senior political authorities and operational commanders prior to the emergence of a deep crisis or outbreak of hostilities will pay dividends. Moreover, it will put us in a far better position for effective crisis action planning by establishing a foundation to meet the exigencies of specific crises.

In particular, decision-making must be prepared to address the speed of battle in the space and cyber domains. Command and control processes must be adapted to operate at network speeds to enable US, allied, or coalition forces to seize and

maintain the initiative. This will require combined, cross-domain command and control. It will also necessitate common understanding among alliance or coalition political authorities and commanders about different national policies, red lines, and rules of engagement. Alliance or coalition forces must be clear about strategic intentions, war aims, political-military objectives, and the desired end state.

Self-defense measures will, of course, include the use of force to respond to an infringement on our rights. Authorization for employment of force may be pre-delegated to commanders, in accordance with approved war plans or rules of engagement. Such pre-delegations will have to be justified in advance given that employment authority may be delegated, but responsibility still rests with elected and confirmed political officials. Pre-delegation of employment authority may be necessary to enable forces to be postured properly for speed-of-light warfare.

Planning must recognize that there will be no separate "home" and "away" games in the event of conflict in space or cyberspace. Such distinctions are neither meaningful nor useful. The space and cyber domains, as noted, are extensions of all nations' homelands. Moreover, effects created in space or cyberspace that impact the homelands of our allies or coalition partners most assuredly are not "away" games for them. Consequently, effective planning must encompass homeland security and homeland defense.

Effective planning also will require improved space and cyber intelligence and situational awareness. Foundational intelligence is needed to help decision-makers and commanders understand potential adversaries' space and cyber capabilities and intentions. This includes knowledge about an adversary's socio-cultural, historical, and other factors that influence how they think and what they value. Such understanding is especially critical for planning and executing shaping activities and deterrence operations.

Strategic indications and warning are needed to enable anticipatory self-defense and damage limitation options. Intelligence, of course, is also essential to support operations planning. This includes monitoring the space and cyber domains, threat warning and attack reporting, characterization, attribution, targeting, and combat effects assessment. The closest coupling of operations and intelligence is essential to conduct warfare at the speed-of-light. Indeed, information fusion out to the tactical edge will enable operational agility.

## Conclusion

The emergence of outer space and cyberspace as new dimensions of competition and potential conflict has made the global security environment more complex, dynamic, and dangerous. SW 10 was valuable because it enhanced our understanding of space and cyber threats, interdependencies, and opportunities. In particular, it highlighted the need for the US to establish an integrated planning process that employs a comprehensive, whole of nations approach to protect and execute operations in the interdependent space and cyber domains.

The comprehensive approach will enable the US, its allies, and international partners to take concerted actions to shape the space and cyber environments, deter aggression, control escalation, and terminate conflict on favorable terms. Centralized planning and decentralized execution of this approach will facilitate implementation of a dynamic, multi-layered, defense-in-depth strategy to ensure an adversary cannot achieve its political aims through the threat or use of force in space or cyberspace. SW 10 should serve as a catalyst for the US national security community to adjust its policies, processes, and structures to ensure that it can conduct the complex lines of operations needed to protect and advance our vital national interests in space and cyberspace.

** The author served as the national security advisor for SW 10.*

**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 for situational awareness at Lockheed Martin Corporation. He is responsible for the development of cross-corporate business strategies and advanced concepts for integrated national security space, intelligence, and information mission solutions.

Prior to joining Lockheed 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. His other awards include the National Reconnaissance Office Medal for Distinguished Service, National Imagery and Mapping Agency Medal for Distinguished Service, Presidential Rank of Meritorious Executive, Defense Meritorious Civilian Service Award, OSD Exceptional Civilian Service Award, and the OSD Award for Excellence. In addition, he received the National Space Club's Robert H. Goddard Memorial Historical Essay Award.

Mr. Berkowitz writings have appeared in Peter L. Hays, et. al., eds., *Spacepower for a New Millennium: Space and US National Security*, (New York: McGraw-Hill, 2000), *Airpower Journal*, *Armed Forces Journal International*, *Comparative Strategy*, *Global Affairs*, *High Frontier*, *Jane's Intelligence Review*, *Jane's Soviet Intelligence Review*, *Journal of the British Interplanetary Society*, *Naval Forces*, *RUSI Journal*, *Signal*, *Space Markets*, *Strategic Review*, *US Naval Institute Proceedings*, *Space News*, *Defense News*, and *The Washington Post*.

