AIR FORCE SPACE COMMAND

Volume 6, Number 4

HIGH FRONTIER

THE JOURNAL FOR SPACE AND CYBERSPACE PROFESSIONALS

INSIDE:

SPACE AND CYBERSPACE: COMPLEMENTARY?

Report Documentation Page

Form Approved
OMB No. 0704-0188

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

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
High Frontier. The Journal for Space & Missile Professionals. Volume 6, Number 4, August 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) **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)**	**68**	

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 April Wimmer
1st Lt Jonathan Simmons
Mr. Gregory V. Williams

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: Advanced extremely high frequency satellite and cyber references.

HIGH FRONTIER

The Journal for Space and Cyberspace Professionals

August 2010 Volume 6, Number 4

Contents

Next Issue: ***Schriever Wargame 2010***

Introduction

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

Cyberspace and its associated technologies offer unprecedented opportunities to the US and are vital to our nation's security and, by extension, to all aspects of military operations.

~ Robert M. Gates, Secretary of Defense, 23 June 2009

This issue we ask the questions for our space and cyberspace professionals: are space and cyberspace complementary, and if so, how? The answers to these questions have strategic implications on how the Air Force will meet the critical needs of the joint warfighter. Each service is tasked by the Secretary of Defense, Robert M. Gates, to provide component support to the newly activated US Cyber Command.[1] Cyberspace is critical to all military operations; therefore, it is not possible to designate one service as the sole provider of cyberspace capabilities. Rather, it is incumbent upon each service to provide distinct cyberspace capabilities using the strengths of their core functions. Cyberspace transcends the domains of air, land, sea, and space and joint force commanders will need the complementary strengths of each service to create the effects they need.

As Airmen, we see cross-domain synergies between air, space, and cyberspace, and it is our job to determine how best to take advantage of these synergies to provide enhanced capabilities to combatant commanders. In Air Force Space Command we believe there is great potential at the intersection of space and cyberspace, and we are looking carefully to assess how we might take advantage of that potential.

What enhanced capabilities lay at the intersection of space and cyberspace? The answer is not clear yet, but I would suggest we can get a glimpse of the answer by looking at the enhanced capabilities that resulted when the intersection of air and space revolutionized our operations (e.g., strike aircraft + GPS = precision strike) and shaped the American way of warfare. I suspect a similar revolution will result as we add cyberspace to this mixture.

This edition covers the vast array of issues associated with the complementary characteristics of space and cyberspace. The authors present strategic level discussions on mission assurance, education, technology, threats, and possible courses of action as we combine and develop space and cyber capabilities. The articles point toward a future where problem solving and technology development in one domain yields complementary solutions in the other domain. We are at the beginning of an iterative process in space and cyberspace, where the complementary nature of the domains will likely evolve as technologies and tactics change. The articles presented do a formidable job of beginning a discussion on the complementary nature of space and cyberspace that will likely last for a very long time.

Our next issue will explore the issues and challenges examined during the Schriever Wargame 2010. Our Title 10 Wargame series advances our strategic thinking and analysis of how to operate in contested space and cyberspace domains. I look forward to the perspectives and ideas that will be shared by the distinguished group of warriors who participated in the games and authors who benefit from war gaming and exercises.

Notes:

[1] Department of Defense, "Establishment of a Subordinate Unified US Cyber Command Under US Strategic Command for Military Cyberspace Operations," memorandum, 23 June 2009.

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.

As Airmen, we see cross-domain synergies between air, space, and cyberspace, and it is our job to determine how best to take advantage of these synergies to provide enhanced capabilities to combatant commanders.

Senior Leader Perspective

Cyberspace Mission Assurance: A New Paradigm for Operations in Cyberspace

Maj Gen Richard Webber, USAF
Commander
24th Air Force and Air Force Network Operations
Lackland AFB, Texas

Col Mark E. Ware, USAF
Director of Operations, 24th Air Force
Lackland AFB, Texas

No one is better suited or better prepared to protect our nation in the 21st century than our US Air Force. We are warriors who guard air, space, and cyberspace and who have always worked to ensure victory before the battle begins. Since our inception in 1947, we as Airmen have honed our skills and proven our worth as we have become very proficient in the air, space, and now cyberspace domains. With the standup of the Air Force's cyber capability under 24th Air Force (24 AF) we now have the added challenge to conduct sustained global operations in, through, and from cyberspace, fully integrated with air and space operations—this is no small feat.

The task is enormous and the threats are many. Cyberspace has emerged as a domain that is essential to the conduct of all Air Force operations. It is a warfighting domain that is just as critical to ensuring our national security as the other domains of land, sea, air, and space. Cyberspace cuts across all domains. However, unlike the other domains, cyberspace is man-made and therefore must be operated and maintained. The complexity of conducting full spectrum operations in cyberspace, while also provisioning and protecting the domain, requires innovative thinking as the Air Force matures command and control processes for cyberspace forces and missions. With the enormity of the domain and the many complexities of cyberspace, we cannot completely protect the entire Air Force network. Like the air and space domains, we must protect the network to the best of our ability at the times and places most in need, and the protection must be focused on the concept of assuring operational missions—cyberspace "mission assurance" based on the need to protect critical missions and assets.

Mission Assurance

We have joint guidance to assist in understanding mission assurance in cyberspace. According to the Department of Defense (DoD) definition, mission assurance is a process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. It is a summation of the activities and measures taken to ensure that required capabilities and all supporting infrastructures are available to the DoD to carry out the national military strategy. We must link numerous risk management program activities and security related functions—such as force protection, antiterrorism, critical infrastructure protection, information assurance, continuity of operations, chemical, biological, radiological, nuclear, and high-explosive defense, readiness, and installation preparedness—to create the synergistic effect required for the DoD to mobilize, deploy, support, and sustain military operations throughout the continuum of operations. However, what does it mean to have mission assurance in the context of cyberspace operations?

First of all, mission assurance is nothing new, however, operating in a newly defined warfighting domain that previously had been relegated to that of "enabler" requires a new way of thinking. Cyberspace operations can and do create effects across the battlespace—both directly and indirectly. Previously, when thinking about cyberspace, most of us thought about it in terms of terrestrial, Internet protocol-based networks. It was easy to take the stance that it is all about whether or not the unclassified and classified networks are available. Frankly, based on the amount of reliance we place on the two major networks to accomplish our wartime mission, let alone our day-to-day mission, it makes good sense that focus should be on network availability. When considering that these two networks are only a portion of the larger cyberspace warfighting domain, simple network availability takes on a whole new look.

Keeping with this relatively simplistic view of cyberspace and focusing just on the military-run unclassified and classified networks, those who depend on these networks demand reliability, as well as availability of those networks and integrity of the data being transferred through them. Again, this is nothing new, and the communications professionals throughout the DoD have strived for exactly this kind of support … reliability, availability, and integrity of the data. The new paradigm comes from the acceptance that there are outside threats to the reliability, availability and integrity of the data that we use to command and control our forces … whether it is during times

Like the air and space domains, we must protect the network to the best of our ability at the times and places most in need, and the protection must be focused on the concept of assuring operational missions—cyberspace "mission assurance" based on the need to protect critical missions and assets.

To achieve mission assurance for the Air Force network, commanders must create an organizational culture wherein we act rather than react to cyberspace threats and incidents.

of peace or times of war. You simply have to look back to the 2008 war in the country of Georgia. Simple denial of service techniques effectively degraded the Georgian military's ability to command and control their forces and conduct operational missions to counter Russian troops and aircraft invading the country. Whatever reliance the Georgian military had on their version of unclassified and classified networks was denied … no reliability, no availability, and unknown integrity of the data. For the US, such a denial of service is unacceptable and therefore the focus of cyberspace must shift from simply assuring the network to assuring the mission. Make no mistake; mission and networks are intrinsically linked. Gone are the days of just focusing on whether or not the network is "up." Now we must focus on whether or not the mission can be accomplished on mission assurance.

Before anything can be protected, we need to understand the critical components, links, and dependencies in the Air Force network germane to the operation. This process of determining what to defend is an ongoing process that can be broken down into two major sets of activities: foundational and mission-specific. We must understand the dependencies and effects of these two sets of activities so that we are prepared when and if cyberspace capabilities are lost, degraded or compromised. To achieve mission assurance for the Air Force network, commanders must create an organizational culture wherein we act rather than react to cyberspace threats and incidents.

Foundational Mission Assurance

Foundational activities are long term in nature and include programmatic elements. These activities are necessary to develop capabilities and provide the underpinnings for network operations, maintenance, and defense. The development of these activities integrates operators into recognizing the difficulties and complex dependencies inherent in cyber operations and helps them to address programmatic activities and initiatives for engaging systemic risk issues to improve the resiliency of cyberspace. These foundational activities must also fully support the mission-specific activities, creating mission continuity, allowing for better defensive operations.

While there are specific defense mechanisms in place for very specific systems operating in the cyberspace domain, the primary foundational defense mechanism is best compared to building a castle wall, which is intended to protect the entire castle (the network) but more specifically the "crown jewels," those items requiring the strongest defense due to their value. Improvements to the defensive systems are like building the castle walls higher and thicker. Unfortunately, due to the threat, this technique can be compared to building a Maginot Line, a defensive barrier that inspires a false sense of security.

Essentially, the Air Force network was similar to the castle needing defense, it had a series of added defense mechanisms combined with that high, thick castle wall … sentries posted far from the castle with orders to report back when invaders have passed, smaller outposts to ward off minor threats and report back, moats to slow the advance of the invaders nearing the castle, drawbridges to prevent direct access through the front gate, and finally defenders posted on those high, thick castle walls fighting to the end to prevent entry. Noble? Yes. Terribly effective? No. The myriad of tunnels, insiders, spies, and so forth, that could gain access to the castle render this concept marginal at best, and outdated/unrealistic at worst.

What is needed is a new paradigm for defense that must be designed into the overall scheme from the beginning, and not simply an add-on protective measure or another ineffective barrier. To more realistically deal with the ever growing threat, the concept of defense in depth must be built. One possible approach is to stop trying to defend everything with a higher, thicker castle wall and instead, focus on defending what is really important—the crown jewels—those systems, entities, capabilities, network elements, that are truly vital to mission accomplishment. By trying to defend everything, we defend nothing.

The approach to defense in depth for the Air Force network should be similar to defending our air bases. We do not try to defend every inch of property on any base. We use fences and armed sentries to deter most would-be intruders. We also identify our crown jewels such as the flight line and other critical assets. We use stationary guards and additional fences to protect these critical assets. Further, we use roaming patrols to monitor activities and respond when needed. As an additional measure, we use electronic sensors to alert our forces to unusual or unwanted activities.

Designing network defense along this defense-in-depth paradigm requires identifying, up front, what our cyberspace crown jewels are. In the case of our air operations centers (AOC), it may be the Theater Battle Management Core System (TBMCS); for air mobility operations, it may be the Global Command and Control Systems which mobility professionals the world-over rely on through unclassified networks. For space operations, it may be the satellite control network which is a "closed" system, or it may be space surveillance systems and the networks that link telescopes and dish antennas to space operators; for ongoing operations in the Persian Gulf, it may be remotely piloted aircraft infrastructure from satellite links, the distributed common ground stations to simply having sufficient bandwidth to ensure the full-motion video they provide gets to the intended user when and where it is needed; for the medical community, it may be databases of medical records.

Whatever the "crown jewel," not everyone needs access. Access should be limited to those with a bona fide need and then protected by a variety of security measures to keep everyone else out. Public key infrastructure, well constructed

passwords, biometrics, known Internet protocol addresses, and additional passwords as required—in other words multiple identification measures. For those old enough to remember the television show, *Get Smart*, the main character, Maxwell Smart, had multiple entry points he had to get through just to reach his headquarters at "Control." Even inside the highly secure facility, Smart often invoked more secure measures to discuss highly classified information. Once again, nothing new here, we do the same today with our special access programs and security clearances. What we haven't yet figured out is a similar approach to the critical warfighting systems and data we access through cyberspace.

Accessing the base library or the base gymnasium can be open to anyone with a valid common access card (CAC). Accessing your e-mail for day-to-day use may only require a CAC reader, proper user name and password, although in the future we may add biometrics and other smart technologies that identify specific users on a computer by the manner in which they type or monitor activities to build user "profiles"—using a series of tests to verify users operating on a system. Access to TBMCS or other crown jewels may require a CAC reader, proper user name, significant password, biometrics, specific computer access credentials from a known Internet protocol address that should allow access, additional user names and password and possibly additional tokens or CAC-like hardware to identify the user. Cumbersome? Perhaps. Necessary? Absolutely.

The point of all this is that the current schema of foundational defense is not sufficient. What is needed is new thinking on how to protect those elements most vital to the mission and mitigate any threat to them so that they are reliable, available and the integrity of the data can be trusted by the warfighter when and where he/she needs the information.

Consequently, when we plan cyber missions, either in support of kinetic or non-kinetic missions, we do not need to assure cyber supremacy across the entire Air Force network. Rather, we must assure cyber supremacy over those portions of the Air Force network at the time and place necessary to support specific missions. Given the nature of the cyberspace domain, we know adversaries are operating inside our network and we will likely never eliminate their activities. However, we must learn to fight through adversary actions when necessary. Mission assurance is a key paradigm shift that will lead us to that capability. Said another way, we can't "boil the ocean" and keep our entire network completely risk free; we need to focus our efforts around the missions we are tasked to accomplish.

Presuming that sufficient steps will be taken to assure our missions by focusing on foundational activities … engineering solutions to move away from the castle wall concept of protection … what about the more dynamic situations that we see today and that will be increasingly important in the future?

Mission-Specific Mission Assurance

Whether or not we have our foundational defenses in place, we must always be prepared for the more dynamic situations. Again, this is nothing new to Airmen as one of the key tenets for applying airpower is flexibility. What is new is the idea of folding cyberspace into the planning mix for those dynamic situations. Historically, the AOC Air Tasking Order process operates on a 72-hour cycle. To better explain mission-specific cyberspace mission assurance, assume that a critical mission is to occur within the next 72 hours. Using the air domain example, this mission will likely require air superiority over a certain location for a specified amount of time to achieve the specific military objectives. The ATO is then assembled to ensure the right aircraft are in the right location with the correct munitions to assure the air superiority mission. Likewise, if needed, tankers will be placed where needed to support—as will airborne command and control, if required. Essentially, this is a scene AOC planners are all too familiar with and it occurs seamlessly on a day-to-day basis in many parts of the world. Frankly, the US Air Force is known throughout the world as the only air force that can conduct air superiority over any spot on the globe for a specified duration. Likewise it is recognized that the US Air Force cannot provide air superiority over the entire globe all the time.

Now take that same superiority concept and apply it to the cyberspace domain. In any dynamic mission that will occur in the next few days, there will be an aspect of planning that must be accounted for. These planning activities are performed to identify critical cyberspace assets necessary for mission execution and are referred to as mission-specific activities. Mission-specific activities are near-term focused. Again, we cannot provide this mission-specific focus across the entire Air Force network, so we will focus only on what is required to ensure success of this specific mission—where we know the time, place and capabilities required to support the objectives.

Using processes similar to an AOC, the 624th Operations Center (624 OC) provides a leap forward in capability to command and control cyberspace capabilities on the battlefield. All of the functions of the 624 OC converge to provide mission assurance when engaging an adversary. The Air Force now has the means to develop a strategy, organize cyberspace forces, task, and control them to achieve operational effects across the cyberspace domain that are integrated with the other warfighting domains.

As the planning progresses, the effects desired in, through and from cyberspace must be determined. Clearly some missions rely heavily on Air Force networks and the systems and information that reside on those networks. Partnering with the

What is needed is new thinking on how to protect those elements most vital to the mission and mitigate any threat to them so that they are reliable, available and the integrity of the data can be trusted by the warfighter when and where he/she needs the information.

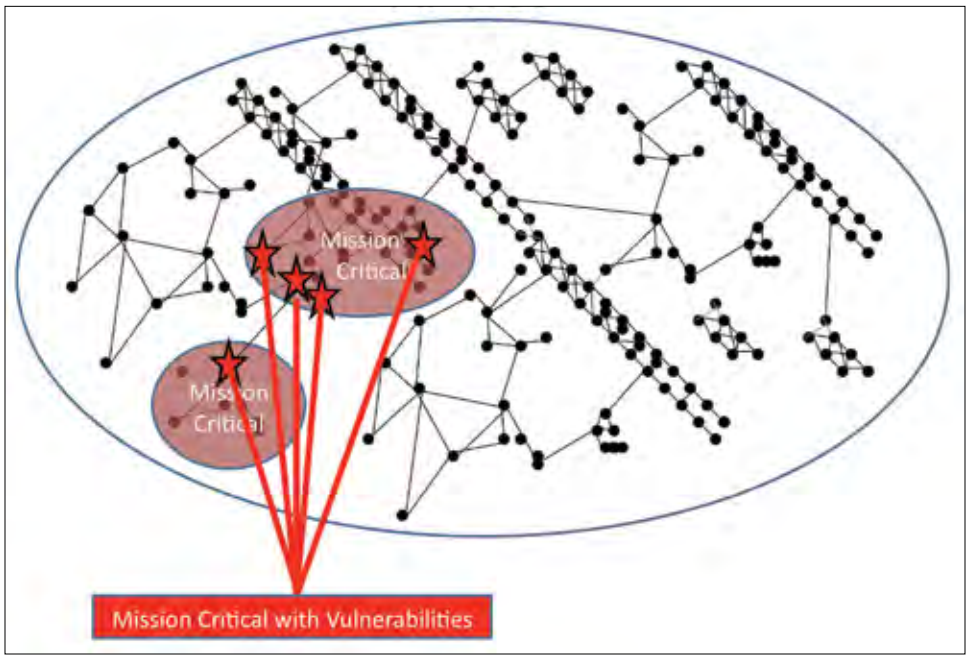


Figure 1. Air Force network cross section. Mission critical assets make up the defended asset list.

supported combatant numbered Air Force and joint planners, the 624 OC must identify which of the Air Force cyber mission tasks are required to achieve the desired effects as outlined by the joint force commander. Likewise, the critical links, nodes, and elements for the use of cyberspace in this mission-specific scenario must be determined. Simply put, planners must "map the mission." While foundational activities "map the network," mission-specific activities must "map the mission." By comparing what is known with what is required, network deficiencies, single-points of failure, alternate path requirements, and so forth, will be determined. Essentially, planners must determine the mission-specific critical asset or defended asset list.

To make the determination of what assets comprise a defended asset list, there are several key factors that must be considered and weighed. First, we must determine the criticality of the asset based on its function to the defined mission task. Among the criteria that must be examined are: operational backup components, network load and performance parameters, assessed adversary capability against the component, critical vulnerabilities, and susceptibility to attack. Figure 1 depicts the groupings of assets based on the mentioned criteria. The end result is a smaller subset of high risk, mission critical assets that have critical vulnerabilities.

Adversary activity is only part of assuring the mission. Our own activities can hinder mission critical functions as much as the adversary. We must also deconflict scheduled maintenance activities on these communication networks and critical components to ensure availability. Cyberspace planners will then ensure backup communications circuits are available in case of failure or disruption of critical links.

Several activities can be performed to help assure the mission. Assuring adequate redundant communications is only part of the solution. We must also identify system vulnerabilities of these critical assets and check for unwanted activity. If new software updates are available, cyber operators will deploy updates to patch these vulnerabilities. In cases where software updates are not available, highly skilled computer programmers can create and deploy the necessary software updates using expedited acquisition and development processes. In addition, the Air Force is developing, equipping, and training hunter teams to deploy network monitoring equipment to locations worldwide. These hunter teams will understand adversary tactics and will be able to detect and disrupt undesired activity to create a sterile subset of the network to assure operations.

By determining mission critical assets, threat vulnerabilities, and deconflicting friendly activities the 624 OC can then produce an Air Force cyber tasking order (CTO) to direct cyberspace forces to conduct a variety of activities (listed below) to help assure the specific mission. This Air Force CTO could include the task to deploy hunter teams either virtually or physically to monitor certain areas of the Air Force network. Additionally, the 624 OC can produce a cyberspace control order to direct configuration or re-configuration of certain portions of the Air Force network to assure the specific mission. By applying air superiority concepts that have been developed and proven by AOCs the world over, the 624 OC can apply integrated cyberspace superiority for specific portions of the Air Force network necessary to assure time-critical joint warfighter missions.

Examples of cyberspace mission-specific taskings include:

- Redirection of cyber sensors. For example, rather than inspect a small subset of traffic over a larger enterprise, tune the Air Force sensors to inspect a much deeper set of parameters of the defended assets. Based on tasking-specific intelligence, operators can tune the sensors to look for specific activity not expected elsewhere on the network.
- Deployment of hunter/engagement teams. For example, deploy (remotely or otherwise) specially trained engage-

By setting the foundational cyberspace defensive schema based on protecting what's important, the "crown jewels," and not just building the castle wall higher and thicker we can more effectively and efficiently assure the day-to-day mission.

ment team to seek out and mitigate adversary presence on and around these critical components.

- Cyber reconnaissance missions against the enemy's rear areas. For example, request reconnaissance (via appropriate Title 50 means) missions inside adversary networks to gather required tip off intelligence.
- Providing expeditionary network capability and access. For example, request combat communications elements extend a tactical network to mitigate choke points, establish secondary communications links, or enable connectivity to adversary networks where expeditionary forces have unique access.
- Intelligence capability to provide warning, determination of adversary goals and objectives, and assessment of effects. For example, request technical intelligence from the 70th Intelligence Wing's Cyber Intelligence, Surveillance, and Reconnaissance Group that will tip off unwanted activity affecting the defended assets.
- Influence operations that can be leveraged to shape the information/cyber environment. For example, plan for and conduct diversions or other influence operations that would take adversary attention away from the enclave in question.

Putting It All Together

In the end, the mission of 24 AF is about providing the joint warfighter with cyberspace effects at the time and place of our choosing—assuring the mission. By setting the foundational cyberspace defensive schema based on protecting what's important, the "crown jewels," and not just building the castle wall higher and thicker we can more effectively and efficiently assure the day-to-day mission. By using known processes to integrate cyberspace capabilities for dynamic mission-specific activities, we can quickly analyze, task, and command and control cyberspace forces to assure the mission for the joint warfighter. We cannot afford to dilute our efforts by trying to assure the entire Air Force network.

You may ask: "So what? What is the value added of using this approach?" The answer is very simple. Using a mission focused approach allows our forces to be prepared to act instead of react. Furthermore, understanding the dependencies allows us to integrate and synchronize cyberspace effects across mission areas to be most effective. This prioritization will help us to protect critical, high-risk assets and stop reacting to low risk activities. Through this approach, we will be better able to protect mission critical assets and ensure our Air Force can fly, fight, and win in all warfighting domains.

Maj Gen Richard E. Webber is the commander, 24th Air Force and Air Force Network Operations, Lackland AFB, Texas. General Webber is responsible for the Air Force's newest numbered air force providing combatant commanders with trained and ready cyber forces which plan and conduct cyberspace operations. Twenty-fourth Air Force personnel extend, maintain and defend the Air Force portion of the Department of Defense global network. The general directs the activities of three wings, two located at Lackland AFB, and one located at Robins AFB, Georgia.

General Webber was commissioned a second lieutenant upon graduation from the US Air Force Academy in 1975. He has commanded a missile squadron, support group, missile operations group, and missile wing equivalent and two space wings. His staff assignments include Headquarters North Atlantic Treaty Organization International Military Staff, the Air Staff, Headquarters Strategic Air Command, Headquarters Air Force Space Command, and vice commander of the Aerospace Command and Control and Intelligence, Surveillance, and Reconnaissance Center.

General Webber is a command space and missile operator with qualifications in the Minuteman II, Minuteman III, Global Positioning Satellite and Counter Communications System weapon systems. Prior to his current assignment, he served as assistant deputy chief for Air, Space and Information Operations, Plans and Requirements, Headquarters US Air Force, Washington, DC.

Col Mark E. Ware is the director of operations for the new 24th Air Force, Lackland AFB, Texas. In this capacity, he is the primary staff advisor to the 24th Air Force commander for the direction and control of US Air Force cyberspace forces and is responsible for the implementation execution of US Air Force policy for cyberspace operations.

Colonel Ware entered the Air Force in 1982 after receiving his commission from Air Force Reserve Officer Training Corps. He has served in North Atlantic Treaty Organization and nearly every geographic combatant command area of responsibility as an operator or staff officer. Colonel Ware commanded at the squadron and group levels and was combat-mission ready in three separate and distinct weapons platforms; UH-1N, F-16, and E-3. He is a command pilot with more than 3,200 hours in the UH-1N, F-16, and E-3.

Senior Leader Perspective

Cyber and Space – A Way Ahead

Brig Gen Edward L. Bolton, Jr., USAF
Director of Cyber and Space Operations
Headquarters Air Force A30-CS
Pentagon, Washington DC

Nearly thirty years ago, science-fiction pioneer William Gibson first used the word "cyberspace" in Neuromancer, his ground breaking story about a globally linked, virtual world that is now just over ten years away. A decade sooner than his prediction, Air Force Space Command (AFSPC) has transferred its nuclear missile mission to Global Strike Command and incorporated cyberspace oversight responsibilities into its portfolio. Against this backdrop, this article compares and contrasts the cyber and space domains to identify their key similarities. It next postulates several major changes we can expect in these two mission areas by the timeframe that Gibson described, the early 2020s. After a review of observations from the recent Schriever Wargame 2010, it argues that the best benefits from the combination of cyber and space can be obtained by the integration of cyber and space capabilities into a seamless set of non-kinetic effects. The article concludes with a summary of three focus areas AFSPC can exploit to best achieve these ends.

Comparing and Contrasting Cyber and Space

Cyber systems, which include computers, communications equipment, embedded microprocessors, and related Internet infrastructure, inhabit a principally commercial domain. The Internet is a voluntary media—a global collection of interconnected networks that provide access to trillions of Web pages. Anyone with a few hundred dollars worth of equipment can provide Internet-based services or applications to the Web and are limited only by their time and technical skills. Conversely, space systems, which include satellites, launch and range assets, and command and control infrastructures, cost in the hundreds of millions of dollars. Space launch and range sites are few in number and their missions are constrained by safety requirements and orbital considerations. Space is a manpower intensive business, with Air Force operators and engineers, systems engineering and technical assistance support, and contractor personnel involved in each phase of the process. The steep entry price, considerable technical challenges, and manpower requirements, limits the number of countries or consortia capable of launching a satellite into space. In 2009, a total of 78 orbital launches took place from 17 spaceports around the world carrying 111 payloads for militaries, civil governments, commercial entities, and universities bringing the total number of active satellites circling the Earth in various types of orbits to 918.[1] Although significant portions of Department of Defense (DoD) space capabilities are derived from commercial sources, the majority of unclassified DoD space assets are developed, deployed, and operated by the Air Force, as the executive agent for DoD space.

Yet, despite these differences, the cyber and space domains do have substantial commonalities. Both cyber and space systems utilize the electromagnetic spectrum at near-light speed, deliver non-kinetic effects, and require microelectronics and communications-based technologies to function. A compelling area for greater synergy though, is the growing intersection between the cyber and space domains, specifically systems that operate at least partly in both—that are cyber-enabled and space-based. Communications satellites predate the Internet but are now nodes on the world-wide communications infrastructure that leverage cable, fiber, and the Internet. Other space data, from weather imagery and satellite television/radio, to position, navigation, and timing (PNT) services, is increasingly available on the Internet. This overlapping of domains can be exploited to improve data compression and spectrum sharing techniques increasing data transfer rates and enhancing data processing capabilities. Also, the evolution towards fused cyber and space information is an opportunity to build in redundancies to strengthen mission resiliency and improve contingency response capabilities. This is already happening today: satellite communications serve as a back up to landlines, with voice over Internet communications as a back up to each. It is reasonable to expect this transition to a merged domain to continue into the next decade.

The Changing Cyber and Space World

Baseball hall of famer Yogi Berra once said, "It is difficult to make predictions, particularly about the future." Regardless, this article lists trends in cyber and space and discusses how they might provide challenges and opportunities in the next decade. The space capabilities of the 2020s are either in final test at major space defense contractor facilities, in preparation for launch at Cape Canaveral AFS, Florida or Vandenberg AFB, California, or are early in their mission tenures on orbit. Within the next 18 months one space-based infrared system (SBIRS) satellite, two advanced extremely high frequency (AEHF) communication satellites, three wideband global satellite communications (WGS) satellites, and six global positioning system (GPS) satellites will bring the next generation of missile warning, communications and PNT services into operation. Each satellite is significantly more capable than the system it will replace. SBIRS will provide the world's most comprehensive missile warning and missile defense data. This generation of GPS satellites will enable a net-centric architecture for PNT. The AEHF satellites have five times the capacity of the satellites they are replacing. WGS satellites have ten times the capacity. Given the typical decade plus service-life of current systems, the space capabilities of the next decade are here today.

Each generation has put more capability at the user's disposal, and given Moore's law, computing power will continue to double every 18 months, incentivizing low-cost production of even more capable systems.

Three trends seem predictive of cyber capabilities in the next decade: the growing intersection between cyber and space systems as previously observed; the increasing use of online services; and the increasing use of mobile cyber systems. More and more of our transactions are migrating to the cyber world. Within the Air Force, permanent change of station processing, travel voucher filing, assignment volunteer status declarations, and other services are now online. Earlier this month, the space squadron commander selection process (the Vigilant Eagle board) was conducted online from the Air Force Personnel Center. Board members used networked computers to review virtual personnel folders without the use of "hard copy" records or scoring sheets. The net is increasingly available while mobile. The fastest selling cyber product in 2010 has been the mobile "smart" phone. According to one of the people responsible for designing the basic architecture and core protocols that make the Internet work, Dr. Vinton Cerf, the mobile phone is nearing 20 percent of the total telephone market with a total of over 4.5 billion units sold.[2] More computer than phone, smart phones have search, photographic and video, entertainment, PNT, weather, text, and social networking capabilities. Each generation has put more capability at the user's disposal, and given Moore's law, computing power will continue to double every 18 months, incentivizing low-cost production of even more capable systems. From a risk perspective, more strongly connecting the cyber and space domains further exposes mission critical systems to potential contagion from hazards within the world's cyber infrastructure. Growing Web-based service and mobile usage reduce the relevance of traditional defensive measures like time and distance, and increase our reliance on capabilities that can be non-kinetically denied from across the globe.

Evidence of the threat-related implications of these trends is already apparent. According to O. Sami Saydjari of the nonprofit Professionals for Cyber Defense, "For about $5 million and between three to five years of preparation, an organization, whether it is transnational terrorist groups or nation states, could mount a strategic attack against the US."[3] International correspondent John Daly, during a 24 May 2010 presentation on Sub-Saharan Africa stated, "The Internet is a growing influence on the radicalization of Africa's predominantly Islamic states."[4] A recent New York Police Department briefing on countering terrorism identified the Internet as an "important venue for radicalization."[5] The study summarized an investigation into the influences on a number of western raised terrorists and described the radicalization or "Jihadization" of seemingly westernized middle class American citizens. Both Maj Nidal Hasan, the accused Fort Hood, Texas shooter, and Faisal Shahzad who allegedly attempted to car-bomb Times Square, are "home grown terrorists" who used radical Web sites and chat rooms to gain religious justification for violent political extremism. In these cases, the virtual world helped precipitate violence or attempted violence in the physical world. It is not inconceivable that via the Internet, future radicals will penetrate, recruit, and indoctrinate here in America to an extent that is currently beyond belief.

Schriever Wargame 2010 Observations

Air Force Space Command recently conducted the sixth Schriever Wargame at Nellis AFB, Nevada. Set in the year 2022, the game explored critical cyber and space issues and investigated the interaction of multiple agencies associated with cyber and space systems and services during a crisis. The various scenarios highlighted the increasing reliance on space and cyberspace as core enablers for all defense and homeland security operations.

As presented during Schriever, a defining characteristic of the early 2020s will be the increased interweaving of the civil, commercial, national, and international cyber and space infrastructures. Independent operation, assessment, or protection will be nearly impossible without acute understanding of space and cyberspace interconnections. During the wargame, it was difficult to clearly attribute or even identify an attack or determine when or if an attack had ended. Throughout the event, the coalition was challenged by a sophisticated adversary that highlighted the absolute need in understanding one's own vulnerabilities, the importance of pre-determined mitigating actions, and the ability to quickly and effectively respond to an evolving crises. (In Cold War defense scenarios, the US and coalition had minutes to respond, we now have seconds). Schriever Wargame 2010 highlighted that precise regional indicators and warnings of intent or proven mechanisms to communicate national security messages were needed in the new integrated cyber and space domain. The coalition discovered that without mature understanding of vulnerabilities, a plan for pre-determined mitigations, and an ability to communicate national security intent led to the rapid global escalation of a regionally-based minor dispute. Or as aptly put by the acting wargame president, former Congressman Tom Davis, "this is a fender bender with strategic implications."[6]

Further, Schriever Wargame 2010 highlighted the necessity of comprehensive vulnerability assessments for an integrated domain with deliberate plans to expedite decisions during a crisis. The Schriever Wargame suggested development of preapproved cyber and space courses of action, along the lines of a cyber and space Single Integrated Operational Plan. These formal coordination processes and well understood approval roles and responsibilities would facilitate both contingency and crisis response that we could face in the future.

The Way Ahead

The short term way ahead calls for a focus on implementation issues and has already made significant strides: the stand up of the 24th Air Force, the creation and population of the 17XX cyber career field and presentation of forces to the joint commander are already underway or complete. After these important organizational considerations are resolved, the following three tenets are offered as emphasis areas to speed the transition into a fully integrated cyber and space command ready to respond to the challenges of the next decade.

Build a strong culture and community. The foundation of any organization is the people in it. The top priority for the command must be to build a community of cyber-savvy and space-smart Airmen that are dedicated to the joint fight and ready for assignment across the cyber and space enterprise.

Fully integrate cyber and space capabilities. The most value from cyber and space systems will be obtained when we can present cyber and space forces as a seamless suite of capabilities to the joint forces commander.

Spread the mission success mentality. The command must transition to a prioritization approach that will focus cyber and space protection efforts on activities to ensure critical missions can continue despite attacks versus defending every node and circuit.

Build culture and community. We must integrate cyber and space operations, engineers and acquirers, regardless of where they work, into one community. AFSPC knows how to do this. Since the birth of the command in 1982, AFSPC has integrated engineers and acquirers into the space community. In the 1990s AFSPC folded missile operators into the command, then combined missile operations (18XX) and space operations (20XX) into one career field, space and missile operations (13XX). Each discipline brought important contributions to the command. The missile operators provided operational expertise, a clearly defined career progression path, and well documented crew force management processes to the force. Space operators and engineers offered in-depth technical knowledge of the overhead and ground systems, understanding of acquisition principles, and space acquisition knowledge. Since that time, many space and missile professionals have been cross-assigned across space, missile, and acquisition assignments. The development of a number of cross-domain professionals, and a community that values the contributions of each, was a successful result of the space, missile, and space acquisition command. This, and the alignment of program offices in Los Angeles with operational wings, meant each program office had a specific commander as their primary customer. This facilitated a peer-to-peer relationship between program office directors and operational commanders that resulted in the customer-service mentality currently held at the space acquisition center. The success of the command's launch and range enterprise, the extended service lives of the overhead systems the command manages, and the successful partnerships with National Aeronautics and Space Administration, Missile Defense Agency, Defense Advanced Research Projects Agency, and the National Reconnaissance Office (NRO) are also examples of the successful legacy of the "space and missile" command.

That success can be duplicated within the new "space and cyber" command using some of the same mechanisms. Building clear career and professional development paths, permitting the appropriate level of cross flow between the domains, aligning operators and acquirers in both domains and building partnerships with other cyber and space centers of excellence will help achieve some of the same positive results. In addition, we should aggressively recruit Guard/Reserve and civilian personnel from cyber industry, specifically manufacturers, telecommunications and software engineers, and Internet service provider professionals. Total force personnel, with full-time careers in the commercial cyber industry can bring advanced tech skills, current training, and a rapid-to-market mentality in the new enterprise. Finally, we should use this opportunity to evaluate special access programs and clearances and reduce stove-piped approaches that limit leadership's ability to manage across the enterprise and provide a comprehensive capability to the joint warfighter.

