AIR FORCE SPACE COMMAND

Volume 7, Number 3

HIGH FRONTIER

THE JOURNAL FOR SPACE AND CYBERSPACE PROFESSIONALS

Cyber Defense - Protecting Operations in an Evolving Domain

INSIDE:

Toward a Single AFNet: Three Reasons Why the Air Force Must Migrate

Mitigating Cyber Friendly Fire: A Sub-Category of Cyber Mishaps

Air Force Cyberspace Strategic Planning Factors

Headquarters
Air Force
Space Command
Peterson Air Force Base, Colorado

Commander
General William L. Shelton

Vice Commander
Lt Gen Michael J. Basla

Director of Public Affairs
Col Kathleen Cook

Creative Editor
Ms. Nadine Sage

High Frontier Staff

Mr. Steve Tindell
Dr. Rick Sturdevant
Maj Sam Baxter
Maj Vanessa Hillman
Maj Merna Hsu
Maj Aaron Teltschik
Maj April Wimmer

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: Image sources: Analytical Graphics, Inc. and AFSPC/PA Graphics.

Back Cover: Supernova Remnant E0102 in the Small Magellanic Cloud. Credit: NASA, ESA, and the Hubble Heritage Team (STScI/AURA). Acknowledgment: J. Green (University of Colorado, Boulder).

HIGH FRONTIER

The Journal for Space and Cyberspace Professionals

May 2011 Volume 7, Number 3

Contents

Introduction
General William L. Shelton 2

Senior Leader Perspective
Toward a Single AFNet: Three Reasons Why the Air Force Must Migrate
Lt Gen Michael J. Basla 3

Mitigating Cyber Friendly Fire: A Sub-Category of Cyber Mishaps
Dr. Dee H. Andrews and Dr. Kamal T. Jabbour 5

Cyber Defense – Protecting Operations in an Evolving Domain
Achieving Cyber Survivability in a Contested Environment Using a Cyber Moving Target
Dr. Hamed Okhravi, Mr. Joshua W. Haines, and Mr. Kyle Ingols 9

Winning in Cyberspace: Air Force Space Command's Approach to Defending the Air Force Network
Ms. Jill Baker, Mr. Shane Morrison, and Mr. Jarret Rush 14

Single Integrated Network Environment: The Strategy for Air Force Network Integration
Lt Col Patrick B. Dunnells 20

Defending the Cyber Alamo: An Indefensible Position in Cyberspace
Mr. Leander J. Brandt, IV 23

Air Force Cyberspace Strategic Planning Factors
Mr. John D. Wright 26

The Air Force Network Architecture
Mr. Steven L. Stoner 31

Preparing the Air Force for Computer Network Operations
SSgt Andrew T. Jones 33

Industry Perspective
Rethinking Cyber Defense
Mr. David W. Aucsmith 35

Book Review
Surviving Cyber War
Dr. Rick W. Sturdevant 38

Next Issue: ***The Space Commission: 10 Years Later***

Introduction

General William L. Shelton, USAF
Commander, Air Force Space Command

Our most pressing need is clear policy, formed by shared consensus, shaped by informed discussion, and created by a common body of knowledge.[1]

~ General Michael V. Hayden, USAF, retired

As the former director of the National Security Agency and Central Intelligence Agency, General Hayden is one of the nation's leading experts on America's needs in the cyberspace domain. I am pleased this edition of the *High Frontier Journal* will help inform the discussion and hopefully enhance the body of knowledge on cyberspace.

Deputy Secretary of Defense, William J. Lynn, recently recognized the need for "a new strategy for cybersecurity" in which "the principal elements of that strategy are to develop an organizational construct for training, equipping, and commanding cyberdefense forces."[2] Air Force Space Command's (AFSPC) charge is to organize, train, and equip Air Force forces to operate effectively in the cyberspace domain. One of my top priorities for the command is to operationalize and normalize cyberspace, thereby enabling our Air Force to (1) provide our portion of that cyber defense force the deputy secretary desires, and (2) build the Air Force contribution to the joint capabilities of US Cyber Command. We laid the organizational foundation with the establishment of 24th Air Force, later designated Air Forces Cyber as the Air Force operational component to US Cyber Command. Further, we established a Cyberspace Professional Development Program and are graduating a cyber force from newly created training and education programs. Finally, we are integrating cyber into the joint fight with efforts such as placing Cyberspace Operations Liaison Elements within combatant commands.

While this is an encouraging start, much more work needs to be done. In this issue of the *High Frontier Journal*, we look at cyberspace from a defensive perspective and how to protect operations in this evolving domain. Unlike the physical domains, cyberspace is engineered and built by humans, and the cyberspace domain changes as quickly as the technology allows. This makes cyber defense an ever-changing challenge, one that requires new strategies and new thinking based on the "common body of knowledge." This *High Frontier Journal* is one small step in understanding this evolving realm.

Defending the rapidly changing cyberspace domain requires agility and adaptation. Our first focus of this endeavor is to establish a single Air Force Network (AFNet). The current multitude of networks and configurations complicates our processes and overall network defense—plus it inhibits enterprise-level operational efficiencies. Lt Gen Michael J. Basla, AFSPC's vice commander, outlines three reasons why the Air Force must migrate to AFNet. Contributing authors further dive into the details of the AFNet architecture from headquarters, center, and squadron perspectives.

Cyberspace defense must be considered from multiple points of view, and we are soliciting all good ideas. I commend SSgt Andrew Jones for his article on training cyber defenders. My generation, as digital immigrants, would be well-served by listening to the ideas of the digital natives who have a better inherent understanding of this domain. Finally, I appreciate the industry perspective, always a mainstay of the *High Frontier Journal*, but more importantly, because industry leads in the cyber realm, not government.

The next issue of the *High Frontier Journal* will examine "The Space Commission: 10 Years Later." The Space Commission influenced numerous organizational changes, such as the merger of US Space Command with US Strategic Command, emergence of a single-hatted AFSPC commander, aligning Space and Missile Systems Center under AFSPC, and the establishment of the National Security Space Institute. With the recent release of the National Space Policy and National Security Space Strategy, Air Force space management realignment and Defense Space Council establishment, now is an appropriate time to reflect back on our recent history as we chart our course for the future. Lessons learned and insights gained can be applied to both space and cyberspace. I look forward to reading your perspectives in the next edition.

Notes:

[1] Michael V. Hayden, "The Future of Things 'Cyber'," *Strategic Studies Quarterly*, Spring 2011.

[2] William J. Lynn III, "Defending a New Domain," *Foreign Affairs*, Sep/Oct 2010.

General William L. Shelton, USAF (BS, Astronautical Engineering, US Air Force Academy [USAFA], Colorado; MS, Astronautical Engineering, US Air Force Institute of Technology, Ohio; MS, National Security Strategy, National War College, Washington, DC) is the commander of Air Force Space Command, Peterson AFB, Colorado. He is responsible for organizing, equipping, training, and maintaining mission-ready space and cyberspace forces and capabilities for North American Aerospace Defense Command, US Strategic Command, and other combatant commands around the world. General Shelton 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 Shelton entered the Air Force in 1976 as a graduate of the USAFA. He has served in various assignments, including research and development testing, space operations, and staff work. The general has commanded at the squadron, group, wing and numbered air force levels, and served on the staffs at major command headquarters, Air Force headquarters and the Office of the Secretary of Defense. Prior to assuming his current position, General Shelton was the assistant vice chief of staff and director, Air Staff, US Air Force, Pentagon, Washington, DC.