# When the Future Dries Up

**Dr. Steven M. Huybrechts**
**Vice President**
**Applied Minds, Inc.**
**Reston, Virginia**

*You glorify the past*
*When the future dries up* ~U2

The fruits of Apollo and Corona have created something marvelous—something very special. It's a shame we now need to tear it down.

While the US space community pats itself on the back for what is, admittedly, a glorious past and present, its doom is a mere 15-20 years away. As a long-term part of this community this author has personally engaged in a lot of this back-patting, especially when visiting the extremely impressive National Reconnaissance Office ground sites or participating in such things as Global Navigation Satellite System negotiations abroad where the US delegation is justifiably proud to be the standard that all others look up to. A major change, though, is coming. It is a strange paradox that the US space community is at once at the top of its game, simultaneously staring into the abyss.

America's space infrastructure is increasingly marginalized—marginalized by new foreign weapons, the growth of the internet, the accelerated march of technology, and a defunct acquisition system. In the halls of the Pentagon, Langley, Fort Meade, and Bolling, decision-makers are increasingly turning to other mediums. In many cases, space is simply seen as too fragile, too expensive. In these pages, an author recently wrote the "Department of Defense (DoD) is presently hesitating at a key decision point regarding the evolution of space technology … a clear and purposeful decision, or lack thereof, will either lead to increasingly assured space-superiority … or a decrease in US relevancy in space."[1] While accurate, this article argues that the choice is starker than this.

## Why Have a Schriever Wargame?

The Schriever Wargame series is the single most important simulation event that the DoD has had in the past decade—a bold and somewhat parochial statement, no doubt. But the Schriever games have illuminated a critical topic we knew almost nothing about. Three or four Schrievers ago, we knew space war only as something entangled with nuclear war. Today we have a sense of and an intuition about its likely course, if only an inkling of how far-reaching globally the impact is likely to be.

What becomes apparent from the Schriever series is that our space architecture consists increasingly of small numbers of fragile, vulnerable systems that cost many times more than what they should (and significantly more than what it costs to deny/destroy them). New technology is increasingly difficult to apply and commercial systems are beginning to surpass military ones in capability. The incredible exponential power of the internet and Moore's law, which is changing life every day, has proven to be difficult to leverage inside our existing space industrial base. Instead of harnessing it, we are allowing it to marginalize our space capabilities.

## Precision and Bold Thinking

The biggest change to the space environment in the past two decades is measured in levels of precision. Precision used to be the sole province of the US military which could drop a bomb on any point on Earth within a few meters, identify individual emitters, track the location of the objects orbiting the Earth, and follow every space launch. But all technology proliferates. Today, terrorists use GPS to locate buildings in New York and China engages old weather satellites traveling at 20,000 mph—these are just two examples of the erosion of our precision advantage. The proliferation of precision has turned a sanctuary (short of global nuclear war) into a potential kinetic, directed energy, and cyber shooting gallery.

*Figure 1. It took more time to get approval of an Acquisition Strategy for GPS III after the 1999 PNT Selected Area Review recommended it than it took to land a man on the moon after President Kennedy's famous speech.*

Given how easy it is now becoming to target space systems, the Schriever Wargame series has taught this author that space deterrence is extremely fragile—national militaries are highly dependent on space assets, space attack can occur instantaneously with almost no warning, and significant destruction can be achieved in a short period of time, which then can limit response options. As a result, nations are motivated to attack first, creating a situation that can rapidly become unstable in a time of heightened tension and mistrust. America needs its space infrastructure to *get* engaged in theater, the temptation to stop us getting there can be great indeed.

Couple these ideas to the recogni-

*Achieving security in a medium such as space, where offense is highly favored and where attacks originate primarily in other mediums (which are often politically difficult to attack), will require the most innovative of thinking.*

tion that we have a dysfunctional acquisition system which is optimized to deploy 20 year old technology in an environment of constant overruns and there is a real problem. In the time it takes the Pentagon to approve a single requirements document, other nations have demonstrated repeatedly the ability to develop and test multiple generations of a new system. Our most impressive space capabilities have, in some cases, become unaffordable and we have lost them. Others are stuck in a time warp—slight modifications to designs essentially unchanged since the Reagan administration.