Integrating cyber and space. We have already seen the increased interdependence of the cyber and space domains as more of our cyber systems use space gathered data and more of our space systems use the cyber medium as part of their command and control infrastructure. Our goal however should be the integration of cyber and space such that we cut across the breadth of assets towards the seamless and synchronized employment of cyber and space effects. These effects can then be integrated into broader non-kinetic options that would be part of the integrated joint campaign. One approach is the reorientation of research, development, and acquisition infrastructure and processes to enable this integrating process. This will include building improved mechanisms to leverage commercial industry's ability to rapidly transition emerging technologies into operational capabilities. By the next decade, AFSPC will need to provide additional operational capacity within the same electromagnetic frequency constraints. Perhaps by emphasizing applications that can reside on current operating systems or use currently available data to form new products this can be achieved. The consideration of cyber payloads on space systems, and other ride sharing and sensor mixing approaches, should be in the trade space as analysis of alternatives are completed to address operational challenges. Also helpful would be an examination of security classification requirements with the intent to reduce the number of stove piped special access

Our goal however should be the integration of cyber and space such that we cut across the breadth of cyber and space assets towards the seamless and synchronized employment of cyber and space effects.

programs. Overly classifying capabilities impede our ability to discuss across domains, develop multi-domain capabilities and grow the knowledge base of integrated cyber and space capabilities.

On the cyber side, we should consider aligning operational cyber wings with program offices designated to serve their acquisition needs. As to future major acquisitions, we will need as a minimum cyber and space fusion centers to monitor integrated cyber and space status. In addition, the virtual training that has already shown great promise in developing more capable soldiers by proving high fidelity, low cost training for combat missions should be a goal.

Mission success. A significant accomplishment for AFSPC is the mission success results in the launch and range mission area. Typically known as mission assurance, the launch and range teams at Patrick/Cape Canaveral, Vandenberg and Los Angeles AFBs, with mission partners in the NRO, the Aerospace Corporation and the United Launch Alliance has over a decade long string of consecutive successful national security spacelift missions. After several launch failures in the late 1990s, a series of studies were commissioned to uncover the root causes of the failures and collect lessons learned during both failed and successful launch campaigns. In parallel, engineers at the Aerospace Corporation documented report findings, best practices, and 40 years of experience into a formal launch verification process. The process, codified in 2001, involves scrutiny of hundreds of components, procedures, and test reports. It uses engineering models to objectively validate contractor data. It concludes with post-flight analyses to gain feedback and monitor performance trends. The sum of this work is 2,500 separate tasks each with defined completion criteria. Based on the mission criticality of the part, process, or test under examination, an appropriate depth (from monitoring thru full independent analysis) for each task is assigned.

A similar process could be put into place for the combined cyber and space enterprise. After assessments to determine how cyber and space support a given mission, tasks, and analyses necessary for mission assurance would be documented and demonstrated on a mission-based priority. Readiness reviews could then be conducted to demonstrate the team's readiness to support a given mission, operate in a degraded environment, and to recover diminished capability if necessary. This core competency could be spread across both the cyber and space mission areas.

Conclusion

A generation after successfully building an integrated space and missile operations and acquisition team, AFSPC has the opportunity to do the same for cyber operations, space operations, and their acquisition support infrastructure. The virtual world foreseen by William Gibson is fast approaching. The links between AFSPC's two domains are apparent and the command's contribution to the integrated joint fight can be enhanced by their combination. Benefits can be realized and risk mitigated by leveraging the lessons learned from the Schriever Wargame series and our successes in building the space and missile team. The command must also specifically integrate the cyber and space infrastructures—systems, processes, and best practices. Foundational to success though, is the launch and range mission success philosophy that is a best practice of AFSPC.

Notes:

[1] Space Foundation, "The Space Report 2010," 62 and 77.

[2] Vinton Cerf, "Foreign Strategic Space and Cyber Trends" (lecture, Air Force Space Command, Peterson AFB, Colorado, 18 May 2010).

[3] Quoted in Jeanne Meserve, "Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid," *CNN.com/US*, 26 September 2007, http://www.cnn.com/2007/US/09/26/power.at.risk/index.html?iref=allsearch.

[4] John C.K. Daly, "From Nigeria to Somalia: Islamic Influences in Africa," (lecture, Alan L. Freed Associates, Inc., AFRICA: US Foreign Policy and Security Challenges Seminar, Capitol Hill Club, Washington DC, 27 May 2010).

[5] Mitchell D. Silber and Arvit Bhatt, "Radicalization in the West: The Homegrown Threat" New York City Police Department, 2007, http://www.nypdshield.org/public/SiteFiles/documents/NYPD_Report-Radicalization_in_the_West.pdf.

[6] Tom Davis, "Schriever 10 Wargame Outbrief" (lecture, Schriever Wargame 2010, Nellis AFB, Nevada, 10 May 2010).

Brig Gen Edward L. "Ed" Bolton, Jr. (BS, Electrical Engineering, University of New Mexico; MS, Systems Management, University of Southern California; MS, National Security Strategy, National War College, Fort Lesley J. McNair, Washington, DC) is the director, cyber and space operations, directorate of operations, deputy chief of staff for operations, plans and requirements, Headquarters US Air Force, Washington, DC. He provides senior Air Force leaders and Air Force major commands vision, expertise, and staff support to fully integrate and synchronize space and cyber capabilities across the spectrum of conflict.

General Bolton has commanded at the squadron, group, and wing level. He has a broad range of experience in operations, requirements, and policy. His staff experience includes serving as a director for defense policy at the National Security Council in the Executive Office of the President. He also led the Range and Network Systems Program Office, then the Launch and Range Systems Program Office. As the deputy director for systems integration and engineering, as well as the principal deputy to the Chief Operating Office at the National Reconnaissance Office (NRO), he won the NRO Leadership Award for 2008 and was awarded the NRO Gold Medal. Prior to his current position, the general served as commander, 45th Space Wing, and director Eastern Range, Patrick AFB, Florida. During his tenure, he oversaw 24 successful spacelift, shuttle, test, and range missions from Cape Canaveral AFS..

Senior Leader Perspective

Integrating and Synchronizing Non-kinetic Effects: USSTRATCOM Forward Integration Team

Brig Gen Michael J. Carey, USAF
Deputy Director, Global Operations
US Strategic Command
Offutt AFB, Nebraska

Virtually all aspects of military operations are affected in some way by the capabilities provided from (space and cyberspace) and it's difficult to overstate their importance to the success of our Armed Forces.

~ Air Force Chief of Staff General Norman A. Schwartz

The integration of non-kinetic effects—space and cyberspace capabilities—across the spectrum of conflict is vital to the success of any US military campaign, from overseas contingency operations to deliberate planning for broader nation-states. Non-kinetic support to operations has long been a focus area for joint force commanders (JFC). In both Iraq and Afghanistan, a variety of non-kinetic systems have served as force multipliers; however, their full operational potential has not been realized because of the fragmented manner in which they are applied to the fight.

US Strategic Command's (USSTRATCOM) mission set includes ensuring US freedom of action in space and cyberspace and delivering integrated kinetic and non-kinetic effects in support of US JFCs. The commander of USSTRATCOM is responsible for planning and conducting space operations (force enhancement, space support, and on-orbit operations) and, as directed, planning and executing space control and force application. USSTRATCOM is further identified as the single point of contact for military space operational matters. The commander of USSTRATCOM is also responsible for synchronizing planning for cyberspace operations, planning against cyberspace threats, coordinating with other combatant commands and appropriate US government agencies prior to the generation of cyberspace effects that cross areas of responsibility, and executing cyberspace operations, as directed. These assigned non-kinetic missions translate to a combatant commander (COCOM)-level responsibility for ensuring the proper level of support is provided to the nation's current conflicts.

The command currently supports US Forces-Afghanistan (USFOR-A) and International Security and Assistance Force (ISAF) lines of operation by providing space force enhancement effects to include positioning, timing, and navigation, communications, meteorological support, early warning, and intelligence, surveillance, and reconnaissance. Additionally, USSTRATCOM provides limited non-kinetic effects through the application of cyberspace and counterspace capabilities. We can employ these capabilities to deny, degrade, disrupt, deceive, and isolate terrorist and insurgent networks in support of strategic communications, security and other USFOR-A and ISAF objectives. While these individual non-kinetic capabilities are currently allocated to the theater, there has been no established mechanism to bring together combined/integrated non-kinetic effects in support of the breadth of missions that span multiple regional commands (RC) and task forces.

During the spring of 2009, as the administration was adjusting the focus more finely on the conflict in Afghanistan, it was apparent, as it had been in previous years, that there was a lack of demand being placed on USSTRATCOM's non-kinetic global capabilities in support of theater operations, namely ISAF. In assessing the likely causes for the lack of demand levied by forward elements, it was obvious we could not adequately evaluate the situation from Omaha, Nebraska, and needed to conduct a brief 60-day assessment in Afghanistan to determine the fundamental problem and devise a course of action to correct deficiencies. With approval from the commanders of US Central Command (USCENTCOM), USSTRATCOM, ISAF, and the Chairman, Joint Chiefs of Staff (CJCS), a small team of USSTRATCOM subject matter experts (SME) was dispatched to Afghanistan in June 2009 to conduct the assessment and execute any resultant course of actions (COA) that included in-theater support.

This USSTRATCOM Forward Integration Team (SFIT) was chartered to fully integrate and synchronize non-kinetic effects in support of the commander, USFOR-A. The SFIT was comprised of members with substantial experience in the disciplines of space and cyberspace operations to determine gaps or seams and highlight opportunities for improved non-kinetic operations support. When the SFIT arrived at the ISAF compound in Kabul, the ISAF staff were in the throes of a 90-day assessment and structural reorganization which would recast the command's requirements to fight the ongoing insurgency. The 90-day assessment, as it became known, provided the best opportunity to adjust manpower levels addressing non-kinetic effects and their adequate integration into standard general purpose forces. The complexities of working in space and cyber-

In both Iraq and Afghanistan, a variety of non-kinetic systems have served as force multipliers; however, their full operational potential has not been realized because of the fragmented manner in which they are applied to the fight.

space are compounded by an expansive international coalition. At the time, with each of the five RCs led by different countries, it was apparent that the team would need to travel to each RC to validate requirements and assess shortfalls.

From the SFIT's 60-day assessment, the team identified the following gaps/seams:

- The lack of a knowledgeable and experienced planning element limited JFCs' ability to integrate space and cyberspace efforts to achieve operational objectives.
- The telecommunications and cyberspace environment was rapidly developing and in many parts of Afghanistan was not well understood.
- No single entity had the capability and capacity to integrate non-kinetic space and cyberspace effects and capabilities in support of the ISAF and USFOR-A at the operational level.
- Inter-agency operational coordination and deconfliction was inadequate for space and cyberspace capabilities across the Afghan combined/joint operations area CJOA.
- Utilization of space and cyberspace effects in the Afghan CJOA was limited. These effects were brought to bear in a singular fashion instead of in a synchronized manner.
- USSTRATCOM was not engaged as a supporting commander for the delivery of non-kinetic effects in Afghanistan, due in large part to a dearth of subject matter expertise on the JFC staffs.

Furthermore, multiple regional commands, task forces, and headquarters elements conduct operations within Afghanistan. What was missing was a standardized understanding or application of USSTRATCOM-presented non-kinetic capabilities because of the fast-paced dynamics of executing operations in the Afghanistan CJOA. There was a need to build an understanding of non-kinetic effects and capabilities with each of the command elements and then work towards making the most of these effects in theater. To address these identified shortfalls, the SFIT was formed to close the gaps and leverage existing non-kinetic opportunities.

The first SFIT began working to better integrate and synchronize space and cyberspace-derived non-kinetic effects in July 2009. An initial estimate of multiple SMEs for deployment to the Afghan CJOA was derived from the following assumption: the five RCs would each require various space, cyber, and information operations (IO) experts to form multidisciplinary teams needed to work non-kinetic issues at the operational level. When the concept of the ISAF Joint Command (IJC) matured, we collaboratively assessed that we would be more effective with fewer planners (space and cyber) at the soon-to-be-formed operational corps-level headquarters and less planners at each of the RCs. We placed team members at RC-South (RC-S) as they had the greatest initial capability shortfall. RC-S, however, had no US cleared special technical operations (STO) facility. RC-East (RC-E), the historic priority of effort located at Bagram Airbase, Afghanistan, did have adequate planning spaces and processes, so it made good sense to place planners at Bagram because they had the most mature non-kinetic planning framework.

In June 2009, the number of savvy space planners in Afghanistan was small and resident only in the CJTF-82 CJ-3 at Bagram. To date, Iraq had been the priority of USCENTCOM's effort, and therefore had the greatest density of capable space planners and operators. The combined force air component commander (CFACC), empowered with space coordinating authority, had approximately one tenth of his allocated space force supporting Afghanistan. With US priorities realigning to win in Afghanistan, the CFACC then redirected a number of space teams to support ISAF and USFOR-A beginning in the fall of 2009, after the initial SFIT assessment concluded. This influx of space personnel in the joint operations area met much of the newly identified shortfall for skilled planners, thus lessening the requirement for SFIT space planners at the RCs. The remaining RCs—North, West, and Capital, were not yet developed adequately to require or support the effects SFIT members could offer and were therefore not manned as such.

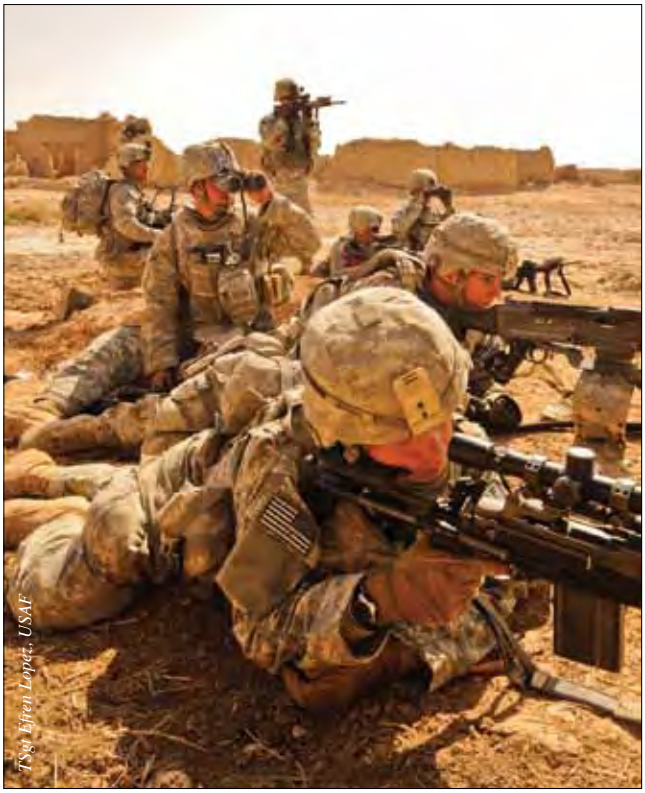

TSgt Efren Lopez, USAF

Figure 1. US Army soldiers engage in a small-arms firefight with enemy forces during Operation Moshtarak in Badula Qulp, Helmand province, Afghanistan, 19 February 2010.

The initial team consisted of a team leader with a broad IO and cyberspace background, cyberspace operations planners, space planners with backgrounds in offensive counter-space, and strategic planners with STO expertise. The team represented a cross-section of USSTRATCOM functional and service components with extensive subject matter expertise in space and cyberspace mission sets. The next SFIT relieved them in January 2010 and remains deployed today. The team now includes an expeditionary cyberspace support element from US Cyberspace Command (USCYBERCOM) tasked specifically to integrate effects provided in and through cyberspace with other op-

The USSTRATCOM Forward Integration Team subject matter experts are able to recommend integration options, new methodologies, and/or maturing systems that will enhance International Security and Assistance Force and US Forces-Afghanistan operations.

erations across echelons in the Afghanistan CJOA. The next SFIT is slated to deploy this summer through early next year in order to provide continuous support to JFCs in Afghanistan.

The SFIT incorporates elements collocated with the IJC, the corps-level command in Kabul, and with the RC-E and RC-S headquarters elements. They provide direct support to the IJC and are responsive to the strategic, operational, and tactical units' needs, to include creating concepts of operations, interfacing with staff elements, educating, and general support to enhance theater employment of USSTRATCOM forces and capabilities. SFIT responsibilities include:

- Providing a multi-disciplinary perspective on planning, targeting, deconfliction, and employment for synchronization of space and cyberspace effects in support of theater operations.
- Providing cross-domain integration, planning, and operations expertise through space and cyberspace forward deployed SFIT SMEs and USSTRATCOM reachback support.
- Coordinating specialized reachback (e.g., system SMEs, service capability providers, inter-agency, intel community).
- Identifying additional capability, capacity, tactics, or techniques that may be employed.
- Capturing and applying lessons learned to enhance employment of space and cyberspace effects.
- Identifying opportunities to apply integrated capabilities, services, and effects into planned and on-going theater or regional operations.
- Assisting in developing new capabilities focused on methodologies to employ space control and cyberspace capabilities to support strategic communications and security operations.
- Facilitating information sharing of space and cyberspace activities across theater, regional, and task force-level commands.
- Establishing unity of effort for non-kinetic effects across the evolving organizational landscape.
- Providing substantial STO support expertise to facilitate stand-up of STO facilities for operational planning and execution.
- Providing input to US Joint Forces Command's Joint Center for Operational Analysis to inform lessons learned and doctrine development for non-kinetic operations integration.

The SFIT works directly with units that have tasking authority over USSTRATCOM-presented forces and capabilities to work through the opportunities and can assist in planning, targeting, scheduling, and employment. If additional resources, expertise, development, study, testing, or authorities are required, a key component of the SFIT is its reachback capability to USSTRATCOM and its functional and service components for support. Additionally, the SFIT maintains situational awareness of operations conducted by space and cyberspace units. Without interruption to the tasking authority, the SFIT also enhances operations by responding to requests for additional or enhanced capability, capacity, tactics, or techniques. The SFIT SMEs are able to recommend integration options, new methodologies, and/or maturing systems that will enhance ISAF and USFOR-A operations.

The reachback concept can be a powerful force multiplier if implemented and used properly. The forward element that leverages a reachback capability must consist of subject matter experts who know who to ask for support and know what questions to ask. The SFIT concept is designed to surge these SMEs and provide them a substantial reachback element that spans to the USSTRATCOM enterprise. They leverage reachback expertise for space and cyberspace to satisfy USCENTCOM's mission requirements and to build products, relay, track, update, and deliver improved non-kinetic capacity for the Afghanistan CJOA. Reachback elements consist of USSTRATCOM headquarters, service and functional components, task forces, and centers of excellence (see figure 2). Based on theater requests, this direct support will be communicated at the highest level necessary between USSTRATCOM, USCENTCOM, and supported commanders in Afghanistan.

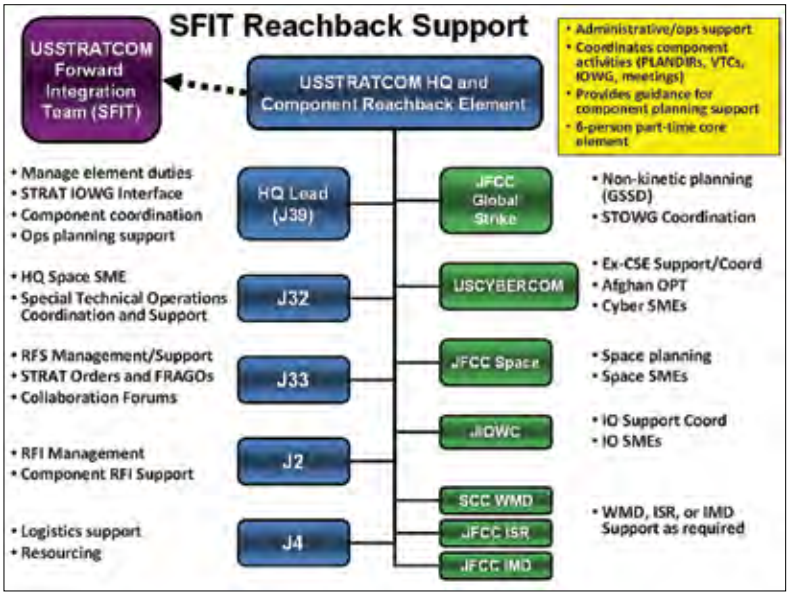


Figure 2. USSTRATCOM reachback construct.

Figure 3. US Air Force A1C Kyle Bridgford verifies network connectivity to the Combined Air and Space Operations Center at an undisclosed location in Southwest Asia, 16 February 2008.

The SFIT concept does not replace, subsume, or duplicate existing organizational constructs engaged in the fight today. JFCs tend to organize based-on combat mediums and the expertise within those mediums. This approach can lead to the development of vertical "cylinders of excellence" with limited horizontal integration or synchronization components. The SFIT includes SMEs that, while possessing substantial training and experience in space and cyber fields, also understand the additional USSTRATCOM non-kinetic core competencies and have established relationships within and across USSTRATCOM headquarters elements and functional/service components. Their expertise can be leveraged at the theater, corps, or regional headquarters level. Given the team's limited size and minimal on-scene support requirements, they represent an agile and rapidly deployable planning and coordination element that can provide immediate integration support to operational commander.

In essence, the supported commander requires skilled planners with appropriate security clearances, and the SFIT provides that capability. Additionally, appropriately cleared and approved working spaces (special compartmented facilities, STO-cells, etc.) telecommunications, and authority to conduct planning and operations is crucial to success. Our teams traveled to each of the RCs and determined only two had any facility in which they could conduct planning, and only one of five had adequately skilled and cleared personnel to conduct space and cyberspace operational planning. Upon conclusion of our initial assessment, we determined no COCOM has all the elements to successfully plan and execute integrated, non-kinetic effects, particularly in space and cyber operations. Therefore, the SFIT offers a small number of USSTRATCOM personnel that can bring to the fight an interim capability for planning to provide the experts needed in IO, space, and cyber operations.

The team provided USFOR-A, ISAF, IJC, and RC leadership access to a team of SMEs focused on effects integration and the maturing of space and cyberspace tactics, techniques, and procedures and capabilities. It aligned USSTRATCOM's reachback/reach-forward resources with presented forces and capabilities to enhance operations in the Afghanistan CJOA. USSTRATCOM will continue to employ the SFIT concept as a means to deliver integrated effects in support of JFCs in multiple geographic regions. In fact, a SFIT deployed in May 2010 to support a US Pacific Command tier one theater exercise in concert with the USCYBERCOM Joint Cyberspace Operations Task Force and the JFCC-Space space control and coordination element to synchronize activities across USSTRATCOM's non-kinetic mission sets. The SFIT, USSTRATCOM's force presentation to JFCs, provides integrated effects. The key elements are skilled personnel in the right numbers, at the right location with adequate planning tools and authority to act.

Brig Gen Michael J. Carey (BA, History, University of Central Florida; MS, Public Administration, University of Oklahoma; MA, National Security and Strategic Studies (with distinction), Naval War College, Newport, Rhode Island) is US Strategic Command, deputy director, Global Operations (DJ3), Global Operations Directorate. He is responsible to the commander on matters of situational awareness, command and control, and integrated plans and operations across space, nuclear, and cyber operations.

General Carey enlisted in the Air Force in 1978 and was later commissioned through the ROTC program in 1983. He has operated the 5D-2 Defense Meteorological Support Program weather satellite, Giant Sapphire space surveillance radar, Atlas I/II/IIA rockets, Colorado Tracking Station, the Minuteman III intercontinental ballistic missile. He has also served as director of Space Forces with deployment experience in support of the Central Air Force commander and chief, Strategic Command Forward Integration Team in support of International Security Assistance Force Headquarters.

The general has held staff assignments at Headquarters Air Force Space Command as politico-military affairs officer, executive officer to the deputy chief of staff for plans, and aide to the commander. He has also served on the Air Staff and for the Directorate for Force Structure, Resources, and Assessment on the Joint Staff. His previous commands include Detachment 7, 750th Space Group, Falcon AFB, Colorado; the 321st Missile Squadron, F.E. Warren AFB, Wyoming; 595th Space Group, Schriever AFB, Colorado; and 90th Space Wing, F.E. Warren AFB, Wyoming. Among his many awards, General Carey has been awarded the Legion of Merit and the Defense Meritorious Service Medal.

Delivering It to the Soldier

Brig Gen Kurt S. Story, USA
Deputy Commanding General for Operations
US Army Space and Missile Defense Command
Army Forces Strategic Command
Peterson AFB, Colorado

Mr. Peter M. Stauffer
Satellite Communications Division Chief
Command Information Office
US Army Space and Missile Defense Command
Army Forces Strategic Command
Peterson AFB, Colorado

National security discussions about cyberspace and space revolve around a few questions. Is there a line that divides the two? Do they merge? Do they overlap? We know that space and cyberspace are independent domains while information derived in or transferred through space assets travels through cyberspace. With cyberspace nodes residing not only in space but also air, land, and sea, cyberspace overlaps and enables activities in all domains.[1] From a Department of Defense (DoD) perspective, cyberspace includes independent networks and infrastructures—including the Internet, telecommunications networks, computer systems, and imbedded processors and controllers.[2] Simply, cyberspace is the "connective tissue"[3] linking units to units up, down, and across the military structure. It seamlessly connects computers to ground stations, ground stations to satellites, and people to people—such as service members in far-away places to their families back home.

The Army sees a future in which America's sons and daughters must prevail across the full spectrum of conflict that stretches from stable peace environments to unstable peace and counterinsurgency operations and all the way to outright war.[4] In an era of persistent conflict, American military forces will find themselves operating under conditions of uncertainty and complexity. The units will maneuver over larger swaths of territory than ever before and will need to be versatile, expeditionary, agile, lethal, and sustainable.

This means that our 21st century Army will increase its cyber demand on the land- and space-based assets that already rely heavily upon the cyberspace domain to pass information. Units increasingly depend upon the information networks that reside in the domain for information, as well as command and control capabilities. These networks include the global information grid, LandWarNet, ground and space collection platforms, and fusion and dissemination capabilities. The networks enable forces to collaborate when needed in near real time. So our reliance on cyber has increased the potential for negative impacts and, if we cannot secure cyberspace and the network to assure the delivery of its enabling capabilities, mission success can be jeopardized. The Army refers to this arena as the cyberspace electromagnetic battleground.[5]

To mitigate these vulnerabilities, DoD is pursuing several strategies: operationally responsive space, multi-domain solutions, and government-academia collaborations to name a few. It is also looking to interagency and intergovernmental partnerships and emerging technology for solutions. This article focuses on these potential solutions and the importance of countering the vulnerabilities.

We begin with an example to illustrate. Private First Class (PFC) Brent Wilson monitored the Force XXI battle command-brigade and below (FBCB2) radios and the intelligence, surveillance, and reconnaissance (ISR) feeds in the special forces operations cell when something caught his attention. He yelled out: "Troops in contact." On that hot August day in 2008 in Iraq, one of the eight special operations teams out on an operation came under fire and needed help. The enemy hit the team with small arms and mortar fire, destroying a truck with communications equipment in it. PFC Wilson noticed the team was unable to communicate, so he began relaying information to its headquarters. He used the FBCB2 to quickly find their grid coordinates. Using the FBCB2, PFC Wilson sent out a flash message, connected with the unit, and thereafter was able to direct the recovery of the engaged unit. His actions led to the capture of four enemy combatants and saved the lives of 12 of his brothers in arms.

The real story here is that PFC Wilson was able to use a space-based communications system to save lives on the battlefield.[6] And, since both the FBCB2 and the satellite to which it was connected reside in the cyber domain, a secure cyber domain enabled PFC Wilson's lifesaving efforts.

From the Past to the Future

During the past eight years of combat in Iraq and Afghanistan, the Army has found itself operating in a hostile environment generally ranging between one of an unstable peace to

Simply, cyberspace is the "connective tissue" linking units to units up, down, and across the military structure. It seamlessly connects computers to ground stations, ground stations to satellites, and people to people—such as service members in far-away places to their families back home.

Figure 1. Fulda Gap area of responsibility in Iraq.

counterinsurgency. Compared to the field of battle a decade earlier, this ground force finds itself maneuvering on a much larger battle field. No longer is a brigade-size unit responsible for a linear, symmetrical, and contiguous battle front like the 378-kilometer Fulda Gap that the 11th Armored Calvary Regiment patrolled during the Cold War. During 2007, one brigade combat team in Iraq estimated that the area of operation was over 31,000 square miles compared to the operation area west of the Fulda Gap that was 100 square miles. Today's Army brigades find themselves responsible for multiple, non-linear and noncontiguous operating areas. The extremely complex network systems that enable this type of operation include: (1) elevated layers of distributed, netted sensors and relays, (2) ISR capabilities that are more responsive to tactical commanders and provide near real-time information, and (3) integrated line-of-site and satellite communications for intra-theater, as well as global communications.

The last eight years have also taught the Army that it must be able to operate in a decentralized fashion. Our current enemy operates within a decentralized manner—this means that we must as well. Also, the missions in the foreseeable future will be carried out more often than not at the lowest levels with fewer Soldiers. So, while the objective may be set by higher headquarters, the execution and success of the mission will be decentralized and will fall to units or soldiers down the chain.[7]

As a result, small-group leaders need the assured communications, ISR, and real-time situational awareness that formerly was located at the higher headquarters—much as the PFC Wilson example illustrates. This need to command, control, and inform forces at subordinate levels across greater distances implicates complex and multi-tiered networks on which information travels. It also impacts the space-based assets and their enabling capabilities, the ground stations that speed satellite data on its way, and the cyberspace that connects the two.

Partnerships and Alliances

Partnerships and alliances offer opportunity to meet head-on some of the threats on this new battleground. For instance, the Purposeful Interference Response Team (PIRT)—which is an interagency group—confers to evaluate the impact of meaconing, intrusion, and jamming (MIJ) on US interests. From that analysis, the team provides options to resolve these incidents. Managed by US Strategic Command, PIRT is composed of representatives from Departments of State, commerce, homeland security, justice, transportation, along with the Office of the Director of National Intelligence, Federal Communications Commission, and other organizations.[8]

Back along the Fulda Border in 1990, a pilot's clipboard had a meaconing, intrusion, jamming, and interference (MIJI) report attached to it.[9] A MIJI event was viewed as a threat to operations. Some would argue that the threat today is even greater based upon the proliferation of counter communications technology—technology that is cheaper, more capable, and easy to obtain on the Internet. Today, the joint spectrum interference resolution (JSIR) requires units and soldiers who experience electronic interference to complete a MIJI-like report and attempt to resolve the problem at the lowest levels feasible. Suspected incidents of hostile interference are reported up the chain to the Joint Spectrum Center or to US Strategic Com-

Figure 2. A sergeant and his soldiers meet with an Afghan community leader.

mand in the case of interference with satellites, ground control sites, and associated user terminals.[10]

It is critical that any interference be reported and resolved. The JSIR process adds to the overall situational awareness on the cyber electromagnetic battleground. Too often, interference is "wished" or "war-gamed" away as just another "blue-on-blue" event and goes unreported. Unfortunately, the result is that no action will be taken when, in reality, leaders need to determine the causes and take appropriate action. Because of the potential effect of an unresolved vulnerability in this area, we must change our old habits and investigate every incident of interference, treating them as hostile until proven otherwise. If the incident is actually hostile in nature, the PIRT acts to resolve the problem.

Why does this process matter? As already mentioned, our military increasingly relies upon cyberspace and electromagnetically enabled capabilities. If the equipment using or delivering those capabilities does not work as it should, our soldiers will find a work-around to get the immediate job done. That is both good news and bad news. The good news is that they are able to figure out alternate or contingency and emergency backups they can use to achieve mission success.[11] The bad news is that soldier solutions may introduce additional vulnerabilities to interception and disruption. Also, if the interference is not reported so that causes can be analyzed, developers cannot design technically sound, standardized solutions to the problem at the enterprise level.

One solution to these technical problems could entail upgrades to equipment like the recent upgrades to the global positioning satellite to make its military signal more jam-resistant.[12] Other solutions might be to perform a counter attack—kinetic or non-kinetic—on the location of the disruption, or simply change tactics, techniques, and procedures. The bottom line is that commanders and their signal officers need to stress the importance of reporting any interference and using JSIR process and PIRT collaboration.

The US is also "building" more robust networks through partnerships with our allies. For example, there are several satellite communication exchange agreements that provide alternative paths in the event of a space or terrestrial outage. The US and Australia signed a memorandum of understanding in 2007 for the joint production and operations of Wideband Global Satellite Communications (WGS). This partnership represents an operational and political union that demonstrates how two is stronger than one.

Emerging Technology

Using Moore's law, processing speed and machines' memory capacity doubles every two years—and processing speed increases demand for data exchange. Developments in the cyber electromagnetic area entreat military and commercial users to take advantage of emerging technology to stay current and to lessen the likelihood of MIJ.

In the case of communications, solutions should be employed from a complete system perspective—space segment, terminal segment, and control segment. The Transformational Satellite Communications System (TSAT) was to provide a very robust space and terminal segment solution. Because of projected costs and scheduled risk, DoD decided to cancel the TSAT program in 2009. This forced DoD to re-look its strategy for robust satellite communications over what is or will become DoD's new legacy systems: advanced extremely high frequency (AEHF), WGS, and Mobile User Objective System (MUOS). Not only must we continue to evaluate and refine tactics, techniques, and procedures, we must seriously evaluate enhancements from emerging technology to our space segments—AEHF, WGS, and MUOS—and to our terminal segments that utilize these critical space assets to enable network centric warfare.

For example, wideband satellite communications systems have utilized dynamic bandwidth allocation for years. Presently, DoD is embarked on the fielding of thousands of Internet protocol terminals at lower echelons where information is generated and consumed in a real-time environment. One technique DoD should employ to protect our communications over WGS is frequency hopping or spread spectrum. These techniques would provide a more robust communications path to ensure the communications are available during electromagnetic interface events.

Still, we must do more. Since AEHF, WGS, and MUOS will be DoD's primary communications for the next 20-plus years, the military services have the opportunity to enhance our existing space segments prior to launches over the next decade. These "investments" come at a price from both a monetary and schedule perspective. The price in robustness can provide many returns in assured communications for the warfighter.

Another example of using emerging technology to mitigate our cyberspace and electromagnetic vulnerabilities are the nano-satellites, built and tested by US Army Space and Missile Defense Command/Army Forces Strategic Command. These satellites, *SMDC One* and *Keystrel Eye* use the latest, state-of-the-art technology. *SMDC One* is being further developed to provide enhanced, assured communications to warfighters. *Keystrel Eye* is a visible imagery satellite demonstrator that offers the tactical-level ground component warrior real-time imagery. Not only will these small satellites provide additional information capability, they will also provide operationally responsive spacecraft for other purposes.

The threats on the cyber-electromagnetic battleground are real. A recent article in the *Washington Post* reported that

Because of the potential effect of an unresolved vulnerability in this area, we must change our old habits and investigate every incident of interference, treating them as hostile until proven otherwise.

Commanders, policy makers, researchers, and developers have an obligation to soldiers like PFC Wilson and his fellow warriors to pursue all avenues that will help ensure networks are fully operational when and where they are needed.

"DoD systems are probed by unauthorized users more than six million times a day."[13] Those systems are worldwide, including the battle fields in Iraq and Afghanistan. Some of those probes are hostile, intended to disrupt the networks and the cyberspace that enable military operations to proceed and succeed. There is no reason to believe that the probes and attacks will cease. Commanders, policy makers, researchers, and developers have an obligation to soldiers like PFC Wilson and his fellow warriors to pursue all avenues that will help ensure networks are fully operational when and where they are needed.

The three areas discussed in this article—forming intergovernmental and international partnerships, promoting JSIR reporting, and harnessing emerging technology—provide a starting point for that pursuit.

Notes:

[1] US Army Training and Doctrine Command (TRADOC) Pamphlet 525-7-8, *Cyberspace Operations Concept Capability Plan 2016-2028*, 22 February 2010, 8.

[2] Deputy Secretary of Defense, memorandum, 12 May 2008.

[3] Michele Flournoy, "Rebalancing the Force: Major Issues for QDR 2010," Center for International Studies, 29 April 2010

[4] TRADOC Pamphlet 525-3-0, *The Army Capstone Concept*, 21 December 2009, 10.

[5] Ibid., 24.

[6] SFC Douglas Wilderman, US Army, "Army Warfighter Panel," *The Army Space Journal* 8, no. 1 (Spring 2009): 29, http://www.smdc-army-forces.army.mil/ASJ/Edition.asp?E=20.

[7] General Martin E. Dempsey, "The Army Capstone Concept and Institutional Adaptation," *Landpower Essay*, no. 10-1, The Institute of Land Warfare, March 2010, 3.

[8] Chairman of the Joint Chiefs of Staff instruction (CJCSI) 3320.02D, 9 January 2009, 8, http://www.dtic.mil/cjcs_directives/cdata/unlimit/3320_02.pdf.

[9] Today, interference is a category that includes meaconing, intrusion, and jamming (MIJ). Thus the acronym MIJ rather than the pre-1992 acronym MIJI.

[10] CJCSI 3320.02D, *Joint Spectrum Interference Resolution*, 9 January 2009, A-4.

[11] PACE – primary, alternate, contingency, emergency. As a standard operating procedure, units should identify their critical systems (weapons, communication, logistical, medical, etc.). After identifying the critical systems, they should designate the alternate, contingency, emergency backups should the primary system be disabled. PACE should be published.

[12] Justin Ray, "First-of-its-kind Satellite for GPS Launched into Space," *Spaceflight Now*, 28 May 2010.