Toward a Single AFNet
Three Reasons Why the Air Force Must Migrate

Lt Gen Michael J. Basla
Vice Commander
Air Force Space Command
Peterson AFB, Colorado

For thousands of years, military leaders integrated and exploited information to achieve success. When Joint Vision 2010 (JV2010) was published in 1996, it stated,

> Throughout history, gathering, exploiting, and protecting information have been critical in command, control, and intelligence. The unqualified importance of information will not change in 2010. What will differ is the increased access to information and improvements in the speed and accuracy of prioritizing and transferring data brought about by advances in technology.[1]

The authors of JV2010 had it absolutely right. As the American way of war evolved from the strategy of attrition employed by Generals Grant, Pershing, and LeMay into a strategy based on speed, surprise, precision, and maneuver, information became the foundation of modern warfare.

As important as information is though, the Air Force never took an enterprise approach to delivering this critical requirement. Instead, different communities established multiple networks to support warfighting functions. Each community isolated their information sharing and command and control. Hence, without an enterprise approach to providing a common communications fabric, the Air Force's ability to effectively leverage the cyber domain could become the weak link in the kill chain. Worse, an adversary could exploit this as a critical vulnerability. This legacy approach inhibited information sharing and severely reduced mission assurance.

In September 2000, Chief of Staff of the US Air Force General Michael Ryan published a Notice to Airmen (NOTAM) calling for the Air Force to "fundamentally change the way we leverage our networks" and made the first mention of the "one Air Force, one network" concept.[2] Most Airmen have never heard of this NOTAM, but even 10 years ago our leaders saw the transformational benefits that a single Air Force network (AFNet) would have on our warfighting capabilities. The Air Force has made some progress toward building a single AFNet in the years since this NOTAM, but more work and support are required. This article provides a brief overview of the factors that inform both the need and urgency with which AFNet migration must occur and the benefits once completed. Simply put, a single Air Force network is crucial to leverage our advantage in the cyber domain. Couple this operational imperative with the increased requirements for mission assurance and the need to realize information technology (IT) efficiencies have made network migration Air Force Space Command's (AFSPC) number one cyber priority.

More than 10 years after General Ryan published his NOTAM, the Air Force continues to struggle with multiple information domains that hamper our ability to share information. Even today, each major command (MAJCOM) commands and controls much of its own IT enterprise, develops its own architectures, and engineers its own solutions to provide core IT services. The resulting patchwork implementation with myriad configurations complicates a commander's ability to control the cyber battlespace. Without control it becomes nearly impossible to command. It also complicates commander's abilities to share information across domains let alone prioritize and deliver the best information for the joint warfighter. Today, through the aggressive efforts of Airmen at the 624th Operations Center, Network Operations and Security Centers (NOSC) and Network Control Centers, the Air Force asserts some semblance of control over the Air Force portion of this domain. However, today's network configuration will stretch the ability to command forces in and through the increasingly contested cyber battlespace.

The Air Force has the organization in place to command forces in the cyber domain with the assignment of AFSPC as lead MAJCOM for cyberspace operations. Twenty-fourth Air Force stood up as the component Numbered Air Force warfighting headquarters for cyberspace operations and was designated by US Strategic Command as Air Forces Cyber under the sub-unified command of US Cyber Command. To truly command across this warfighting domain, though, there must be a way to control its related capabilities and forces. Today, three NOSCs operate and maintain 14 distinct networks on the NIPRNet alone. With such complexity and the flood of new services pushed daily from industry and pulled by users, it is increasingly difficult to operate and maintain secure operations within this environment; mission assurance suffers as a result. Further challenging our migration efforts is the level of comfort some commanders have under the current model of "owning" their piece of the AFNet. However, like General Ryan, I believe we simply cannot continue to operate and maintain these disparate networks. We must reduce complexity by collapsing these networks into a single Air Force domain.

Even as cyberspace capabilities offer our forces distinct advantages at the strategic, operational, and tactical levels, our adversaries can also use this domain in an asymmetric strike. We need to aggressively put in place changes that will, in the longer term, equip our forces with a more responsive, resilient, and ultimately more defendable network.

Today's myriad of configurations, services, and systems fielded are the Achilles' heel of our Air Force. With the fluid and ever-changing threats to our cyber assets, today's network control centers, NOSCs, and enterprise service units protect our network via an endless stream of software patches, information assurance vulnerability alerts and NOTAMs. Despite these efforts, the operational commander still cannot be certain about

the absolute cyber security posture of forces. By migrating to a single domain, configurations can be more easily standardized, day-to-day operations and maintenance can be more readily regimented, and ultimately, the operational commander can have greater assurance that forces are secure from attacks through the cyber domain. While one network possesses its own vulnerabilities, these are offset by improved ability to equip, train, operate, and monitor.

As challenging as these attacks through cyberspace may be, the Department of Defense (DoD) faces an equally daunting challenge of confronting these threats while finding ways to reduce the federal budget deficit. Late last year, Secretary of State Hillary Clinton stated "[The deficit] poses a national security threat in two ways: it undermines our capacity to act in our own interest, and it does constrain us where constraint may be undesirable."[3] In January 2011, Secretary of Defense Robert M. Gates announced a series of efficiency decisions designed to save the DoD more than $150 billion over the next five years primarily by reducing overhead costs, improving business practices, and culling excess or troubled programs.[4] To this end, the Air Force announced a 25 percent reduction in our communications infrastructure budget across the Future Years Defense Program.[5] To meet this ambitious goal, we need to eliminate unnecessary redundancy, consolidate the delivery of core IT services, and reduce the cost of delivering those services to forces in the joint fight. By migrating to a single AFNet, we will simplify the delivery of these services, reduce the operations and maintenance burden to deliver these services, and ultimately control cost. Further, by taking an enterprise approach to this domain, we can continue our efforts to commoditize IT buys to drive down procurement costs, leverage economies of scale to deliver the services where and when required, and converge technologies to reduce the IT footprint. Many of these benefits could be realized to a much smaller degree without a single AFNet, but with the single network, we will preserve and improve cyberspace capability while meeting cut back requirements. A single AFNet allows the professionals who work with the network to have focused training and develop in-depth expertise on one network instead of being responsible for the intricacies of multiple networks.

Network migration has not been easy, but with our renewed operational focus, we have made great strides toward completing this effort. Through 2010, 17 bases migrated into the AFNet single network; four bases successfully shifted to this common network in December alone. If we were to continue at this steady pace, we would be on track to finish in the 2015 or 2016 timeframe. Because this time line is certainly late to need, AFSPC put together a team to find ways to accelerate the schedule.

Speed alone is not the measure of success; operational impact is critical. At one base, the wing commander informed the migration team that the migration was a non-event, and if he had not been in-briefed, he would not have known it was happening. At another base, the outbrief was cancelled because the migration went so smoothly that there was nothing to brief. These are certainly encouraging reports, but some migrations may not be so smooth—there may be unforeseen issues on bases with combatant commands and MAJCOM headquarters. We must prepare for the most challenging efforts. The MAJCOM vice commanders will have met in late April to discuss the best way ahead.