Achieving security in a medium such as space, where offense is highly favored and where attacks originate primarily in other mediums (which are often politically difficult to attack), will require the most innovative of thinking. This kind of thinking was prevalent at the dawn of the space age, but has today given way to the conservative certainty that, necessarily, accompanies any mature mission area upon which daily operations and national—actually world—economic health depend. We must recognize that, while traditional space force enhancement missions (satellite communication; positioning, navigation, and timing [PNT]; intelligence, surveillance, and reconnaissance; etc.) are mature, the space control mission area in this new multi-polar space environment is in its infancy—to it we must apply highly creative, bold thinking. This thinking will inevitably require major changes in the traditional mission areas as well.

Below is, I hope, some bold thinking.

## The Joint Space Operations Center – Think Wikipedia

When it comes to data, *assuredness* and *currency* are both of value. In a 1960s nuclear war, assuredness was more important than currency, in a 2020 space war, their values are reversed.

When you go online to look something up, do you go to EncyclopediaBritanica.com (the major validated encyclopedia on the Web) or Wikipedia (written by anyone and everyone)? The answer is that most of you choose Wikipedia. In 2010, Wikipedia had over 1,000,000 entries, 50,000 searches per second, and was growing by over 30,000,000 words per month—faster than a human could read them if he/she read 24 hours a day. EncyclopediaBritanica.com has a comparatively paltry 100,000 entries and generally less than 1,000 hits per second, not all of which are searches.[2] Wikipedia offers currency, EncyclopediaBritanica.com offers assuredness.

A space war begins and occurs "at the speed of light." Its major events happen on the other side of the world. It can be over in hours. The Joint Space Operations Center (JSpOC) must become a Wikipedia, not the EncyclopediaBritannica.com that it is today.

Actually, today's JSpOC systems (not its people who have one of the toughest jobs in the Air Force) are neurotically hyper-conservative even by EncyclopediaBritanica.com standards. These systems reject even data from Air Force space ground stations, let alone data from other government entities. Given that much of the best data out there will be in places like foreign-owned space industry, there is a long, long way to go. The JSpOC needs to be radically re-engineered to take in *all* data from *all* places at "the speed of light," albeit tagged with a confidence level.

Currency is achieved by casting a wide instantaneous net for data—a useable level of assuredness is achieved through aggregation and comparison of many data sources rather than rigid stovepipe integrated tactical warning and attack assessment certifications. Studies suggest that Wikipedia has four errors for every three in EncyclopediaBritanica.com. But the Wikipedia model allows one to cross-check the answer on Google—instantaneous, personal aggregation of raw data is the new way


*Figure 2. Space Telepresence and Collaboration System under development in Glendale, California.*

of the world. Sticking with a Cold War mindset of assuredness is to ensure that data at the JSpOC will be irrelevantly late, substandard, and is to ignore the information revolution occurring all around us.

## More JSpOC – Telepresence

If I told you that we would have full motion video of the volume of all the world's oceans, 24/7, tracking every moving fish, you would be pretty skeptical. The volume of space to geosynchronous Earth orbit (GEO) is 220,000 times the volume of the world's oceans. We don't actually *know* where anything is in space; all we really know is that when we looked at it last week, it was in a certain orbit so we assume it is still there—we must recognize now the impossibility of "tracking all the dots, all the time." As a result, understanding what is going on in space is less about watching the dots and more about understanding the medium of space, how it behaves, how objects in it behave, and what likely actors are up to.

A minimally sufficient set of experts, then, to understand a complex space event such as a space war will never ever all be sitting at Vandenberg—by its nature, the "space situational awareness (SSA) system" is not a set of sensors and computers but is instead a combination of sensors, knowledge tools and, most importantly, the network of the national set of space experts who must be able to meaningfully collaborate on a timescale measured in minutes. These experts are likely to simultaneously be at Vandenberg, Peterson, Schriever, Chantilly, Langley, Goddard, Wright Patterson, Los Angeles, and Albuquerque—not to mention places like Canberra, Luxembourg (SES), Dulles (Iridium), Paris, and so forth. Rather than a large command center, we should think of the JSpOC as the nexus of a world web of connections that can be exercised at "the speed of light" during confrontation. Required, then, is a well thought through telepresence system pre-configured to access all these sites and a set of long distance collaboration tools allowing multiple users to access the richly visual and computationally intensive data set that underpins SSA.