[13] Ellen Nakashima, "New Cyber Command Chief Warms of Possible Attacks: US military networks in war zones could be targeted, …" *The Washington Post*, 4 June 2010, 2.

Brig Gen Kurt S. Story (AA, New Mexico Military Institute; BS, Mercer University; MA, University of Texas) is the deputy commanding general for operations, US Army Space and Missile Defense Command/Army Forces Strategic Command on Peterson AFB, Colorado. He acts for the commander on space, computer network operations, ground-based midcourse defense and integration of theater missile defense. Additionally, he ensures integration and synchronization of all the command's operational space and missile defense activities and assists the commander with command, control, and direction of the Army Service Component Command to US Strategic Command.

General Story's assignments include rifle platoon leader, scout platoon leader, and executive officer, 3rd Infantry Division; executive officer and operations officer, 200th Aviation Company; commander, O and R Troops, 4th Squadron, 11th Armored Cavalry Regiment; deputy commander, Space Defense Operations Center, J-3, US Space Command; S-3 and executive officer, 2nd Squadron, 17th Cavalry, 101st Airborne Division; professor of military science, University of Colorado – Colorado Springs; commander, 4th Squadron, 2nd Armored Cavalry Regiment; G-3 aviation officer, III Corps; chief of staff, US Army Space Command; G3 chief of operations, US Army Space and Missile Defense Command/Army Forces Strategic Command; and commander, 1st Space Brigade. His last assignment was as director of operations (J3), Joint Forces Component Command – Space, Vandenberg AFB, California.

Mr. Peter M. Stauffer (BA, Providence College, Rhode Island; MBA, Mount Saint Mary's College, Rhode Island) is the satellite communications division chief, Command Information Office/G6, US Army Space and Missile Defense Command/Army Forces Strategic Command. He is responsible for executing US Strategic Command-assigned missions that include: Consolidated Wideband Satellite Communications (SATCOM) system expert (SSE), Wideband Global SATCOM (WGS) SSE, Global Broadcast Service SSE, Mobile User Objective System (MUOS) SSE, and operational control of regional SATCOM support centers. He also serves as the US operational project manager for the US/Australia WGS memorandum of understanding. Mr. Stauffer served in the Army as a signal corp officer. He has held several positions within the command since 1989.

Senior Leader Perspective

The Time Has Come for the Bachelor of Science in Cyber Engineering

Dr. Kamal Jabbour, ST
Air Force Senior Scientist, Information Assurance
Air Force Research Laboratory, Information Directorate
Rome, New York

In 1985, Robert Brodsky noted, "The time has come for the [bachelor of science] in astronautics." His call followed a quarter century of space research and exploration made possible by a collaborative cadre of professionals drawn from across a broad spectrum of disciplines. The engineers and scientists who molded the American astronautical effort originated primarily from the aeronautics field. They understood little of rocket propulsion, orbital mechanics, or proximity operations. Yet, in response to executive orders to launch a space program to catch up with the Soviet leading edge, American universities embraced the concept of "rocket science," calling it aeronautics engineering and eventually aerospace engineering, and scurried to develop curricula to support the emerging discipline.

In the same fashion that engineers and scientists recognized the importance of space to national security in the second half of the 20th century, we acknowledge the critical role of cyber engineering to national security in the new millennium. We must evolve from the original concept of cyber security as a *supported* domain into the reality of cyber operations as a *supporting* domain. The US Air Force vision of global vigilance, global reach, and global power requires a cadre of professionals educated with breadth of science, social sciences, and humanities, and depth in physics, engineering, math, and cyber operations, who can meet the challenges of the dynamic domain of cyberspace.[1]

The time has come for the bachelor of science (BS) degree in cyber engineering. The urgency to shorten exponentially the acceptance of cyber engineering as a legitimate discipline derives from the vulnerability of our national security to threats from cyberspace, the superior educational preparation and technical strengths of potential adversaries, the deliberate tendency of American higher education to resist change, and the time lag between creating a curriculum and graduating the first class of students.

This article provides a comparative analysis between the impetus to create the BS in aeronautical engineering and that of a BS in cyber engineering. First, we examine the origins of engineering education in the US leading to the creation of a BS in astronautics. Then, we look at the evolution of computer engineering out of electrical engineering, and examine the circumstances that necessitate a further evolution into cyber engineering.

Evolution of Engineering as an Academic Discipline

Manufacturing of metal goods and scientific instruments for military purposes provided the foundation for the first mechanical engineering academic program in the US at Rensselaer Polytechnic Institute (RPI) in 1824.[2] Continued demand for professionals to oversee the construction of water supplies, defense structures, and transportation networks prompted RPI to award the first civil engineering degree in 1835. Infrastructure and industrial applications dominated engineering education and practice for the subsequent decades.

Although the capital incentives of the Morrill "Land Grant" Act of 1862 spurred the creation of engineering colleges, American engineering educators continued to embrace mechanical and civil engineering principles with emphasis on practical application. In the 1870s, engineering curricula turned progressively more scientific in content, driven increasingly by the needs of an industrialized nation.

The Wickenden Report in 1934 observed that "engineering research in Europe depended on those who studied pure science, while American engineering lagged in the intellectual rigor required to make significant advances in engineering education."[3] In the decade following World War II the American higher education system shifted from adopting European models of education to establishing new academic disciplines. Engineering science entered the mainstream through substantial influx of federal funding for research and graduate education and a renewed emphasis on science and mathematics as foundations for the undergraduate curriculum. In this article, we focus on aeronautic engineering—precursor to aerospace and astronautic engineering, and electrical engineering—precursor to computer and cyber engineering.

Transition From Precursor Engineering Disciplines

The lack of undergraduate degrees in aeronautical engineering did not deter the Wright brothers from building and testing a flying machine in 1903. Foreseeing the potential for air power, theorist Giulio Douhet predicted that "the sky is about to become another battlefield, no less important than the battlefields on land and sea."[4] Yet it took Massachusetts Institute of Technology (MIT) many years to establish the first academic *course* in aeronautics. Taking the lead, the University of Michigan offered the first BS program in aeronautical engineering in 1916

The urgency to shorten exponentially the acceptance of cyber engineering as a legitimate discipline derives from the vulnerability of our national security to threats from cyberspace …

While we have a firm understanding of the persistent qualities of space for aeronautical and astronautical engineering applications, we are only beginning to understand the dynamics of cyberspace.

while MIT offered advanced graduate degrees.

By the end of World War I, military strategists embraced the importance of aircraft to national security and defense, with federal directives giving incentive and financial support for a period of rapid expansion of aeronautical engineering degree programs. By the time the US entered World War II in 1941 American college students were studying aeronautical engineering at 37 BS programs comprised of coursework in physical sciences, mathematics, and engineering science.

The subsequent move to aerospace undergraduate degree programs was equally sluggish. When the Soviet Union launched Sputnik in 1957, American universities started considering changes necessary to deliver academic degrees in aerospace engineering. An aeronautical engineering curriculum provided a solid foundation, but required additional courses in fluid mechanics, stress analysis, chemistry, electrical engineering, gas dynamics, and rocket propulsion.[5] The aerospace engineering degree developed at California Polytechnic Institute (Cal Poly) received accreditation in 1969—11 years after the launch of Jupiter in 1958 and eight years after the manned flight of Project Mercury in 1961. Colleges that supplemented Cal Poly's aerospace engineering program included Virginia Tech, Georgia Tech, University of Kansas, and Iowa State.[6]

The US, the United Kingdom and the Soviet Union recognized space as a defense domain with the signing of the Outer Space Treaty in 1967. Accomplishments of the National Aeronautics and Space Administration—including Moon walks, space station occupancy, collaboration with Russian cosmonauts, and testing of spacecraft systems—provided a sound basis for the BS in astronautical engineering. Twenty years later, the first pure astronautic engineering degree program emerged in the US. Today, only a handful of degree programs educate the cadre of astronautic engineers necessary to "create a space-oriented culture … of … professionals who could directly influence the development of systems and doctrine for use in space operations."[7]

The evolution from electrical engineering towards cyber engineering bears a striking similarity to the birth of astronautics. Thomas Edison employed the financial resources of industry to gain patent rights to the incandescent light bulb in 1880. Academia responded with the BA in electrical engineering in 1894. By the turn of the century the electrical industry and electrical engineers established the profession with an increasingly dependent economy. The formation of the Office of Scientific Research and Development in 1941 and war-time demands for military superiority vectored electrical engineers onto military applications.

Although the history of computing started before World War II, we consider 1948 the watershed year in the evolution of computers. On the technology front, Bell Laboratories tested the first transistor circuit, International Business Machines (IBM) developed the selective sequence electronic calculator that computed eventually the moon-position tables used for the Apollo XI mission, and the University of Manchester built the small-scale experimental machine—"the Baby"—the first stored-program computer. That same year, Claude Shannon defined the bit as the fundamental unit of data in *The Mathematical Theory of Communication*, and Norbert Wiener published the book *Cybernetics*.

It took a quarter century for the first BS degrees in computer engineering to receive accreditation (University of Connecticut in 1972 and Syracuse University in 1973). During that period, IBM developed FORTRAN in 1954, Texas Instruments invented the integrated circuit in 1958, the Advanced Research Projects Agency built the ARPANET in 1969, and Intel released the 4004 microprocessor in 1971.

In all cases, the development of specialized BS degrees followed practical application albeit with the intent of assuring national security. By the late 1950s, engineering deans realized that growth in academic programs came through expansion of graduate programs to support fundamental research that emphasized engineering science, with about 70 percent of all research money from the federal government. The preliminary path to the BS was first via practical and military application, followed by graduate research, then introduction of courses culminating in the undergraduate degree.

Anatomy of an Operational Threat Environment

The operational environment of air—or the absence thereof—differentiates between aeronautics and astronautics. Daniel Bernoulli quantified the physical laws that govern the flight of air-breathing aircraft, while Johannes Kepler derived the laws that govern extra-atmospheric orbiting spacecraft.

While we have a firm understanding of the persistent qualities of space for aeronautical and astronautical engineering applications, we are only beginning to understand the dynamics of cyberspace. In cyberspace, the operational threat environment differentiates between computer engineering and cyber engineering. Computer systems that operate reliably in a permissive and threat-free environment can fail catastrophically in a contested environment where an antagonist seeks intentionally to disrupt, deny, degrade, defeat or destroy these systems.

A cyber attack seeks to achieve the basic objective of modifying the state of a process by modifying the flow of control or the data in the target processor. The modification of the state of a process can cause a processor to execute a different instruction than originally planned, operate on different data, or force an alternate execution path with often-adverse effects.

Early malicious code developers included all elements of a cyber attack—access to a target, command and control (C2),

effects delivery and malware (malicious software or hardware) propagation—in a self-contained package like a worm or a virus. This approach led to decentralized control and decentralized execution of early malware.

Modern developers adopted a modular approach to malware design, breaking up the stages of initial delivery and installation, centralized C2, centralized delivery, and decentralized execution of special-purpose payloads. Initial access seeks to embed malware onto the target computer to modify its flow of control. Following initial access to a computer, the malware may install a lightweight program to provide C2 entry point for additional malware. Finally, effects delivery targets the tenets of information assurance by attacking confidentiality through decryption and theft, integrity through malicious manipulation, and availability through denial or destruction—extending potentially the effects from cyber activity onto missions in other domains.

We categorize cyber threats through the technical capabilities necessary to exploit specification and implementation vulnerabilities in a target system. Supply chain access refers to embedding malicious logic, software or hardware, during manufacturing or delivery of components or systems. Physical access permits an attacker to copy and execute malware onto a machine through routine operation. Remote access without user assistance targets system-level processes on a machine, while user-assisted remote access targets common applications.

The Case for Cyber Engineering

The discriminator between reliability and security creates a requirement for the new field of cyber engineering, rooted in mathematical rigor and immutable science. Mistaking reliability for security led to functional shortcomings in computer engineering education. The curriculum of a typical BS degree in computer engineering includes a general foundation in mathematics, physics, electrical engineering, and computer science, and a specialization in computer hardware, software, and systems. The end product has been a cadre of computer engineers who can design, develop, build, and test *reliable* computer systems. However, the computer engineering curriculum lacks the specialized courses to design, develop, build, or test *secure* computer systems for assured operation in a contested high-threat environment.

The first hints of the limitations of computer engineering surfaced in 1981 with the Elk Cloner, the first computer virus to spread via floppy disks. In 1988, the Morris worm spread across the ARPANET by exploiting vulnerabilities in the Unix operating system. In the quarter century since, millions of malicious programs turned cyberspace into a battlefield, while the academic establishment continued to focus on building reliable systems that turn insecure at first contact with a world full of malevolent actors.

Let us take another look at the role of space in national security. Spurred by the findings of the 2001 Report of the Commission to Assess US National Security Space Management and Organization, the USAF launched a program to develop a space cadre with the intent to "create a space-oriented culture … of … professionals who could directly influence the development of systems and doctrine for use in space operations."[8] In 2004, General Lance W. Lord, commander of the Air Force Space Command at Peterson AFB, Colorado, created a Space Education Consortium to develop the courses and curricula for a rigorous academic program. These developments followed the recommendations of the Commission report that, "Commanders would be better able to exploit the full range of combat capability at their disposal if they were educated from the beginning of their careers in the application of space systems."[9]

In a parallel to space, President George W. Bush declared cyber security a national priority in 2001. Eight years later, a secretary of defense memorandum reiterated that, "Cyberspace and its associated technologies offer unprecedented opportunities to the US and are vital to our nation's security and, by extension, to all aspects of military operations."[10]

Today, almost every weapon system, every industrial control system and every financial transaction depend on cyberspace—an interconnected mesh of fractal entities that generate, process, store, and transmit data. American universities have yet to develop the courses and the curricula to educate engineers to design, develop, build, and test engineering systems for secure operation in a contested cyber environment. The time has come for the BS degree in cyber engineering.[11]

Educational Preparation of Cyber Engineers

Evolving from computer engineering in a permissive threat-free cyber environment towards cyber engineering in a contested cyber environment requires an understanding of cyber vulnerabilities and threats. Information assurance professionals represent risk to information systems as a function of the likelihood of a given threat exercising a particular potential vulnerability, and the resulting impact of that adverse event. We posit that vulnerabilities and threats occur in concert.

Vulnerability is inherently internal to a system. Threat is inherently external to a system. Vulnerability mitigation is often under the control of the system operator. Threat mitigation is mostly beyond the control of the operator. Vulnerability in system specification presents hard mitigation challenges. Vulnerability in system implementation offers lower barriers to successful mitigation.

Cyber engineering curricula must address both the mathematics of sound system specification and the engineering of secure system implementation. Formal methods for design specification and verification address the front end of operation in a contested environment, while designing for testability and mission assurance addresses the system implementation phase.

Using an accredited curriculum in computer engineering as a starting point, we propose the following evolution towards cyber engineering:

1. Increase the mathematical content of the curriculum to at least one course every semester through additional coursework on discrete mathematics, cryptography, and formal methods. Scientists looking for the scientific underpinning of cyber operations are bound to conclude that mathematics forms much of this foundation.

2. Introduce *defensive* design methodology to all engineering design courses, including hardware design (how to prevent, detect, and operate through hardware Trojans); software design (how to prevent, detect, and operate through stack overflows); and system design (how to prevent, detect, and operate through macroscopic vulnerabilities in systems of systems). This change necessitates a sweeping examination, and potential revision, of electrical engineering, computer engineering, and computer science courses to ensure that their content takes into consideration an operationally realistic contested cyber environment.

3. Develop new courses on tactical cyber offense (adversarial access to cyber systems, persistent stealthy operation inside non-cooperative systems, and cross-domain effects delivery through cyber means); operational cyber defense (avoidance and prevention through vulnerability mitigation and threat disruption, timely threat defeat and fight through, survivability and mission assurance); and strategic vigilance (situation and mission awareness, deterrence, and trust).

The complexity of cyberspace and the comprehensive nature of the proposed BS in cyber engineering degree suggest a five-year program of study. The additional year of instruction allows significant mathematical depth, some at the graduate level, to enable the creation of provably invulnerable and resilient systems. A fifth year of education on fundamentals provides a firm preparation for the uncertainty of cyberspace evolution, and prepares cyber engineers to lead in a changing environment.

Conclusions

This article presented a call for development of BS degree programs in cyber engineering to meet the demand for a professional cadre educated on the science of information assurance, and prepared to operate in a contested cyber domain and to assure critical military missions in land, sea, air, and space against threats in cyberspace.

The deliberate pace of change in academia and the inherent pipeline delay between degree creation and student graduation, at a time when potential adversaries hold a clear advantage in technology and manpower, elevate the need for a BS degree in cyber engineering to an urgent matter of national security.

Acknowledgment:
The author expresses his gratitude to Dr. Marla A. Jabbour (PhD in higher education) for her contribution to the historical component of this article.

Notes:

[1] Kamal Jabbour, ST, "Cyber Vision and Cyber Force Development," *Strategic Studies Quarterly*, Spring 2010, 63-73.

[2] The Rensselaer School became the Rensselaer Institute in 1833, and in 1861 the institution became Rensselaer Polytechnic Institute, http://www.rpi.edu/about/history.html.

[3] William E. Wickenden, Report of the Investigation of Engineering Education, 1923-1929, Pittsburgh, Society for the Promotion of Engineering Education, Vol I, 1930, Vol II, 1934.

[4] Ezra Bowen, quoted in *Knights of the Air* (1980), part of *Time-Life's The Epic of Flight* series, 24, 26.

[5] Barnes Warnock McCormick, Conrad F. Newberry, Eric Jumper, eds., *Aerospace Engineering Education During the First Century of Flight*, American Institute of Aeronautics and Astronautics, 2004.

[6] According to the Accreditation Board for Engineering and Technology (ABET), several universities offer accredited undergraduate programs in aerospace or astronautical engineering with origins dating back to the nineteen thirties and forties. A methodical examination of the curricular evolution at these institutions is beyond the scope of this article. Of note, the BS in Astronautical Engineering at the US Air Force Academy received ABET accreditation in 1973.

[7] Report of the Commission to Assess US National Security Space Management and Organization, 2001, http://www.fas.org/spp/military/commission/report.htm.

[8] Ibid.

[9] Ibid.

[10] "Establishment of a Subordinate Unified US Cyber Command Under US Strategic Command for Military Cyberspace Operations," Secretary of Defense, memorandum, 23 June 2009, http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyber_command_gates_memo%5B1%5D.pdf.

[11] Louisiana Tech University plans to launch a BS degree in cyber engineering in fall 2010. The first graduates of this new program are likely to march in the 2014 commencement ceremonies, ushering the way for formal accreditation of the program.

Dr. Kamal Jabbour, ST (BE Electrical Engineering with Distinction, American University of Beirut; PhD Electrical Engineering, University of Salford, UK) a member of the scientific and professional cadre of senior executives, is senior scientist for information assurance, Information Directorate, Air Force Research Laboratory (AFRL), Rome, New York. He serves as the principal scientific authority and independent researcher in the field of information assurance, including defensive information warfare and offensive information warfare technology. He conceives, plans, and advocates major research and development activities, monitors, and guides the quality of scientific and technical resources, and provides expert technical consultation to other Air Force organizations, Department of Defense, and government agencies, universities, and industry.

Dr. Jabbour began his professional career on the computer engineering faculty at Syracuse University, where he taught and conducted research for two decades, including a three-year term as department chairman. In 1999, he joined the Cyber Operations Branch at AFRL through the Intergovernmental Personnel Act, and transitioned gradually from academia to government.

In response to President Bush's National Strategy to Secure Cyberspace, Dr. Jabbour created the Advanced Course in Engineering (ACE) Cyber Security Boot Camp to develop the best ROTC cadets into future cyber security leaders. The ACE combines advanced academic training, hands-on internships, officer development, and weekly eight-mile runs into a challenging cyber security boot camp. The ACE received designation of a Chief of Staff Special Interest Item for its role in developing officers for the new Air Force Cyberspace Command.

Dr. Jabbour has received one US patent, published more than 60 papers in refereed journals and conference proceedings, and supervised 21 theses and dissertations.

Mission Assurance in the Face of Cyber Attacks

Dr. Martin Libicki
Senior Management Scientist
RAND Corporation
Arlington, Virginia

Lt Gen Robert Elder, USAF, retired
Research Professor
George Mason University
Fairfax, Virginia

During the Armed Forces Communications and Electronics Association conference on Cyberspace in January 2010, many Air Force general officers said roughly the same thing when talking about defending against cyber attacks. The goal, they observed, was not so much to defend the network, as it was mission assurance. Some went further to talk explicitly about "fighting through" a cyber attack. This was a welcome development. Everything about the US Air Force—and its sister services—is about getting the mission done. Integrating concerns about the threat to Air Force—and by extension, Department of Defense (DoD) networks—into that rubric marks the maturity of cyberspace as a medium of warfare.

Left unsaid, however, was how to do this. To be sure, there is no lack of knowledge within the Air Force on how to protect its networks and the assets that sit on it. The creation of the 24th Air Force (24 AF) signifies an intensification of this focus. But if mission assurance is *only* about defending networks, why go through the trouble of differentiating the two? Why proclaim a goal of fighting through a cyber attack if confident that such attacks can be defeated before any damage is done?

The reality is that we cannot be confident in stopping all cyber attacks. DoD can try. It may even succeed if the attacks are amateurish, not sustained, and the attackers unlucky. But in cyberspace, offense is cheap and defense is expensive. Attackers have to find the one unguarded hole to get started; defenders have to plug all holes. DoD's global information grid is very large, and not particularly well segmented. Accidents happen.

Thus a plan which provides mission assurance *only by defeating all cyber attacks* is not particularly robust. The Air Force—and by extension DoD—also needs to think about how to carry out its mission in the event that some cyber attacks do, in fact, succeed. Indeed, by thinking carefully about its own use of information—what it really needs, how badly, how quickly, to what level of fidelity, and with what level of confidentiality—it will be better prepared to cope with everyday error, not to mention acquire a better feel for how to prioritize its entire information portfolio.

From an operational perspective, commanders are just as concerned with naturally occurring battlespace degradations as they are with those that are adversary induced. Air crews always prepare to lose elements of support and prepare for operations in degraded communication conditions; however, with increasing dependence on cyberspace for off-board targeting, navigation, and timing, there is a need to establish mechanisms to complete assigned missions when the normal cyber capabilities are contested or congested. This is mission assurance, and achieving this requires close coordination between the air, space, and cyber communities. The first step is to understand that mission assurance is not the same as information assurance, and that mission assurance is the responsibility of every operational commander, not just those responsible for cyberspace operations.

This article lays out some of the steps to solving this problem. It does not and cannot purport to actually solve it. *That* requires an operational/engineering analysis of no small effort. But by laying out the various components of the problem, and making a first-order estimate of their consequences and their seriousness, we hope to indicate how to start addressing the challenge of fighting through cyber attacks.

Such an analysis would serve several purposes. One is to distinguish work-arounds from plan-arounds. Warfighters are a fatalistic lot intimately familiar with Murphy's law; things go wrong especially in warfare, and competent militaries anticipate as much in general terms, keep their options open, and make the best of things. Unfortunately, improvisation only goes so far—which is why contingency planning is also a tried and true aspect of warfare. Such planning, for instance, may reveal single points of failure (SPOF) that need to be hedged. Another purpose is to prioritize cyber defense dollars. Not even DoD can afford perfect defense; if nothing else, excruciating cyber-defense makes operations slow to a crawl. Yet, some facets of mission assurance deserve more resources than others; the trick is to identify them. One of the side-benefits of such analysis, incidentally is to revisit the question of what information is really needed for mission accomplishment—is information that is not worth protecting really worth acquiring? A third purpose is to determine if the difference between mission capability in the

The first step is to understand that mission assurance is not the same as information assurance, and that mission assurance is the responsibility of every operational commander, not just those responsible for cyberspace operations.

An adversary sophisticated enough to carry out serious cyber attacks on US forces may also be capable of carrying out a serious electronic warfare and space warfare campaign.

absence of successful cyber attacks and mission capability in the presence of successful cyber attacks is big enough to warrant a different strategic posture (that is, might cyber threats keep US military forces from doing everything they are expected to do?).

What is the Nature of Threat?

As a general rule, the threats from cyberspace can be grouped into three categories: exploitation, disruption, and corruption. Each of them hinders mission assurance, but each does so differently.

Exploitation is eavesdropping and the consequent theft of data. It is, by far, the most common form of attack against DoD systems. Past thefts have resulted in the loss—more precisely leakage—of at least several terabytes worth of information: "at least" because we only know about the thefts which have been discovered and revealed. Quite possibly, material has leaked over the time it took you to read this paragraph. It would be prudent for defense planners to assume that leakage will occur in wartime as well. Indeed, it would be imprudent to assume that the adversary is not listening into whatever wartime traffic traverses cyberspace. Hence the question: what should warfighters do differently if they suspect that they are, in fact, being listened to?

Disruption makes networks and systems misbehave, run more slowly, or stop running at all. Attacks on Web sites that make them inaccessible (such as happened to Estonia in 2007) are a form of disruption. That noted, disruption is relatively rare in peacetime largely because the rewards from disrupting others are hard to envision. Not so in wartime, when the value of disrupting the other side can be great. Disruption can result from malicious or natural causes to include unintended consequences of seemingly unrelated activities. Hence the question: what should warfighters do differently if they believe that their access to connectivity and network services may be interrupted?

Corruption occurs when data and processes are maliciously altered. It may include data destruction, but, more insidiously, data and (sometimes) processes could be altered so that they look right but work wrong: for example, a false target inserted or a real target deleted. Corruption may be even rarer than disruption in peacetime; in wartime, however, an adroitly planned attack could lead to unexpectedly poor military performance by the target—or worse. Supply chain attacks (supplying corrupted components for systems) raise the possibility that military equipment could be filled with components programmed to fail or to awry when most needed. Hence the question: what should warfighters do differently if they have reason to suspect that the data they are getting from a particular source has been tampered with?

Note that the answers to these three questions are likely to be different from one another. Cyber threats are multi-headed phenomena. Furthermore, today's level of cyber attacks may be a poor guide to what may occur in wartime. Although security practices are likely to intensify in wartime (or comparably elevated infocons), information security often slips in war zones under pressure to carry out missions. Furthermore, whereas cyber-spying has a value in peacetime (and is thus constantly being tried), disruption and corruption primarily benefits the enemy in wartime; only then would threats rise to unprecedented levels.

What is the Extent of the Threat?

Part of a useful planning exercise for mission assurance is to have a rough sense of how bad things are likely to be under a barrage of cyber attacks. An exercise that assumes that every war (or even a particular war) will see the complete collapse of the global information grid, the complete transparency of all communications, and utter corruption of all information that warfighters rely on is likely to be useless (a three-way disaster is, anyway, logically impossible; if the global information grid collapses, how will adversaries be able to eavesdrop on us?). People will not take such an exercise seriously; if they do, they will conclude either that the alternatives are unaffordable or that nothing short of reversion to the warfighting methods of, say, 1960 is likely to be possible.

Planning must therefore consider the art of the possible (for the adversary). This, in turn has two aspects. One is to determine what a highly talented adversary can do and the other is to determine the likelihood that in one or another scenario, such an adversary will, in fact, be present to do this. Cyber skills are not evenly distributed. The US has gotten involved in three wars over the last dozen years and in no case was there a known problem with deliberately induced disruption or corruption (there probably was not much cyber eavesdropping either). The same good luck would probably not characterize a conflict with a near-peer competitor, or even a conflict with a state or nonstate entity supported by such a competitor. Although, as a rule, planning to the maximum threat has its problems (e.g., counter-insurgency is not a lesser included case of major combat operations), it is probably a good start when calculating the cyber threat. Lesser wars have required the US to fight alongside host nation militaries (e.g., Afghanistan, Iraq, and South Vietnam) and this introduces a class of vulnerabilities far more worrisome than working with our traditional allies normally do.

One further caveat. An adversary sophisticated enough to carry out serious cyber attacks on US forces may also be capable of carrying out a serious electronic warfare and space warfare campaign as well. At the very least, therefore, assuming that if terrestrial networks are knocked out by a cyber attack, warfighters can always use point-to-point radio frequency and/or terminal-to-sat communications may be inconsistent if they too, are being imperiled. Conversely, many of the techniques that can be used to assess and improve the ability of US forces to fight through a cyber attack may apply when carrying out similar

assessments of fighting through electronic warfare or threats to space-based capability.

The Role of Exercises

The next step is to simulate such an environment. Quick thought and long experience both suggest that the first good approximation to the cyber attack capabilities of sophisticated adversaries would be those that we, ourselves have (a second approximation would factor in their unique pathologies, as well as attacks they might pull off that would strike us as "unfair"). Such red team tests, however, need to start with good assumptions: for example, what do others know in advance about the role of US systems, what kind of social engineering would they carry out, what on-site access would they have? One of the great benefits of exercises is to highlight capabilities that would be useful should degradations occur; such exercises constitute, in effect, advocacy for mission assurance resourcing.

The blue response should also be exercised. Doing so would provide realism for such a test. Frequent exercises would inculcate warfighters in the smooth application of known responses to cyber attacks. Conversely, permitting up-from-the-ranks responses may also reveal operational work-arounds that might never occur to engineers and planners. It would also suggest how far work-arounds can go in assuring mission performance, and, by subtraction, what plans ought to be made to provide capabilities that on-the-spot work-arounds cannot adequately address. Perhaps needless to add, these have to be exercises that, like other exercises, focus on mission accomplishment rather than simply test how users and systems administrators react to cyber attack. Indeed, better results may result from *not* highlighting the cyber elements of play. If planners wish to exercise the ability to carry out missions while adversaries are lurking and listening on the network, some provision should be made to play an over-informed adversary (if not by using a real opposing force then through scripts that reflect information gleaned in real-time from blue forces through red eavesdropping).

Mission Assurance if Someone's Listening

As long as networks work, missions can be carried out (e.g., the airplanes fly) whether or not someone is listening in. However, an over-informed adversary is a tougher adversary (e.g., the airplanes fail to find the now-hidden target) and thus the advesary's ability to tap defense networks can imperil mission assurance. Red teaming may indicate the likelihood of adversary listening posts within various networks (presumably less for classified networks, and more for unclassified ones) and the degree to which information can be exfiltrated in near real time. Overall, an estimate that unclassified networks are being listened in on is a prudent one.

The next question to answer is how such penetration may affect mission assurance and what might be done to minimize the impact—hence OPSEC. A key question is the extent to which sensitive information (e.g., troop movements) are echoed onto the NIPRnet and the extent to which forces, alerted to that possibility, can tighten up on communications (without such precautions getting in the way of actually carrying out their missions). A question from another angle is whether the deliberate insertion of false information into the flow of one's own chatter can either mislead or at least confuse whoever is listening without doing the same to one's own.

Mission Assurance in the Face of Uncertain Networks

Cyber attacks are likely to constitute only one risk to the continuity of communications: threats from jamming and physical destruction have to be factored in as well. Physical threats are often dealt with through redundancy—multiple lines out of a base, stand-by spectrum. Similar redundancy can mitigate the risk from some cyber attacks (if the Internet is down, then phone and fax might work). But the *type* of redundancy is different. Three networks running the same protocol may offer no more protection against a clever cyber attack than running just one network would. Heterogeneity rather than duplication is the key, but heterogeneity is not necessarily beloved by systems administrators since it multiplies their work and even complicates the application of security protocols (e.g., configuration management, patch application). Furthermore, the pattern of faults induced by a cyber attack is different from those associated with physical attacks. On the one hand, they can take place with near-zero warning; on the other hand, as cyber attacks, they tend to be temporary. Cyber attacks may permit the network to operate but eliminate address updating, cause messages to be randomly misdirected, or eliminate important support services such as authentication (leaving operators contemplating whether to run networks without it for a while, and risk deeper contamination).

Serious operational engineering may be needed to gauge the vulnerability of missions to network problems. Such an analysis might take operations at a high level of aggregation (e.g., interdiction) and then determine what supporting operations have to be carried out to make such an operation possible (e.g., air tasking order planning, target acquisition, logistics, etc.). These supporting operations can be hierarchically decomposed into their own subordinate operations. Using a strategy-to-task framework, subsequent steps would determine what information is needed to support such operations, how timely it has to be, where it comes from, and what communications are needed to deliver it. Further analysis would indicate what has to be communicated *from* mission planning for adequate command-and-control. With that, one can start establishing the relative criticality of various information flows and the prospects for alternatives to limit the risk to mission assurance from network outages. Granted, such an analysis might not do justice to the

Cyber attacks are likely to constitute only one risk to the continuity of communications: threats from jamming and physical destruction have to be factored in as well.

intermittent impediments to informal give-and-take that is hard to measure but nevertheless critical to mission accomplishment, but that may be exactly the kind of problem that real-time workarounds can address or at least illuminate.

The results should consider not only the cyber networks themselves, but also the ability of the normally interconnected systems to function with limited connectivity and the backup tactics, techniques, and procedures for the agile and adaptable human network to accommodate these problems. They should then inform communications decisions such as network architecture, heterogeneity, as well as storage, bandwidth, and caching strategies.

Mission Assurance in the Face of Corruption

Similar, almost identical, analyses can indicate the sensitivity of mission accomplishment to corrupt data (and, to some extent, algorithms)—by substituting "accuracy" for "timeliness" in the prior paragraph. Remediation planning is quite different, though. Many of them entail data authentication strategies (e.g., where should digital signatures be applied), file replication, and selected redundancy (e.g., checking flows data against stocks data). Other strategies entail the use of reasonableness tests and the development of sophisticated algorithms that may suggest the possibility of corruption. The search for corruption also plays a role in after-action analysis: if a mission failed, are there ways to determine whether deliberately corrupted data (or algorithms) played a role?

The issue of supply-chain attacks is a trickier issue. Very few have been found, and those that have induced the greatest suspicion are designed to permit eavesdropping rather than induce failure. It is also difficult to distinguish a rogue component that is induced to fail from one that was simply not built well in the first place (i.e., a cheaper but counterfeit product that does not meet specifications). A strategy to minimize such attacks (i.e., through component inspection) may be warranted, but one to work around such attacks may be too hard for now.

The Role of Training

There is a reluctance to degrade our sensors or the systems that provide situational awareness and support operational decision-making because of concerns that this would lead to loss of training or endanger safety. While it is important to ensure that safeguards are in place to conduct activities safely, we potentially endanger Airmen by leading them to become excessively dependent on their systems. Pilots have long been taught to trust their instruments, but not to depend on any single instrument as their single source of information. However, we are increasingly training our aircrew members as system operators rather than pilots or navigators. This works well when the systems are working properly. On the other hand, most key positions on an air operations center operations floor maintain manual backups to allow them to continue their work when a system goes down. Again, this assumes a loss of some capability, but not a total loss of connectivity. These time-tested approaches to military operations can be adapted to be relevant to 21st century integrated air, space, and cyber operations.

Conclusions

If we mean what we say about mission assurance, then the aerospace community has to understand what it means to operate in an environment degraded by cyber attacks and how to overcome such impediments. This is an effort in which the Air Force Space Command and its 24 AF play a critical role, not least by creating realistic scenarios to plan against. But the problem is one that must be owned by operators across the aerospace spectrum, as well as warfighters in other media. It goes to the heart of warfighting and cannot be delegated to specialists.

Dr. Martin Libicki (MCP, City Planning, University of California, Berkley; PhD, University of California, Berkeley) is a senior management scientist at RAND since 1998, focusing on the impacts of information technology on domestic and national security. This work is documented in commercially published books, *Conquest in Cyberspace: National Security and Information Warfare*, and *Information Technology Standards: Quest for the Common Byte,* as well as in numerous monographs, notably *Cyber-Deterrence and Cyber-War, The Costs and Benefits of Moving to the ICD-10 Code Sets, How Terrorist Groups End* (with Seth Jones), and *Who Runs What in the Global Information Grid*. He was also the editor of the RAND textbook, *New Challenges New Tools for Defense Decisionmaking*. His most recent assignments were on the subjects of multi-factor authentication, organizing the Air Force for cyber-war, exploiting cell phones in counter-insurgency, developing a post-9/11 information technology strategy for the US Department of Justice, using biometrics for identity management, assessing DARPA's Terrorist Information Awareness program, conducting information security analysis for the FBI, and evaluating In-Q-Tel. Prior employment includes 12 years at the National Defense University, three years on the Navy Staff as program sponsor for industrial preparedness, and three years as a policy analyst for the General Accounting Office's Energy and Minerals Division.

Lt Gen Robert J. Elder, USAF, retired (BS, Electrical Engineering, University of Detroit, Michigan; MS, Engineering, University of Detroit; PhD, Engineering, University of Detroit) joined the research faculty at George Mason University following his retirement from the Air Force in July 2009 as the 47th commander of 8th Air Force. General Elder served as the first commander of Air Force Network Operations and led the development of the cyberspace mission for the Air Force. He also served as the air operations center commander and deputy air component commander for Operations Enduring Freedom and Iraqi Freedom. He has held senior leadership positions with the Joint Staff, Air Force staff, and NATO and served as the commandant of the Air War College.