There will be challenges inherent to this type of service-wide effort. Technical issues yet to be uncovered will emerge. Given today's tough fiscal environment, we will need advocacy from all the MAJCOMs for funding to complete this effort. Additionally, there must be cooperation in defining the core services the AFNet will provide and partnership in executing the plan that all the MAJCOMs helped develop.

For the past 10 years, the Air Force pushed to create a single AFNet. Operationally, a single AFNet streamlines information sharing and simplifies the processes required for a commander to command and control forces via this cyber capability. From a mission assurance perspective, the AFNet simplifies the operation and maintenance of the service's network and reduces the number of threat vectors enemies can exploit. Finally, a single AFNet reduces operations and maintenance costs and enables many of the economies of scale required to absorb a 25 percent reduction in IT infrastructure;[6] affordability is a distinct advantage of migration to a single AFNet. As the Air Force continues to mature cyber forces, a single AFNet will be a critical component in our ability to successfully maintain freedom of action in this domain.

Notes:

[1] Joint Vision 2010 (JV2010), Chairman of the Joint Chiefs of Staff, 1996, 16, http://www.dtic.mil/jv2010/jv2010.pdf.

[2] Notice to Airmen, NOTAM 00-05, September 2000.

[3] Secretary of State Hillary Rodham Clinton *says deficit is national security threat*, Capital Hill, 18 September 2010.

[4] US Department of Defense, "DoD News Briefing with Secretary Gates and Admiral Mullen from the Pentagon," Secretary of Defense Robert M. Gates and Chairman, Joint Chiefs of Staff Admiral Mike Mullen, news transcript, 6 January 2011, http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4747.

[5] Ibid.

[6] Ibid.

Lt Gen Michael J. Basla (BS, Mathematics, University of New York; MS, Teleprocessing Science, Air Force Institute of Technology, University of Southern Mississippi) is vice commander, Air Force Space Command, Peterson AFB, Colorado. He assists the commander in organizing, equipping, training, and maintaining mission-ready space and cyberspace forces and capabilities for North American Aerospace Defense Command, US Strategic Command, and the other functional and geographic combatant commands with missile warning, positioning, navigation and timing, communications and cyber capabilities. The command 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. The command comprises more than 46,000 space and cyberspace professionals assigned to locations worldwide and deployed to an additional 35 global locations. General Basla also directs and coordinates the activities of the headquarters staff.

Mitigating Cyber Friendly Fire: A Sub-Category of Cyber Mishaps

Dr. Dee H. Andrews
Senior Scientist
Air Force Research Laboratory
Mesa, Arizona

Dr. Kamal T. Jabbour
Senior Scientist
Air Force Research Laboratory
Rome, New York

Friendly fire accidents leading to fratricide have tragically been a part of warfare since humans first began combat. Difficulties with proper combat identification are a constant challenge in kinetic warfare on today's battlefield despite the advent of digital aids such as blue force tracker (digital communications systems which provide situational awareness [SA] for all levels of command on the battlefield.) It is an unfortunate fact that friendly fire accidents will be with us in kinetic warfare for the far foreseeable future.

As recent experience has proven, friendly fire is not confined to the kinetic domain. Cyber friendly fire, a subcategory of cyber mishaps, that lead to cyber damage, is now a complicating factor in cyber operations. As is the case with kinetic friendly fire, cyber friendly fire is the non-intentional damage or disruption of blue forces while trying to defend attacks from red or gray forces, or in trying to attack red forces.

In this article we discuss briefly traditional kinetic friendly fire and combat identification, and then we explain how our understanding of that type of activity can help us better understand the cyber friendly fire phenomenon and how it might be mitigated.

Kinetic Combat Identification and Friendly Fire

The goal of combat identification (CID) is to improve unit combat effectiveness while preventing fratricide (friendly fire) and minimizing collateral damage. CID is the process that human shooters or sensors go through to identify entities on the battlefield prior to making shoot/don't shoot decisions. To perform CID, the warfighter uses all available means at their disposal to sort the entities on the battlefield prior to applying combat power.

The Joint Chiefs of Staff define combat identification as: "… the process of attaining an accurate characterization of detected objects to the extent that high confidence and timely application of military options and weapon resources can occur."[1]

Fratricide is defined as "the employment of friendly weapons and munitions with the intent to kill the enemy or destroy his equipment or facilities, which results in unforeseen and unintentional death or injury to friendly personnel."[2]

Fratricide Rates

A review of reported kinetic fratricide rates through the twentieth century and into the twenty first century shows that those rates are not decreasing despite the introduction of advanced technologies designed to increase target identification performance. This lack of progress in reducing the rates is partly due to the increased accuracy and lethality of modern weapons. In the kinetic world when blue warfighters shoot at targets, be the targets red or blue, they are more likely to hit and kill them than in the past. Reliance on technology alone is a flawed strategy because technology is not infallible; technology may fail or be unavailable, and it may be undermined by technology developed by an adversary. Human SA will always be part of the equation because, ultimately, the human gives the order and pulls the trigger. For example:

- From World War II, Korea, Vietnam, and the Gulf War, analysts concluded that about 15 percent of US casualties were the result of fratricide.
- First Gulf War, 35 of 146 US combat deaths, about a quarter, were the result of fratricide. In an article published at the end of 2001, the author indicates that of the first four Americans killed in the initial months of the operation in Afghanistan, three were killed by friendly fire.[3]

Most of the 20th century conflicts demonstrate a consistent fratricide rate of 10 to 15 percent. However, in addition to the reported fratricides, analysts have always assumed that fratricide rates might be even higher than reported. This may be true because fratricide is such a horrible phenomenon that combat units may sometimes look for any reason to discount fratricide as a possible cause of casualties. For example, analysis of fratricide data collected from the three combat training centers (National Training Center, Joint Readiness Training Center, Combat Maneuver Training Center) shows that fratricide rates are five to eight times the previously acknowledged rate. Even if we assume that warfighters are more prone to fire with less caution in a training setting, this higher rate of fratricide is startling.[4]

Cyber Friendly Fire Working Definition

Modifying the US Army Training and Doctrine Command definition for friendly fire above, our working definition for cyber friendly fire is: The employment of friendly cyber defenses and weapons with the intent of either defending the blue cyber systems from attack from red or gray forces, or attacking the enemy to destroy or damage their people, equipment, or facilities, which results in unforeseen and unintentional damage to friendly cyber systems. We consider cyber friendly fire to be a sub-category of cyber mishaps.

Cyber fratricide is not only cyber affecting cyber, it is cross domain. The cyber domain can cause unintended consequences in the air, space, land, and sea domains. Cyber can also be affected by these domains and threats from the electromagnetic spectrum, lasers, nuclear, biological and chemical weapons, and environmental factors. Cyber friendly fire is **not** an insider threat, which is intentional harm to, or theft from, a blue cyber system.

Unclassified examples of cyber mishaps that could have been caused by the unintended consequence of cyber fires:

A significant majority of cyber friendly fire incidents in the military domain are by nature highly classified. So, providing examples at that level in this article is not possible. However, the following are four non-classified examples of cyber friendly fire incidents:

1. An example from a non-military domain illustrates the danger of cyber friendly fire. In 2009, a Federal Aviation Administration (FAA) software technician installed a patch to an FAA system. This patch was installed arguably as a defense against an ongoing or imminent cyber threat against the FAA system or comparable systems. The unintended result was that a large part of the air traffic control system in the eastern US mistakenly came down for a number of hours. These types of inadvertent friendly fire incidents have happened in the Department of Defense (DoD), and there is always the threat of them happening again.