An interesting corollary to this point is a direct finding of the *Schriever Wargame 2010 (SW 10) (the 6th Schriever game)* Industry Cell. The *Schriever V Wargame* postulated the need for a "CSpOC" which combines allies and commercial entities into the JSpOC. While potentially a reality for allies, how can we possibly integrate what may be 100+ companies into the JSpOC—surely each cannot have their own representative and most companies will be loath to pass sensitive operational data through another company's representative. Instead, the JSpOC could establish a high definition instantly-accessible telepresence link between Vandenberg and each company allowing the JSpOC to immediately collaborate with relevant corporate officers in time of crisis.

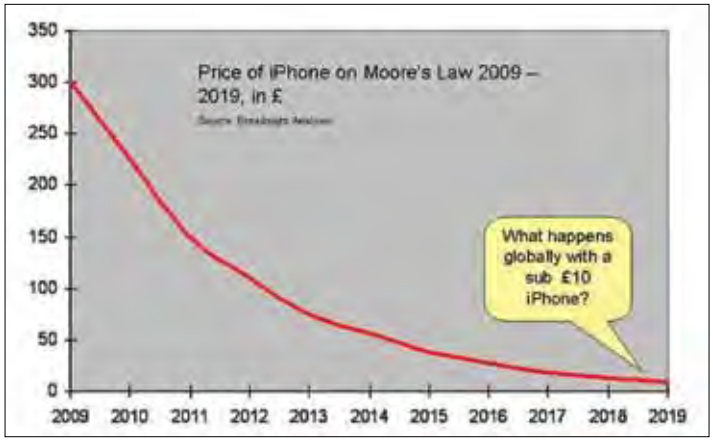



*Figure 3. Satellites being built today will be operating in a world of content, communication, and innovation that we do not even understand.*

## Satellites – Think iPhone

Today's satellites are technical marvels in the same way that dinosaurs were biological marvels—the asteroid has already hit, though, and it is called *the internet*.

The problem with satellites in the current phase of the internet age is that they take 5-10 years to build and are then untouchable on-orbit for another 10-15. In the 20 years, then, between a system's technology freeze date and its end of service, computing power has increased almost 15,000 times and vast networks of connected individuals on Earth have invented entirely new ways of doing almost everything. Ask yourself who in five years (or even now) will buy a paper map? Listen to music from a CD? Open a Yellow Pages book? Go to a video rental store? Read a paper newspaper? Watch a TV weather report? A mere five years ago these were all critical components of modern life. By building single purpose (missile warning, PNT, etc.) giant stovepipe systems, our space infrastructure not only presents fragile temping targets to adversaries, but worse runs counter to the phenomenon that is the internet rather than harnessing it.

A more robust model would be holistic, distributed, and open—it would leverage the power of the network of knowledge/people that is the Internet, adapt rapidly, and degrade gracefully. Instead of building single large stovepipe systems to cover all requirements of a specific mission area (i.e., missile warning), such a model would start by asking what types of capabilities need to be on orbit to satisfy the set of military and intelligence mission areas. This set may be, for example, a number of infrared sensors, general purpose radio frequency (RF) emitters in bands a/b/c, general purpose RF receivers in bands d/e/f, a number of telescopes, a number of flash detectors, and so forth As much as possible, these would be launched on individual smaller spacecraft and all would be connected by second generation high bandwidth laser communications. All computing power would be pushed to the ground where it can

*Today's satellites are technical marvels in the same way that dinosaurs were biological marvels—the asteroid has already hit, though, and it is called the internet.*

*The more our space systems can be integrated with those of our allies and the more they can be integrated into the fabric of global commerce, the harder they will be politically to attack in all but the most extreme of conflicts.*

be rapidly upgraded—all platforms and sensors would be individually addressable, essentially a giant iPhone in space.

A mission in this model is essentially an application (app) that addresses a set of the available platforms/capabilities. "Anchor" apps are the traditional mission areas (PNT, communications, missile warning, etc.) but just like the iPhone which began with four anchor apps (telephone, text, email, and calendar) and now has over 250,000 available, most never imagined by the iPhone creators, the space constellation would be opened up to a network of space application designers across the national security community who could pick and choose what space capabilities to include in their applications and how to interface them to data sources and capabilities in other mediums. What an explosion of never-dreamed-of capability this could produce! The space medium, with robotic platforms in predictable locations, is uniquely suited to this model of distributed development. Anchor apps could undergo rigid requirements processes while simultaneously the network could be set loose, innovating a host of unanticipated capabilities.