Cybersecurity: Challenging Questions with Incomplete Answers

Mr. Jeff Kueter
President, George C. Marshall Institute
Arlington, Virginia

The mid-May 2010 confirmation of General Keith Alexander to head the Pentagon's newly formed US Cyber Command (USCYBERCOM) brought a temporary reprieve to the barrage of questions surrounding the purpose, mission, and planned activities of the Department of Defense's (DoD) effort to secure and defend cyberspace. General Alexander's confirmation was delayed for months by what press accounts described as "questions on the Hill over exactly what the command's roles, authorities, and operational scope would be" and he was confirmed "even though the administration has not fully resolved policy issues governing offensive action in cyberspace."[1] In other words, the fundamental concerns that delayed the confirmation for months remain unresolved and likely will subject the new command to intense oversight from Congress and an array of interest groups.

The seriousness of the cyber security threat is widely recognized. High publicity events keep the issue on the front pages. For example, Google's partnership with the National Security Agency in the wake of the well publicized attacks on the ubiquitous Internet site was front-page news.[2] In early 2010, McAfee released a survey report documenting the widespread and diverse nature of cyber attacks, which concluded that 80 percent of information technology executives believed a serious cyber attack would occur in the next five years.[3] A 2009 McAfee report prepared by Mr. Paul Kurtz, a former White House Homeland Security adviser, found that many countries are preparing to engage in cyber warfare and espionage creating conditions for the emergence of a 'Cyber Cold War.'[4] These and similar findings routinely make their way to the front of television broadcasts and into prominent newspapers and Web sites.

To say that the Internet has transformed society is as obvious as acknowledging its vulnerability. The average American, and consequently, the average American's congressman and their staffs, recognize both but lack appreciation, understanding, and insight of the issues involved and the costs and consequences of the available options. Policy makers and the public lack the detailed knowledge required to critically judge what can or should be done to address its weaknesses and vulnerabilities. That fact coupled with the immaturity of the policy consensus on what to do explains the intensity of the questioning of General Alexander and the broader concerns about the government's plans for defending cyberspace.

An individual's daily interactions with the Internet define their perceptions of the security concerns, and the broader framework of public policy issues shapes how they view the role of government. Protection of identity, financial information, and privacy dominate the individual citizen's worries about securing cyberspace. And those worries get communicated directly and indirectly (through direct contacts, public opinion surveys, or the news media, for example) to policy makers and their staffs, which in turn, shape their perceptions about priorities. It is no surprise then that proposed government actions are judged in part by how they will affect these individual level factors.

If the importance of cyberspace to American military and economic power is not in dispute, neither is the need for government to take steps to protect American interests in cyberspace. The generality of such a statement enables the formation of consensus in support of it. Parsing it reveals the fissures. What are American interests in cyberspace? Should government protect commercial networks? What are the limits on governmental authority over private communications? What are the limits of US government authority over international networks and systems? How will government action be coordinated between military and civilian agencies? What constitutes offensive action? Are there salient differences between offensive and defensive actions in cyberspace? Who makes the decision to initiate offensive actions?

These questions and many others emerged over the past few months as congressional staff, policy analysts, journalists, and the public considered the implications of the new USCYBERCOM. Most remain unresolved. Many require the emergence of a national consensus that shows little signs of developing. The Comprehensive National Cybersecurity Initiative, launched by President George W. Bush and expanded by President Barack Obama, is a vehicle to marshal thinking on these and related topics. Nevertheless, perhaps it will craft the needed consensus, but that remains an ongoing and incomplete effort. Recognizing these questions and the issues involved is essential as the DoD's USCYBERCOM begins its work in earnest for they will remain areas of key concern for congressional oversight and public interest in the months to come.

Challenging Questions

Despite widespread agreement that a cyber command was required, General Alexander's confirmation was delayed nearly six months from the Pentagon's October 2009 target date. News accounts of the confirmation process left little doubt that the delay was the result of lingering questions about the role of the command and approaches for addressing cybersecurity challenges. General Alexander's published replies to 28 questions submitted by the Congress reveal the breadth of concerns. They are roughly divisible into the following topics: (1) organization of the command and reporting and oversight requirements, (2) extent of the command's authority, (3) operations and tactics, and (4) strategy.

Organizational Concerns

Establishing a new governmental authority raises a host of organizational concerns. Notably, to whom does the organization answer and how is it funded. In its *Cyberspace Policy Review*, the Obama administration openly acknowledged the need for greater coordination and integration among governmental entities. They point out that: "Responsibilities for cybersecurity are distributed

across a wide array of federal departments and agencies, many with overlapping authorities, and none with sufficient decision authority to direct actions that deal with often conflicting issues in a consistent way."[5] To address this fragmentation, the Obama administration empowered a special assistant to the president and a cybersecurity coordinator and established a cybersecurity office within the National Security Council to oversee, direct, and coordinate responses across the federal government. The *Cyberspace Policy Review* speaks of the need to enhance the federal government's partnership with the private sector and to work closely with "like-minded" nations.

Despite these efforts, the Government Accountability Office recently criticized the government for failing to define agency roles and responsibilities and called for the creation of standards to judge progress for those plans that are developed. A cyber wargame sponsored by the Bipartisan Policy Center plainly revealed the limited coordination presently in place, as well as the paucity of thinking about how to respond to serious cyber attacks at the highest levels of government.[6]

Specific to the DoD's efforts, General Alexander's answers to the Congress on this point were straightforward— USCYBERCOM reports to US Strategic Command, but will "work closely" with a host of senior DoD leaders and "coordinate" activities with the armed services, as well as the intelligence community, civilian agencies, and the private sector. Effectively coordinating activities across department and agency lines is easier planned than accomplished, which is a fact that seasoned congressional staffers and policy observers are well aware of and are assured to follow with close attention.

Of particular concern to the Congress was the acquisition authority of the new command. In several different questions they probe for clarification on this point, asking how the "dual-hat" nature of the new position would influence acquisition and procurement practices among the affected agencies. General Alexander's answers assured lawmakers that there would be no confusion of appropriations authority. Legislators are protective of the appropriations process and their power to direct it. Six congressional committees have asserted jurisdiction over cybersecurity policy and budgets. As the government begins procuring hardware and funding technology development, strict congressional scrutiny of those expenditures is virtually certain.

Extent of Authority

Organizational questions pique the interest of staffers and policy wonks, but questions regarding how the government will protect cyberspace resonate with the general public. Legal regimes governing cyberspace are poorly developed and detailed policy guidance remains to be crafted. Steps taken over the next few years will literally break new ground in defining the government's roles and responsibilities.

With respect to defending government information systems and networks, there is little question about the appropriateness of government action. Adding definition to areas of responsibility, limits of authority, and channels for oversight are current challenges, lending to a blending with organizational concerns. The Congress is particularly interested in how the intelligence community will interact with the new military command and with how the military's efforts will interact with civilian agencies. The role of the National Security Agency (NSA) as a partner for USCYBERCOM, specifically, and as a contributor to the US cyberspace response, generally, is a particularly controversial topic. The NSA brings unique skills and extensive experience to the challenge, but its controversial past, particularly allegations of warrantless wiretapping, is cited as a source of anxiety.[7]

When the focus becomes the defense of private networks, how far the government can or should go become much murkier. The USCYBERCOM's mission is "to secure our freedom of action in cyber space and mitigate the risks to our national security that come from our dependence on cyberspace and the associated threats and vulnerabilities."[8,9] General Alexander told the Congress that USCYBERCOM's mission did not include the defense of .gov and .com domains, but suggested they would prepare to "provide military options" to protect those domains if requested by the president or the secretary of defense. That reply implies recognition that the interconnection of information networks and government reliance on private networks will eventually require a broad mandate for the command.

The nature of information networks and the threats posed to them raises concerns that the limited view is unsustainable and it is inevitable that military and intelligence assets will be drawn into the defense of other governmental networks, as well as private ones. If government relies on a commercial network to meet a government need, should or will the government take steps to protect and defend it? The answer appears under development.

Operations

General Alexander said the major challenge facing USCYBERCOM is "improving the defense of our military networks as they exist today" and that improvement requires "much greater situational awareness and real-time visibility of intrusions into our networks."[11] More broadly, the controversy is the role offensive actions will play in the planned defense of US government and related computer networks. Put another way, the balance between defense and offense in US cyberwarfare plans matters.

The Congress is clearly interested in issues surrounding offensive cyber operations. They posed several questions to General Alexander touching on the topic, including how offensive operations would be authorized and by whom and whether the use of force in cyberspace is affected by the War Powers Act or the United Nations Charter. Those questions reach to the heart of oversight in matters of war particularly if offensive cyberoperations might potentially lead to a cyber or shooting war.

Additionally, they raised the challenge of attribution and the implications for the lawful employment of force. The Congress was particularly interested in how the sources of cyber attacks could be distinguished between foreign governments or sub-national groups (such as criminal organizations or terrorist groups) residing in any particular location. Detecting the source of a cyber attack is technically demanding and may prove impossible to guarantee consistently as the sophistication of attacks continues to grow. Those difficulties suggest that defense will be the principal focus of US efforts, which is the general thrust of answers provided to Congress by General Alexander.[12] The range of offensive options available or planned remains unclear as are details about how or when they might be used.

The interconnections between computer networks that cross

national boundaries present additional challenges. Government networks are connected with private networks and, in turn, both are connected with foreign networks. These connections will complicate offensive actions, as well as defensive approaches. On the offense, an adversary may not maintain separate civilian and military networks, complicating the selection of 'targets' and limiting damage. An even greater complication arises when that adversary relies on foreign or multi-national networks. US planners will need to assess to what extent US offensive or defensive actions should degrade or destroy those networks and strategies for handling the inevitable diplomatic and public relations fallout arising from whatever actions they take.

Strategy

The National Military Strategy for Cyberspace Operations calls for US superiority in cyberspace to guarantee freedom of action and ability to deny similar freedom to prospective adversaries.[13] In its questions, the Congress asks if this remains the objective of US policy. General Alexander's answer was not provided publicly, but elsewhere he acknowledged the military's goal of cyberspace 'superiority,' which he distinguished from 'dominance or supremacy.'[14] In other contexts, notably space, demands for US superiority is seen as aggressive and destabilizing, and believed to generate fear of US actions and distrust of US motives.

As the USCYBERCOM evolves, reactions from other governments and non-governmental organizations will define the parameters of future strategic discussions. Early indicators of objections along these lines are visible in the late 2009 press accounts of emerging US-Russian talks on cybersecurity issues at a United Nations forum. *The New York Times* reported the US had acceded to a Russian request to discuss the issues in a United Nations committee on disarmament and international security.[15] Among Russia's desires was a 'ban on offensive cyberweapons.' In a June 2010 speech at the Center for Strategic and International Security, General Alexander cited the Obama administration's support for opening talks with the Russians.[16] Whether talks are imminent or not, these reports suggest familiar Cold War concepts—banning offensive action despite verification and enforcement uncertainties—may form the starting point for international discussions.

Application of another Cold War artifact can be seen in attempts to construct a deterrence framework for cyberspace. Some believe a mutually assured destruction approach can be applied to cyberspace because the costs of cyber warfare among the great powers would be too high as are the prospects a cyber war escalating to actual hostilities.[17] Others see little prospect for cyberdeterrence, citing "attribution, predictable response, the ability to continue attack, and the lack of a counterforce option" as "significant barriers."[18] When asked by Congress whether he believed the US had demonstrated capabilities that would deter potential adversaries, General Alexander replied "not in any significant way," noting that it was not yet possible to ascertain whether US responses, exercises, and war games would or have deterred the criminal, terrorist or state actors that operate in cyberspace.[19]

Conclusion

Crafting effective responses to the security challenges posed by cyberspace is complicated by a host of perceptual and practical questions, the answers to which are unclear and subject to considerable disagreement and debate. The issues discussed are only a sample of those raised over the last several years as recognition of the need for government action has grown. Still, the lack of clear consensus across a range of issues will stimulate political and policy debates for years to come. The challenge for USCYBERCOM, as well as the other elements of the US government and the private sector charged with erecting defenses to cyberattacks, will be operating effectively in an arena where being second-guessed and regularly criticized unfortunately will be a fact of life.

Notes:

[1] Ellen Nakashima, "Gen Keith Alexander Confirmed to Head CyberCommand," *Washington Post*, 11 May 2010.

[2] Ellen Nakashima, "Google to Enlist NSA to Ward Off Attacks," *Washington Post*, 4 February 2010.

[3] Stewart Baker, *In The Crossfire: Critical Infrastructure in the Age of Cyber War*, 2010.

[4] Elinor Mills, "Report: Countries Prepping for Cyberwar," *CNN.com*, 17 November 2009, http://www.cnn.com/2009/TECH/11/17/cnet.cyberwar.internet/index.html.

[5] The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, 2009, i, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[6] Ellen Nakashima, "War Game Reveals US Lacks Cyber-Crisis Skills," *Washington Post*, 17 February 2010.

[7] Ellen Nakashima, "Pentagon Computer Network Defense Command Delayed by Congressional Concerns," *Washington Post*, 3 January 2010.

[8] Advance Questions for Lt Gen Keith Alexander, Nominee for Commander, US Cyber Command, (2010): 1.

[9] Ironically, a nearly identical set of statements can be easily found describing the goals of the nation's space policy.

[10] Advance Questions for Lt Gen Keith Alexander, 19.

[11] Ibid., 8.

[12] Ibid., 12.

[13] *The National Military Strategy for Cyberspace Operations*, December 2006, http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf.

[14] Advance Questions for Lt Gen Keith Alexander, 18.

[15] John Markoff and Andrew Kramer, "In Shift, US Talks to Russia on Internet Security," *New York Times*, 13 December 2009.

[16] Siobhan Gorman, "US Backs Talks on Cyber Warfare," *Wall Street Journal*, 4 June 2010.

[17] Shane Harris, "The Cyberwar Plan," *National Journal*, 14 November 2009.

[18] Martin Libicki, *Cyberdeterrence and Cyberwar*, (RAND Corp: Santa Monica, CA, 2009): xix.

[19] Advance Questions for Lt Gen Keith Alexander, 21.

Mr. Jeff Kueter (BA, Political Science and Economics, University of Iowa; MA, Security Policy Studies and Science and Technology Studies, The George Washington University; and MA, Political Science, The George Washington University) is president of the George C. Marshall Institute, a public policy institute focused on scientific and technical issues impacting public policy. An expert on space security and missile defense, he has testified on both before the US Congress, serves as a contributor on strategic issues for the print and television media, and is the author of analytical pieces exploring aspects of the space security and missile defense debates.

Focused on national security and energy/environment policy, Mr. Kueter manages the day-to-day operations of the George C. Marshall Institute, authors its policy papers and analyses and engages the public and the policy making community.

Exploring the Complementary Nature of Cyber and Space Operations

Mr. Joshua T. Hartman
Senior Fellow
Center for Strategic and International Studies
Washington DC

Over the last two decades the nature of warfare has changed dramatically. Technology and capability advances, driven largely outside of the Department of Defense (DoD), have forced a reassessment of our security advantages and vulnerabilities in space and cyberspace. Technology application from these areas broadens the number of options available to manage and overcome potential adversaries. However, greater dependence on space and cyber systems coupled with an inability to prevent adversaries from marginalizing these systems creates new challenges in maintaining security. An understanding of how to leverage and integrate operations between these domains will provide the US with valuable capabilities in the joint fight.

The purpose of this article is to add to the foundation of thought regarding the deployment of space and cyber operations in the context of each other. It is designed to stimulate discussion on how operations within these two domains could and could not be complementary. As such, the analysis provides a comparison of space and cyber operations in two ways. First, it considers the use of space and cyber capabilities through the six functions common to joint operations.[1] Second, it discusses the employment of space and cyber operations through the six phases of joint campaign operations.[2]

For the purposes of this article, I define space operations to include the tactics, systems, planning, and effects associated with counterspace, space protection, and force enhancement missions. The domain of space is a physical space starting at an altitude of 100 kilometers extending beyond geosynchronous orbit. I define cyber operations as the tactics, systems, planning, and effects associated with network defense, exploitation, and attack. The domain of cyber is a physical space existing within designated information technology (IT) infrastructure or data paths. The assessment assumes a US policy that will limit space operations such as to minimize debris creation and allow cyber options to provide full spectrum effects, as the capability will allow.

Joint Functions

Joint Publication (JP) 3-0 provides the lens that joint warfighters attempt to view any contribution to the battlespace. In it, six joint functions categorize the activities necessary to integrate and synchronize all combatants through the multiple domains leveraged during operations. The six functions include: command and control (C2), intelligence, fires, movement and maneuver (M2), protection, and sustainment. A skilled commander determines the mix and emphasis of each function in the context of all domains. Therefore, understanding space and cyber operations in this joint context becomes important to both the joint commander and the forces in each domain.

C2 enables direction by a commander over assigned and attached forces in the accomplishment of the mission. This function provides status of information, allows command of subordinate units, facilitates planning, and produces the coordination of operations and capabilities. C2 could not occur without space and cyber. All space and cyber operations are structured in some form around information. The three missions from each domain require, and in many ways facilitate, the unimpeded access to and flow of information. Space protection and network defense becomes the most important mission to ensure continuity of C2 from space and cyber perspectives.

Intelligence provides an understanding of the operational environment. It informs when, how, why, where, and what effects to produce. Intelligence assets require tasking, collection, processing, exploitation, and dissemination (TCPED) of information. Space and cyber systems collectively provide the core functionality of the TCPED process. Focusing on force enhancement and network exploitation missions, space and cyber operations become the primary provider of technical intelligence data. Systems from each domain create access and persistence that enables broad and robust intelligence collection capability. Used in a coordinated manner, they create a complementary intelligence insight that neither could perform separately. For example, space provides a good source for strategic and operational intelligence, while cyber can provide good insight on intent, force structure, or system parameters at a much lower level. Each provides a piece of the puzzle and together the larger context begins to form.

The ***fires function*** leverages weapon systems to provide lethal or non-lethal effects on specific targets. Space, in its force enhancement mission, provides targeting solutions, battle damage assessment and has played an increasing role in providing joint fire support to other domains. Additionally, space systems offer strategic attack through offensive counterspace missions.

... greater dependence on space and cyber systems coupled with an inability to prevent adversaries from marginalizing these systems creates new challenges in maintaining security.

Cyber systems, through network exploitation and attack missions, will provide joint fire support to other domain operations either separately or in synchronization of other domain systems, to interdict enemy capabilities, conduct strategic attack, and employ information operations. In so much as space effects are limited by policy, I offer that the key difference between space and cyber in the fires function lies in cyber's ability to provide strategic attack effects outside of its domain. However, coordinated use of space and cyber will still allow for increased synchronization of forces and effects across multiple domains.

M2 pursues positional advantages prior to or during operations. Both space and cyber provide unique advantage to M2 over other systems. Given the reach and connectivity of these domains, space and cyber operations provide a positional speed, access, and persistence that cannot be replicated in other domains. Space and cyber architectures provide flexibility in physical deployment and operation that can be leveraged in a relatively non-threatening or escalatory manner prior to operations. However, the concept of M2 differs in space and cyber from that of other domains. The use of a distributed architecture and interconnectivity between multiple nodes allows for M2 of information, as well as assets, creating additional options (and threats) for the joint commander.

Protection involves ensuring joint force capabilities through a number of warfighting tasks. In protection of themselves in the space protection and network defense missions, space and cyber systems may run operations with active and passive measures. Given the nature of technology and the use of data as a commodity in each domain, many of these measures are similar if not the same. It should be noted, while the increased use of space and cyber systems in a distributed architecture provide great advances in capability, it also creates a large and complex protection task. In protection of force structure outside of the domain, the contribution of each would depend largely on the task, but space is likely to play a much larger role (the primary cyber role for this function is operations security). For example, in a personnel recovery mission, cyber is unlikely to play a role, while space intelligence systems will play a significant role in locating and supporting extraction of the personnel. At a strategic, level the use of each domain provides an efficiency of force, enabling a smaller physical presence and corresponding force protection requirement.

Sustainment ensures the continued availability of logistical supplies and personnel required to maintain the mission for an extended period. Today neither domain plays a significant role in this function. However, the future will see an increased use in DoD for the sustainment function. For example, DoD is growing the use of radio-frequency identification for logistical processes and supply chain management. Additionally, cyber systems will play a greater role as systems like the joint strike fighter becomes operational, downloading maintenance status and depot requirements to computers on the ground prior to landing.

Joint Campaign Phases

Major operations typically incorporate the full spectrum of joint functions. Their success depends upon the consideration and integration of diplomatic, informational, military, and economic aspects of the environment. To characterize the potential scope of any operation, JP 3-0 discusses six phases of a joint operation, shown in figure 1. While not all six phases will be fully represented in an individual operation, an assessment of space and cyber across each will provide a useful basis to discuss the contribution of space and cyber operations in each.

Phase 0 – Shape

During the Phase 0, activities are design to create a strategic environment that will prevent hostilities from occurring, to include strategic deterrence. This phase will solidify relationships with partners and allies. A primary objective of Phase 0 is to collect and portray information that will influence perceptions and behavior of adversaries and allies. Shaping activities should start long before hostilities are expected and are best integrated as common practice rather than crisis management procedures.

Space and cyber operations have several similarities during and can be extremely useful for informing Phase 0 activities. In each domain, information is the primary commodity. Therefore, space and cyber systems become effective tools for execution of information campaigns in the US, as well as allied and adversary countries. Each capability provides access and persistence for intelligence collection and strategic communication that is essential prior to hostilities. Moreover, proper leverage of and coordination between each domain will aide development and communication of perceptions on adversary intent, as well as establishing specific national and military objectives for future phases (these benefits and similarities remain available throughout all six phases).

Additionally, in near-peer conflict our cyber and space systems are likely to be the initial target of any aggressive adversarial action. Adversaries will attempt to

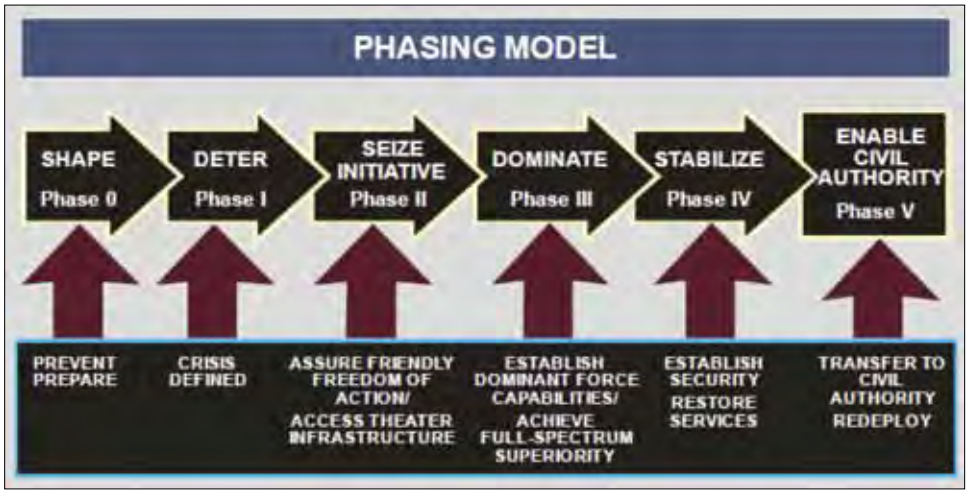


Figure 1. Joint campaign phases.

For conventional conflicts, while forces in each domain must work together, space will be the most useful opportunity in providing information on an adversary build-up toward operation.

monitor US space and cyber activity as they develop operational plans. This provides the US an opportunity to establish false operating patterns or confuse adversaries by changing space and cyber operating patterns prior to hostilities.

Neither space nor cyber provide a good form of strategic deterrence for Phase 0. Attribution for each domain is extremely difficult to establish. Moreover, asymmetries in each domain, and a lack of internationally accepted norms make the cost-benefit of taking action favor non-US actors.

Space systems provide a much better opportunity to shape partnerships and allies' perceptions. Many countries are familiar with space data, have access to commercial equivalents, or have working agreements in place for data sharing. Cyber operations lack the maturity for that level of familiarization, development of commercial equivalents, or establishment of data sharing arrangements.

The nature of the cyber domain allows the shaping function to go much further than that of space operations. Using cyber, a state may generate content or activity that destabilizes the internal situation of an undesirable adversary, creating a distraction or shift in the strategic environment. This in turn may convince a potential adversary that the strategic situation is not favorable for conflict or may change priorities of that adversary.

Phase I – Deter

Phase I can be characterized by deterring a potential adversary from action, while demonstrating one's own capabilities and resolve. This form of deterrence, different from the strategic deterrence associated with Phase 0, focuses on carrying out the actions necessary for operational level of war and come after the specific crisis has been defined.

Effects of space and cyber in Phase I may be limited in comparison to typical measures: diplomatic demarches, predeployment activities, overflight denial, and force presence. However, they may be just as effective, both in public and private display. In this phase, space and cyber operations may have the same general effect, but their application would be completely different. Together they cover the spectrum of strategic to tactical.

Cyber has the ability to be a much more surgical and tactical tool than space today. Deployment of mission tailored intelligence operation in cyberspace would make a very purposeful message to an unwanted adversary about the costs associated with initiating military operations. Further, creating focused denial of service, as well as increasing the level of network-probing maneuvers would leave the same effect.

In space, much more strategic and public measures would be the norm for this phase. Activities would involve denial of service from space borne assets disrupting, but not harming stability of life within the borders of a potential adversary. Additionally, displaying the operationally responsive space augmentation capability for specific or regional space requirements would send the loudest message regarding resolve and capability to an unwanted adversary.

Phase II – Seize the Initiative

Seizing the initiative, Phase II, involves offensive operations at the earliest possible time to disadvantage your adversary. Activity in this phase is not limited to battlefield operations. For example, the deployment of forces may be enough to stop initial aggression of an adversary. During this phase, access to the current or potential theater infrastructure and timely and accurate knowledge about an adversary's activities is critical.

Due to the nature of the domains, space and cyber capabilities similarly provide theater access without requiring personnel presence, creating an efficiency of force. The combination of access to persistence in observation of critical infrastructure allows a complementary relationship between space and cyber. Space may monitor the external situation, while cyber may monitor and act upon the internal situation. Each will contribute to a robust C2 capability. This provides great advantage in time and space with respect to Phase II activities.

Both space and cyber provide inherently flexible capability for one's force to seize the initiative while encumbering an adversary's initiative. For example, using space situational awareness systems and network monitoring establish trip wires and lines of defense allowing timely warning of adversarial activities. Deployment of additional space assets for executing satellite maneuvers for theater augmentation in addition to or separate from launching denial of service operations from both domains may also have decisive effects.

In Phase II, opportunities for coalition support are more likely. This allows for valuable contributions by allied partners with space capabilities. However, given maturity of cyber operations, neither the US nor its partners are likely to coordinate or collaborate on individual cyber capabilities. In this context, the joint commander should consider the diplomatic and military effects and management of long-term coalition support.

Another key difference between space and cyber in Phase II will be the concept of surprise. Both space and cyber will prepare combat forces for seizing the initiative and employing surprise. In surprise, combatants must plan, prepare, and execute without being noticed. In countering surprise, planning, preparation, and execution must be brought out into the open. Space will be of great value in the planning and preparation of surprise, while cyber will offer capability in its execution. For conventional conflicts, while forces in each domain must work together, space will be the most useful opportunity in providing information on an adversary build-up toward operation. Likewise, space would become the primary target of denial and deception in order to establish surprise. For irregular warfare

or counter terrorism, cyber will be the most useful tool because potential adversaries will not likely form in the open prior to operations. Rather, they will slowly increase Internet chatter or operate on seemingly closed networks.

Phase III – Dominate

Phase III of the joint campaign focuses establishing superiority across the full spectrum of operations and creating recognition by the adversary of that superiority. This phase typically involves meeting the strategic operational objectives that will lead to continued capability in the next phase.

With a focus across the full spectrum of operations in Phase III, space and cyber will play an essential role. The options and methods will be very similar to operations carried out in Phase II. One of the greatest contributions to achieving space and cyber dominance will likely be efficiency of force and a synchronization of effects across the spectrum enabled by operations from each domain.

Space and cyber will partner up to provide joint fire support. Each will remain available for strategic attack, force enhancement, network exploitation, as applicable. Increased capability will come though coordination of denial of service operations. However, in Phase III, cyber will provide a broader scope of joint fire support through interdiction and focused information operations.

Strategic objectives associated with space will include elimination of adversarial threats and freedom of action for allies and partners. All three missions, counterspace, space protection, and force enhancement must still be available. If damage to the space network has occurred, regeneration of that architecture or capability must occur back to minimal acceptable levels.

Separately, cyber objectives require functioning and cooperative IT infrastructure, networks, and data paths. Similarly to space, its three primary missions, network defense, exploitation, and attack, also must be available. Planners for both domains must transition shift and balance their perspective. While remaining prepared for potential operations elsewhere, preparation for stabilization and support to civil authorities must begin.

Phase IV – Stabilize

Phase IV occurs while there is limited or no functioning, legitimate civil governing authority, forcing the joint commander to provide that governance and establishment of civil stability. Interaction with local but likely informal community leaders and nongovernmental organizations will be a focus of attention

In this phase basic services will be critical, but providing security, albeit at a much more tactical level will be equally important. Space and cyber systems will be required to aid the ongoing security efforts while filling gaps for local in regional communications and computer infrastructure. Space systems will provide important support on land use and critical infrastructure damage.

Phase V – Enable Civil Authority

Phase V focuses support for legitimate civil governance. This support will be of the same nature provided in Phase V, but will be requested and monitored by the legitimate civil government. Again, the access and persistence of space and cyber operations in combination will both support legitimate government activities and create a check and balance for maintaining the legitimacy of those activities.

Today's operating environment is becoming increasingly technically oriented. The new environment is changing rapidly, creating many opportunities, as well as opening up new vulnerabilities that demand our attention. Space and cyber systems sit at the forefront of those demands. Each stands to provide great contribution to joint operations within the separate domains. However, together, in complement, they will produce greater and currently unrealized benefits. The complementary nature and associated benefits of the two domains should be explored, developed, and integrated into joint operations. With this, the DoD stands a better opportunity to grow capabilities while minimizing vulnerabilities in a rapidly evolving technical battlespace.

Notes:

[1] Defined in Joint Publication 3-0, *Joint Operations*, 22 March 2010.

[2] Ibid.

Mr. Joshua T. Hartman (BS, Space Physics, US Air Force Academy; MS, Strategic Intelligence/Middle East Affairs, Joint Military Intelligence College; Business Graduate Studies, California State [Long Beach]) is a Senior Fellow at the Center for Strategic and International Studies. Additionally, he is an independent strategy consultant to government and industry organizations. He has led a career though multiple levels of the government, focused on development and execution of strategy and programs covering acquisition, missile defense, cyberspace, intelligence, and space. Recently, Mr. Hartman was the senior advisor to the under secretary of defense for acquisition, technology and logistics and the director of the Space and Intelligence Capabilities Office. Mr. Hartman began his career as an Air Force officer. His assignments included jobs at Space and Missiles Systems Center, National Reconnaissance Office, Joint Chiefs of Staff, Office of Secretary of Defense, and the Naval Research Laboratory. After separating from the Air Force, Mr. Hartman was a professional staff member on the House Armed Services Committee and the House Appropriations Defense Subcommittee.

Re-thinking Warfare:
How Does the Integration of Space and Cyber Forces Impact a Combatant Commander's Air-Sea Battle Concept?

Col Michael J. Lutton, USAF
Commander, 381st Training Group
Vandenberg AFB, California

Col Johndavid Willis, USAF
Commander, 17th Training Group
Goodfellow AFB, Texas

Dr. Christopher T. Yeaw
Member, Senior Executive Service and
Chief Scientist, USAF Global Strike Command
Barksdale AFB, Louisiana

Access to the global commons—air, sea, space, and cyberspace, remain vital to the national security of the US and the security of our allies.[1] Yet nations around the world seek to limit access to key regions through strategies designed to blunt US efforts to project diplomatic, informational, military, or economic influence. More than other nations, Iran and China continue to challenge access to the global commons and could potentially "deny [the US] the ability to project power into a region, thereby allowing aggression or other destabilizing actions to be conducted."[2]

China, for example, continues to "develop … computer network attack capabilities … counterspace systems and the ability to jam, blind, or otherwise disable satellites and their terrestrial support infrastructure."[3] China's move toward greater capability to deny access to areas of the Pacific is best understood when examined overtime (see figure 1).[4] The People's Republic of China's efforts likely began in the early 1990s when confronted by US naval forces in a standoff over Chinese military activities aimed at influencing Taiwan and accelerated later in the decade.[5]

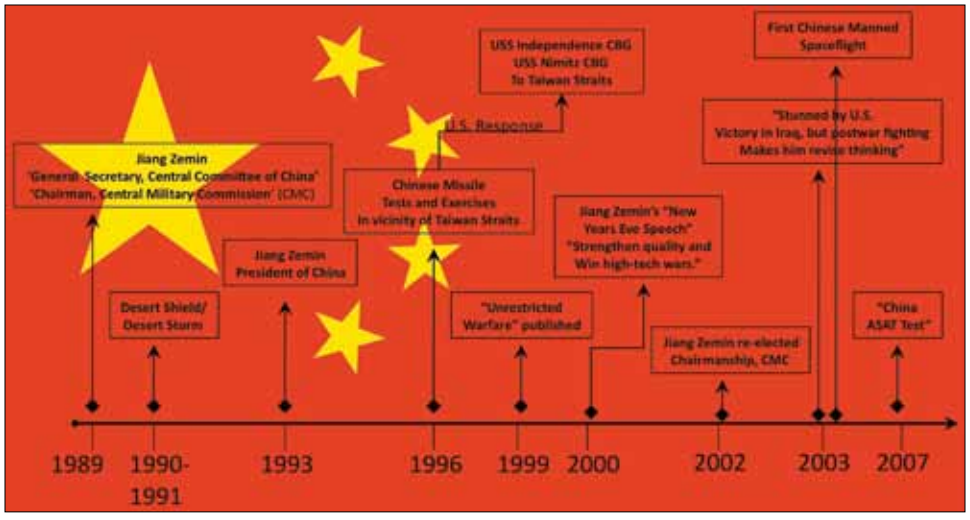


Figure 1. Engineering transformation.

Within the Persian Gulf, Iran continues to be a looming menace to physical and economic security. With the Iranian development of a uranium enrichment capacity and the discovery of documents indicative of nuclear warhead integration with existing ballistic missile technology, many of Iran's neighbors and close allies of the US are justly worried. Furthermore, Iran continues to develop capacity to interdict maritime traffic through the Straits of Hormuz disrupting significant energy supplies for much of the world (see figure 2).[6,7] In fact, as Abdullah Toukan and Anthony Cordesman note "analysts see Iran posing several threats to the region," for example, a "threat to the stability of the Gulf States. Iran … annexed the islands of Abu Musa, which dominate the entrance to the Straits of Hormuz."[8] Additionally, Iran's growing offensive cyber capability continues to cause concern and adds to Iran's repertoire of anti-access capabilities.[9] Iran even demonstrated the ability to counterspace-based communications as early as 2003.[10]

Figure 2. Abu Musa Island.

To turn the tide on emerging anti-access strategies and technologies developed to counter US interests, the most recent *Quadrennial Defense Review* leveraged existing work being done by the Department of the Navy and the Department of the Air Force and "directed further enhancements to US forces and capabilities [through] a joint air-sea battle concept."[11] This article proposes that the integration of space and cyberspace forces changes warfare for the combatant commander's air-sea battle concept in three areas: joint planning, timing and tempo of joint operations, and deterrence/escalation control options.

Joint Planning

Focus drives thinking and thinking drives planning. With the pre-disposition of many geographic combatant commands to view the space and cyberspace domain as the sole purview of US Strategic Command (USSTRATCOM), artificial blind-spots may develop during planning of a joint air-sea battle concept. For example, the historical focus of US Pacific Command (USPACOM) tilts to-

ward a pre-disposition to color anti-access as solely focused on air and maritime forces. Likewise, the US Central Command (USCENTCOM) area of responsibility, with a Straits of Hormuz scenario, tends to be viewed solely as a bi-polar, air and maritime, anti-access concept. As highlighted above, USPACOM and USCENTCOM likely face counterspace and cyberspace threats, as well as air and maritime threats. Consequently, the unintentionally limited focus on the physical domains of air and sea lead to an incomplete plan not accounting for anti-access in the space and cyberspace domains.