2. In March 2010, the DoD allowed access to social networking sites (SNS) from DoD computers. Shortly thereafter, two unanticipated consequences resulted: (1) a high percentage of base bandwidth was consumed by access to SNS, hampering critical operations on those bases, and (2) operational security concerns ensued from inadvertent posting of sensitive information.

3. In response to ongoing or imminent cyber threats to similar commercial or military systems, security patches of legacy systems disrupt occasionally system functionality. If the security patches are considered defensive cyber fires, then the resulting unintended consequences may qualify as cyber mishaps.

4. The Air Force accident investigation board has released its results concerning the possible causes of the 29 March 1999 crash of the unmanned aerial vehicle (UAV) Global Hawk No. 2. The mishap occurred when Global Hawk inadvertently received a test signal for flight termination from a test range on Nellis AFB, Nevada which was outside the frequency coordination zone in which the UAV's mission was being flown. This caused Global Hawk to go into a termination maneuver involving a pre-programmed, rolling, vertical descent from an altitude of 41,000 feet. Global Hawk No. 2, valued at approximately $45 million, crashed at China Lake Naval Weapons Center, California. When it crashed, there was no fire, and China Lake personnel secured the site. Since the "kill" sequence was intended as a defensive cyber fire against an out-of-control or rogue aircraft, its accidental use qualifies arguably as a cyber mishap with an unintended kinetic consequence.[5]

Cyber Friendly Fire Implications

Blue force cyber capabilities can be severely reduced or taken out entirely by a cyber friendly fire incident. A major difference between traditional and cyber friendly fire is the difficulty in gauging the potential damage to blue or grey forces that a cyber action might cause. In traditional kinetic friendly fire we can make estimates before we launch a weapon about the size of damage radius from where the weapon will impact. That is true all the way from a rifle bullet to a nuclear weapon. We can make tactical decisions based on that relatively certain knowledge of the danger the weapon launch poses to blue forces. Knowing where all blue forces are at all times is certainly a challenge, but it can be done. However, due to the "system of systems" nature of blue cyber, it is very difficult to know exactly what effect our blue defensive or offensive actions will have on blue assets since we can't be sure exactly how far out the cyber action might spread. The difficulty in doing a damage estimate before cyber action is taken makes cyber friendly fire difficult to identify and mitigate.

Current State of Friendly Fire Awareness in the Air Force

The cyber friendly fire problem is recognized by some cyber specialists in the Air Force, as demonstrated by attendance at two cyber friendly fire workshops that the Air Force Research Laboratory co-hosted with the 24th Air Force over the last couple of years. However, recognition is not broad, and we are unaware of any attempt to measure or mitigate the problem yet. There is currently no system for reporting cyber friendly fire incidents when they occur. Consequently, there is no database of these incidents for analysts to examine.

Potential Mitigation Strategies

There may well be technical means for mitigating the cyber friendly fire threat. One might think about software that could automatically scan the blue network once informed of a potential cyber activity and warn the cyber warrior about how far the action would impact the rest of the blue network, and what the potential for harm might be. If such software could provide that estimate then the blue warrior could make a risk-reward tradeoff to decide whether to go ahead with the action. Of course, since cyber operations happen so very quickly, there may not be time to do this type of analysis depending on the action contemplated, especially if the blue network is under attack.

General Cyber Friendly Fire Situational Awareness

Dr. Mica Endsley tells us that increasing cyber SA through technical means is feasible.[6] Dr. George P. Tadda and Dr. John S. Salerno took the Endsley concept of SA from her seminal paper.[7] The "perception, comprehension, projection" trilogy is at-

tributed universally to Endsley, and Tadda and Salerno mapped them to networks.

"Cyber SA enables mission assurance by using network perception, mission comprehension, and adversary projection to posture cyber networks and minimize adverse effects on the mission." They cite three key issues that must be addressed:

1. Perception
   - 'Sensing' elements within the network.
   - Real-time, dynamic, persistent, temporal, and automated information of all cyber systems physical/logical locations, configurations, and vulnerabilities.

2. Comprehension
   - Use of cyber systems to support a mission (asset-to-mission mapping).
   - Assessment of impacts of activities to the network or missions.

3. Projection
   - Anticipation of future enemy courses of action.
   - Anticipation of issues with the network.

The comments above involve cyber SA in general. We can extend those ideas to the unique case of cyber friendly fire SA. A key question is whether the SA of cyber warriors can be raised to the degree that they will recognize the possibilities of cyber friendly fire as they take an action. Again, due to the "system of systems" nature of large blue force networks, it will sometimes, or even often, be the case that a cyber warrior will not be able to know the complete set of ramifications of their actions. So, raising the SA for cyber friendly fire, and keeping it raised throughout the period of cyber operations, may not be possible at all times.

Another difficulty is that even if SA is raised about the potential for friendly fire, will that really do any good? Will the increased SA really be able to prevent a friendly fire incident? Also, the frenetic pace of cyber operations may not allow enough time for the cyber warrior to warn other blue forces of his/her actions before time necessitates the activity. This is especially true in cyber defense. If the warning can go out fast enough, it might be possible for a blue force site that might be affected by a cyber action from another site to put up some type of firewall or other defense, or perhaps even shut down for a period of time, to prevent being affected by the action. However, certain cyber actions may be long lasting and it could be difficult for a cyber site to protect itself completely.

Will the cyber warrior become paralyzed from action as they contemplate what negative effects they might have on blue forces? This phenomenon has been reported on kinetic battlefield. Especially after there has been a fratricide, analysts report that the units in the immediate vicinity sometimes show some reluctance to fire weapons for a period of time. That reluctance can, of course, result in a dangerous situation when enemy forces are in the area. While we would not typically assume that cyber friendly fire incidents would cause blue force loss of life typically, it is still in the realm of possibility unfortunately.

> Although researchers have recently started to address the cognitive needs of cyber decision makers, there is still a big gap between human analysts' mental model and the capability of existing cyber situation-awareness tools. Existing approaches to gain cyber situation-awareness … only work at the lower (abstraction) levels. Higher level situation-awareness analyses are still done manually by human analysts, which makes it labor-intensive, time consuming, and error prone.[8]

Possible Human Factors Causes of Cyber Friendly Fire Incidents

A report produced by the US Army's Center for Army Lessons Learned cites primary causes of kinetic fratricide (US Department of the Army, 1992) as poor SA, combat identification failures, and weapons errors; with contributing factors including anxiety, confusion, bad weather, inadequate preparation, and leader fatigue. The report states that these contributing factors are a critical dimension of realistic training conditions. Inadequate training is often cited as a contributing factor by studies of fratricide; other factors that have been cited include poor leadership, inappropriate procedures, language barriers, lack of appreciation of own platform position and heading, an inability to communicate changing plans or situations, and disorientation, confusion, and carelessness of blue forces.

All of the causes above for kinetic friendly fire can be applied in general to cyber friendly fire. Every cause cited can take its effect on cyber warriors, including bad weather that can disrupt microwave links and contribute to cyber fratricide.

Confusion about platform position in the blue network can certainly lead to misguided actions, although the direction of the cyber platform will probably not be an issue. Poor CID can lead to problems in both the cyber and kinetic spheres.