Finally, the iPhone offers an example of how this model can actually increase robustness. While the device generally uses GPS to develop position, it also searches out signals of opportunity from cell phone towers and local Wi-Fi networks for a robust solution which degrades gracefully. Exiting the Metro at Crystal City in Arlington, a 16 year old can use her iPhone to navigate the tunnels where no GPS receiver will work—not as accurately as but better than nothing. Opening a distributed, open, holistic space infrastructure to the vast network of developers will yield similarly-innovative solutions to many space missions rendering them more robust than current purpose-built single point of failure systems.

## International – A Case for Foreign Entanglements

Would you rather declare war against one nation or against 10? Multi-national satellite systems are safer from attack than those owned by a single nation.

Would you burn down the local Costco if your wife was the primary breadwinner in the family and she worked there? Dual-use satellite systems that benefit all nations are safer from attack than those that benefit only DoD. GPS, upon which global commerce and so much more depend, is much harder to attack than a classified spy satellite.

The more our space systems can be integrated with those of our allies and the more they can be integrated into the fabric of global commerce, the harder they will be politically to attack in all but the most extreme of conflicts. This integration should be a stated goal and benefits all parties, not to mention the peoples of the world.

## Space and Time – Think Navy

During combat, the US Air Force usually will define a certain portion of airspace above the conflict zone and attempt to control it—controlling it generally means trying to track every object flying through it.

The Navy's task is quite different. Even in peacetime, the Navy is attempting to maintain some influence over the vastness of the world's oceans. Since there is no Airborne Warning and Control System/Joint Surveillance Target Attack Radar System equivalent for the entire ocean, this task generally entails a deep understanding of the medium, where its choke points are (i.e., Straits of Malacca), what types of systems are operating in it (i.e., Exocet missile), and the directions from which attacks can come (i.e., submarine firing depth). In this way, space is more like the sea than the air. Relative to the maritime domain, space control is complicated by its greater vastness but is simplified by the laws of Kepler.

Transitioning from a sanctuary to a contested environment mindset will require a much deeper understanding of the medium of space. How do antisatellite weapons approach their targets in low Earth orbit/medium Earth orbit/highly elliptical orbit/GEO given the laws of Kepler? What is the equivalent of an aircraft carrier's keep-out zone given the laws of Kepler? Are there choke points like geosynchronous transfer orbit or GEO? Which orbits are safer? Which are not? All space operators, designers, decision-makers, acquisition professionals, and policy makers need to be able to answer these types of questions as a matter of basic training. Yet many of the answers to these questions are not well understood today by anybody.

## Satellite Communications Industry – Tell Them What You Want and You Will Get It

Western companies are now the largest operators of spacecraft on orbit. SES, Intelsat, and Eutelsat alone have over 100 operating GEO spacecraft and 20 more on order.[3] Commercial operators have become critical to national security operations as varied as flying remotely piloted vehicles and Pacific naval maneuvers. Industry benefits from economies of scale and a dramatically more efficient acquisition system—satellite operators can acquire systems at lower cost and on much more rapid timelines.

DoD's approach to the space industry assumes a benign environment and a glut of supply, which is basically what we have seen the past 10 years for a number of reasons, none of which are likely to repeat themselves. Most capacity is purchased on the spot market at high cost, although there have been moves recently to purchase more capacity in bulk to obtain larger discounts.

The two problems with the current model are:

1. It will break down in a contested environment. As simultaneously capacity is reduced through attack or jamming and there is a clamor for bandwidth from militaries, media, and commercial interests due to crisis, DoD will likely find that it cannot secure the service required.

2. It passes up a golden opportunity to greatly reduce cost by leveraging industry's more efficient acquisition model.

A better model would be to establish serious long-term contracts directly with satellite operators. These contracts could include clauses that would give DoD first rights to bandwidth during crisis (at a premium) and would lower peacetime costs through bulk buy. DoD should give industry specific requirements, such as anti-jam, in these contracts and guarantee a fixed level of purchase for a fixed number of years. This action would free industry to design and launch systems tailored to DoD's needs at greatly reduced costs relative to acquiring additional government systems.

### International Traffic in Arms Regulation – Think the Traditional Air Force that Flies Planes

When our pilots encounter F-16s flown by a hostile nation, they have the advantage of understanding the characteristics of the system that they are facing—because we built it. This is not true facing MiGs or Mirages. Why on Earth would we not want the same advantage in space? In many ways, exporting satellites is better than exporting planes/tanks/ships/etc.—they tend to be on orbit when delivered and so cannot easily be reverse-engineered.