Even with the publication of the *Quadrennial Defense Review*, joint planning within the Department of Defense (DoD) is further hindered by the lack of a commonly agreed upon definition of anti-access strategy. Current concepts tend to focus on one or two domains at the expense of others. In fact, the current definition proposed by RAND researchers falls short and again focuses primarily on air and maritime domains.[12] In order to close the existing blind-spot in joint planning, a commonly agreed upon definition of anti-access strategy such as *"the ability to utilize elements of national power—diplomatic, informational, military, or economic—to effectively counter the use of the air, land, sea, space, or cyber domains"* better serves the combatant commanders and the joint planning community, as well as the nation.[13]

With a common definition established, the primary gap in existing joint operational planning needs to be closed—the linear phasing of joint operations. To apply space and cyberspace forces to a linear phasing model,[14] in an anti-access environment, is a misapplication of military capability and likely establishes suboptimal military conditions for the combatant commander. Phasing serves two purposes for joint planners—"systematically achieving objectives that cannot be achieved concurrently by arranging smaller, related operations in a logical sequence" and as "a framework for assessing risk to portions of an operation or campaign, allowing development of plans to mitigate this risk."[15]

Yet, the Joint Publication 5-0 phasing model fails to capture the fact that space forces are likely in a near constant state of Phase II activities because of the location of space assets relative to threat regions with existing anti-access strategies and capabilities. Furthermore, cyberspace forces must also constantly assure freedom of action for command and control of all joint forces, as well as the dissemination of intelligence information—both enduring joint operational functions. Furthermore, cyberforces are likely being engaged, temporally, before air, space, and maritime forces.[16] Consequently, joint planners are challenged by a phasing model ideally tailored for land-centric force operations.

In the development of an air-sea battle concept to counter anti-access strategies, planners need to consider a different conceptual framework that allows for the integration of air, space, cyberspace, and maritime forces in an anti-access environment. For example, an anti-access planning framework might include influence, access, and stabilize as the inter-related lines of operation for joint anti-access planning.

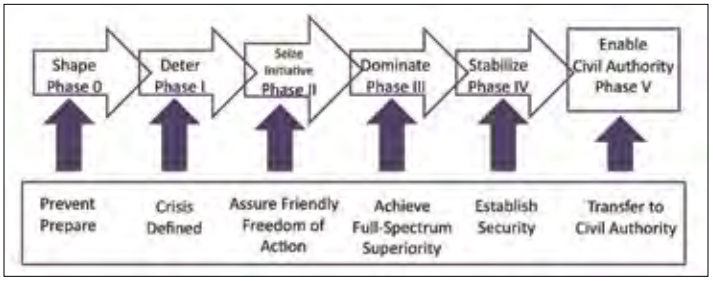


Figure 3. Joint phasing model.

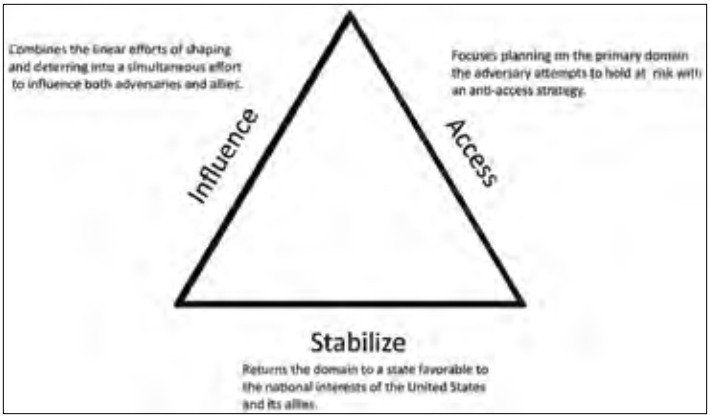


Figure 4. Anti-access planning lines of operation.

The anti-access planning lines of operation are designed to counter anti-access strategies and leverage the capacity of all joint forces through the application of operational functions to maximize the application of joint forces in time and space. The operational art associated with defeating an adversary anti-access strategy pivots on the ability to conduct all three activities simultaneously—influence through access stabilizes the situation and counters the adversary's strategy. For example, joint forces influence Iran or the People's Republic of China through access to a domain or domains that remain critical to the national security of the US and our allies. In so doing, the joint force establishes the domain or domains in a state favorable to the US national interests and its allies—ideally, without a crisis or conflict occuring.

Yet as joint planners take on the challenge of developing an air-sea battle concept to counter emerging anti-access strategies across all domains, the planners must re-think the timing and tempo of joint operations in light of space and cyberspace forces. What changes with the addition of space and cyberspace forces? What are the ranges of space and cyberspace operations? These are but a few of the questions a multi-domain air-sea battle concept must address.

Timing and Tempo of Joint Operations

The inter-relationship of the operational factors of time, space, and force drive the timing and tempo of joint operations. With the addition of space and cyberspace forces to the combatant commander's air-sea battle concept, joint forces leverage critical capabilities required to influence, access, and stabilize areas where anti-access strategies are being executed or contemplated. For example, satellites in low Earth orbit routinely travel at speeds near 17,000 miles per hour and complete one orbit around the Earth in approximately 90 minutes.[17] Cyberspace forces networked with space forces "close" vast expanses of space and time for the joint force. In fact, given the current timing and tempo standard set for joint force operations, the ability to conduct joint force operations without integrated space and cyberspace forces is inconceivable.

As noted earlier, emerging anti-access strategies and technolo-

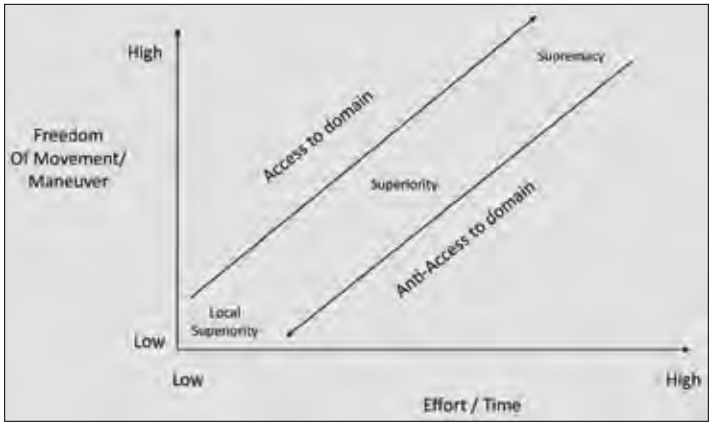


Figure 5. Domain Superiority versus Anti-Access.

gies are developed to counter US interests by holding one or more domains at risk. If the space and cyberspace domains are held at risk, which is likely the case, the joint force risks a disruption in the timing and tempo of joint operations required to influence access and stabilize a situation.

Superiority in any domain allows freedom of movement and maneuver but comes with an associated level of effort over time. Anti-access strategies seek to remove the advantage of superiority in a domain via conventional or unconventional means and disrupt timing and tempo. Figure 5 illustrates the relationship between superiority in a domain, like air, space, cyberspace, or maritime, and anti-access to a domain, like People's Republic of China (PRC) counterspace activities or Iranian naval activities.[18, 19] As noted earlier, an air-sea battle concept designed to counter anti-access strategies and capabilities should be based on three lines of operation—influence, access, and stability.

A range of military operations are required to accomplish these lines of operation. Most are familiar with the existing range of military operations (ROMO) that extends from humanitarian assistance on the permissive end of the spectrum through nuclear war at the extreme end of the spectrum.[20] However, the unique nature of space and cyberspace forces places them in no single position within the ROMO. In fact, space and cyberspace forces now permeate all aspects of the ROMO and networked architectures integrating the joint force have become ubiquitous allowing for higher tempo and more effective timing of joint operations. Consequently, space and cyberspace forces become lucrative targets for an adversary—disrupt timing and tempo through an attack on space or cyberspace assets and the joint force becomes vulnerable to defeat.[21]

In fact, the greatest limitation for both space and cyberspace forces is adequate situation awareness necessary to determine hostile intent in order to attribute activities to a nation or warn of an impending attack. Cyberspace attacks, for example, occur in an environment in which the weapons are information packets routinely exchanged peacefully between actors, ranging from individuals to governments. Therefore, attack detection, attribution and effect are not always understood and, in fact, are often inscrutable—space operations are no less different. Despite the ambiguity of cyber warfare, it nonetheless remains clear that cyber attacks are occurring.[22] In 2008, attacks against DoD information systems used by the joint force, for example, were up 19.6 percent with the trend almost tripling to 60 percent over 12 months.[23]

With certain ambiguity surrounding possible space and cyberspace attacks designed to disrupt timing and tempo of a joint air-sea campaign, the air-sea battle concept requires a more complete understanding of the range of space and cyberspace operations to frame the challenges of uncertain intent in an anti-access environment where the first echelon of attack may come in space or cyberspace, thus disrupting joint anti-access lines of operation—influence, and stabilize, as previously noted.[24]

In the depiction of the comparative range of operations of figure 6,[25] the threshold for when a hostile action constitutes war is driven by intent and effects. If the intent of an actor is to render military forces incapable of carrying out a defense or to destroy critical infrastructure, military, and control networks, or is accompanied by kinetic attacks, then the act constitutes a *casus belli*. This definition leaves computer network exploitation and actions to prepare for attack, such as "leave-behind" reconnaissance tools or devices, below the threshold of cyber warfare. From this perspective, the definition of cyber warfare is any attack in cyberspace intended to render an opponent incapable of defense, disrupt, or damage an opponent's critical infrastructure, and/or disrupt or damage military command and control networks.[26]

A similar construct exists for space forces operating *in* the space domain. Like cyberspace, space forces operating in the space domain rely on sensors and defensive capabilities to build situation awareness of impending hostile attacks and prevent attacks with defensive acts. Like cyberspace, adequate situational awareness of actions in the space domain remains challenging and below an acceptable standard for joint operations in an anti-

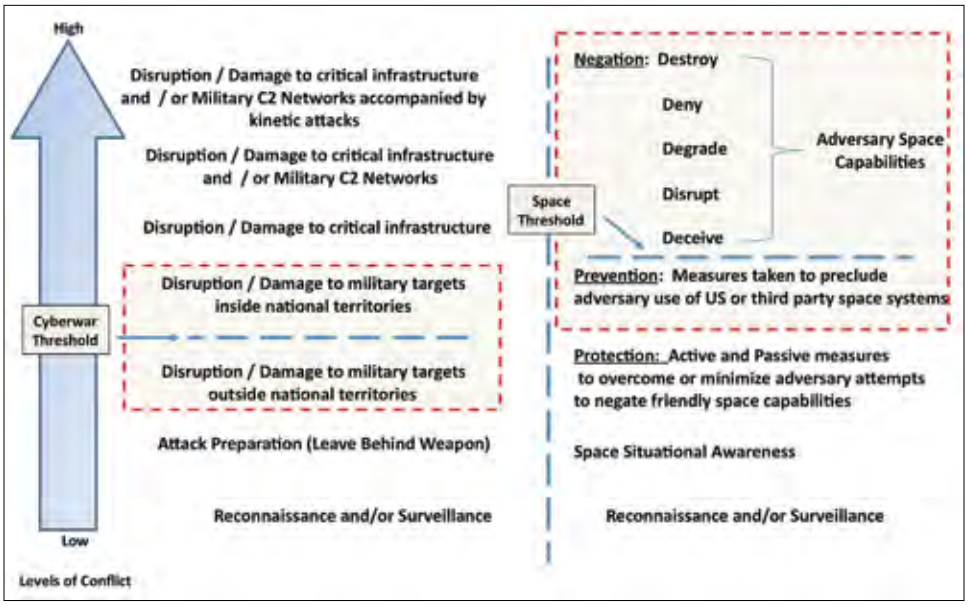


Figure 6. Comparative range of operations.

access environment where the first actions may occur in space or cyberspace. Because situational awareness remains challenging, the ability of an air-sea battle concept to deter across all domains and control escalation to prevent disruption of the global commons remains in questions. Consequently, elements of an adversary's anti-access strategy may be successful and threaten the national interests of the US.

Deterrence and Escalation Control

As noted in the 2010 *Quadrennial Defense Review*, air-sea battle further enhances capabilities required to counter anti-access strategies aimed at closing off areas vital to the national interests of the US and its allies. Expeditionary air and maritime forces continue to serve as a signal of US resolve and unequivocally indicate national intent. These forces in fact contribute directly to deterring adversaries from executing anti-access strategies and thus serve to control escalation. How will the integration of space and cyberspace forces in a combatant commander's air-sea battle concept contribute to deterrence and escalation control?

Space-based assets provide "the ability to look deep into denied areas" while poised to provide situational awareness on potential threat activities like ballistic missile launches.[27] Space-based assets also contribute to "net-centric warfare … sensors, communications, and information handling."[28] In a mutually supporting relationship, space forces are inextricably linked to cyberspace forces—"if we fail to ensure the right information gets to the right person, not only will we have failed … people in harm's way will die."[29] While space-based assets contribute to net-centric warfare, space forces also defend space-based assets, negate an adversary's use of the space domain, and maintain situational awareness of the space domain.[30]

Cyberspace forces also provide a set of complimentary "core capabilities … computer network operations [for the joint air-sea battle concept] … computer network attack, exploitation and defense."[31] Like space operations, these activities are designed to enhance situational awareness, defend friendly assets and negate an adversary's capability to operate in the cyberspace domain. Thus, cyberspace forces like air, sea, and space forces provide a range of options to deter an adversary from executing an anti-access strategy. In so doing, these forces contribute directly to escalation control as well.

As noted earlier, expeditionary air and maritime forces continue to serve as a signal of US resolve and unequivocally indicate national intent. The scenarios discussed above also contain a nuclear component—an emerging nuclear threat, like Iran, or a nuclear armed country, like the PRC. Consequently, the air-sea battle concept must develop capacity to deter along nuclear, air, space, cyberspace, and maritime lines of operations while also controlling escalation along these same axes.

To effectively deter adversaries and control escalation, the joint air-sea battle concept must control the space and cyberspace domains to achieve dominance in three critical operational functions: command and control, intelligence, and joint fires. By controlling these domains, the air-sea battle concept offers the joint commander not only the ability to dominate an adversary with unrivaled command and control of joint forces in time and space but also the ability to seamlessly pass intelligence to joint forces enhancing situation awareness. With effective command and control coupled with intelligence of the situation disseminated to widely dispersed forces, the joint commander may also use the space and cyberspace domain to deter or control escalation through joint fires designed to shape the battlespace.

As illustrated in figure 7,[32] several integrated events might occur along conventional, cyber, space, and nuclear axis during a hypothetical scenario. The effective command and control of these events, coupled with intelligence, allows the joint commander to control escalation consistent with national objectives while also utilizing space and cyberspace forces to escalate joint operations to deter further adversary actions and signal resolve to accomplish national or alliance objectives. Yet, as figure 7 indicates, the adversary may also choose to escalate. Consequently, effectively postured defensive capabilities in space and cyberspace to thwart adversary attempts to escalate are required to compliment offensive actions along with assets designed to promote situation awareness. To effectively utilize space and cyberspace forces to deter an adversary or signal intent through escalation, a combatant commander's air-sea battle concept needs to consider the following—command and control of space and cyberspace forces, signaling intent with space and cyberspace forces and synchronization of space and cyberspace forces.

Command and control of joint forces is a prerequisite for effective joint operations and all joint operations are unique. Consequently, command and control of joint forces must be tailored

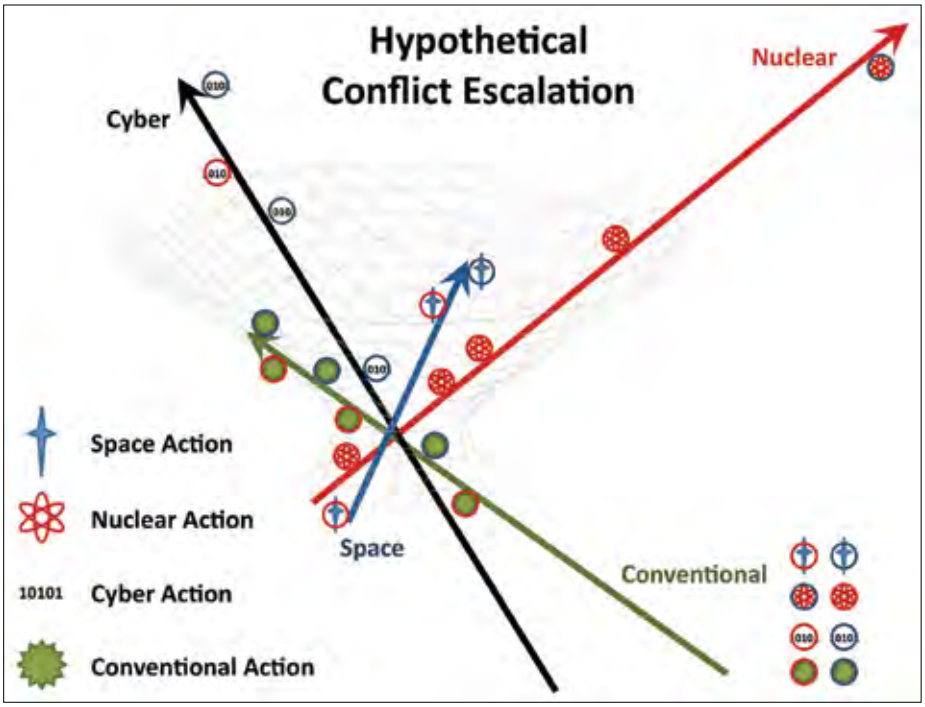


Figure 7. Four axis deterrence and escalation matrix.

For command and control to be effective, the command and control architecture must define authorities that allow the joint force to gain and maintain the initiative in space and cyberspace while deterring adversaries aims.

to the situation. To employ space and cyberspace forces, the joint force must tailor the command and control architecture through integration with elements of USSTRATCOM, specifically, the Joint Functional Component Commander, Space and US Cyber Command (Joint Functional Component Commander, Network Warfare and Joint Functional Component Commander, Global Network Operations). For command and control to be effective, the command and control architecture must define authorities that allow the joint force to gain and maintain the initiative in space and cyberspace while deterring adversaries aims. Furthermore, command and control must be responsive enough to escalate joint operations to signal intent, again dependent on authorities prescribed in the command and control architecture. The authorities prescribed must also be flexible enough to achieve the objectives and missions across the range of operations where space and cyberspace forces operate to either deter or signal intent through escalation.

As joint operations continue to advance in complexity and increase in scope, the development of space and cyberspace forces must maintain pace. Like other joint forces, space and cyberspace forces are capable of deterring and signaling intent. Space and cyberspace forces conduct negation, protection, and situational awareness operations and as such are able to move up or down an escalation axis to deter an adversary or signal intent. As noted in figure 6, cyberspace forces are capable of conducting a wide range of operations. These operations remain critical to a credible deterrent force and serve as a means to escalate in order to signal intent.

Even with effective command and control and a credible force capable of deterrence and escalation control, space and cyberspace forces must be effectively synchronized with other joint forces to contribute to the air-sea battle concept. Synchronization of space and cyberspace forces occurs in time and space. Synchronized joint actions are designed to deter an adversary from conducting an anti-access strategy in an area or region vital to US national security. If deterrence fails, joint actions must be prepared to escalate in order to regain influence and access in order to stabilize the environment to secure national security objectives.

As noted previously, space and cyberspace forces allow the joint force to compensate for extremes associated with time and space—space and cyberspace forces cover vast amounts of the operating area with greater relative speed than any other element of the joint force. To effectively integrate space and cyberspace forces, the joint force should leverage these inherent capabilities to offset the limitations of other joint forces.

For example, in future crisis situations, the joint force might establish an I-day to mark the beginning of joint operations.[33] The I-day connotes the beginning of offensive space and cyberspace operations to deter an adversary's anti-access operation. The I-day activities run the full range of the operations short of the cyber warfare threshold; however, space and cyberspace forces conducting I-day activities remain postured with other joint forces to escalate as required to secure national interests. By establishing an I-day construct, space and cyberspace forces are more effectively synchronized in time and space.

Conclusion

Throughout the history of the US, access to the global commons remained critical to our economic security, as well as the national security of the US—little has changed, in that respect, in two hundred plus years. Access to air, sea, space, and cyberspace underpin our national security. Yet, some nations today challenge our access to these global commons.

The recent *Quadrennial Defense Review* leveraged existing work being done by the Department of the Navy and the Department of the Air Force and "directed further enhancements to US forces and capabilities [through] a joint air-sea battle concept."[34] To address the realities of the modern battlefield, the joint air-sea battle concept must integrate space and cyberspace forces and be prepared to face a nuclear armed adversary. The integration of USSTRATCOM forces with geographic combatant command forces remains a critical link in the success of the air-sea battle concept.

By effectively integrating space and cyberspace forces into a combatant commander's air-sea battle concept, the joint force is provided additional options during joint planning. Furthermore, the timing and tempo of joint operations is accelerated in favor of joint forces allowing a degree of superiority unmatched by adversaries. Finally, the addition of space and cyberspace forces contributes to the deterrence of adversary anti-access strategies while allowing the joint force to maintain a range of escalatory options necessary to signal US intent. By re-thinking warfare, the integration of space and cyberspace forces strengthens the lethality and expands the range of options in the combatant commander's air-sea battle concept.

Notes:

[1] The White House, defense information, http://www.whitehouse.gov/issues/defense.

[2] *Quadrennial Defense Review Report* (Washington, DC: Department of Defense, 6 February 2006), 31; Anthony H. Cordesman, "Iran's Evolving Threat," *Center for Strategic and International Studies*, Report, 21 January 2010, http://csis.org/publication/irans-evolving-threat.

[3] *Quadrennial Defense Review Report*, 31; "Military Power of the People's Republic of China," *Annual Report to Congress*, 2009, www.defenselink.mil/pubs/pdfs/China_Military_Power_Report_2009.pdf, 14.

[4] This figure was developed through research of the following sources: Robert Lawrence Kuhn, *The Man Who Changed China: The Life and Legacy of Jiang Zemin* (Crown Publishing, 2005), 191, 403, 542, 545; Ashton Carter and William Perry, *Preventive Defense: A New Security Strategy for America* (Washington, DC: Brookings Institution Press, 1999), 92, 97-98; Additionally, Clara Moskowitz's article "Liftoff! China Launches Third Manned Space Flight," *SPACE.com*, 25 September 2008, http://www.space.com/missionlaunches/080925-zhenzhou7-launch-wrap.html; Craig Covault's "Chinese Test Anti-Satellite Weapon," *AviationWeek.com*, 17 January 2007, http://www.aviationweek.com/aw/generic/story_channel.

jsp?channel=space&id=news/CHI01177.xml. The figure first appeared in a student paper written by Lt Col Mike Lutton for the US Naval War College, "Defending the High Ground: How should Pacific Command's Theater Campaign Plan evolve in light of the People's Republic of China counterspace initiatives?".

[5] For further information on the standoff with US Naval Forces see Ashton B. Carter and William J. Perry, *Preventive Defense: A New Security Strategy for America* (Washington, DC: Brookings Institution Press, 1999). Figure also developed with input from Dr. Christopher Yeaw.

[6] Cordesman, "Iran's Evolving Threat;" and Abdullah Toukan and Anthony H. Cordesman, "GCC – Iran: Operational Analysis of Air, SAM and TBM Forces," *Center for Strategic and International Studies*, Report, 19 August 2009, http://csis.org/publication/gcc-iran.

[7] Image available at www.arabianbusiness.com as seen in the article written by Dylan Bowman, "UAE federal council slams Iran over Abu Musa," ArabianBusiness.com, 16 August 2008.

[8] Toukan and Cordesman, "GCC – Iran," 5.

[9] Chairwoman Yvette D. Clarke (D-NY), "Securing The Modern Electric Grid From Physical And Cyber Attacks," Opening Statement, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee On Homeland Security, 21 July 2009, http://hsc.house.gov/SiteDocuments/20090721141443-38588.pdf.

[10] Lt Col Kendall Brown, ed., *Space Power Integration: Perspectives from Space Weapons Officers* (Maxwell, AL: Air University Press, 2006) chapter 2, 30-31, http://aupress.maxwell.af.mil/Books/Brown/brown.pdf.

[11] *Quadrennial Defense Review Report*, 32.

[12] Roger Cliff et al., *Entering the Dragon's Lair: Chinese Antiaccess Strategies and Their Implications for the United States* (Santa Monica, CA: Rand Corporation, 2007), 11.

[13] Lutton, "Defending the High Ground."

[14] Joint Publication 5-0, *Joint Operational Planning*, IV-36, http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf.

[15] Ibid., IV-33.

[16] "In 1998, there were a total of 5,844 attacks detected on Department of Defense (DOD) networks. By 2008, that number had exploded to more than three million attacks per year." Jim Wolf, "Hacking at Pentagon Persists," *The Washington Post*, 9 August 2000.

[17] Lockheed Martin, low Earth orbit, fact site, http://www.thetech.org/exhibits/online/satellite/4/4a/4a.1.html.

[18] Lutton, "Defending the High Ground."

[19] Ibid.; For further information on Iranian maritime capabilities see Cordesman, "Iran's Evolving Threat;" and Toukan and Cordesman, "GCC – Iran."

[20] Joint Publication 3.0, *Joint Operations*, I-6 to I-8.

[21] Lt Col Johndavid Willis, "From the Cold War to the Cyber War: A New National Security Strategy," paper, 2-3.

[22] Ibid., 3.

[23] Larry M. Wortzel, Preventing Terrorist Attacks, Countering Cyber Intrusions, and Protecting Privacy in Cyberspace, Testimony before the Subcommittee on Terrorism and Homeland Security, US Senate, 17 November 2009.

[24] Willis, "From the Cold War to the Cyber," 3, The concept of an e-ROMO was developed by Lt Col Johndavid Willis.

[25] Adapted and modified from Lewis, "The 'Korean' Cyber Attacks," 6. Space operations material was adapted from Joint Publication 3-14, Space Operations, pg II-5 –II-6.

[26] James A. Lewis, "The "Korean" Cyber Attacks and Their Implications for Cyber Conflict," 23 October 2009, 3-4.

[27] John M. Logsdon and Audrey M. Schaffer, eds., *Perspectives on Space Superiority,* "Space Superiority" by Robert Dickman, Washington, Space Policy Institute, Security Policy Studies Program, Elliott School of International Affairs, December 2005, 70.

[28] Ibid.

[29] Ibid, 69.

[30] Joint Publication 3.14, *Joint Operations*, Chairman, US Joint Chiefs of Staff, Joint Operations, xi.

[31] Joint Publication 3.0, *Joint Operations*, Chairman, US Joint Chiefs of Staff, Joint Operations, Figure III-1.

[32] This figure and concept developed in academic year 2010 by Dr. Christopher Yeaw and the Mahan scholars.

[33] The concept of I-day was first developed by Col Chuck Patillo, commander, 32d Information Warfare Flight in late 1999, early 2000.

[34] US Department of Defense, Office of the Secretary of Defense.

Col Michael J. Lutton (BA, English, Kent State University; MS, Systems Management, Lesley College; MA, Military Operational Art and Science, Air University; MA, National Security and Strategic Studies, Naval War College) is the commander, 381st Training Group, Vandenberg AFB, California. He is responsible for training USAF missile operations and missile maintenance, as well as US and coalition space forces. A career space and missile operator, Colonel Lutton graduated from the US Air Force Weapons School and served as weapons officer instructor, operations officer and weapons squadron commander. He has served staff tours at the major command and headquarters Air Force level. Colonel Lutton holds multiple advanced academic degrees and is a graduate of Air Command and Staff College and the Naval War College.

Col Johndavid Willis (BS, Computer Science, University of Memphis; MA, International Affairs, Columbia University; MA, National Security and Strategic Studies, Naval War College) is the commander, 17th Training Group, Goodfellow AFB, Texas. He is responsible for training USAF intelligence, surveillance, and reconnaissance professionals assigned worldwide. His career includes assignments at the squadron, group, major command and joint command levels, focused on strategic intelligence analysis, signals intelligence, computer network operations, force protection, counterinsurgency, counterterrorism, air mobility, and reconnaissance operations. Colonel Willis holds multiple advanced academic degrees and is a graduate of Command and General Staff College, Western Hemisphere Institute for Security Cooperation and the Naval War College.

Dr. Christopher T. Yeaw (PhD, Nuclear Engineering and Engineering Physics, University Of Wisconsin) is a member of the Senior Executive Service and serves as the chief scientist for US Air Force Global Strike Command advising the commander on the full range of scientific, technical, and deterrent policy elements for America's intercontinental ballistic missile and bomber force. Dr. Yeaw has served as a Department of Energy (DOE) chief scientist where he coordinated and managed nuclear national security operations and analyses performed by various elements across the DOE complex. Dr. Yeaw also served as principal advisor on nuclear and strategic issues to the assistant secretary of state for verification and compliance, Department of State (DOS). While at the DOS, he had the distinction of being the first nuclear diplomat on the ground in Libya, and retrieved the nuclear weapons documents that Pakistani scientist A.Q. Khan provided to that country's covert nuclear weapons program.

Examining the Inherent Right of Self-Defense

Col Guillermo R. Carranza, USAF
Staff Judge Advocate
Headquarters 24th Air Force
Lackland AFB, Texas

Since 1945, the Charter of the United Nations (UN) has prohibited "the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the UN," unless the use of force is specifically authorized by the UN Security Council (UNSC) or undertaken in self-defense.[1] The right of self-defense is protected in Article 51 of the charter, which states that: "[n]othing in the … charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a member of the UN, until the UNSC has taken measures necessary to maintain international peace and security.…"[2]

The US has long held that "Article 51 characterizes [the right of self-defense] as 'inherent' in order to prevent its limitation based on any provision of the charter" and that customary practice "enables any state effectively to protect itself and its citizens from every illegal use of force aimed at the state."[3] However, this interpretation is not universally accepted. Some take the position that the UN charter restricts the pre-existing right of self-defense and that use of force is authorized "only once an actual attack has occurred" while others contend "the word 'inherent' in the language of Article 51 preserves the customary international law with regard to self-defense which existed at the time of the charter's adoption."[4]

This ambiguity in the charter coupled with a series of increasingly restrictive opinions issued in the last 24 years by the International Court of Justice (ICJ) pose a continuing challenge to the US as it comes to terms with the increasingly dynamic threats posed by states and non-state actors in each of the warfighting domains, but particularly in space and cyberspace.

An underlying cause of some of these challenges can be traced back to the founding of the UN:

> When the charter was written, the council was expected to have at its disposal the armed forces necessary to implement its decisions … Based in part on this expectation, the charter limits the power of individual states to use force in exercising their 'inherent' right to defend themselves against armed attacks.… But the council, forced to rely on ad hoc contributions of troops from its member states and crippled by disagreements among its permanent members, has been unable to play its intended role. States have therefore been left to deal unilaterally … with threats that differ from the conventional armed attacks contemplated in the charter.[5]

One result has been that "the [US] and other states have rejected some of the limits imposed by the ICJ on their right of self-defense. Most states have disregarded them in practice … [and even some] security experts and scholars who accept as legally correct the restrictive use of force rules supported by the ICJ have nonetheless concluded that those rules are inadequate to deal with modern necessities."[6]

The Right of Self-Defense

The US believes the right of self-defense is not limited by the charter, but that it can be exercised "only when necessary and only to the extent it is proportionate to the threat defended against."[7] It is important to note, however, that the US defines necessity in a manner that "is less constraining than the view of the [ICJ], which requires an actual or imminent 'attack' before [use of] force" can be authorized in self-defense.[8] "Virtually every administration since President Harry S. Truman has … advanced arguments for flexible use of force standards … based on the gravity of the danger, the likelihood of its realization, the exhaustion of other means for prevention, the extent to which UN charter-based procedures and values support the action, and the proportionality of the action contemplated relative to the danger perceived."[9]

Proportionality in this context "is the degree of force that is reasonable in terms of intensity, duration and magnitude required to decisively counter the hostile act or demonstrated hostile intent … but no more than that."[10] However, the US also believes "there is no requirement that an act of self-defense use the same means as the provocation, that the object of the [response] be either a similar type of target or the means used in the offending attacks, or that the action taken be contemporaneous with the provocation, particularly if the attacker is responding to a continuing course of conduct."[11]

The Nicaragua Case

The terms "use of force" and "armed attack" are not defined in the UN charter. One of the few things commentators seem to agree on is that the two terms are not synonymous.[12] "The prevailing view among international legal scholars seems to be that the term 'use of force' in the UN charter encompasses only the use of military force."[13]

> The choice of using the term 'force,' as opposed to 'war,' 'aggression,' or 'military conflict' is significant in that it encompasses situations which include hostile acts that fall short of the technical state of belligerency. This fundamental proscription against the use of interstate force is traditionally regarded as being confined to the use or threat of 'armed' force, meaning the possible resort to a violent weapon that inflicts human injury.[14]

However, in *Nicaragua v. US*, the ICJ went on to say that not every use of force, even if military in nature, equates to an armed attack. Essentially, the court found that "[t]he scale and effects of some uses of force will simply not be significant enough to amount to an armed attack under Article 51. To

qualify as an armed attack, therefore, an attack must be 'of a certain scale … serious, not trivial.'"[15]

Whether actions in cyberspace would amount to an armed attack or even a use of force has never been formally settled in international law. However, the "plain language of Article 51 … in no way limits itself to especially large, direct or important armed attacks."[16] The Department of Defense's (DoD) initial assessment of international legal issues related to cyberspace operations adopted a more flexible "equivalent effects" framework to determine whether cyber activity would trigger the right to use force in self-defense:

> If we were to limit ourselves to the language of Article 51, the obvious question would be, 'Is a computer network attack an 'armed attack' that justifies the use of force in self-defense?' If we focused on the means used, we might conclude that electronic signals imperceptible to human senses don't closely resemble bombs, bullets, or troops. On the other hand, it seems likely that the international community will be more interested in the consequences of a computer network attack than in its mechanism. It might be hard to sell the notion that an unauthorized intrusion into an unclassified information system, without more, constitutes an armed attack. On the other hand, if a coordinated computer network attack shuts down a nation's air traffic control system along with its banking and financial systems and public utilities, and opens the floodgates of several dams resulting in general flooding that causes widespread civilian deaths and property damage, it may well be that no one would challenge the victim nation if it concluded that it was a victim of an armed attack, or of an act equivalent to an armed attack. Even if the systems attacked were unclassified military logistics systems, an attack on such systems might seriously threaten a nation's security. For example, corrupting the data in a nation's computerized systems for managing its military fuel, spare parts, transportation, troop mobilization, or medical supplies may seriously interfere with its ability to conduct military operations. In short, the consequences are likely to be more important than the means used.[17]

Some legal scholars outside the DoD also agree that while "cyber-force" may not be "'armed force' in the literal sense, resort to cyber-force may be viewed as a form of intervention that can produce certain harmful or coercive effects in other states," violating the UN charter's prohibition against a threat or use of force and possibly constituting an armed attack, but only to the extent that physical manifestations of cyber-assaults are sufficiently destructive.[18] What constitutes sufficient destruction remains an open question.

The Oil Platforms Case

More troubling is the ICJ's *Oil Platforms* decision, which limits "applicability of the right of self-defense [to] instances involving the defense of [vital] interests in foreign territory and in areas outside sovereign territory," as well as "the right to invoke self-defense … where there is no 'conclusive' proof of specific intent on the part of the adversary" to target a particular nation's interests.[19] The *Oil Platforms* case, which arose from the circumstances surrounding the US re-flagging of oil tankers in the Persian Gulf during the 1980s, has particular relevance to the discussion of space and cyberspace defense. "There is a striking similarity between US policy … 'regarding freedom of navigation' in the Persian Gulf that was the basis for … US participation in the Tanker War and US policy of freedom of access to space and freedom of action in space."[20] Similarly, US policy regarding cyberspace is also couched in terms of freedom of access to, and the free flow of information in, cyberspace.[21] Moreover, defense of space and cyberspace necessarily "involve the defense of commercial assets important to US national security and may even go beyond operations to defend friendly forces and commercial interests … to defense of the domain itself."[22]

In *Oil Platforms*, the ICJ held that US military operations against Iranian oil facilities could not be justified as self-defense, even after the US was able to attribute two separate instances of hostile acts to Iran. With regard to the missile strike on the vessel *Sea Isle City* "[t]he first factor considered by the court was the location of the vessel at the time of the attack … While the location of the vessel was but one of several reasons why the court determined the right of self-defense was inapplicable … [o]ne scholar has taken the position that the opinion of the court can be read to impose a strict 'sovereign territory' test on the right of self-defense."[23] The second factor advanced by the court was that attacks on non-US registered vessels and aircraft could not be "equated with an attack on the [US]"[24] Finally, the ICJ concluded that because the Silkworm missile fired at the *Sea Isle City* was not technically capable of individually targeting this particular ship and because there was no evidence the particular attack, or the related Iranian mine-laying operations that damaged the *USS Samuel B. Roberts*, were specifically intended to harm US vessels or US interests, the US could not justify its use of force against Iranian facilities as self-defense.[25]

The *Oil Platforms* decision portends significant legal difficulties for the US if the effects of space and cyber defense measures are deemed to rise to the level of a use of force. Vital US interests in space and cyberspace are not always located inside US sovereign territory. Aside from the physical infrastructure found in foreign countries, the space segment of the space and cyberspace architecture, and the undersea cables traversing international waters are all located in the global commons. Any of these could be the subject of attack or used to enable an attack on another element of the interconnected network. The ephemeral aspect of cyberspace adds an additional complication. "Cyberspace is not 'real' in any tangible sense … [although] it can have very real effects in the spatial world we inhabit. But … cyberspace is neither a 'real' place nor is it situated in a 'real' tangible space…."[26] If applied to cyberspace, the narrow focus of the *Oil Platforms* analysis would restrict the right of self-defense to such an extent that it would become largely unavailable.