Implications for Cyber CID Education and Training

Education and training is key to better cyber CID performance. Education and training that provides cyber warriors with practice that is extended beyond normal practice times can be very helpful. The goal should be to encourage automaticity to ameliorate the effects of stress by making the warriors more resilient. While we sometimes do not think of cyber warriors fighting in teams, the fact is a significant portion of warriors on a net make up an extended team. Training for cyber teams can help to prevent warriors reverting to the sense that they are alone in the fight. Shared SA can result from quality team training.

Forcing cyber warriors to train in "uncomfortable territory" can help to reduce stress when the real engagements and defenses start. The more difficult we can make the training with constantly changing threats that are dynamic, the more resourceful the warriors will be. It is important to design training scenarios that force cyber warriors to test their assumptions. In that way they may increase their SA about other blue entities that might be affected by their actions. It is important to train cyber warriors to "think outside the box" to avoid cyber friendly fire.

Cyber Surety Program

One approach to increasing situational awareness to mitigate cyber friendly fire could be through a cyber surety program something like the nuclear community has established. The nuclear surety program is defined as, "Materiel, personnel, and procedures that contribute to the security, safety, and reliability of nuclear weapons and to the assurance that there will be no nuclear weapon accidents, incidents, unauthorized weapon detonations, or degradation in performance at the target."[9] Such an approach would be helpful in reducing cyber friendly fire incidents specifically, and cyber mishaps in general.

Research Questions

As researchers we find the following questions important:

- How can we improve our working definition of cyber friendly fire?
- How prevalent is cyber friendly fire?
- What are case examples of real world instances?
- What are the root causes?
- What are possible mitigating solutions, both technical and human factors, for cyber friendly fire?
- Are there cyber analogs of the blue force tracker technology that have helped to mitigate physical friendly fire accidents?

To address some of these questions we have constructed a cyber friendly fire test bed at Pacific Northwest National Laboratory, where we are currently constructing cyber friendly fire scenarios and metrics. These will be used to run experiments to see whether friendly fire SA can be raised, if so, how, and what difference does it makes in the rate of cyber friendly fire.

Conclusion

The threat of cyber friendly fire and resulting cyber fratricide may never be completely eliminated despite our best technological and human factors efforts. The scale of cyber systems and their many intricacies are perhaps too complicated. However, we believe it is possible to at least mitigate the threat to a great degree. A concerted effort to both research and develop solutions to cyber friendly fire is a worthy objective and we strongly encourage the DoD to take it seriously.

Notes:

[1] Joint Publication (JP) 3-09.3, *Joint Tactics, Techniques and Procedures for Close Air Support*, 2003, III-20, http://www.dtic.mil/doctrine/jel/new_pubs/jp3-09-3.pdf.

[2] US Army Training and Doctrine Command Source (TRADOC) 525-58, *Military operations: US Army operations concept for combat identification*, US Department of the Army, Fort Monroe, VA: Training and Doctrine Command, 1993, 1.

[3] M. T. Owens, "Fratricide and Friction: Perfection in war," National Review Online, 11 December 2001, http://old.nationalreview.com/comment/comment-owens121101.shtml.

[4] Kenneth Steinweg and Stephen Bowman, "Piercing the Fog of War Surrounding Fratricide: The Synergy of History, Technology, and Behavioral Research," Army War College, accession number ADA279536, study project, Carlisle Barracks, Pennsyvania, 1994.

[5] Sue Baker, "Results of Global Hawk accident investigation board released," Aeronautical Systems Center Public Affairs, report, 23 December 1999, http://www.fas.org/irp/program/collect/docs/n19991223_992288.htm. Report states: 10:14 a.m. PST at the South Range at China Lake Naval Weapons Center, California.

[6] Mica R. Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems," 1995, *Human Factors: The Journal of the Human Factors and Ergonomics Society* 37, no. 1 (March 1995) 32-64.

[7] George P. Tadda and John S. Salerno, "Overview of Cyber Situation Awareness," in *Cyber Situational Awareness: Issues and Research*, S. Jajodia et al., eds. (New York: Springer, 2010), 15-35, http://www.springerlink.com.

[8] Sushil Jajodia et al., eds *Cyber Situational Awareness: Issues and Research,*" (New York: Springer, 2010), 5.

[9] Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms,* 8 November 2010, as amended through 31 January 2011,Joint Education and Doctrine Division, J-7, Joint Staff.

Dr. Dee H. Andrews (BS, Psychology, Brigham Young University; PhD, Instructional Systems, Florida State University) is a senior scientist (ST) with the Human Effectiveness Directorate, 711th Human Performance Wing, of the Air Force Research Laboratory in Mesa, Arizona. Previously he held the position of division technical director for the Warfighter Training Research Division of the Air Force Research Laboratory. Previously he worked as a senior research psychologist for the Army Research Institute for the Behavioral and Social Sciences in Orlando, Florida. Prior to his work with the Army he was a research psychologist and training analyst with the Naval Air Warfare Center – Training Systems Division in Orlando, Florida. He has been elected to Fellow status in the Human Factors and Ergonomics Society, the American Psychological Association, the Royal Aeronautical Society of the United Kingdom, and the Air Force Research Laboratory. His research interests include: cyber training, learning organizations, simulator design, flight training, advanced distributed learning, accelerated learning, and distributed mission training.

Dr. Kamal T. Jabbour (BE Electrical Engineering with Distinction, American University of Beirut; PhD Electrical Engineering, University of Salford, UK) is a member of the scientific and technical cadre of senior executives, and 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. 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. He contributed to building the Offensive Cyber Operations Program at AFRL before assuming his current position. His research focuses on building cybercraft that shapes cyberspace as the domain for the new revolution in military affairs.

Achieving Cyber Survivability in a Contested Environment Using a Cyber Moving Target

Dr. Hamed Okhravi
Member, Technical Staff
Cyber Systems and Technology Group
MIT Lincoln Laboratory
Lexington, Massachusetts

Mr. Joshua W. Haines
Assistant Group Leader
Cyber Systems and Technology Group
MIT Lincoln Laboratory
Lexington, Massachusetts

Mr. Kyle Ingols
Member, Technical Staff
Cyber Systems and Technology Group
MIT Lincoln Laboratory
Lexington, Massachusetts

Evolving cyber threats in a contested environment provide a challenge in protecting operations and critical assets. Traditional cyber protection mechanisms can prove ineffective when facing a motivated, well-resourced adversary. As a result, many mission critical systems remain vulnerable to advanced, targeted cyber attacks despite the significant amount of effort and resources used to secure them. Complex systems and commercial off-the-shelf components often exacerbate the problem.

Although protecting the mission critical systems is a priority, recent cyber incidents and alerts have shown that we cannot rely completely on hardening individual components.[1,2] As a result, new attention has been given to game-changing technologies to achieve mission continuity in a contested environment. In fact, the Air Force chief scientist's report on technology horizons mentions the need for "a fundamental shift in emphasis from 'cyber protection' to 'maintaining mission effectiveness' in the presence of cyber threats" as a way to build inherently intrusion-resilient cyber systems.[3] Moreover, the White House National Security Council's progress report mentions a "moving target (systems that move in multiple dimensions to disadvantage the attacker and increase resiliency)"[4] as one of the administration's three key themes for cyber security research and development strategy.