Export restriction on all but the most sensitive spacecraft systems should immediately be lifted and encouraged as much as possible. There is an added benefit in that nations that purchase our systems will be more likely to share them back with us in the case that ours are destroyed.

### Schriever Wargame 2012 – Think Tactical

Five Schriever games in a row have provided great insight into the operational level of a space conflict. The placement of the Schriever V Wargame and SW 10 a year apart with common leadership between the two was highly successful—SW 10 was in many ways a much richer, more nuanced version of the Schriever V Wargame. What is missing is the tactical aspect. The Schriever Wargame 2012 should be held in conjunction with a set of *space exercises* to explore the tactical nature of the game.

### Space Acquisition – Think Depth, Local Empowerment, and Stability

The once mighty space acquisition system producing the greatest wonders of the classified security community, and directly responsible for America's dominant information advantage, is now seen in many parts of the Pentagon as the worst performing of the troubled military procurement systems. "Oh, the most expensive page in DoD," a recent offhand remark by one of DoD's highest ranking officials when offered a one page summary of space programs by the Air Force in the presence of this author, illustrates the climate.

Our collective inability to halt this decline has led to highly fragile systems and is pricing us out of the space business. For example, DoD once paid between $100 - $200 million a year to field a weather satellite program in two orbits (Defense Meteorological Satellite Program [DMSP]). Under National Polar-orbiting Operational Environmental Satellite System (NPOESS), it would have paid $800 million to $1 billion for that same privilege. With DMSP, we routinely had multiple vehicles ready for launch, with NPOESS, we were one launch failure from a multi-year gap in capability.

Much as we would like to wish it away, building satellites to survive the rigors of space without any human intervention is more art than science. Highly complex, with little design margin, unforgiving, temperamental, with thousands of oblique rules learned the hard way—from past failures. Building a satellite involves a thousand decisions any one of which can manifest itself either as a failure of the entire system on-orbit or as rework during the integration and test phase when a satellite's "burn rate" is at its highest.

The following difficult, perhaps impossible, changes are required to regain our ability to pioneer an Apollo, or a Corona:

1. Government Program Office personnel and leadership need *depth*, not *breadth*. Ideally, a SPO director and his/her direct reports will spend his/her entire career not just in space acquisition but in the acquisition of space systems of a specific mission type (i.e., infrared missile warning or protected satellite communications).

2. Contractor program office personnel and leadership need *depth*, not *breadth*. We must acknowledge to ourselves that there really isn't competition in the space industry base. With two and one-half large primes, none "allowed to fail" and the government picking up the tab for the inevitable overruns, the only competition is that between creative proposal writers and innovative costing. Competition at the second and third tier suppliers is often nonexistent. There are few if any examples of an incumbent contractor/government team foundering on a follow-on

*Ideally, a SPO director and his/her direct reports will spend his/her entire career not just in space acquisition but in the acquisition of space systems of a specific mission type (i.e., infrared missile warning or protected satellite communications).*

*We need to get back to building strong competent teams (this is the most important thing to do) and giving them the freedom to innovate within flexible requirements to solve problems.*

system. Just the opposite is true for the outsider—they almost always run into significant difficulties (future imagery architecture, GPS IIF, space-based infrared system, etc.). The skills required for any system are so specialized that there is likely only one contractor team capable of building any particular system. *Sole source within a mission area needs to be the norm, not the exception.*

3. Budget instability from year to year creates huge cost increases in space programs and damages the industrial base. Why? Because contractor manning must be charged somewhere. Most space programs are executed by prime contractors with 2nd and 3rd tier sub-contractors. The prime contractor must provide for their manning and will maintain it in years of lower budget magnifying the effect to the subs. A 15 percent cut in program level may translate into a 70 percent cut to sub-contractors. The US is not realistically going to divest from any of its major space capability areas and all must be maintained, which implies a regular launch rate of replenishment satellites. If the distributed model discussed above cannot be implemented, why not establish an enduring budget line for each capability area which the program manager can then count on year after year to maintain his/her capability rather than arguing over each satellite one at a time every year first at Peterson AFB, then in the Pentagon and then yet again on Capitol Hill? "One at a time" is the most expensive way to purchase anything.