Equally problematic is the ICJ requirement for conclusive proof that attacks are specifically intended to harm the victim State's personnel, property or interests before any use of force in self-defense can be justified.[27] "If international law requires conclusive proof of an attacker's intent, then there will exist no right to use force in self-defense to 'defend space' in the sense

By defining the right of self-defense in such a limited manner, the ICJ creates an environment where "there is very little effective protection against states violating the prohibition against the use of force, as long as they do not resort to armed attack."

of preserving freedom of access and action in that domain. A state would be free to emplace 'space mines' or other such devices that would endanger space operations, so long as they were not directed at any specific state."[28]

Similarly, a requirement to attribute cyberspace attacks with such particularity is not only impractical, but it would practically render the right to self-defense in cyberspace moot. First, "the Internet protocol addresses networked computers use can easily be spoofed, or faked, so an attack that seems to come from one computer actually comes from another in a different location."[29] Additionally, "the fact that attacks were routed through Internet servers located in [one country] does not necessarily mean the attacks originated in [the same country]. Online attackers commonly use 'stepping stones'—computers owned by innocent parties but controlled by the attacker—in their assaults. The stepping stone computers can be anywhere in the physical world because real-space is irrelevant to activity in cyberspace. This possibility opens point of attack origin up to manipulation, as well as obfuscation…."[30] Moreover, "neither the repetition of … attack[s] nor their having the same point of origin can conclusively or even substantially support attacker attribution … the repetition of attacks with the same attack signatures can indicate that there was one attacker; but it can also indicate that there were multiple attackers, each using the same attack tools."[31] Thus, while divining an attacker's intent is clearly required to justify a response in self-defense, the ICJ's *Oil Platforms* construct would impose an unobtainable standard of proof for victim states.

The Armed Activities Case

In *Armed Activities*, the ICJ continued to limit the right to use force in self-defense by further restricting "the concept of 'armed attack' to [those] attacks committed by or attributable to a state."[32] In pertinent part, the ICJ summarily rejected Uganda's claim that it was the victim of an armed attack because it "failed to show that … rebel attacks could be attributed to the [Democratic Republic of Congo]."[33] In the court's interpretation, "attacks carried out by non-state actors that are *not* attributable to a state are not armed attacks within the scope of Article 51, and therefore do not entitle the victim state to respond with force in self-defense."[34]

To reach this conclusion in *Armed Activities*, the court relied on a principle first articulated in the *Nicaragua* decision that "an armed attack [is] attributable to a state when committed by irregular forces 'sent by or on behalf of a state' over whom the state exercised 'effective control.'"[35] Effective control "requires that the State 'direct and control the activities of the … [non-state actors]—or at least expressly sanction and adopt their actions—before their acts will be attributable to that state.'"[36] This very restrictive interpretation of self-defense doctrine has particular significance for cyberspace where technical attribution of an Internet protocol address does not equate to understanding who is behind an attack and where shadowy "patriotic hacker" groups are becoming increasingly prevalent.[37]

Many scholars have severely criticized the ICJ's *Armed Activities* decision, in part because it lacked thorough analysis, but also because "[t]he language of Article 51 specifically describes states' right to self-defense as 'inherent,' suggesting that the court many not be able to diminish that right by restricting it to attacks conducted by a state because '[t]he right of self-defense is a *right* to use force to avert an attack. The source of the attack, whether a state or non-state actor, is irrelevant to the existence of the right."[38]

Policy Implications

By defining the right of self-defense in such a limited manner, the ICJ creates an environment where "there is very little effective protection against states violating the prohibition against the use of force, as long as they do not resort to armed attack."[39] Such uncertainty inevitably invites those with hostile intent to act with impunity. Thus, "states are … frequently faced with threats caused by the misconduct or failures of other states, and have to deal with them without UNSC support. The result has been the repeated use of force by states in a variety of situations that fail to meet applicable legal standards."[40]

> [A] limited use of force can sometimes prevent or deter a significant threat … how the international community reacts is likely to turn on factors related to legitimacy rather than on the specific legal categories into which the uses of force fall. Uses of preventive force that secure international support tend to be those that are necessary to address conduct internationally condemned or universally regarded as improper, and which are limited in scope and duration.[41]

There also is some support for the proposition that states may lawfully undertake proportionate countermeasures to defend themselves against actions that do not rise to the level of a use of force or armed attack. "The use of countermeasures is a product of the shortcomings inherent in a decentralized international legal system. Without a hierarchical enforcement structure, measures of self-help may be the only means to ensure the fulfillment of international obligations."[42]

Both the *Nicaragua* opinion and a separate opinion issued by Judge Bruno Simma in the *Oil Platforms* case raise the possibility that some form of "forceful" countermeasures or defensive military action could, in some circumstances, be justified, even absent an armed attack of the grave magnitude contemplated by Article 51.[43] As with self-defense, a state's use of countermeasures must be for the purpose of "protecting itself against further harm, either directly by blocking further hostile

acts against itself or by persuading its tormentor to cease and desist."[44]

As applied in a self-defense-like construct, Judge Simma described the use of countermeasures as follows:

> [T]he permissibility of strictly defensive military action taken against attacks (falling short of armed attack) cannot be denied. What we see in such instances is an unlawful use of force 'short of' an armed attack ('aggression armée') within the meaning of Article 51.… Against such smaller-scale use of force, defensive action—by force also 'short of' Article 51—is to be regarded as lawful. In other words, I would suggest a distinction between (full-scale) self-defense within the meaning of Article 51 against an 'armed attack' … on the one hand and, on the other, the case of hostile action … below the level of Article 51, justifying proportionate defensive measures on the part of the victim, equally short of the quality and quantity of action in self-defense expressly reserved in [Article 51 of] the UN charter.[45]

Judge Simma's analysis regarding the state of customary international law, however, does not reflect that of a majority of ICJ jurists, in part because the international community has not yet begun to formally distinguish or reconcile the apparent conflict between a smaller-scale use of forceful countermeasures and the general prohibition against the threat or use of force.[46]

Although application of a forceful countermeasures doctrine has never been legally tested, it is reasonable to assume that states will act to stop, or prevent, disruptive activity in space and cyberspace, regardless of whether the activity meets a technical "use of force" or "armed attack" threshold, particularly when the second or third order effects of these acts would reasonably threaten national security, public health, and safety or the reasonably predictable effect is significant harm to property or the state's economic well-being. "[D]eciding whether a particular form of cyber-based attack meets … conditions of necessity and imminence depends on the particular perceptions of the threatened state. A targeted government's decision to respond also depends on that state's vulnerabilities and the potential for damage by a particular cyber attack."[47]

In the DoD's initial assessment "[t]he most likely result is an acceptance that a nation subjected to a state-sponsored computer network attack can lawfully respond in kind, and that in some circumstances it may be justified in using traditional military means in self-defense."[48] The practical application of such a policy of course depends on how the US and the rest of the international community resolve these political and diplomatic issues.

Notes:

[1] UN Charter article 2(4); See also article 39, "The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken … to maintain or restore international peace and security"; article 42, "Should the Security Council consider that measures [which do not amount to a use of force] would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security.…"

[2] UN Charter article 51, article 51 goes on to say that "… [m]easures taken by members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."

[3] Abraham D. Sofaer, "Terrorism, The Law and The National Defense," *Miliary Law Review* 126 (1989): 89, 94.

[4] Vida M. Antolin-Jenkins, "Defining the Parameters of Cyberwar Operations; Looking for Law in all the Wrong Places?," *Naval Law Review* 51 (2005): 132, 162 n. 115. See also Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law* 37 (1999): 885, 907-09; and Walter Gary Sharp, *Sr., Cyberspace and the Use of Force* (Falls Church, VA: Aegis Research Corp., 1999), 120, 139-40.

[5] Abraham D. Sofaer, *The Best Defense: Legitimacy & Preventive Force* (Hoover Institution Press: Stanford University, 2010), 2.

[6] Ibid., 90.

[7] Sofaer, "Terrorism, The Law," 96.

[8] Sofaer, *The Best Defense*, 4.

[9] Ibid., 97. See also note 46 and accompanying text.

[10] Eric Talbot Jensen, "Computer Network Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense," *Stanford Journal of International Law* 38 (2002): 207, 218.

[11] Department of Defense (DoD) Office of General Counsel, "An Assessment of International Legal Issues in Information Operations," 1999, 16.; Christopher C. Joyner and Catherine Lotrinote, "Information Warfare as International Coercion: Elements of a Legal Framework," *European Journal of International Law* 12 (2001): 825, 845 (a government under cyber attack would be permitted to respond immediately in self-defense to thwart the attack, but if the government discovers it has been victimized weeks after a cyber assault, international law suggests this should be treated no differently than foreign espionage.).

[12] Antolin-Jenkins, "Defining the Parameters of Cyberwar," 151.

[13] Ibid., 152-53.

[14] Joyner and Lotrinote, "Information Warfare," 845.

[15] Stephanie A. Barbour and Zoe A. Salzman, "The Tangled Web": The Right of Self-Defense Against Non-State Actors in the Armed Activities Case," *International Law and Politics* 40 (2008) 53, 65, citing Military and Paramilitary Activities (*Nicar. v. US*), 1986 International Court of Justice (ICJ) 14, 53-54 (June 27) and Oil Platforms (*Iran v. US*), 2003 ICJ 161, 190-92 (November 6).

[16] John Lawrence Hargrove, "The 'Nicaragua' Judgment and the Future of the Law of Force and Self-Defense," *American Journal of International Law* 81 (1987): 135, 139.

[17] DoD General Counsel, "An Assessment of International," 18.

[18] Joyner and Lotrinote, "Information Warfare," 849 and 854-55.

[19] Darren Huskisson, "Protecting the Space Network and the Future of Self Defense," *Astropolitics* 5 (2007): 123, 130.

[20] Ibid., 129.

[21] See generally President Barack Obama, "Remarks by the President on Securing our Nation's Cyber Infrastructure," White House, 29 May 2009, http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure; see also Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, White House, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[22] Huskisson, "Protecting the Space Network," 129.

[23] Ibid., 131, citing Gregory E. Maggs, "The Campaign to Restrict the Right to Respond to Terrorist Attacks in Self-Defense Under Article 51 of the UN Charter and What the US Can Do About It?," *Regent Journal of International Law* 4 (2006): 149, 158.

[24] Huskisson, "Protecting the Space Network," 133, citing Oil Platforms (*Iran v. US*), 2003 ICJ, 191-92.

[25] Ibid., 135, citing Oil Platforms (*Iran v. US*), 2003 ICJ, 191-92. See also Barbour and Salzman, "The Tangled Web," 66 ("Attacks directed at another state do not entitle the accidental victim to self-defense.").

[26] Susan W. Brenner, "Cyberthreats: The Emerging Fault Lines of the Nation State," 2009, 9.

[27] Huskisson, "Protecting the Space Network," 134 (Describing how

the court discounted evidence, to include overhead imagery of purported Iranian missile sites; analysis of missile fragments from previous missile attacks demonstrating the fragments came from Iranian Silkworm missiles; and testimony of Kuwaiti officers who witnesses missile attacks, including one who saw the flight of the missile which hit the Sea Isle City. With regard to the mine struck by USS Samuel B. Roberts, the Court characterized evidence of moored mines in the area where the ship was struck along with evidence that the moored mines had serial numbers that matched those recovered from the Iran Ajr as "highly suggestive, but not conclusive.").

[28] Ibid., 136.

[29] Brenner, "Cyberthreats," 88.

[30] Ibid., 132, citing Jiangqiang Xin, et al., "A Testbed for Evaluation and Analysis of Stepping Stone Attack Attribution Techniques," 25th IEEE International Performance Computing and Communications Conference, Phoenix, 2006, http://www.public.iastate.edu/~zhanglf/doc/Testbed_TridentCom2006.pdf.

[31] Brenner, "Cyberthreats,"136.

[32] Barbour and Salzman, "The Tangled Web," 61, citing Armed Activities on the Territory of the Congo (*Dem. Rep Congo v. Uganda*), 2005 ICJ 116 ¶¶ 146-147 (Dec 19).

[33] Ibid., 60.

[34] Ibid., 61-62 (emphasis original). The ICJ has made similar pronouncements before and after the Armed Activities decision was issued in Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 ICJ 131, 136 (July 9) and in Application of the Convention on the Prevention and Punishment of the Crime of Genocide (*Bosn. & Herz. v. Serb. & Mont.*), 2007 ICJ 97, 128-148 (Feb 26).

[35] Barbour and Salzman,"The Tangled Web," 71.

[36] Ibid.

[37] See generally Elizabeth M. Lynch, "Adam Segal Discusses US-China Relations in a Cyber World," 14 April 2010, http://chinalawandpolicy.com/tag/patriotic-hackers/; Mayank Chhaya, "India must employ patriotic hackers," *Sify News*, 11 April 2010, http://sify.com/news/india-must-employ-patriotic-hackers-news-national-keljucaidhh.html; Michael Goldfarb, "Patriotic Hackers," Weekly Standard.com, 6 May 2009, http://www.weeklystandard.com/weblogs/TWSFP/2009/05/patriotic_hackers.asp; and Roland Oliphant "Patriotic Hackers," *Russia Profile*, 11 August 2009, http://www.russiaprofile.org/page.php?pageid=International&articleid=a1250009640&print=yes.

[38] Barbour and Salzman, "The Tangled Web," 88 (emphasis original); See also Giuliana Ziccardi Capaldo, "Providing a Right of Self Defense Against Large Scale Attacks by Irregular Forces: The Israeli-Hezbollah Conflict," *Harvard International Law Journal* 48 (2007): 101, 106-108.

[39] Barbour and Salzman, "The Tangled Web," 61, citing Ablrecht Randelzhofer, article 51, *The Charter Of The United Nations: A Commentary* 788, 791 (Bruno Simma ed., 2002) (internal quotations omitted).

[40] Sofaer, *The Best Defense,* 131-32.

[41] Ibid., 72-73.

[42] Huskisson, "Protecting the Space Network," 142 n. 50; See also Matthew J. Sklerov, "Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defense Against States who Neglect their Duty to Prevent," *Military Law Review* 201 (2009): 1, 11-13; and DoD General Counsel, "An Assessment of International Legal Issues," 17, ("There is … a general recognition of the right of a nation whose rights under international law have been violated to take countermeasures against the offending state, in circumstances where neither the provocation nor the response involves the use of armed force.… Discussions of the doctrine of countermeasures generally distinguish between countermeasures that would otherwise be violations of treaty obligations or of general principles of international law (in effect, reprisals not involving the use of armed force) and retorsions—actions that may be unfriendly or even damaging, but which do not violate any international legal obligation. The use of countermeasures is subject to the same requirements of necessity and proportionality as apply to self-defense.… The international law doctrines of self-defense, reprisal, and countermeasures all require that a nation invoking them do so with the intent of protecting itself against further harm, either by directly blocking further hostile acts against itself or by persuading its tormentor to cease and desist.… These doctrines also demand that a state do only what is necessary and proportional in the circumstances.").

[43] Hargrove, "The 'Nicaragua' Judgment," 138 (arguing that, although it did not specifically say so, the court strongly suggested that a victim of an illegal act involving the use of force could legally respond with forceful countermeasures.).

[44] DoD General Counsel, "An Assessment of International," 17.

[45] Barbour and Salzman, "The Tangled Web," 66 n. 54, citing Oil Platforms 2003 ICJ 324, 331-32 (Nov 6) (separate opinion of Judge Simma) (internal footnotes omitted); see also *Nicar v. US* 1986 ICJ, 110 (The court discussed the theoretical viewpoint that "[a] right to act in this way in the case of intervention would be analogous to the right of collective self-defence [sic] in the case of an armed attack, but both the act which gives rise to the reaction, and that reaction itself, would in principle be less grave." However, the court declined to comment further as this discussion was beyond the scope of the particular matter in dispute.).

[46] See Barbour and Salzman, "The Tangled Web," 67 and n.5, citing *Nicar v. US* 1986 ICJ, 128 ("whatever response an illegal attack may permit does not negate '[t]he obligation to refrain from the threat or use of force as embodied in the charter.'") (emphasis original). But see Natalia Ochoa-Ruiz and Esther Salamanca-Aguado, "Exploring the Limits of International Law relating to the Use of Force in Self-Defence," *European Journal of International Law*, 16, (2005): 499, 508 n. 48, (discussing the US position that armed force may legitimately be used "to protect its essential security interests when diplomatic and peaceful measures had failed ('as a last resort'), and when the use of force had proven to be 'reasonable and appropriate.'").

[47] Joyner and Lotrinote, "Information Warfare," 860.

[48] DoD General Counsel, "An Assessment of International," 25.

Col Guillermo R. Carranza (BA, International Relations, Tulane University; JD, Tulane University; LLM, George Washington University) is staff judge advocate, Headquarters 24th Air Force, Lackland AFB, Texas. He is responsible for providing legal services to the command and provides functional oversight of judge advocates, civilian attorneys, and paralegals assigned throughout the command. As the Air Force's newest numbered air force, 24th Air Force provides combatant commanders with trained and ready cyber forces to plan and conduct cyberspace operations. 24th Air Force personnel extend, maintain and defend the Air Force portion of the Department of Defense global network.

Colonel Carranza received his commission by direct appointment in 1989. He has previously served as staff judge advocate and chief of staff, Joint Functional Component Command-Network Warfare at Fort Meade, Maryland; staff judge advocate, Combined Air Operations Center in Southwest Asia; staff judge advocate, Joint Task Force-Global Network Operations in Arlington, Virginia; deputy staff judge advocate, Headquarters Air Force Office of Special Investigations at Andrews AFB, Maryland; staff judge advocate, Prince Sultan AB in Saudi Arabia; instructor, civil law division, Air Force Judge Advocate General's School at Maxwell AFB, Alabama; medical law consultant, 882nd Training Group, Sheppard AFB, Texas; assistant staff judge advocate, 20th Fighter Wing at Royal Air Force Upper Heyford; and assistant staff judge advocate, 93rd Bomb Wing at Castle AFB, California.

Space and Cyberspace: Complementary?

Cerfing (Cyber)Space

Dr. Christopher K. Tucker
Principal
Yale House Ventures
Alexandria, Virginia

The inventor of the Internet (Advanced Research Projects Agency Network [ARPANet]), and more specifically the co-creator of transmission control protocol/Internet protocol (TCP/IP), Vint Cerf has ventured into the world of wiring up space, what has been dubbed the "Interplanetary Internet" (IPN). In doing this, Cerf and his team have created a new protocol, disruption-tolerant networking (DTN), capable of dealing with the delays and disruptions of space communications. Cerf and others took this as an opportunity to solve some of the inherent security problems of TCP/IP and the fundamentals of today's Internet. Moreover, it just so happens that when you engineer your core network technology to inherently deal with disruptions, there are enormous security benefits. This article will discuss the cyberspace security lessons learned from the space-based DTN experience. And, it will also discuss the potential for and benefits of replacing TCP/IP with DTN as the core protocol powering the Internet of the future—interplanetary or not.

Background

In 1998, after 25 years of the Internet's evolution, Vint Cerf began envisioning the Internet in 2025. Realizing that the Internet had come to span the planet Earth, Cerf took on the challenge of networking the solar system. This challenge had its root in the flurry of manned and robotic space exploration that the National Aeronautics and Space Administration (NASA) and others had planned and underway. Cerf knew that TCP/IP was simply not designed to deal with the delays and disruptions inherent in networking in space. So naturally, Cerf in concert with team members from NASA's Jet Propulsion Laboratory, Goddard Space Flight Center, the Mitre Corporation, and Intel Research, Cerf began inventing a protocol that would enable complex space missions—DTN.

As the co-creator of TCP/IP during the original ARPANet project, Cerf had experience the nascent days of the Internet when their hub at the University of California, Los Angeles was connected only to a handful of other nodes. Notably, this sparse network diagram closely resembled the IPN experiments that Cerf and his team later initiated. The experiment simply involved uploading the new DTN protocol software onto a few spaceborne platforms and conducting some dial tone experiments.

DTN, like the original TCP/IP was relatively simple to demonstrate. But, this ease belied the enormous amount of security that was built into DTN which TCP/IP never enjoyed. The driving motivation of all this security work was the avoidance of a future headline such as "15-Year-Old Takes Over MarsNet." DTN has many TCP/IP security lessons learned embodied in its implementation. As national security decision-makers decide on how to staunch the information bleeding, or perhaps more aptly the hemorrhaging that currently characterizes the current cyber-threat environment, an analysis of DTN is clearly in order.

Lessons from Space Communications

When Cerf and his team embarked on their quest to achieve an IPN, it quickly became clear that the brittleness of TCP/IP would simply not do. When speaking at the Open Mobile Summit in San Francisco in 2009, Cerf summed up the network communications challenge posed by space:

> There was a little problem called the speed of light. When Earth and Mars are closest, we're 35 million miles apart, and it's a three and a half minute trip one way, seven minutes for a round trip. Then when we're farthest apart, we're 235 million miles—20 minutes one way, 40 minutes round trip. Just try using TCP/IP for a 40 minute round trip.… [Moreover] The planets rotate, and we haven't figured out how to stop that.… It's a very disruptive system, and it's potentially a variably delayed system, because these planets are moving further apart based on our orbits.[1]

The example of communications between Earth and Mars is illustrative. But, similar delays and disruptions can occur with much shorter distances. Satellite to satellite communication links are orders of magnitude shorter, but yet pose similar patterns of disruption and delay, as has been shown in NASA experiments.[2]

The continuous connection that TCP/IP assumes would fundamentally never exist in a space scenario. When using TCP/IP, a lost connection means that most applications simply will cease working. At the most basic level, DTN was designed address this challenge of delay/disruption by simply hanging onto packets until they can be safely transmitted.

Achieving Mission Success Despite Disruption

If we have learned anything with modern networking (and

As national security decision-makers decide on how to staunch the information bleeding, or perhaps more aptly the hemorrhaging that currently characterizes the current cyber-threat environment, an analysis of DTN is clearly in order.

In the world of satellite to satellite communication, or interplanetary communications, disruptions due to solar flares, orbital dynamics, or any number of other mitigating circumstances cannot be allowed to compromise a mission.

networked) technologies, delay and disruption are hardly unexpected. Whether traversing space, the Internet, or mobile networks, the common denominator of all missions is that they must "fight through" disruptions. In the world of satellite to satellite communication, or interplanetary communications, disruptions due to solar flares, orbital dynamics, or any number of other mitigating circumstances cannot be allowed to compromise a mission. At the tactical edge of a military network, disruptions due to power outages, broken physical links, radio frequency jamming, and more cannot be allowed to compromise a mission. Dependent on commercial cellular infrastructure, first responders must be able to conduct their mission, despite the crush of calls during a catastrophe that make cellular service intermittent.

And, in the realm of cyber-security threats, missions need to "fight through" network penetration with core network infrastructure that is capable of preventing the exfiltration and modification of data, as well as the denial of service. Running a mission, or simply conducting business, requires that users be able to access critical information available over the network without being denied by their adversaries. Even under attack by a sophisticated, internal adversary, operators need to have access to critical information, and know that it will not be disclosed.

The key DTN feature that enables mission success is that unlike TCP/IP, it does not discard data in times of disruption. It implements a "store and forward" model which is different from the way IP multi-casting currently works.[3] DTN provides secure, persistent storage for the data that traverses the network, until delivery is assured. This can be thought of as a DTN cache. The data can be marked with metadata that can be encrypted with different keys from the keys used to encrypt the payload data itself. In this way, DTN maintains the cryptographic integrity of the data in motion and at rest in these caches. And, to provide an extra measure of disruption tolerance, the DTN team has been adapting a convolutional/erasure algorithm scheme (the same sort of encoding associated with RAID devices) that allows data to be reconstituted despite the loss of up to 15 percent of the data traversing the network.

Hardening the Internet's Core

In a TCP/IP environment, current cyber-security measures are commonly limited to protecting our organizations' perimeters and perhaps encrypting our file systems, which just happen to be unlocked at boot. Data exfiltration, modification, and the denial of service are commonplace. And, our responses to network attacks that breach our perimeter are limited. In general, we must take compromised components offline, and curtail our mission-readiness.

If atop TCP/IP you used public key infrastructure and Internet protocol security and insisted on having all devices authenticate, then indeed you would materially improve your organization's security. Assuming that you could trust all the certificates that this construct would rely on, it would harden the core of your network, rather than simply relying on your perimeter defenses. And, many organizations have done just that. But, that is a massive added expense, and a level of technical know-how that typically exceeds that possessed by average organizations.

DTN, at its core, was designed to bring this overlay of security measures into the core design of the network. And, it drew upon other mature techniques learned from other parts of the information and communications technology domain to build an IPN that would not be hijacked by 15-year-olds.

DTN leveraged encryption and structured fragmentation in order to protect against data exfiltration. It used signing and erasure coding to protect against data modification. It looked to diffusion-based replication strategies that protect network resources against denial of service. And, DTN used cache over-encryption in order to achieve dynamic access control. While one would need a forensic analysis of DTN's security architecture in order to trust such an innovative approach to securing network traffic, it is clear that DTN represents an enormous leap in terms of the "built-in" security provided by the core network protocol. It is useful to perhaps dwell on each of these four DTN security features.

As a result of these technical security measures, DTN is able to provide a high level of assurance that missions will continue despite network compromise, and the disruptions and delays due to compromise. In the face of network compromise, DTN enables assured availability and confidentiality. DTN uses a diffusion-based replication strategy, that leverages an encrypted cache architecture, in order to move data to the right user, despite delay and disruption. DTN is designed to provide this level of availability and confidentiality despite network penetration by an adversary who can gain access to both client and data storage nodes, and even eavesdrop on network traffic.

A Critical Layer of Indirection

For those intimate with the inner working of today's Internet, DTN is indeed somewhat unfamiliar. It does not follow many of the assumptions that drive today's Internet.

> [DTN uses] a flexible node addressing scheme in lieu of the traditional IP naming conventions. DTN architecture revolves around a data-centric model, not a network-centric model.… DTN uses a unique, new naming convention for routing the data bundles—not packets—throughout the network. Data is protected while at rest and can be stored along the network path to the destination if the network is not stable.[4]

DTN in some ways is more akin modern wireless telecommunications networks, where each device has an endpoint

identifier (EID) that specifies and uniquely identifies it as an endpoint connected to the network. The information about the location of a given endpoint on the network is given by a "locator" which may change as the network topology changes. In this framework, ongoing communication is not disrupted when a locator changes since endpoints are identified by their EIDs and not their locators.

In the worlds of telecommunications and mobile computing devices, it is not uncommon that a given end device will be connected to more than one IP address. As a user moves from cell tower zone to cell tower zone, it may touch the network (and even the Internet) in multiple places at the same time. To do this, such locators help to dynamically bind the routing layer and the physical endpoints. When you introduce such a layer of indirection, you have the benefit that the device no longer cares which network path(s) you are traversing. The device could simultaneously traverse multiple networks at the same time.

DTN is designed on just such principles. So, as the network topology is disrupted for any reason, communication does not cease. And, due to the caching strategy employed by DTN, data is not lost when a node drops out of the topology. Quite simply, the data finds other ways to make its way to its intended recipient, even if it takes a while.

Security Early and Often

TCP/IP was designed with little regard for security. It was designed to get messages through networks which were assumed to offer high availability. As a result, it is rife with security vulnerabilities because it does not enforce security measures early and often. DTN on the other hand promptly prevents unauthorized applications from having their data carried through or stored in the DTN. It prevents unauthorized applications from asserting control over the DTN infrastructure. It prevents otherwise authorized applications from sending bundles at a rate or class of service for which they lack permission. DTN promptly discards bundles that are damaged or improperly modified in transit, ensuring the highest level of integrity. And, DTN promptly detects and de-authorizes compromised entities.[5]

> [DTNSEC] utilizes hop-by-hop and end-to-end authentication and integrity mechanisms. The purpose of using both approaches is to be able to handle access control for data forwarding and storage separately from application-layer data integrity. While the end-to-end mechanism provides authentication for a principal such as a user (of which there may be many), the hop-by-hop mechanism is intended to authenticate DTN nodes as legitimate transceivers of bundles to each-other. Note that it is conceivable to construct a DTN in which only a subset of the nodes participate in the security mechanisms, resulting in a secure DTN overlay existing atop an insecure DTN overlay. This idea is relatively new and is still being explored.
>
> In accordance with the goals listed above, DTN nodes discard traffic as early as possible if authentication or access control checks fail. This approach meets the goals of removing unwanted traffic from being forwarded over specific high-value links, but also has the associated benefit of making denial-of-service attacks considerably harder to mount more generally, as compared with conventional Internet routers. However, the obvious cost for this capability is potentially larger computation and credential storage overhead required at DTN nodes.[6]

Adopting and Adapting

DTN is not just an idea. It has been implemented in an open source software stack that has been through the bureaucratic processes to determine that export restrictions should not prevent its distribution to other space-faring nations. The DTN protocol suite could easily be adopted by commercial infrastructure providers such as CISCO, Juniper, F5, Huawei, Alcatel-Lucent, and US Tellabs. Google, no doubt by virtue of Cerf's employment, has already rolled DTN into its Android platform in order to take advantage of its ability to overcome the disruption and delay in mobile networks. Microsoft could, no doubt, roll out DTN in upcoming releases of Windows operating systems.

The Internet is continually adapting, with the term "Internet year"[7] used as the provocation to every innovator to remind them how fast they must act, or else be overcome by events. It would only take a handful of Internet years to ensure DTN is ubiquitously available. Some public sponsorship would be required, akin to the Defense Advanced Research Projects Agency support currently being applied to the exploration of DTN's battlefield benefits.[8] But, the scale of resources that would be required to enable the adoption of and adaptation to DTN would inevitably be orders of magnitudes less than that required to secure a TCP/IP based Internet.

In short, it is easier to build a body that doesn't bleed with DTN than it is to stem the hemorrhagic bleeding we experience in TCP/IP networks.

Ending Internet Hostilities

For a long time, popular culture has embraced the notion that the Internet is rather safe, in terms of cyber security. Even more sophisticated enterprise views of security have assumed that their perimeter security measures are keeping their operations safe and secure, in the face of possible cyber threats. It is high time, however, that we begin to understand that whatever cyber activities we engage in, we are engaging in them over a hostile Internet infrastructure. It is hostile in large part because TCP/IP as a protocol leaves users and enterprises wide open to panoply of attacks simply because of its original design. And, its vulnerabilities have become so well understood that random 15 year olds can wreak enormous amounts of havoc.

Unless the user or enterprise is very sophisticated in its se-

It is high time, however, that we begin to understand that whatever cyber activities we engage in, we are engaging in them over a hostile Internet infrastructure.

curity investments atop this insecure infrastructure, they will be utterly defenseless in the face of rising, organized Internet hostilities—whether posed by nefarious nation states, non-state actor networks, organized crime, or lone bad actors.

Many billions of dollars are currently being amassed and spent to address these hostilities. And, epic engineering efforts are currently being envisioned. In this context, it is not too much to ask that we evaluate the fundamental shortcomings of today's Internet, and entertain a wholesale switch to a stronger and secure foundational protocol.

Acknowledgement:

While "Cerfing (Cyber)Space" suggests that Cerf alone is responsible for the future of the Interplanetary Internet, Cerf takes great pains to acknowledge the contributions of his colleagues Robert Durst, MITRE; Adrian Hooke, NASA; Scott Burleigh, JPL; Keith Scott, MITRE; Leigh Torgerson, JPL; Kevin Fall, Intel Research; David Israel, Goddard Space Flight Center; and Jay Wyatt, JPL.

Notes:

[1] Cade Metz, "Vint Cerf mods Android for interplanetary interwebs," *The Register*, 5 November 2009, http://www.theregister.co.uk/2009/11/05/vint_cerf_on_mobile/.

[2] NASA Successfully Tests First Deep Space Internet, NASA press release 08-298, 18 November 2008.

[3] Nicole Ferraro, "Vint Cerf Details Interplanetary Plans for DTN," Imnternet Revolution, 29 September 2009, http://www.internetevolution.com/author.asp?section_id=466&doc_id=182432.

[4] Lt Col Bruce D. Caulkins, "Proactive Self Defense in Cyberspace," US Army War College Strategy Research Project, 2009.

[5] Vint Cerf, et al., "Delay-Tolerant Networking Architecture," Internet Engineering Task Force, IETF, 2007, http://www.ietf.org/rfc/rfc4838.txt

[6] Ibid.

[7] Eric Reiss, "Calculating the length of an internet year," FatDUX, blog, 22 September 2009, http://www.fatdux.com/blog/2009/09/22/calculating-the-length-of-an-internet-year/comment-page-1/.

[8] Disruption Tolerant Networking (DTN), Strategic Technology Office, STO, http://www.darpa.mil/sto/strategic/dtn.html.

Other Citations:

Cerf, Vint, et al. "Interplanetary Internet (IPN): Architectural Definition." InterPlaNetary Internet Research Group, IPNRG. 2001. http://www.ipnsig.org/reports/memo-ipnrg-arch-00.pdf.

Cerf, Vint, et al. "Delay-Tolerant Network Architecture: The Evolving Interplanetary Internet." InterPlaNetary Internet Research Group, IPNRG. 2003. http://www.ipnsig.org/reports/draft-irtf-ipnrg-arch-01.txt.

Cerf, Vint, et al. "Delay-Tolerant Networking Architecture." Internet Engineering Task Force, IETF. 2007. http://www.ietf.org/rfc/rfc4838.txt.

Fall, Kevin. "A Delay-Tolerant Network Architecture for Challenged Internets." SIGCOMM. 2003 August. http://conferences.sigcomm.org/sigcomm/2003/papers/p27-fall.pdf.

Fall, Kevin. Delay-Tolerant Networking for Extreme Environments. Powerpoint Presentation to Intel Research, Berkeley, California. http://www.ipnsig.org/reports/Kevin-paper.pdf.

Farrell, S and V. Cahill. "Security Considerations in Space and Delay-Tolerant Networks." Proceedings of the 2nd IEEE International Conference on Space Mission Challenges for Information Technology.

Hooke, Adrian J. "Towards an Interplanetary Internet: A Proposed Strategy for Standardization. Jet Propulsion Laboratory. California Institute of Technology. Pasadena, California, USA. 2003. http://www.ipnsig.org/reports/SpaceOps-Oct-2002.pdf.

Kate, A., G. Zaverucha, and U. Hengartner. "Anonymity and security in delay-tolerant networks." 3rd International Conference on Security and Privacy in Communication Networks (SecureComm). 2003.

Dr. Christopher K. Tucker (BA, Political Economy, Columbia College, Illinois; MA, MPhil, and PhD, Political Science; Graduate School of Arts and Sciences, New York) manages Yale House Ventures, a portfolio of social ventures and technology companies that span the worlds of energy, geospatial, sensor, cyber-security, open source, and social media technologies, across the domains of defense/intelligence, international affairs, civilian government, commercial industry, nongovernmental organizations, and academe.

Dr. Tucker was previously senior vice president for the Americas and National Programs at ERDAS, a leading technology provider for geospatial exploitation, analysis, data management/dissemination, information sharing, and collaboration across the defense, intelligence, civilian federal, state/local, and commercial sectors—worldwide. Dr. Tucker came to ERDAS by way of the acquisition of IONIC, the world leader in interoperable Web-mapping, location based services, imagery management, and distributed geoprocessing, where Dr. Tucker served as president and chief executive officer. (CEO) While commercial technology companies, IONIC/ERDAS's core businesses have always been defense and intelligence.

Dr. Tucker is on the Board of Directors of the Open Geospatial Consortium (www.opengeospatial.org), an international industry consortium of 350+ companies, government agencies, and universities participating in the development of technical standards to that support interoperable solutions that "geo-enable" the Web, wireless and location-based services, and mainstream IT. Dr. Tucker is also on the Board of Directors of the US Geospatial Intelligence Foundation (www.usgif.org), where he is on the management committee, working closely with the president and CEO to advance the geospatial intelligence (GEOINT) community, technical interoperability, and intelligence tradecraft. Dr. Tucker served on the National Research Council's Committee on National Geospatial-Intelligence Agency's (NGA) GEOINT research priorities, helping to define the research and development (R&D) investment strategy that NGA must undertake in order to transform to its future concept of operations. Dr. Tucker serves on the secretary of the interior's National Geospatial Advisory Committee.