Our approach to developing the necessary survivability involves a combination of research, prototyping, architectural development, and evaluation. We have researched architectural ideas that make it difficult for adversaries to impact mission critical systems and prototyped an architectural component that provides platform heterogeneity as a proof-of-concept. We have also developed an analysis and assessment tool that can evaluate the attack paths into a system and support the architectural component in determining the appropriate orientation based on the current threat level. We are in the process of developing analysis and experimentation frameworks to thoroughly measure the effectiveness and protection offered by the components discuss in this work; we leave them as the future work here.

We describe two components for achieving cyber survivability in a contested environment: an architectural component that provides heterogeneous computing platforms and an assessment technology that complements the architectural component by analyzing the threat space and triggering reorientation based on the evolving threat level. Together, these technologies provide a cyber moving target that dynamically changes the properties of the system to disadvantage the adversary and provide resiliency and survivability.[5]

Trusted dynamic logical heterogeneity system (TALENT),[6] the architectural component, provides a framework to migrate, in real-time, mission critical applications across heterogeneous platforms. We hypothesize that in critical warfighting systems, the mission itself is the top priority, not individual instances of the subsystems. By live-migrating the critical application from one platform to another, TALENT can thwart cyber attacks and provide resiliency. This means the information collected by the attacker about the platform during the reconnaissance phase becomes ineffective at the time of attack.

TALENT provides heterogeneity at the hardware and operating system levels while it preserves the state of the mission critical application.[7,8] This means we should be able to run the application on top of processors with different instruction sets.

By accurately measuring risk for mission critical networks, attack graphs allow network defenders to understand the most critical threats and select the most effective countermeasures. Network Security Planning Architecture (NetSPA),[9] the assessment component, analyzes critical networks against the current threat level using attack graphs and reachability analysis. NetSPA assesses the effects of known and zero-day attacks, computes the impact of possible compromises, and proposes countermeasures.

By integrating the architectural and assessment components, a critical warfighting system can achieve cyber survivability against aggressive cyber attacks. NetSPA assesses the potential compromises and reacts to changes in the current threat level by triggering reorientation. TALENT then performs reorientation by dynamically changing the platform of the critical applications to the platform recommended by NetSPA. Together they implement a polymorphic system that can operate through aggressive compromises in a contested environment.

Architectural Component

The architectural component of a cyber survivable system

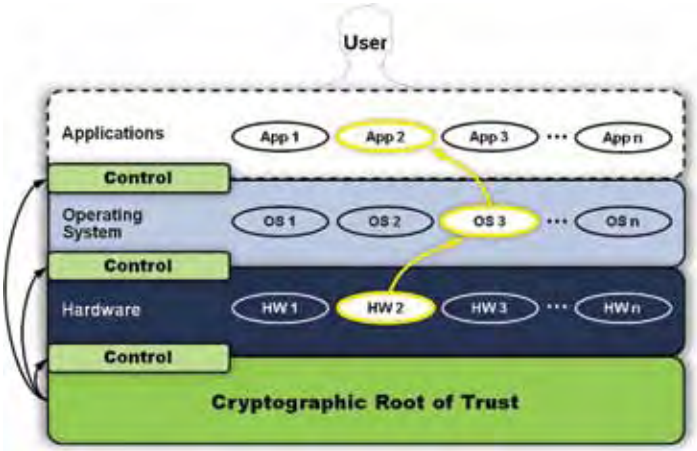

Figure 1. A dynamically composable platform of heterogeneous components.

must be able to dynamically provide heterogeneity. Figure 1 illustrates a dynamically composable platform of heterogeneous components. Heterogeneity at different levels can mitigate various attacks. Application-level heterogeneity mitigates architecture specific exploits and malicious compilers. Operating system (OS)-level heterogeneity mitigates kernel specific attacks, OS-specific malwares, and OS persistent attacks (rootkits). Hardware heterogeneity can thwart supply chain attacks, malicious/faulty hardware, and architecture specific attacks. TALENT is not a complete defense against all these attacks; it can, however, provide survivability in the presence of platform specific attacks by means of dynamic heterogeneity.

In order to provide dynamic heterogeneity, TALENT migrates both the environment (e.g., files and network connections) and the state of a critical application across different platforms. Figure 2 illustrates a heterogeneous migration process. To address the challenge involved in using heterogeneous platforms including binary incompatibility and loss of state and environment, TALENT uses two key ideas: OS-level virtualization and portable checkpoint compilation.

Environment Migration

An important goal of the architectural component is to preserve the environment of a mission critical application including the filesystem, configuration files, open files, network connections, and open devices. Many of the environment parameters can be preserved using virtual machine (VM) migration, but VM migration is only viable with homogeneous OS and hardware. Because we want to *change* the OS and hardware while migrating a live application, VM migration is not applicable. TALENT uses OS-level virtualization to sandbox an application and migrate the environment.

OS-level virtualization is a method in which a kernel allows for multiple isolated user-level instances. Each instance is called a container (jail or virtual environment). The method was originally designed to support fair resource sharing, load balancing, and cluster computing application. OS-level virtualization provides an environment in which all resources (devices, filesystem, memory, sockets, etc.) are virtualized.

Note that the major difference between OS-level virtualization and hardware-level (e.g., Xen and VMWare) is the semantic level at which the entities are virtualized. Hardware-level hypervisors virtualize disk blocks, memory pages, hardware devices, and central processing unit cycles, whereas OS-level virtualization works at the level of file systems, memory regions, sockets, and kernel objects (e.g., inter-process communication [IPC] memory segments and network buffers.) Hence, the semantic information often lost in hardware virtualization is readily available in OS-level virtualization. This makes OS-level virtualization a good choice for use cases where this information is needed like monitoring or sandboxing at the application level.

TALENT uses OS-level virtualization to migrate the environment of a critical application. When reorientation is requested by the assessment component, TALENT migrates the container of the application from the source machine to the destination machine. This is done by synchronizing the filesystem of the destination container with the source container. The OS keeps track of open files and the same files are opened in the destination.

To preserve network connections during migration, the internet protocol (IP) address of the container's virtual network interface is migrated to the new container. Then the state of each transmission control protocol socket is transferred to the destination. The network migration is seamless to the application, and the application can continue sending and receiving packets on its sockets. Many OS-level virtualization frameworks also support IPC and signal migration. In each case, the states of IPC and signals are extracted from the kernel data structures and migrated to the destination. TALENT supports these features by utilizing the underlying virtualization layer.

Application Migration

Migrating the environment is only one step in backing up the system because the state of running critical applications must also be migrated. To do this, a method to checkpoint (store the state of) running applications must be implemented. Once all checkpointed program states are saved in checkpoint files, the state can be migrated by simply mirroring the file system. TALENT uses a portable checkpoint compiler (PCC) to preserve the state of a running application and provide application migration.[10]

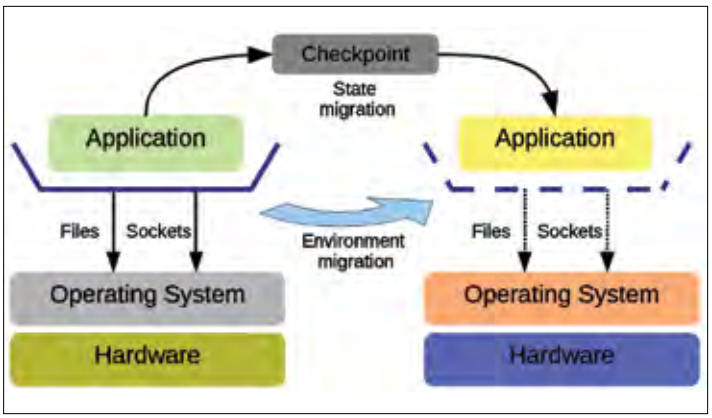

Figure 2. A heterogeneous migration process.