4. Additional layers of program oversight only exacerbate the problem. Washington inside the beltway is simply too far away from the reality of space acquisition to effectively deal with its details. Recent space acquisition woes have led to more and more layers of oversight which simply distract the program manager, further increasing the problem. We need to get back to building strong competent teams (this is the most important thing to do) and giving them the freedom to innovate within flexible requirements to solve problems. If Washington wants to help fix space programs, it should focus on oversight of "the acquisition system" (i.e., the people, resources, industrial base, and budget stability) rather than on oversight of programmatic details, such as acquisition strategies, fee structures, and milestones which are much better left to the field.

*Notes:*

[1] Lt Col Ryan R. Pendleton, "You Say You Want a Revolution: Will ORS Spark Innovation in DoD Overhead ISR?," *High Frontier* 6, no. 3 (May 2010).

[2] Stacy Schiff, "Can Wikipedia conquer expertise?" *The New Yorker*, 13 August 2010.

[3] *Wikipedia*, "List of the largest fixed satellite operators," http://en.wikipedia.org/wiki/List_of_the_largest_fixed_satellite_operators.

**Dr. Steven Huybrechts** (BS, Physics and Computer Science, McGill University; MS, Aeronautical and Astronautical Engineering, Stanford University; MS, National Security Studies, National War College; PhD, Aeronautical and Astronautical Engineering and Mechanical Engineering, Stanford University) is a senior vice president overseeing programs for Department of Defense (DoD) and the intelligence community at Applied Minds, Inc, a company working at the crossroads of art, information, science, technology, design, and society. Applied Minds is a collection of some of the US' top designers, thinkers, engineers, and computer scientists and employs a unique group of interdisciplinary artists, scientists, and engineers with skills in architecture, electronics, mechanical engineering, electrical engineering, software development, system engineering, and storytelling.

Previously, Dr. Huybrechts was a member of the Senior Executive Service of the Department of Defense serving as the principal director for command, control, and communications, space, and spectrum in the Office of the Secretary of Defense where he had oversight responsibility for most of the nation's military space, networks, command and control, communications, navigation warfare, meteorology, oceanography, and spectrum allocation activities. He also spent 11 years with the Air Force Research Laboratory where he was responsible for selecting and managing many of the nation's highest priority space experiments as well as directing the Air Force's research portfolio of spacecraft structure, control, power, thermal, and optics technologies.

Dr. Huybrechts was named a Fellow of the American Institute for Aeronautics and Astronautics at the age of 33, the youngest Fellow ever inducted in the institute's history. He received the DoD Distinguished Civilian Service Award, the Presidential Rank Award for Distinguished Service, the Fleming Award, the National Defense University President's Award, the RNASA Stellar Award for Space Achievement, Air Force Materiel Command's Science and Technology Achievement Award, a Joint Meritorious Service Medal and is a Space Fellow of the Air Force Research Laboratory. He is the author of 36 technical articles, five magazine articles, and 10 patents.

*Book Review*

# National Security Space Strategy Considerations

**National Security Space Strategy Considerations.** By Robert E. "Rick" Larned, Cathy W. Swan, and Peter A. Swan. Raleigh, North Carolina: Lulu.com, 2010. Graphics. Appendices. Bibliography. Pp. viii, 100. $9.95 Paperback ISBN: 978-0-557-31774-5

Looking backward more than half a century, US space strategy has been based on two fundamental, guiding principles set forth by President Dwight Eisenhower. "Freedom of space" and "space for peaceful purposes" remain the foundational goals for US space strategy generally and US national security space (NSS) strategy specifically, even though civil and military leaders perhaps have neglected to enunciate adequately the details of either one. Now, three retired Air Force officers—Brig Gen Rick Larned, Col Cathy Swan, and Lt Col Peter Swan—insist the country needs a forward-looking, clear, comprehensive, and stronger NSS strategy, one that considers in equal measure all three parts of a space system's lifetime—acquisition, operation, and sustainment. The nation needs a new strategy, they argue in *National Security Space Strategy Considerations*, because today's leaders face far different, less predictable challenges compared to what their predecessors confronted in the mid-twentieth century, and because NSS strategy has not kept pace with increasing demand for, dependence on, and threats to NSS operations.