Dr. Tucker was the founding chief strategic officer of In-Q-Tel, the Central Intelligence Agency's venture capital fund, focusing his efforts on developing In-Q-Tel's overall strategy for tackling the agency's priority information technology problems. As such, Dr. Tucker was responsible for managing the technical portfolio, issues of organizational design, and relations with the intelligence community, industry, and media.

As special advisor to the executive vice provost of Columbia University, Dr. Tucker was responsible for a range of issues having to do with strategic institutional development, R&D portfolio management, federal science and technology policy, and the organization of interdisciplinary research. While at Columbia, Dr. Tucker co-founded the Center for Science, Policy, and Outcomes and taught several courses at the Columbia School of International and Public Affairs.

Space and Cyber: A Valuable Strategic Alliance

Mr. Rich Baich, CISSP, CISM
Principal, Security and Privacy Service
Deloitte & Touche LLP
Charlotte, North Carolina

Information superiority is an important factor in the past, today, and in the future. A nation's ability to effectively communicate, making sure information is authenticated and arrives in a timely fashion, has been critical to national security for thousands of years. Whether it was the use of smoke signals to alert villages of enemies approaching or soldiers on horseback delivering notes across geographies to provide information to others exemplifies that the ability to deliver accurate information has been vital to civilizations since records have been kept. The capability to provide information confidentially with the appropriate level of integrity, coupled with the highest levels of availability, has been crucial to a nation's success throughout history. Adversaries have been able to target and intercept the transmission of communication (data flow) for as long as there has been a need to communicate. In fact, adversaries quickly realized they could use the same communication methods to deceive, confuse, or influence others. For example, introducing additional smoke signals could change the message or confuse the intended parties. In an April edition of *Business Week*, the magazine provided detail on how this type of exploit had been targeted at specific Department of Defense individuals. Space operations' and cyber operations' functionality has changed how data is transmitted; however, the use and the desire to deny, deceive, and disrupt information transmitted has not changed. To effectively overcome the exploitation of these operations, space and cyber need to work together sharing leading practices, strengthening public and private alliances, and taking action to develop strategic deterrence.

Today, information travels at the speed of light through a variety of complex infrastructures. These infrastructures can provide various levels of security resulting in a sense of confidence that the information being passed is accurate. Different levels of protection, as well as disguise, can be used to protect/hide this data as it moves across different mediums to include encryption and stenography. Space operations have focused for years on the importance of verifying the destination of their communications due to the severity of impact related to successful exploitation. If a satellite feed could be redirected to another location the amount of information passed to a potential adversary could be extremely damaging to a nation's security. Do organizations today understand and verify the destination of their cyber transmissions? Did the data leaving your organization actually arrive at the destination it was intended to be delivered? Adversaries have taken the time to redirect and disguise data exfiltration through existing cyber networks. There is opportunity to mitigate these risks by focusing on data transmissions and finding anomalies associated with the transmission destinations.

Cyber security vendors and practitioners can learn from space experiences. Due to the sensitivity of space programs, supply chain controls and vetting have been in place for many years. High reliability requirements for space assets have driven clean and secure software standards to be employed. These are issues that cyber security operators are just beginning to tackle. One of the main differences between space and cyber is space built security into its architecture taking the time to understand the threats, the vulnerabilities, the probability of occurrence, and the value of the assets they were trying to protect. This enabled space operators to better understand the risks associated with the decisions and the investments being made, ultimately driving a culture of security in the space program lifecycle. An example is cloud computing; cloud computing was put into an operational environment prior to investing time and resources integrating security controls into the operations and architecture. In general, cyber is trying to embed these similar qualities into the cyber operational lifecycle after the fact causing funding, cultural, architectural, and human capital related issues.

Any space asset can become a weapon, as can any information technology host. There is no clear definition for a space weapon or a cyber weapon. However, a satellite could be used to destroy other space assets much like a cyber asset could be used to destroy other cyber assets. The ability to monitor and have situational awareness of space or the Internet provides a maze of misdirections resulting in a difficult ability to succeed at timely attribution.

Space and cyber are mediums that can be used to perform a variety of missions to include intelligence collection, exploitation, and attack. Space and cyber assets are often used by many different companies and nations to perform a variety of tasks. The interdependencies of these tasks and their impact to our global economy are often overshadowed by the cybersecurity related news flashes. We find organizations and governments focused on the interdependencies of their critical infrastructures as it relates to cybersecurity. The US military has recently made a decision to establish the US Cyber Command; US Space Command was established in 1985 with the intent to help institutionalize the use of space in the US deterrence efforts. US Cyber Command should also have deterrence somewhere within its mission and goals.

A White House Web site from the Office of Science and Technology Policy stated the following regarding US Space Policy:

> Ensure freedom of space by assessing possible threats to US space assets and identifying the best options, military and diplomatic, for countering them; accelerating programs to harden US satellites against attack; and establishing contingency plans to

ensure that US forces can maintain or duplicate access to information from space assets if necessary.

The US continues to struggle with the mission of US Cyber Command; one could suggest that replacing cyber for space in the description above could help describe the mission more appropriately.

In a speech delivered by Secretary of State Hillary Clinton earlier this year, she mentions:

> Governments and citizens must have confidence that the networks at the core of their national security and economic prosperity are safe and resilient.… Our ability to bank online, use electronic commerce, and safeguard billions of dollars in intellectual property are all at stake if we cannot rely on the security of information networks.… Disruptions in these systems demand a coordinated response by governments, the private sector, and the international community.… States, terrorists, and those who would act as their proxies must know that the US will protect our networks. Those who disrupt the free flow of information in our society, or any other, pose a threat to our economy, our government, and our civil society. Countries or individuals that engage in cyber attacks should face consequences and international condemnation. In an interconnected world, an attack on one nation's networks can be an attack on all. By reinforcing that message, we can create norms of behavior among states and encourage respect for the global networked commons.…

There are hints of deterrence related strategies coupled with acknowledgements of the cyber threats. Rather than treating cyber as a new unknown there is opportunity to leverage existing space program policies, programs, and projects to help accelerate the measurable effectiveness of US Cyber Command.

An attack on one is an attack on many. This is a powerful phrase often used when discussing deterrence. Space manufacturers have recognized that there are important dependencies related to the services provided and enabled as a result of space assets and the space networks. Consequently, space vendors have begun to allow various countries to share the capabilities of their space assets. For example, by allowing the US, France, Australia, and Japan to all use the same space asset to carry out various services from space, the space vendors are creating a potential strategic alliance with various countries. If another country were to destroy that particular space asset, in essence they would have to deal not with just their intended target but other potential countries. This approach is similar to a strong modern day alliance such as the North Atlantic Treaty Organization. Conflicts of the past have shown that strong and effective alliances often win wars.

Cyber security predominantly utilizes the Internet with various different peripherals providing a variety of services. Cyber traffic passes through various countries; the Internet architecture today provides a similar strategic alliance for vendors and counties. The interdependencies today disprove the "Cyber Pearl Harbor" example often used today because the goal of Japanese attack on Pearl Harbor was to crush the American's war making capability. With the Pacific Fleet demolished, America would not be able to wage war. Destroying a server or rendering a Web server incapable through malware injections does not have the same impact as destroying the Pacific Fleet; one could quickly replace a server to enable the data transmission destroyed by an adversary.

Alliances have proved to be a cornerstone of success since the Peloponnesian Wars back in 431 BC. We find that history repeats itself and the enemies desire to exploit, deceive, and disguise communications continues as new technology drives the battle for timely, accurate, and dependable information. This information is an enabler resulting in real-time decisions which could impact loss of life, nations' secrets and retribution from the potential enemy states. Space and cyber face similar interests from adversary related to exploitation during peacetime and potential kinetic damages during war time. Space and cyber function as intelligence tools today. An adversary's ability to use these tools while exploiting others for national/state gain and influence produce a real threat to global stability. There is strength in numbers; consequently, space and cyber operations should continue to strive to establish alliances with other nations, resulting in a strong deterrence posture.

Mr. Rich Baich (BS, US Naval Academy; MBA and MSM, Management, University of Maryland University College) is a principal in Deloitte & Touche LLP's Security and Privacy Service, where he leads the cyber threat and vulnerability management practice. He is a leading security and privacy practitioner for the financial services industry and a contributor to the Center for Security and Privacy Solutions. Most recently, he co-authored the paper entitled "Cyber Crime: A Clear and Present Danger."

He has led multi-national teams in both the private and public sector, advising global organizations to effectively and efficiently balance risk, technology, and data management decisions with data protection, regulatory compliance issues, privacy, and security controls. Mr. Baich's operational experience includes designing, assessing, and delivering security and privacy regulatory remediation strategies.

As former chief information security officer (CISO) for ChoicePoint, Mr. Baich held enterprise-wide responsibility for the architecture, design, risk, business continuity, and implementation of information and technology security. He also served as the organization's official executive representative to internal and external customers, audit, regulatory, and law enforcement on information security matters.

Mr. Baich's security leadership roles include naval information warfare officer for the National Security Agency, senior director for Professional Services at Network Associates (now McAfee) and after 9/11, as special assistant to the deputy director for the National Infrastructure Protection Center at the Federal Bureau of Investigation. He is currently serving as a reserve commander in the Information Operations Directorate at NORAD/Northern Command Headquarters in Colorado Springs, Colorado. Prior assignments include tours within the Real Time Military Analysis Center, the Reserve Armed Forces Threat Center, the Center for Information Dominance, the Information Operations Technology Center, and the National Reconnaissance Office.

Industry Perspective

The Cyber Kill Chain: a Foundation for a New Cyber Security Strategy

Lt Gen Charles Croom, USAF, retired
Vice President, Cyber Security Solutions
Lockheed Martin
Information Systems & Global Solutions
Gaithersburg, Maryland

The conventional wisdom in some corners of the cyber security world is that the defenders of critically important information technology assets are locked in an asymmetric battle in which the enemy enjoys a perpetual advantage. For every shield deployed by defenders, adversaries invent hundreds, even thousands, of new weapons and tactics. Only one of the adversaries' millions of fired rounds must penetrate the defenses, while the defenders are faced with the impossible task of stopping every bullet.

As is often the case, however, the conventional wisdom is fundamentally overstated. Yes, the battle is asymmetric when fought on the adversaries' terms, but the advantage does not always belong to offense, unless we allow it to be. Every successful commander knows that shaping the battlefield—choosing where, when and how to fight—is essential for securing a strategic advantage and, ultimately, defeating the enemy. For too long in cyber space, the enemy has been allowed to choose the terms of battle. It is time for that to change. Given the value of our nation's cyber assets — not only for defense, but including critical infrastructure like energy and healthcare information technology (IT) services—adopting this new cyber security vision is not just desirable, it is imperative.

Contemporary defensive approaches presuppose the adversary has this advantage. But this advantage is not inherent, by changing the defender's perspective; we can win, meaning we can stop the intruders from achieving their goals, by understanding how the adversaries operate, and adjusting defenses to cut off their avenues of attack. Our industry already has many of the tools and processes required to detect and repel network intruders, and we are rapidly training our workforce and developing new technologies and procedures to close the gaps that remain. What the cyber security community as a whole has not done, but what is very much within our reach, is to use and share our emerging understanding of enemies' tactics to develop a new concept of operations.

To understand the adversaries, first, there needs to be an appreciation that different threats have different tactics, and the most-insidious grouping of attackers are categorized as advanced persistent threats (APT). Second, based on analysis of today's attack patterns, we view APT intrusions differently. Instead of events, they are progressions of linked actions. Each intrusion, therefore, requires the aggressors to pass through sequential steps before they can meet their ultimate objectives. Viewing attacks in this manner, in the context of an attack kill chain, provides a road map for a new security strategy. The defender can interrupt an intrusion by mitigating just one phase, whereas, the attacker must be successful at all phases. But the defender can further achieve strategic advantage, by mitigating across all phases of the kill chain. The adversaries would then have to change their methodology for every single phase to be successful. Finally, no tool or process alone today can accomplish this level of intelligence analysis; skilled analysts, collaborating with others to share indicators of intrusions, are an essential component to this successful strategy. Neutralizing today's cyber security threats is not rocket science, but rather a broader vision, implemented cohesively, and supported by improved training, processes, and metrics.

The Security Imperative

The critical importance of cyber security can be summed up in two words: mission resiliency. Whether in the context of sensitive data, defense systems, or public and private infrastructure, our nation's most-critical systems and assets must continue to operate, in all situations, even in the midst of an intrusion. On the battlefield, mission resiliency depends on agile access to trustworthy information, when and where needed, giving commanders accurate situational awareness and the freedom to execute their battle plans while staying inside the adversary's decision cycle. Clearly, the pervasive dependence on information technology to execute critical missions—across defense, government and industry sectors—makes winning the fight in cyberspace as important to our nation as dominance on the battlefields of land, air, sea, and space.

As our reliance on information technology to execute a wide range of missions has increased, so has our adversaries' onslaught against it. Understanding the nature of this onslaught and the actors behind it is essential for devising effective cyber security strategies.

This is important considering the exponential increase in volume of attacks. Symantec, a leading developer of security software, noted in its Global Internet Security Threat Report, volume XV, that almost three million new malicious code signatures were written in 2009, which was more than in the previous 15 years combined. These data suggest that there are more unknown than known threats, yet many of today's cyber security solutions are focused on defensive blocking to address threats with known signatures—absolutely required yet not comprehensive.

There is common recognition that defenses are likely missing a significant portion. Dick Schaeffer, retired National Security Agency director of information assurance stated that with industry best practices, we are capable of—when implemented

We must include processes to bring visibility and auditing of the manufacturing of electronic systems, and consider anti-tamper technology for those devices that travel outside of our physical control.

properly—turning away an estimated 80 percent of cyber attacks that storm the network access points. This is because the majority of attacks—although they have grown increasingly sophisticated over time—continue to be primarily opportunistic in nature, designed for hit-and-run network disruption, or personal data theft. They rely on a high volume of attempts, hoping to discover unguarded or inadequately guarded assets. By implementing best practices and closing gaps with integrated defenses, organizations can neutralize most of these attacks. The solutions and procedures to manage these exists today, and are in use by many forward thinking agencies, each organization must identify the best way to utilize them for themselves.

What of the attacks that fall outside of this notional 80 percent? Herein lies the great challenge faced by the cyber security community. The unknown threats, and APT, theoretically fall within the 20 percent category though we believe we have the opportunity to predict and manage them.

Advanced Persistent Threats

Because of the high-value of today's IT assets, the nature of our enemies has changed, and so have their strategies. We find ourselves confronted today by more dangerous and effective adversaries, including organized crime, terrorists, and nation states seeking economic, political, or military gain. These highly motivated and well-funded groups and individuals are stealthier, more patient and more persistent. Their intent is not to "smash and grab," but to establish a presence deep inside their target networks, where they can exfiltrate data over long periods without alerting victims to their presence. Think of them as the cyber equivalent of the espionage mole.

These advanced persistent threats cannot be thwarted by the traditional approach of deploying bigger and more-numerous defensive shields. They often employ social engineering strategies that target specific individuals as points of entry—a practice known as "spear phishing"—and they have the resources to develop customized malware and "zero-day" exploits that patching and anti-virus software cannot detect or mitigate. Above all, they are persistent. Once their barrage on external defenses has succeeded in placing one spear in the network corpus, they probe continuously, looking for vulnerabilities that will enable them to advance their intrusion *from the inside*, where externally facing defenses are not effective. Moreover, APT intrusions are not isolated or discrete events, but rather elements of a concerted campaign that can span years in length. The persistent threats adapt to the defenders, reassessing after attempt, and choosing branches and sequels to the campaign.

Because these targeted intrusions take time and are expensive to mount, their sponsors focus on highly valuable information—the kind that resides within government and critical infrastructure information technology systems and networks. In addition to representing high-value targets, these systems are particularly vulnerable by the nature of their structure and legacy components. Government networks, both civilian and defense, are heterogeneous across agencies, and often they are a consolidation of many systems and networks acquired and built over time to different standards. The security solutions for these systems and networks and the software residing on them were not conceived and implemented as a cohesive whole and therefore remain porous to a knowledgeable intruder. From the architect who did not consider the integration of disparate systems, to the developers who did not consider security in their code development and exposed application level vulnerabilities, too many of these infrastructures and environments are ill-designed to repel today's advanced threats.

Further, APT is not just targeting networks and systems that are in place today, but also indirectly targeting via the supply chain as another threat vector where adversaries can insert malicious code or hardware to establish a command and control (C2) channel once the component is installed on the environment. We must include processes to bring visibility and auditing of the manufacturing of electronic systems, and consider anti-tamper technology for those devices that travel outside of our physical control.

The Advanced Persistent Threats 'Kill Chain'

Before cyber defenders can win the battle against advanced persistent threats, they must understand how their adversaries operate. At Lockheed Martin, we have analyzed APT intrusions and identified seven phases that characterize their progression, which we describe in defense parlance as the "kill chain."[1] We

Figure 1. Cyber Kill Chain.

use this methodology to defend our enterprise network every day. For the defender, the most-important lessons of the kill chain is that it clearly shows the adversary must progress successfully from each stage to the next before it can achieve its desired objectives; just one mitigation disrupts the chain and defeats the adversary. The more mitigations the defenders can implement across the chain, the more resilient the defense becomes. The components of the kill chain include:

1. **Reconnaissance**. Research, identification and selection of targets, often represented as crawling Internet Web sites looking for email addresses or information on specific technologies.

2. **Weaponization**. Coupling a remote access Trojan with an exploit into a deliverable payload, typically using an automated tool. Increasingly, data files such as Microsoft Office documents or Adobe PDF files serve as the weapon delivery device.

3. **Delivery**. Transmission of the weapon to the target. The three most-prevalent delivery vectors for weaponized payloads are e-mail, Web sites, and USB removable media.

4. **Exploitation**. Triggering of the attacker's code. Most often, the weapon exploits an application or operating system vulnerability. It might simply exploit the user by persuading him to open an executable attachment, or leverage a feature of the operating system that auto-executes code.

5. **Installation**. Installing a remote access Trojan or backdoor on the victimized system, allowing the attackers to affect all users of the system and to maintain persistence across system reboots.

6. **C2**. Accomplished most often with an outbound beacon to an Internet controller server, which establishes the C2 channel. This connection provides the manual "hands-on-the-keyboard" access that is required by most APT malware.

7. **Actions on objectives**. The final stage required for a successful intrusion. The most common objective is data exfiltration: collecting, encrypting, and stealing information from the compromised system. Attackers might also seek to violate data integrity or availability. Yet another objective might be to move laterally through the victim's IT environment, spawning new kill chains on subsequent targets.

Attack Reconstruction and Synthesis

Seeing and understanding the kill chain progression from the adversary's perspective provides invaluable guidance for analyzing intrusions when they are detected. A given detection will typically provide a limited set of attributes for any single phase of an attack, but further analysis can reveal many other features and provide options for multiple courses of defensive action. Furthermore, detecting an intrusion in one phase allows defenders to track the attack to prior phases that were executed successfully without detection. The early intrusion phases can then be analyzed to gather information that will help disrupt future attacks earlier in the kill chain.

Equally as important as analyzing an intrusion from its inception is following it through to the conclusion it would have reached had it not been detected. By synthesizing what *might* have happened, defenders can discover the techniques that attackers planned to employ in subsequent phases, such as installation of a backdoor.

For example, an adversary could send a zero day exploit within a spear phishing email to an individual in the organization. The exploit would not be discovered by the anti-virus software at the gateway or the workstation, but the delivery of the email included indicators that were associated with a known APT campaign, and the intrusion is blocked at the delivery phase. The malicious code is then debugged, and a zero-day exploit is identified and shared with the defense industrial base community. The adversary had a new Exploit, but did not change the delivery mechanism; and if they did, most likely, the C2 channel, would be the same one they always use, and the intrusion would be caught there. This realization allows the defender to be much more effective in developing resilient mitigations, mounting a proactive defense instead of playing catch-up, and prioritizing investments in new technology and processes.

An Enterprise Approach to Cyber Defense

Armed with knowledge of our adversaries' strategies, how does the defender exploit that knowledge to develop a robust defense that assures mission resiliency in the face of even the most sophisticated intrusions? The answer is a reconfiguration of our approaches to cyber defense, complemented by advanced tools built to defend against the highest-priority threats, with trained staff using mature processes. This, plus closer partnerships, and more information sharing will enable the cyber security community to neutralize the attackers' current advantage.

The essence of the solution is an enterprise approach that treats cyber security holistically, not as a collection of discrete functions—from network access control and data-leak prevention to system audits and forensic analysis—that have tradition-

The essence of the solution is an enterprise approach that treats cyber security holistically, not as a collection of discrete functions—from network access control and data-leak prevention to system audits and forensic analysis—that have traditionally operated within organizational silos.

Figure 2. Lockheed Martin Security Intelligence Center.

ally operated within organizational silos. This new approach is built on three pillars: integrated solutions, proactive services, and resilient systems.

The ***integrated solutions*** pillar closes the gaps between excellent commercial products that often are deployed piecemeal and with little coordination by separate IT organizations. Point solutions can be effective as far as their specific capabilities take them, but by themselves they are not a comprehensive defense. They require integration into a seamless security fabric that can be stretched across the entire software and hardware enterprise. In addition to technology, such an end-to-end system of systems also exemplifies that the analysts themselves cannot be specialists using a single tool or technology, but instead must be multidisciplinary experts, creatively linking data together in new ways to address the current challenge at hand.

Yet another important aspect of the integrated approach addresses performance metrics. For example, traditional metrics, such as attacks detected and mitigated, does little to shed light on the actual amount of data leaking from a network. Measuring the wrong things provides a false sense of security and must be replaced with a more mature set of metrics. Recently, government and industry cyber defense experts identified 20 security controls—called Consensus Audit Guidelines (CAG)—to help organizations become more effective in knowing what they need to defend against and how well they are doing it. CAG documentation identifies specific attacks that are mitigated by each control, lists best practices for automating controls, and defines tests to determine whether each control is effectively implemented. As part of an integrated solution, the CAGs can serve as a baseline for continuously measuring cyber security and ensuring audit compliance, certainly to address the 80 percent of cyber attacks.

With an integrated solution in place, the second pillar of an enterprise approach, ***proactive services***, provides the technology solutions and planning to address both known and unknown threats. Developing and integrating the best IT security products is a team sport, whether it is through public/private partnerships, research and development with laboratories and universities, or collaboration with the defense industrial base. This teamwork is essential if we are going to leap ahead of the adversaries.

We have teamed with industry partners to create a cyber security technology alliance. Participating in the alliance are Cisco, Intel, McAfee, Microsoft, Symantec, Juniper Networks, EMC, RSA, VMware, NetApp, CA Technologies, Dell, Hewlett Packard, and APC. The partners have installed their latest solutions, supported by technical experts, at our new NexGen Cyber Innovation and Technology Center. They also are testing live, simulated customer solutions on a global cyber range that provides realistic environments through a connected, high-speed test range. These solutions provide a secure end-to-end foundation that offers effective protection from known and unknown threats and creates an environment for understanding our enemies' offensive strategies, which in turn informs our defensive actions across global cyberspace. The alliance leverages the test range to perform advanced repeatable exercises, using current intrusion techniques that can accelerate the defender's learning curve to combat sophisticated attacks.

At the same time, the alliance partners, national laboratories, and major universities collaborate on research and development efforts to better address the difficult challenge of identification and mitigation of unknown threats. These solutions are tested and integrated to ensure effective assimilation within customer environments.

The goal of all of this research and experimentation is to identify threats as early as possible and eliminate the element of surprise. There are indications and warning signs, inherent within data streams that can provide this visibility into potentially harmful intrusions before they achieve their objectives. Analyses of attacker behavioral patterns are helping predict precursor events before a real intrusion, and therefore become an indicator and warning alarm bell for the defender.

The third pillar of the enterprise approach, ***resilient systems***, addresses the eventuality that a system, no matter how well defended remains vulnerable, and may at some point be victimized by a successful attack. Because of this reality, a fully integrated and tested solution should be regarded only as a solid foundation and not a fully adequate defense against persistent, sophisticated, and ever-changing threats. To reach the next level of effectiveness, the solution must ensure mission resiliency even during—and immediately after—an intrusion.

Manual techniques and processes are not sufficient to handle the magnitude of the threat. Speed of recovery is essential, and it can occur only when we remove time-consuming operator actions. That means introducing autonomic recovery—

The 'Cyber Security' Alliance leverages the test range to perform advanced repeatable exercises, using current intrusion techniques that can accelerate the defender's learning curve to combat sophisticated attacks.

We have described the kill chain process to turn asymmetric battle to the defender's advantage; and if the industry can leverage partnerships, and collaborate with better information sharing, the defenders can start to win.

machine-to-machine interactions that can respond to the threat at the speed that the intrusions are occurring. Assimilation of libraries of data; fusing multi-source intelligence and network operations data; selecting courses of action; and implementing those actions across global networks demands a significantly higher level of autonomic C2 of the network than currently exists. One approach to autonomic recovery is a self-healing system in which software and hardware either repairs itself or returns to a trusted state, while continuing to operate through the attack.

Rising to the Challenge

Achieving the 80 percent security solution is not revolutionary. The technology and processes exist today. Nevertheless, effective implementation will require something that can prove difficult—cultural change. Our adversaries are not smarter or more experienced, but to defeat them we must take a new approach to how, when and where we deploy our resources against them. In an environment where friends and foes share the same global cyberspace, we cannot dig our moat wide enough or deep enough to ensure that no attacker reaches our gates. We can, however, stop the enemy from achieving his aims, which are theft of our data and disruption of our systems. Combating the remaining 20 percent of sophisticated APT is achievable; we are seeing modern resilient systems being demonstrated within national labs, and within research and development teams. We have described the kill chain process to turn asymmetric battle to the defender's advantage; and if the industry can leverage partnerships, and collaborate with better information sharing, the defenders can start to win.

To do so, defenders must implement integrated solutions that overcome the barriers created by discrete organizations with piecemeal systems and tools. We must also recognize cyber defense for what it is—a risk management challenge for the *entire* organization, not an office within the information technology function. Defense of cyberspace is mission critical to the entire organization, and decisions affecting the deployment of cyber defense resources must reflect that reality. Commanders must lead the change. It is commander's business. What are our most-critical missions? What is our most-valuable information? Where does it reside? How long will it retain its value and how long must it be protected?

To be truly effective against the latest generation of cyber enemies, we all must expand our view of the battlefield. We must implement new strategies for defense with intelligence-driven processes such as modeling intrusions on a kill chain. We must develop new technologies, deploy them in a more integrated fashion, and put them in the hands of skilled analysts with mature processes. And lastly, we must be agile and adapt to a changing threat environment to achieve and maintain a mission-resilient posture.

The cyber war *can* be won if we cultivate an enterprise-wide vision implemented by highly trained professionals with as much persistence as our enemies.

Notes:

[1] The Cyber Kill Chain and the concept that an unbroken sequential chain of events for success was conceived by Eric Hutchins, Senior Cyber Intel Analyst, and the Lockheed Martin EBS team.

Lt Gen Charles "Charlie" Croom, USAF, retired (BS, Electrical Engineering, Rutgers University, New Jersey; BA, Economics, Rutgers University; MBA, Management and Business Administration, Webster College, Missouri) joined Lockheed Martin Information Systems and Global Solutions as vice president of Cyber Security Solutions in October 2008. In this capacity, he shapes the corporation's cyber security strategy with insight from his 35 years of distinguished service, leadership, and technology experience from the US Air Force.

General Croom co-chaired a National Security Telecommunications Advisory Committee Task Force on "Strengthening Government and Private Sector Collaboration" which issued a May 2009 report recommending that the president direct the establishment of a Joint Coordinating Center. He currently serves on the boards of the National Cyber Security Alliance and the Internet Security Alliance.

General Croom retired as a US Air Force lieutenant general, director of the Defense Information Systems Agency (DISA), and the commander of the Joint Task Force for Global Network Operations in September 2008. While at DISA, he led a worldwide organization of more than 6,600 military and civilian personnel to serve the information technology and telecommunications needs of the president, secretary of defense, Joint Chiefs of Staff, combatant commanders, and other Department of Defense stakeholders.

General Croom's career spanned four commands to include: major command, numbered air force, Air Staff, defense agency, Joint Staff, Office of the Secretary of Defense, and unified command levels. He received distinguished graduate degrees from both Squadron Officer School, and Air Command and Staff College at Maxwell AFB, Alabama. Additionally, he has completed executive development programs at Harvard University, Cornell University, and the National War College.

Industry Perspective

Beyond Data Services: Cloud Processing for Net-Centric Information Distribution

Dr. Matthew Presley
Senior Project Leader
Computers and Software Division
The Aerospace Corporation
El Segundo, California

The Department of Defense Information Enterprise Architecture (DoDIEA) states that deployment of services and data "focuses the [DoD] on the challenges of transforming its approach from deployment of systems to the delivery of information."[1] Delivering information to the warfighter to gain and exploit information superiority is the principal goal of net-centricity, a concept that is shaping the architecture of modern defense and intelligence information systems. The directive of net-centricity, as embodied by the concept and architecture of the global information grid (GIG), encourages data collectors to post all information for immediate access by data users, especially the warfighters. This notion of posting all data, even before processing it, shares its philosophical roots with the observation by Sir Tim Berners-Lee that, "It is the unexpected reuse of information which is the value added by the Web."[2] The DoDIEA prescribes a service-oriented architecture (SOA) for the design of information delivery systems to realize this goal of global data access by the warfighter and intelligence community. Many satellite ground systems are applying SOA in migrating at least some of their capabilities for net-centric distribution of mission data.

The Space-Based Infrared System (SBIRS) Wing of the US Air Force is currently developing services that expose overhead persistent infrared (OPIR) mission data to authorized users for exploitation in intelligence products. Services will potentially include live data streaming, replay of archived data streams, and *ad hoc* query support. The SBIRS data is vital to areas ranging from strategic and tactical battlespace awareness to weather and industrial modeling. These new services will allow users to access and incorporate live and archived OPIR data in unanticipated but remarkable ways to maintain the information high ground.

Under the direction of the SBIRS Wing, the Space Syndication Project at The Aerospace Corporation investigates and prototypes future software architectures to provide insight supporting the long-term incorporation of new technologies into SBIRS. Our approach focuses on embodying the major tenets of net-centricity: sharing, collaboration, and access. Deployment of data services represents a necessary first step for delivery of these concepts. The next step in this evolution should be to augment services with a cloud-based infrastructure for OPIR data processing and distribution. Our goal in describing this architecture is to introduce design features that could be used in future data distribution systems. The proposed architecture uses SBIRS OPIR data distribution as an example, but the concept is applicable to all net-centric data distribution systems, particularly any with an especially high data volume.

Realizing Net-Centricity

The goal of network centric warfare is to interconnect warfighters and collected sensor data to "achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization."[3] Achieving a shared awareness of the battlespace requires delivering the right information to the right people at the right time. This entails transmitting vital data while conserving limited resources, especially bandwidth, storage, and processing. The DoDIEA warns, "As computing infrastructure evolves to better support net-centric operations, it must take into account the needs of the edge users—those at the forward or leading edge of the mission operations environment."[4] While it is imperative, according to the "sharing" tenet of net-centricity, to distribute as much data as possible there is a practical limitation to the amount of bandwidth connecting data provides with subscribers, especially who often operate in separate hemispheres. Providing all collected data can counter-intuitively violate the "access" tenet of net-centricity when information needed by the user is trapped within vast quantities of unnecessary data that consume the user's resources. For example, receiving a global SBIRS OPIR data stream is unacceptable to a bandwidth-constrained edge user who only needs OPIR data in a 100-kilometer radius of his current position. Attempting to deliver high volume data to too many users can likewise overwhelm the resources of the data provider.

A practical solution to this problem delivers to a user only the data required by the user, which is generally only a small subset of all of the data collected by the data provider. Anticipating all possible subsets, permutations, and encodings of client data needs is impossible. The service provider is left making educated guesses and satisfying the specific needs of only a few clients. However, it is the goal of net-centricity to provide for unanticipated users and unexpected uses of data. Thus, we need some means by which a client can provide a specification of their required data to the service provider in a manner that is easy for the service provider to accommodate, and that can be done very quickly to ensure a rapid speed of command and tempo of operations. The most general mechanism that solves this problem is to allow the user to upload data processing algorithms into the distribution system. This is possible when the distribution system is a computational cloud that supports what we refer to as net-centric data processing.

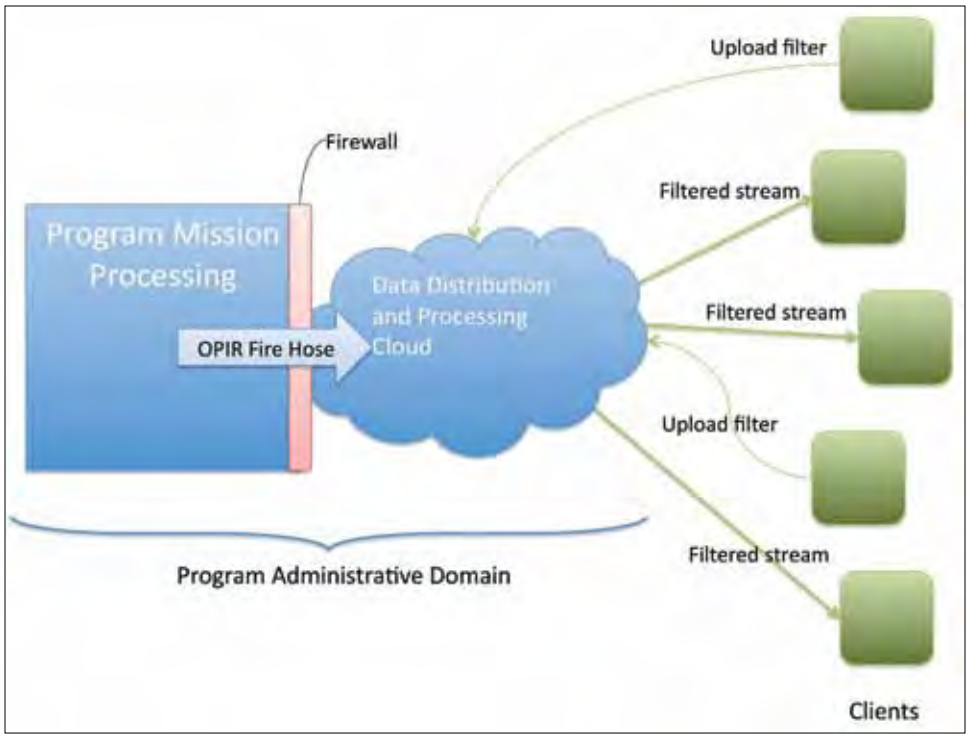


Figure 1. Notional high-level view of the data distribution and processing cloud..

Net-Centric Data Processing

The concept of net-centric data processing is foundational to our proposed architecture: the data distribution and processing cloud (DDPC). The notion of considering the network as both a distribution and processing infrastructure directly addresses the net-centric criteria. Considering data processing as part of the distribution problem allows us to exploit computational efficiencies to reduce both data volume and latency. In other words, moving the processing is often more efficient than moving the data.

Figure 1 illustrates the basic net-centric processing concept for distributing OPIR data: the *OPIR fire hose* pouring large quantities of collected data into the DDPC, encoded in a standard format. The cloud is physically a collection of extensible servers and online storage. The location of the servers is important only with respect to the bandwidth to mission processing, the origin of the data. Typically, a multi-Gbps connection(s) is necessary, so a local interconnection (i.e., LAN) for supporting the OPIR fire hose is the most cost-effective networking solution. A one-way firewall between the mission facility and the DDPC prevents access to mission processing from the DDPC. Traditional data services are accessible by processes inside the cloud and can themselves be executed from within the cloud. Clients are connected via secure network, local and remote, to the DDPC.

Data clients can resolve wide-area bandwidth issues by up-loading into the cloud a refined specification of the data needed from the cloud, thus reducing the data transferred to manageable levels. Specifically, clients upload their own data processing element into the DDPC to selectively distribute only the data they need and at the time and format of their choosing. The DDPC provides multiple means to express filtering logic, including virtual machine images, scripts, and complex event processing languages. For example, the Space Syndication Project advanced prototype supports uploading Java and JavaScript, with plans to support Python, Ruby, XPath, and PHP. The ability to execute filtering software on a local network with the OPIR fire hose data mitigates problems with bandwidth and latency incurred when pushing high-volume data across a WAN. Ideally, the client filtering logic would reduce the data to the client's desired minimal data set and/or down sample the data to acceptable levels of accuracy using much less bandwidth.