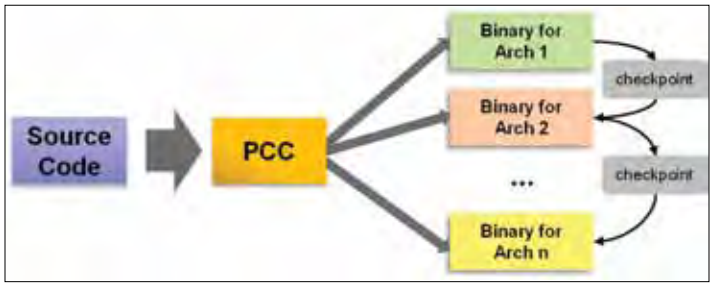

Figure 3. A portable checkpoint compilation process.

Figure 3 illustrates a portable checkpoint compilation process. PCC allows compilation to occur independently on various operating system/hardware pairs. The resulting executable program, including the inserted checkpointing code, functions properly on each platform on which it was compiled.

Using PCC, TALENT achieves both transparency and scalability. Transparency is obtained by performing automatic code analysis and checkpoint insertion. This prevents the end user from modifying code to indicate where checkpointing should be performed or what specific data should be checkpointed. Scalability is obtained in two ways. First, the frequency of checkpointing bottlenecks in the checkpointing process can be controlled. Second, through the use of compressed checkpoint file formats, the checkpoints themselves remain small as the amount of data processed by the program increases.

In order to achieve portability across heterogeneous platforms, the checkpoint file must have a portable format. Storing the checkpoint in a simple binary file can cause incompatibility if the destination platform has different bit instruction size (32 vs. 64 bits) or endianness (little vs. big). Thus the checkpoint file format has to be portable. We use the HDF5 format in TALENT.[11] HDF5 is an open, versatile data model that can represent complex data objects. It is a portable data model that can represent various bit-ness and endianness. Like Extensible Markup Language (XML),[12] HDF5 is self-describing. Unlike XML, HDF5 uses a binary format which allows efficient parsing of the data.

Analysis and Assessment Component

NetSPA, our attack-graph generation and reachability analysis tool, provides the assessment component of a cyber survivable system. By analyzing the impact of possible attacks and reachability of mission critical systems in a network, NetSPA facilitates platform reorientation based on the evolving threat level.

Data Collection

NetSPA's network model supposes that an individual host possesses one or more interfaces which have listening addresses. These interfaces have zero or more open ports, accepting connections from other hosts. A host and its interfaces may have rules that dictate how network traffic may flow to, and through, the host. A port has zero or more vulnerability instances, particular flaws or configuration choices which may be exploitable by an attacker. Each interface on a host is connected to a link, representing some combination of hubs and switches connecting a set of interfaces together. An attacker is able to obtain one of four access levels on a host: "root" or administrator access, "user" or guest access, "DoS" or denial-of-service, or "other," a confidentiality and/or integrity loss. The combination of a host and an access level is an attacker state. An attacker obtains a host's reachability if "root" or "user" access is achieved. Reachability and credentials serve as prerequisites to exploitation of a vulnerability instance.

NetSPA requires only a few core pieces of knowledge to build an attack graph. For a given host, the tool must know which credentials can be acquired at a given access level on the host and which ports the host can reach. For a given port, NetSPA requires knowledge of the port's vulnerabilities. For each instance of a vulnerability, the tool must know what is required to exploit it and what is gained by exploiting it.

NetSPA requires a large amount of data to compute the needed information, but system administrators often collect this data as a matter of course. The core pieces are network topology, vulnerability information, and credentials. NetSPA itself runs offline using the provided data, minimizing the risk of an attacker obtaining the source data or resultant graph. NetSPA can collect the raw information from Nessus scans, firewall rulesets, Open Vulnerability Assessment Language (OVAL)-based scanners, and vulnerability databases such as the National Vulnerability Database and Bugtraq.[13, 14]

Computing Reachability

Computing reachability is crucial in determining how to react to aggressive cyber attacks. In a contested environment, critical warfighting applications must be migrated to portions of the network that are not easily reachable from the external network through a zero-day attack.

A straightforward method to compute reachability is to try to reach every known target IP address and port from every host in the network. Such an approach would generate a reachability matrix, where a row represents a source interface on a host, a column represents a target port, and each cell indicates whether or not the source can reach the target. This is correct, but it scales poorly in terms of both space and time.

We have made three improvements to the straightforward approach. We collapse sections of the matrix into reachability groups, saving large amounts of both time and memory. Filtering rulesets are collapsed into binary decision diagrams,[15] allowing the reachability system to traverse a set of filtering rules in constant time. We also hypothesize a "generic attacker" by selecting a link on which the attacker will begin and allowing the attacker to use the most advantageous source IPs.

Reachability groups identify redundancies in the reachability matrix and collapse submatrices into single subrows before computing the contents, saving both time and space. First, intra-subnet reachability which is not influenced by any filtering devices can be collapsed into a single subrow, because every source interface within the subnet will have the same reachability to all ports within that same subnet. Second, inter-subnet reachability can be collapsed by identifying sets of interfaces within a subnet which are treated identically by the filtering

devices on the network. If the source IP addresses of a set of interfaces on the same subnet match in the same set of filtering rules on the network, the interfaces are grouped together and reachability is computed for only one of them.

Building Attack Graphs

An attack graph specifies the sequences of vulnerabilities an adversary can exploit in order to gain access to a critical system. It is a valuable tool for understanding the impact of known and zero-day (unknown) vulnerabilities and studying the consequences of stepping-stone attacks on a mission critical system. NetSPA can generate attack graphs using the reachability analysis and the information collected about the current environment. As the threat evolves in a contested environment, attack graphs can help us understand which subnets are secure or which platforms can survive the current threat level. The assessment capability provided by NetSPA supports the reorientation of the critical platforms.

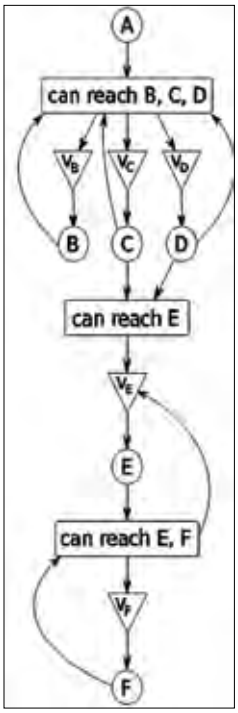

Figure 4. A multiple-prerequisite graph.

In order to build the attack graphs, NetSPA uses a data structure called a multiple-prerequisite (MP) graph. The MP graph also shows all hosts which can be compromised from any host the attacker has compromised. In figure 4 for example, host F is capable of compromising host E. The MP graph uses the following three node types:

- State nodes represent an attacker's level of access on a particular host. Outbound edges from state nodes point to the prerequisites they are able to provide to an attacker. In figure 4, state nodes are circles.
- Prerequisite nodes represent either a reachability group or a credential. Outbound edges from prerequisite nodes point to the vulnerability instances that require the prerequisite for successful exploitation. In figure 4, prerequisite nodes are rectangles.
- Vulnerability instance nodes represent a particular vulnerability on a specific port. Outbound edges from vulnerability instance nodes point to the single state that the attacker can reach by exploiting the vulnerability. In figure 4, vulnerability instance nodes are triangles.