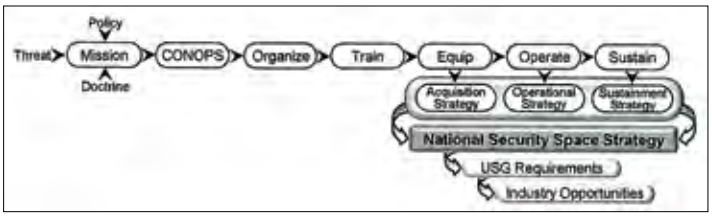
Larned and the Swans structure their monograph around a conceptual approach that, depicted linearly, begins with mission, which is driven or informed by policy and doctrine and is related directly to a perceived threat. They contend that policy should be more explicit, and doctrine needs a fresh look. The threat, which "is getting more real every day," demands an answer to the question of whether to move defensive or offensive weapons into space. How a mission will be accomplished is embodied in a concept of operations (CONOPS), which the authors describe as the backbone of any strategy.

Once a CONOPS is established, supporting units must organize and train for the mission. The authors outline certain organizing principles that have withstood the test of time and measures of effectiveness that "provide constructive, definitive indicators of performance" for acquisition, operations, and sustainment organizations, respectively. "Because organizational changes are relatively easy to make," they observe, "they are an attractive option for giving the appearance of 'progress' or 'improvement'" (p. 37). Although they believe now is the time to consider whether the United States is organized properly for a real space war, the authors caution that "no organization is so imperfect that good people can't make it work." Training makes the difference between success and failure, and the treatise defines several areas where space training needs more attention.


The conceptual model in *National Security Space Strategy Considerations* leads one from organization and training into three supporting strategies or elements of a new NSS strategy, each with its own catch phrase. First, "lead better, follow well, buy smart" with respect to acquisition. To explain the meaning of this phrase, the authors cite six successful leaders—Col Lee Battle, defense secretary David Packard, deputy NRO director Dr. Robert Naka, undersecretary of defense Dr. Paul Kaminiski, and Maj Gen Tom Taverney and Col Jim Rendleman—whose recommendations for improving acquisition are historically consistent. Second, "protect and serve" in the operational realm. Determining the best mix of space, air, and surface capabilities to support a particular mission should start with focusing on the mission; focusing on mission durability instead of constellation durability—knowing when not to turn to space forces—can save money and improve operational effectiveness. Third, "strengthen for the future" regarding sustainment. Together, these elements can infuse NSS strategy with vitality and robustness. This involves recognizing certain 'inescapable aspects" of today's space forces in order to maximize the residual value of existing constellations while preparing for an efficient transition to next-generation systems. An effective NSS strategy depends on carefully identifying US government needs and deriving industry opportunities from those needs; balancing needs and opportunities can create an "effective partnership for progress." Ultimately, a successful strategy depends on its implementation being an "extended, continuing process" focused on staying relevant as operational demands change.

In reaching the "bottom line" of their short study, Larned and the Swans summarize "nine red herrings" or falsehoods they think have inhibited development of an improved NSS strategy. Undoubtedly, these purported untruths include points that might raise the hackles of some civilian and military NSS experts: (1) we have no national space strategy; (2) ORS will make space more operationally responsive; (3) we need weapons in space to protect our satellites; (4) space support is not there for us when needed; (5) the space acquisition process is broken; (6) one-of-a-kind platforms—NSS core or "Big Space" satellites—are unworkable; (7) launch is not sufficiently responsive for war fighting; (8) there must be a separate military space service; and (9) the aerospace industry cannot get the people it needs to do the job. Certainly, ample room for disagreement exists.

While the content of *National Security Space Strategy Considerations* should generate valuable discussion, even sterling debate, this slender volume is not without blemish. Some readers might question how accurately the authors depict the connections and relationships among their collection of strategy considerations. A linear diagram, like the one used in the book, could be best or might have limitations.




At one point, for example, the authors' reasoning seems too circular for representation by a linear model. They write, "Other aspects of Space Strategy, e.g., concept of operations, organizational considerations, training requirements, etc., flow from the Strategy" (p. 28). Perhaps a depiction that includes feedback loops or matrices might be a more suitable graphic. Any criticism or confusion aside, Larned and the Swans have given us abundant material on which to reflect.

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


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 cyberspace 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, Suite 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@sgis.com or digital copy, http://www.af.mil/subscribe.

**AFSPC/PAI**
**150 Vandenberg St.**
**Ste 1105**
**Peterson AFB, CO 80914**
**Telephone: (719) 554-3731**
**Fax: (719) 554-6013**

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

**Air & Space Power Journal:**
**www.airpower.maxwell.af.mil/airchronicles/apje.html**