Figure 2 illustrates data processing within the DDPC. Any data processing element uploaded into the cloud creates some type of resulting stream of OPIR data. The new stream might be a proper subset of an input stream, a fusion of multiple input streams, or an augmentation the input stream(s) with derived data such as semantic tagging. Regardless, the output is generally some type of data stream of interest to the client who

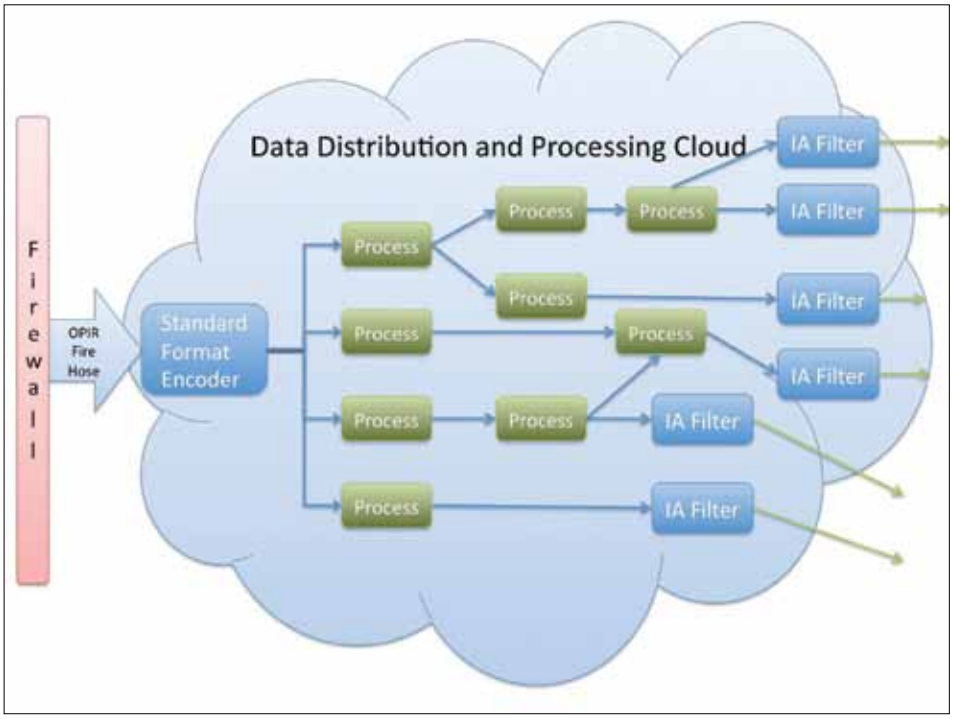


Figure 2. Data processing chains within the cloud.

uploaded the code. All data processing elements and their corresponding output streams have their metadata recorded in a cloud registry and are accessible within the cloud. Any such substream has its metadata placed into the cloud registry, allowing uploaded data processing elements to subscribe to other elements instead of directly to the OPIR fire hose. Subscribing to a data filter, such as a geographic filter, reduces both the computational and bandwidth requirements for a processing element. Subscribing to the stream from a semantic markup element could reduce the complexity of a new uploaded algorithm. Chaining together sets of simple data processing algorithms can result in highly sophisticated and efficient streams of OPIR intelligence.

Data subscribers, especially edge users, also can suffer from constraints in data storage and processing and from intermittent connectivity, all of which are partially mitigated via cloud processing. The cloud's ability to host data processing for filtering, fusion, and augmentation relieves the burden from the user's processing resources. Similarly, offering storage in the cloud reduces the user's local storage requirements. Cloud storage also can be used as a data cache to compensate for periods of disconnection. The user's cloud processing elements can continue to execute and store results in a cloud data cache until connection is reestablished, at which point data is provided to the user. It should be noted that these benefits are general to cloud computing and are not unique to our notion of net-centric data processing. Figure 3 illustrates an edge user leveraging a cloud not provided by a mission data provider, although the user's processing element within the cloud leverages other data distribution clouds. The DoDIEA addresses this concept, at least in part, through their notion of GIG computing nodes.

Collaboration

A fundamental characteristic of net-centricity is collaboration "between knowledgeable entities in the battlespace."[5] This collaboration occurs by linking these entities together to build a more precise shared awareness of the battlespace to translate information superiority into combat efficacy. Given that the DDPC exists to aid in this goal, the ability of different users to collaborate is paramount to its success. Hence, collaboration features must be built into the infrastructure.

The first step in collaboration is a common data language. The opportunities for collaboration increase in proportion to the robustness and expressiveness of the data encoding, ideally with both syntactic and semantic data standards in place. However, even basic conformity to simple syntactic encodings (e.g., XML or HDF5) within the data cloud is helpful. Currently, the OPIR focus group is standardizing syntax and data models for OPIR data.[6] In figure 2, the "Standard Format Encoder" translates SBIRS OPIR binary data into standardized representations of SBIRS event types. This encoding facilitates the development of uploaded data processing elements.

The second step for collaboration support is the cloud registry. As stated above, the registry allows a client to register the output of an uploaded processing element so that other elements can subscribe to its output as opposed to always subscribing to the fire hose. Allowing users to subscribe to *each other's* streams, instead of only their own, enhances collaboration between users. This sharing of work reduces redundancy not only of development, but also in cloud processing and bandwidth usage. For example, if a client uploads an algorithm that filters all data outside a given geographic area, other users requiring the same geographic constraint should subscribe to the same filter instead of replicating it. This collaborative effort leads to a geometric growth of overall cloud capability.

The third step for enhancing collaboration within the cloud is to transform the collaborative cloud users into an online intelligence generation community by leveraging the benefits of social networking sites such as Facebook, Twitter, and StackOverflow. When a user first considers working with the DDPC, the initial task should be to gain an understanding of the existing filters and streams and to find other users that have similar interests in OPIR data. Discovering other user interests and efforts is a means to learn the current state of the DDPC processing *and* the near future expectations for new features. Certainly, a good search feature that allows some level of discovery within the registry is essential, but it represents only a basic tool. It is through following the efforts of other users where most relevant information will be found. Social networking tools support a dynamic mechanism to find new information upon creation. Analysts can form *ad hoc* groups to review and discuss different techniques for processing data. Developers can subscribe to the efforts of others to gain instant notification of any new relevant algorithms or intelligence products. The

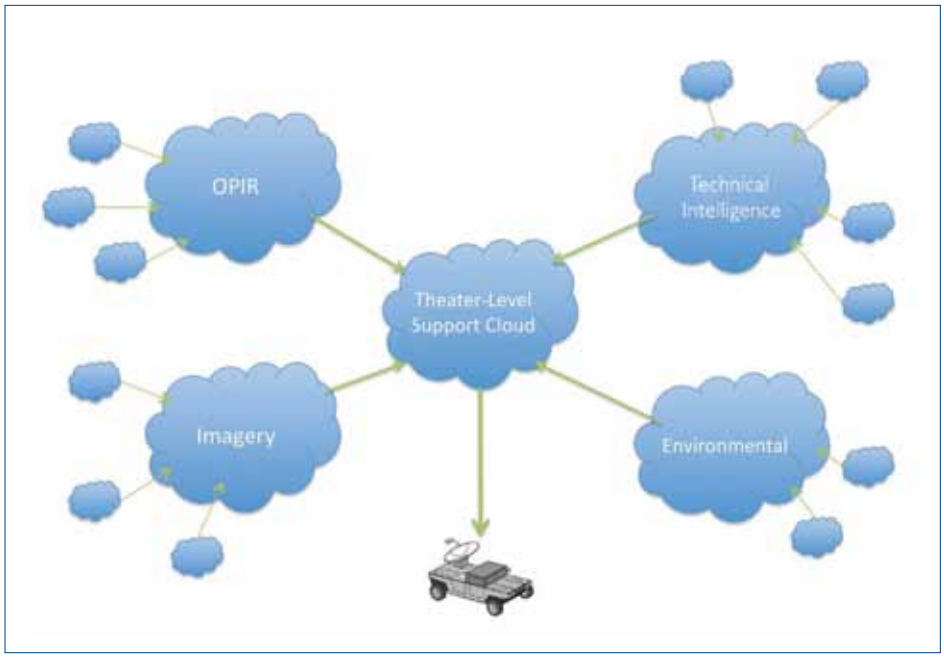


Figure 3. Edge user exploiting multiple clouds.

Net-centric data distribution is effective only if policies are in place to encourage distribution, not stifle data access with onerous procedures.

immediate nature of results publication through this medium will drive the increasing speed of command and tempo of operations.

Policy

The greatest challenge in adopting net-centricity is not development and deployment of technology. Success for net-centricity hinges instead on reconsidering how intelligence and commands flow through the warfighter's organizational structures. Sophistication and flexibility of data processing and distribution mechanisms provide no benefit without commensurate flexibility of policies and processes. Net-centric data distribution is effective only if policies are in place to encourage distribution, not stifle data access with onerous procedures. The approval process for uploading data processing elements, or even providing the software to cloud administrators to upload on a user's behalf, must be relatively quick and simple.

Ideally, a single application process for cloud access is a sufficient review for granting the applicant use of the cloud. Once provided access, the user can upload data processing logic based on resource consumption levels specified within a cloud service level agreement (SLA). However, no per-upload review of processing logic should be employed. This would discourage rapid innovation and place an unsustainable administrative burden upon the cloud administrators. The SLA specifies the contract between the cloud administrator and the client regarding levels of processing, inter- and intra-cloud bandwidth consumption, cloud storage levels, and levels of service availability.

The cloud provider cannot be held accountable for the robustness or accuracy of data delivered by one cloud user to another. If such an agreement is necessary then this must be made between the mutual users, perhaps with some automation support within the cloud itself.

Security and Safety

We assume that the DDPC executes on a secure network. However, additional information assurance is necessary to protect OPIR data and to build trust in the DDPC's security, both to the data provider and the data clients. There is always a tension between the goal of net-centricity to share data widely and the need to ensure that unauthorized users are prevented from accessing the data. We contend that our approach, particularly uploading data processing code into the cloud, neither increases nor reduces the security concerns already raised with net-centric approaches. This proposal does not attempt to provide a comprehensive specification of the required security mechanisms and processes, but will highlight some of the more salient aspects.

Figure 2 illustrates one of the key security mechanisms within the DDPC. Information assurance filters help ensure that each specific client is limited to the data for which they are authorized. These filters are automatically applied to any data flowing out of the cloud to a specific network or user, depending on the particular security policy. Each user-specific filter ensures that only approved data is transmitted to a given client on the external distribution network. In the case of per-user security, some type of data encryption can also be applied. This encryption is needed if the client filter(s) are adding client-sensitive data and/or the type of data provided to the client must remain private.

The cloud administrators must tightly control network connections into and out of the cloud. The sole means to exfiltrate data from the cloud is via a network connection. Thus, the cloud should impose strict limits on the ability of uploaded software to initiate network connections to locations outside of the cloud. Of course, the sole means of proper data subscription is also through the network, but the network connections from the cloud to proper clients can be specified via SLA and controlled via the cloud infrastructure. Allowing arbitrary network connections to external hosts is unnecessary and insecure.

Protecting client data processing from misbehaving code from another client can be achieved by executing all uploaded code within virtual machines to provide a sandbox, the environment outside of which the code cannot affect. This technique prevents a single programmer's mistake from becoming a catastrophe. Furthermore, the sandbox of the virtual machine provides the interface between the executing code and the rest of the cloud, which limits the ability to perform unauthorized actions. The virtual machines can themselves be sandboxed providing multiple layers of security. For example, the Space Syndication Project's simple cloud engine (SCE) executes each process within its own virtual machine, where each process is itself a Java virtual machine (JVM) that sandboxes code within a specific SCE interface. Restricting data processing code to a scripting language, such as JavaScript or Ruby, executing within the JVM provides yet another boundary around the uploaded code. The most restrictive processing paradigm within the SCE allows the code access only to specific data streams for input and output. No other access to the cloud beyond reading and writing data to streams is possible by the uploaded code. Fortunately, stream data transformation is by itself sufficient to enable net-centric data processing.

Inter-Cloud Processing

In his article, "Cloud Computing and the Internet," Vint Cerf asserts that each cloud, such as those provided by Amazon, Google, Microsoft, and Apple, is an isolated system. He compares Internet clouds to the state of networking in the 1960s, when DEC, IBM, HP, and others had isolated, proprietary networks. His point is that the next step of the Internet could be a merging of proprietary clouds via open standards, opening up

the future to "the richness of the Internet's undiscovered territory in the decades ahead."[7]

We consider the inter-cloud capability to be a fundamental means to provide rich data to all users, but especially the edge users, as depicted in figure 3. We have, thus far, described the potential of a single data provider using a cloud to engender a community of collaborative users. The ultimate realization of net-centric data processing within the broader goal of net-centricity delivers interoperating clouds that provide the warfighter, regardless of technical disadvantages, all of the information and processing power to leverage information superiority into overwhelming combat strength. Intelligence collects within domain-specific clouds feeding autonomously executing software within a theater-level support cloud that provides processing, storage, and bandwidth. The theater processing is tailored for each specific edge user's particular technical issues, such as limited bandwidth and intermittent connectivity. For example, images and video can be down sampled for limited bandwidth, and data can be cached during periods of disconnection. Theatre processing can also consider tactical issues of intelligence genuinely useful to the warfighter. For example, the user's position can be monitored so that only geographically relevant data is provided.

Another benefit of multiple clouds is that a data collection organization, such as SBIRS, might determine that supporting a net-centric distribution cloud falls outside of their scope or capability. In this case, an intermediary cloud, such as the OPIR cloud in figure 3, can act as the sole subscriber to the SBIRS OPIR fire hose. SBIRS, now having only a single client, need not provide a processing cloud of its own. The intermediary cloud can be supported by another data collection organization, or potentially by one tailored specifically to support a processing cloud that subscribes to multiple data sensors. Data subscribers needing SBIRS data can access and process the SBIRS data stream within the intermediary cloud and fuse the data with streams from other sensors.

A Net-Centric Future

We must continue to seek ways to exploit our overwhelming information and technical superiority into greater combat strength and national security. Embracing net-centricity offers a means to further this goal. Accepting network-centric warfare requires rethinking how networks are utilized and, more importantly, how information flows to the warfighters. We have no illusions that the concept of uploading executable code into a secure processing cloud will meet more skeptics than supporters. Indeed, net-centricity itself continues to have skeptics, although fewer than before. However, there is a massive volume of information to process, myriad ways to process it, numerous warfighters that need it, and several practical limitations of transmitting information for global accessibility. This problem will persist into the foreseeable future, so long as the quantity and need for data outstrips global bandwidth. We can hope to solve it only by transforming the GIG from a service and data grid, which provides only a means to access data, into a true computational grid providing both data and the means to transform data into actionable intelligence.

Notes:

[1] *Department of Defense Information Enterprise Architecture (DoDIEA)* version 1.1, Department of Defense Office of the chief information officer, May 2009, http://cio-nii.defense.gov/sites/diea.

[2] T. Berners-Lee, *Linked Data*, 7 July 2006, http://www.w3.org/DesignIssues/LinkedData.html.

[3] D. Alberts et al., *Network Centric Warfare*, 2nd Ed, C4ISR Cooperative Research Program (CCRP), August 1999.

[4] *DoDIEA*.

[5] Alberts et al., *Network Centric Warfare*.

[6] Overhead Persistent Infrared Focus Group, http://www.gwg.nga.mil/ofg.php.

[7] Vinton Cerf, *Cloud Computing and the Internet*, Google Research Blog, 28 April 2009, http://googleresearch.blogspot.com/2009/04/cloud-computing-and-internet.html.

Dr. Matthew Presley (BS, Mathematics, Harvey Mudd College, California; MS, Computer Science, University of California, Los Angeles (UCLA); PhD, Computer Science, UCLA) is a senior project leader in the computers and software division of The Aerospace Corporation.

Dr. Presley leads the Distributed Information Systems Laboratory at The Aerospace Corporation researching distributed computing and building advanced prototype software demonstrating the application of net-centric computing concepts to satellite ground systems. The work investigates various architectural approaches to ground system design, including service-oriented architecture, cloud computing, resource-oriented architecture, and stream and event driven architecture. The results of this work are used to advise multiple national security space programs and agencies including space-based infrared system, global positioning system, and the National Reconnaissance Office.

Dr. Presley has worked in parallel and distributed computing for over 20 years. His work includes parallel discrete-event simulation engines and theory at National Aeronautics and Space Administration Jet Propulsion Laboratories where he was a member of the Time Warp Operating System team. Prior to his current position at The Aerospace Corporation, Dr. Presley was chief scientist and senior vice president of engineering at Agari Mediaware where he led development of an enterprise service bus tailored towards integration of rich media applications. Dr. Presley has also taught operating system principles in the Department of Computer Science at the University of California, Los Angeles.

Demonstrating Cyberspace Superiority in an Acquisition World

Col Robert L. Tremaine, USAF, retired
Associate Dean, Outreach and Mission Assistance
Defense Acquisition University
San Diego, California

April 27, 2010, the Space and Missile Systems Center (SMC) showed its cyberspace superiority during an intensive two and half-day acquisition event under Air Force Space Command's (AFSPC) recent Guardian Challenge (GC) competition.

Designed to test their personnel's inherent leadership and functional expertise, SMC selected six four-person teams to compete for the coveted distinction of 1st place along with all the bragging rights. Each of the six teams, comprised of captains, majors, and equivalent civilian personnel, had the functional bases covered with various levels of Defense Acquisition Workforce Improvement Act (DAWIA) certifications in place. Program management, systems engineering, budgeting, cost estimating, and contracting were well represented. Soon after the teams formed with their impressive lineups, they practiced their acquisition skills. In short order, they were about to head into a perfect acquisition storm. All they would have is each other in the face of a tough scenario and a few vital artifacts. The team's collective skills would become their primary navigational aid. No outside support was allowed. In little time, they would be involved in a major event that "enhanced esprit de corps and demonstrated the power of teamwork," one of AFSPC's key competition objectives. Planning for the event actually started a couple of months prior when two key partners, the Defense Acquisition University (DAU) and SMC, teamed up to produce a real world challenge facing the space community today: how to best satisfy a shortage in satellite communications bandwidth.

Background

Two years ago, AFSPC Headquarters expanded GC (largely an operational-centric exercise) to the acquisition community. Headquarters felt all command personnel should have an opportunity to demonstrate their talents—not only the operators but also the acquirers who deliver these crucial operational systems. Ironically, the space acquisition community did not have a competition exercise that tested them in the field before. This was a first of its kind and represented a transformational opportunity. SMC learned a lot after their first GC engagement although many personnel were not so sure it was such a good fit.

The Competition Essentials

About seven weeks before actual game day, during this second installment SMC solicited DAU's help to build an end-to-end acquisition competition. Based on lessons learned after their previous competition outing, this year's event needed to be more challenging and encompassing. Consequently, the DAU-SMC design team created a set of competition material rich in detail that would stimulate critical thinking—the kind that acquirers tend to enjoy. In the aggregate, the artifacts would also quickly situate and stretch the competitor's abilities, and ultimately represent a real-world space acquisition experience. The artifacts included:

- Robust space acquisition scenario
- Three viable satellite materiel options:
  - Option 1: Hosted payload on a commercial satellite (e.g., sharing space with other planned payloads)
  - Option 2: Dedicated pay-for-service commercial satellite
  - Option 3: Leased pay-for-service commercial satellite with an option to buy
- Competition timeline
- Competition instructions and rules of engagement

By design, these artifacts were intended to quickly acclimate the teams and taper any competitive variances without inhibiting their ability to innovate—an important tenant in the acquisition profession and decidedly one that DoD Instruction 5000.02 emphasizes. Each of these artifacts had also been carefully refined after a comprehensive beta test conducted just two weeks prior to the real contest. The beta test revealed a few shortcomings that inhibited game play including time constraints, lack of a concept of operations (CONOP), and the downside of a "planned" delayed release of the materiel options available (the development team initially felt that too much data too fast would overwhelm the competition teams). All these deficiencies were reconciled before competition execution day.

Robust Space Acquisition Scenario

The satellite product-line specific scenario selected was designed to trip a few intellectual switches. Each team would be responsible for developing a robust and innovative acquisition strategy that called for vital satellite services to fill a critical and urgent communications gap. When combined with the Air Force's distributed common ground station, more communi-

cations bandwidth would better enable Global Hawk to provide intelligence, surveillance, and reconnaissance capability to the warfighter in the US Central Command (CENTCOM) area of operations (AO). Each team was also given a representative CENTCOM CONOP that confirmed bandwidth demands had already exceeded available capacity. The CONOP inferred the warfighters were forced to forfeit an operational advantage they had previously enjoyed. They could no longer fully exploit crucial imagery data. Worse, the effectiveness of combat operations in their AOR could soon be at risk.

Day 1		Day 2			Day 3
1200	1400	0700-0730	0730-1000	0900-1600	0800-1200
Issue Competition Warning Order (WARNORD)	Up To 5 Questions Due From Each Team	Provide Strategic Overview to Teams	Teams Prepare and Deliver Part I A/B Results to Evaluators	Teams Prepare Innovative Acquisition Strategy for Evaluation	Teams Separately Brief Part II Results to Evaluators
- KEY OBJECTIVES -					
• Review & Assimilate Scenario • Develop Situational Awareness • Understand Competition Objectives • Understand Evaluation Rubric	• Confirm Operational Imperatives • Reconcile potential Acquisition or Operational Issues • Generate up to 5 questions pertaining to Scenario and other artifacts	• Prepare to fine tune team heading after receiving answers to questions • Teams Prioritize Individual Assignments	• Identify Risks and companion Mitigation Techniques (Part 1A) • Develop Evaluation Criteria for the three options provided (Part 1B) •Teams turn-in Part IA/B Assignments	• Determine most suitable and optimal COA • Address 5000.02 Requirements • Prepare Robust Presentation (Part II) for Assessment	• Evaluate Teams • Determine Winner •Survey Teams • Complete After Action Report

Figure 1. Competition timeline.

The Competition Timeline

From start to finish, the pace of the competition would be very ambitious (figure 1). From the time they received the warning order (WARNORD) on Tuesday at 1200 to the time they delivered their presentation finale to the evaluators on Thursday at 0800, time was recognized as a premium. Even though the competition was appropriately sized for the set timeframe, there was no occasion to be idle. The teams had to respond to a short fuse with little time to distill a lot of data. A critical analysis was essential. The teams had to: (1) identify and mitigate programmatic risk (part 1A worth 20 points), and (2) develop a comprehensive set of evaluation criteria (part 1B worth 20 points) before they could narrow their selection of three available (given) options. Parts 1A and 1B were also expected to help narrow the teams focus on the more critical elements early and ease them into the development of a more comprehensive acquisition strategy, later. After they submitted part 1A and part 1B results to the evaluators, they would need to turn their attention to part II (worth 60 points) and build a defendable acquisition strategy.

Competition Instructions and Rules of Engagement

Part of the competition's success would depend on a thorough understanding of the competition instructions. As a result, SMC published a number of imperatives to safeguard game play including:

- Rules of engagement that specified game expectations, team interactions, and taboos.
- A well understood communications plan that characterized all dialogue internal and external to the teams.
- Specific scoring criteria and an accompanying evaluation rubric for all deliverables that clearly stated how the 100 points available would be awarded and under what conditions.

Game Day

On game day, the high energy level was apparent. Six teams were ready to play. Already in the hunt for the trophy, they had to overcome two major obstacles first—a tight timeline and too much data.

Aside from their inherent level of expertise, the competition teams had some additional help through virtual access to the Defense Acquisition Guidebook, and other very useful Internet links. However, the teams were prohibited from seeking advice and counsel from external sources as a measure to level the playing field. This decision created some inherent experience limitations. As a result, the teams were armed with just what they could deduce, as well as what they could supplement from the net. They had no silver bullets and no secret weapons. They had just each other—a distinct advantage found in warfighting operations that tends to fortify everyone's mettle.

Each team received their WARNORD simultaneously at high noon on "day one" at their respective locations. Five teams were operating in conference rooms spread across SMC's Los Angeles AFB; one team was operating out of

Figure 2. Participants of Guardian Challenge.

SMC's Kirtland AFB, New Mexico site. The teams had just a couple of hours to digest the data and could generate up to five questions on any aspect of the game—from basic clarification questions to more detailed questions about any of the material provided. As part of the original plan, DAU and SMC established a command and control post to field these questions and also guide the competition. Within two hours, questions started to roll-in like clockwork:

- "Is a fiscal year (FY) 13 president's budget and updated FY14 program objective memorandum (POM) funding profile available for consideration with the criticality of the program, or are we to assume all deltas in future years will be approved in the future POM submittals?"
- "If a launch is delayed due to late arrival of government-furnished equipment, the commercial payloads may need to be compensated for lost revenues. What is the monthly dollar figure for slipping a launch for each of the commercial satellites manifested (Intelsat-19, Insat-3E, SES New Skies NSS-21, and Intelsat-20)?"

With similar tenor, the teams immediately quantified some of the unknown variables and assessed them up-front. Understanding and reconciling the operational requirement was crucial but their ability to carefully manage the ongoing uncertainty, a constant in the acquisition profession, could become a competitive advantage. The more probing questions the team asked to mitigate most of the uncertainty, the better acquisition strategy they could build as they pressed ahead.

Results

In no time, the teams quickly dove deeply into the data stack. What the teams were able to achieve in a condensed amount of time was extremely notable—testimony to their determination. In the end and after performing the cost-schedule and performance trades, each team selected the same option—a dedicated pay-for-service satellite versus option 1 (sharing real estate on another satellite [e.g., hosted payload]) or option 3 (leasing a satellite with an option to buy). Early, and in part 1A of the competition, the team had to list three to five key programmatic risks for all the options. The risks associated with their final selection would resurface in part II and require a more thorough assessment.

From a competitive perspective, what differentiated the teams had more to do with their:

- Acquisition approach (from capability needs to key performance parameters)
- Programming, planning, budgeting, and execution strategy
- Detailed integrated schedules
- Identification of major programmatic risks and key mitigation strategies within the context of the risk cube
- Systems engineering approach and associated processes.
- Assessment and reconciliation of the major design considerations
- Other programmatic considerations including coordination with external stakeholders across the enterprise, harvesting existing technology from cancelled programs, potential integration with other space command and control mission suites

Figure 3. Winning team from Kirtland, AFB representing the Space and Development Wing.

Looking back at the dynamic basis of the competition and the end result, all six teams deserve a lot credit. Each team focused their efforts with considerable intensity. The pressure did not let up once the competition began, and the teams did not let down at all.

Ultimately, the team from Kirtland AFB representing the Space Development and Test Wing won the honors, as well as the bragging rights this year.

Feedback

After the competition ended, the development team launched a survey that sought unvarnished feedback from each team

PARTICIPANTS: How Would You Rate YOUR participation?	Strongly Disagree	Disagree	Agree	More than Agree	Strongly Agree	% Green
Tested my fundamental acquisition knowledge	○	○	●	●	●	96%
Verified my ability to apply key acquisition principles	○	○	●	●	●	96%
Reinforced my strengths required by area of expertise	○	○	●	●	●	92%
Uncovered my training needs in acquisition life cycle	○	○	●	●	●	88%
Gave me a better feel for typical acquisition issues	○	○	●	●	●	92%

EVALUATORS: Observations on Participants	Strongly Disagree	Disagree	Agree	More than Agree	Strongly Agree	% Green
Tested their fundamental acquisition knowledge	○	○	●	●	●	100%
Verified their ability to apply acquisition principles	○	○	●	●	●	100%
Reinforced their strengths required by area of expertise	○	○	●	●	●	88%
Uncovered their training needs in acquisition life cycle	○	○	●	●	●	88%
Gave them a better feel for typical acquisition issues	○	○	●	●	●	88%

Figure 4. Participation rating for evaluators and participants.

More junior personnel had an earlier opportunity to demonstrate their collective cyberspace superiority and test drive their acquisition skills across the entire acquisition integrated framework—within their own product line at their own base alongside their own colleagues.

member, as well as the eight senior evaluators. Their views mattered since it represented the goodness of this event, what everyone had to say about the ride and whether or not SMC's participation in GC should continue.

Rating Their Participation

Figure 4 shows how the individual participants and evaluators rated the participants' general performance. The ratings were consistent between both groups. In the narrative section of the survey, both the individual participants and evaluators amplified the need for more training. One individual even remarked that he needed to treat training courses more seriously." A well known fact, training in operational exercises has always been the key ingredient to their success in real world situations. In a similar fashion, "training like you fight and fighting like you train" in the acquisition profession could possibly promote more successful outcomes and maybe even boost performance.

Summary

At the first glance, an acquisition competition conducted as part of an operationally-centric GC exercise might appear to be a little unusual. However, the very prospect can provide some significant dividends in the form of "experience gains" that are so vital to the cyberspace acquisition profession. This competition showed just that. What else made the competition relevant and meaningful? More junior personnel had an earlier opportunity to demonstrate their collective cyberspace superiority and test drive their acquisition skills across the entire acquisition integrated framework—within their own product line at their own base alongside their own colleagues. With more of these type of engagements complemented by other more focused training, SMC might be able to help overcome some the experience limitations identified in a recent March 2010 Government Accountability Office report that indicated "insufficient numbers of experienced space acquisition personnel and inadequate continuity of personnel in project management positions." Perhaps, exercises like GC can help confirm other critical acquisition functions that need to be strengthened to overcome these very real challenges.

Should the acquisition community continue to participate in future GC exercises? Aside from the fact that this event achieved the GC goals, the answer is indeed "yes" and can be best summarized by the survey results where one competitor said what many others echoed: "This is definitely a rewarding experience. The given scenario tested my acquisition knowledge and skill sets ...." This competition also validated the importance of DAWIA certification under a real world scenario. What students demonstrate in the classroom is just one component; what they can apply in the field is even more significant, however.

In retrospect, the operational and acquisition communities indeed seem to share many of the same training imperatives after all—which an expanded GC set out to prove. If the DoD moves toward implementing qualification standards for acquirers much like the operational community has in place today, events like GC can create experience breakthroughs for the acquisition community since they simulate real-world scenarios that acquirers face every day within their own organizations. While GC is unique to AFSPC, other material developers across the DoD enterprise might be well-served by demonstrating their mettle in similarly constructed competitions. In the long run, nothing shows an organization's preparedness and key competencies like competitions. And, something like an acquisition competition in the context of a GC-like event just might take acquisition training to the next level.

***Author's note**: The author thanks Dean Andy Zaleski, Mr. Woody Spring, Col Chuck Cynamon, Mr. Rick Agardy, and Ms. Donna Seligman for their tireless support in the development and analysis of this acquisition competition. While all were extremely busy with their other chief duties, they were the reason this event was so meaningful and successful.*

Col Robert L. Tremaine, USAF, retired (BS, US Air Force Academy; MS, Systems Management, Air Force Institute of Technology, Canadian Forces Command and Staff College; Military Research Fellow, Harvard Business School; US Army War College) has over over 28 years of extensive leadership experience as an accomplished acquisition professional with level III certifications in both program management and systems engineering. His skill sets covers all aspects of designing, building, testing and fielding air, missile (cruise and defense), and space systems. Over his military career, he managed air, missile, and space development programs valued between $250 million to $3.2 billion. He is currently the associate dean for outreach and mission assistance at the Defense Acquisition University (West Region), in San Diego, California where he teaches and consults to the Department of Defense. He has published numerous articles in both the *Defense Acquisition Review Journal* and *Defense AT&L Magazine* in a wide variety of acquisition topics.

Book Review

Emerging Space Powers: The New Space Programs of Asia, the Middle East, and South America

Emerging Space Powers: The New Space Programs of Asia, the Middle East, and South America. By Brian Harvey, Henk H. F. Smid, and Théo Pirard. Chichester, United Kingdom: Praxis Publishing, 2010. Illustrations. Tables. Annexes. Bibliography. Index. Pp. xxx, 626. $44.95 Paperback ISBN: 978-1441908735

A previous issue of *High Frontier* (vol. 6, no. 2) highlighted the growing importance of international cooperation and collaboration in space. A new book, *Emerging Space Powers*, reinforces many of the points made by contributors to that issue. Its authors explain how seven countries, each in their own way and for their own reasons, are striving to develop indigenous space capabilities. What becomes strikingly apparent as one digests the narrative, however, is how extensively those countries have attempted to advance their own spacefaring status by relying on more experienced space powers or by collaborating with other, less-capable aspirants. For each of the countries identified as "emerging space powers," the authors supply historical background and details about current satellite programs, launcher development, organizational structures, facilities, and national purposes.

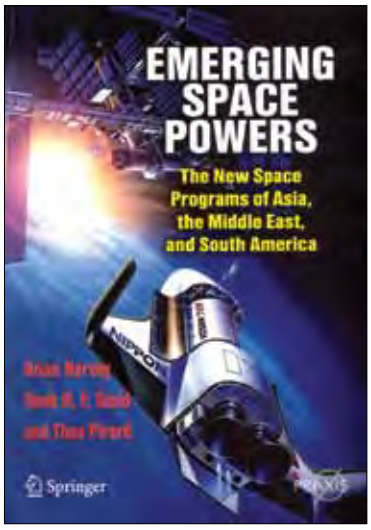
Brian Harvey, a prolific writer on space topics, authored the first six chapters in *Emerging Space Powers*, which update his earlier volume titled *The Japanese and Indian Space Programmes: Two Roads into Space* (Praxis, 2000). After Japan thoroughly investigated a series of launch anomalies in the 1990s, it returned to space in August 2001 using its new H-IIA booster. In 2003, it recovered a satellite from orbit for the first time. That same year, Japan's Institute of Space and Astronautical Sciences and its National Space Development Agency merged to form the Japan Aerospace Exploration Agency. During 2008–2009, several space shuttle missions carried parts of the Japanese Experiment Module to the *International Space Station*. Despite its progress, however, Harvey concludes, "Japan had been overtaken by China and faced a strong challenge from India."

As for India, Harvey emphasizes how recent accomplishments continue to support that nation's original purpose for going into space—to benefit the poor masses in remote villages through satellite communications, weather observations, and remote sensing. Even as India, beginning in 2000, relied on Ariane V launches from Kourou to orbit three generations of INSATs, it cooperated with Russia on navigational satellites; and, in the face of US opposition, India angled to purchase Russia's powerful KVD-1 rocket engine. India's Nambi Narayanan also developed the Vikas engine that sent *Chandrayan* to the Moon in 2008. By limiting its ambitions and focusing on a narrow range of activities, India has maintained one of the most cost-effective space programs in the world. Furthermore, India's space industry has spurred technological advances in such diverse areas as materials, electronics, fuels, optics, electromechanical systems, and computers.

Chapters 7 and 8 of *Emerging Space Powers* address Iran's space program. Authored by engineer Henk Smid, they span the years from Iran as a founding signatory of the United Nations Committee on the Peaceful Uses of Outer Space in the late 1950s, to the first steps in 1977 toward what finally became the Iranian Space Agency in 2004, and onward to launch of the *Omid* communications satellite on a Safir-2 booster in February 2009. Unable to obtain information from official sources in Iran, Smid relied primarily on Iranian television, Internet blogs, Google Earth, and insights from his Iranian friends to piece together a narrative. Despite the questionable accuracy or outdated nature of such raw material, he has painted a reasonably coherent picture of Iran's space-related accomplishments and goals.

Smid also wrote chapters 9–11 on Brazil's activities, which he traces back to early 1957. The creation of an Organizing Group for the National Commission on Space Activities in 1961 placed Brazil among the earliest nations to officially include space activities within its government program. For a half century, Brazil has used space probes and satellites for roughly three purposes, all closely related to its geographical vastness and environmental diversity: science, communications, and Earth observation. For the period 2005–2014, its National Space Activities Program focuses on improving the Brazilian people's quality of life "by generating wealth and creating jobs through scientific research and by increasing awareness of issues regarding their territory and environment."

Israel, North Korea, and South Korea each receive a chapter's worth of Théo Pirard's attention. A journalist with Belgium's Space Information Center, Pirard describes the Israeli space program as "a by-product of the 1979 peace treaty with Egypt." Focused on intelligence and security, Israel nurtures a space industry specializing in low-cost, low-mass spacecraft and cultivates a strategic partnership with India. Recently, Israel has promoted "commercial ventures to enter the global business of space applications." North Korea, on the other hand, remains most secretive when it comes to space and, according to Pirard, has demonstrated "the art of launching 'ghost-satellites'!" With technological contributions from Iran and Pakistan, North Korea has steadily improved its launch vehicles. By comparison, South Korea has "established cooperative links with a great number of space agencies and industries around the world" to develop a national launch vehicle and high-quality microsatellites for commercial applications.



The weakest portion of *Emerging Space Powers* is the four-page final chapter, which purports to set the previously discussed programs in a global context and comment on their distinctive features. By concentrating heavily on India and Japan, the authors leave to the reader an inordinate amount of potentially fruitful comparative analysis. Despite this, the book provides an excellent starting point for anyone unfamiliar with the space-related history and aspirations of Japan, India, Iran, Brazil, Israel, North Korea, and South Korea.

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

U.S. AIR FORCE

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) 554-3523
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