Attack graphs for all but the smallest networks are too large for hand evaluation. NetSPA uses two approaches to this problem: automatic graph simplification and automatic recommendation generation. The former aims to reduce the size of the graph by collapsing similar nodes together. The latter treats the attack graph as an intermediate structure, not a final product, and extracts useful information from the graph for presentation to the user.

Building Recommendations

Even visually simplified attack graphs can be large and unwieldy. The core information from the graph should be extracted by the tool and presented in a more immediately useful form.

Often an attacker must compromise a directly accessible host through a filtering device in order to attack a group of hosts behind the filtering device. Attack graphs can be used to identify these bottlenecks and produce a list of the critical vulnerabilities which allow the attacker to compromise the bottleneck hosts. Defenders can then migrate the critical applications to subnets and platforms not affected by these vulnerabilities.

We form recommendations by computing, for each individual prerequisite in the graph, which vulnerability instances need to be removed in order to prevent the attacker from reaching the prerequisite, and which states the attacker cannot reach with the prerequisite absent.

We accomplish this by rebuilding the MP graph for each potential recommendation, noting which vulnerability instances are actually necessary to reach the selected prerequisite and which states are no longer achievable. Some prerequisites may yield identical recommendations. We discard duplicates in these cases.

We weight recommendations based on the number of critical hosts denied the attacker. A user could supply per-host "asset values" or weights to prioritize steps that protect critical servers.

Cyber Moving Target

The architectural and assessment components provide a system that dynamically moves in multiple dimensions in order to survive in a contested environment (see figure 5). The reachability analysis and attack graphs provided by NetSPA assess the cyber threats to a mission critical application in a hostile environment and facilitate reconfiguration and reorientation when facing a new threat. The assessment includes both known and zero-day (hypothetical) vulnerabilities so that the impact of previously unknown weaknesses can also be analyzed. Upon detecting a change in the threat level (as a result of a new vulnerability being discovered or an actual attack detection event), TALENT, the architectural component, facilitates the reconfiguration and reorientation of the critical applications by dynamically changing their platform and subnet to a survivable combination based on the recommendations provided by the assessment tool. In essence, the two technologies implement

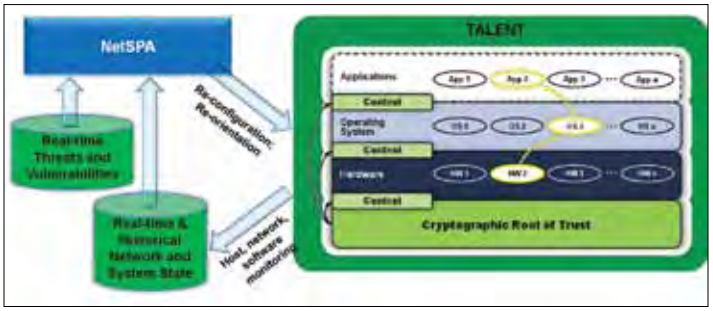

Figure 5. The architectural and assessment components provide a system that dynamically moves in multiple dimensions in order to survive in a contested environment.

an OODA loop (observe, orient, decide, and act) in which the observe and decide phases are provided by NetSPA and the orient and act phases are implemented by TALENT.

A system that deploys these components can provide a cyber moving target (also known as a polymorphic system) that changes its properties in a hostile environment. Cyber exploits are often feasible against a set of platforms (hardware/operating systems). By dynamically changing platform properties, a cyber moving target can mitigate platform specific exploits. The destination platform and subnet are chosen intelligently based on the result of reachability and attack graph analysis to resist the current threat level.

A Cyber Survivable Future

We believe cyber security must shift focus from cyber protection technologies to cyber survivability. Security incidents in highly protected environments have illustrated the fact that a motivated adversary can compromise even the most secure systems. We believe that new cyber security paradigms must leverage architectural and assessment technologies to create a cyber moving target that disadvantages potent adversaries and facilitates recovery and mission survivability after a successful compromise. It is imperative that we clearly understand the mission impact of potential security breaches and implement operate through capabilities in order to continue the mission objectives of the critical applications during and after a cyber incident rather than deploying protections and hoping that they can resist attacks.

In a contested environment with motivated, well resourced adversaries, it is likely that traditional cyber protection technologies will be bypassed or disabled as a result of previously unknown attacks. Achieving cyber survivability for critical warfighting systems necessitates the use of game-changing technologies that can get ahead of the adversaries.

In this work we described architectural ideas that can help improve the survivability of a mission critical system against cyber adversaries and prototyped an architectural component to demonstrate their feasibility. We also described an evaluation tool that analyzes the possible attack paths to a system and supports the architectural component. We are in the process of developing analysis and experimentation techniques to quantify the effectiveness and protection offered by these components which we leave as the future work.

Notes:

[1] Lolita C. Baldor, "New Threat: Hackers Look to Take Over Power Plants," *The Associated Press*, August 2010, http://abcnews.go.com/Business/wireStory?id=11316203.

[2] Rodney H. Brown, "Stuxnet worm causes industry concern for security firms," *masshightech.com*, October 2010, http://www.masshightech.com/stories/2010/10/18/daily19-Stuxnet-worm-causes-industry-concern-for-security-firms.html.

[3] "Report on Technology Horizons: A Vision for Air Force Science & Technology During 2010–2030," AFST-TR-10-01-PR, US Air Force Chief Scientist, May 2010, http://www.af.mil/shared/media/document/AFD-100727-053.pdf.

[4] Cybersecurity Progress after President Obama's Address, The White House National Security Council, July 2010, http://www.whitehouse.gov/administration/eop/nsc/cybersecurity/progressreports/july2012.

[5] Anup Ghosh, Ivan Arce, "Guest Editors' Introduction: In Cloud Computing We Trust - But Should We?," *IEEE Security & Privacy* 8, no. 6, (November–December 2010): 14-16.

[6] Hamed Okhravi et al., "TALENT: Dynamic Platform Heterogeneity for Cyber Survivability of Mission Critical Applications," Secure and Resilient Cyber Architecture Conference (SRCA'10), McLean, Virgina, 29 October 2010, https://register.mitre.org/sr/papers1/TALENT.pdf

[7] Daniel Geer et al., "Cyber*In*security: The Cost of Monopoly," September 2003, http://cryptome.org/cyberinsecurity.htm.

[8] D. Williams et al., "Security through Diversity: Leveraging Virtual Machine Technology," *IEEE Security & Privacy* 7, no. 1 (January–February 2009): 26-33.

[9] Kyle Ingols et al., "Modeling Modern Network Attacks and Countermeasures Using Attack Graphs," Annual Computer Security Applications Conference (ACSAC '09), 7-11 December 2009, 117-126.

[10] Gabriel Rodríguez et al., "CPPC: a compiler-assisted tool for portable checkpointing of message-passing applications," *Concurrency and Computation: Practice and Experience* 22, issue 6 (April 2010): 749-766.

[11] HDF4 Reference Manual, The HDF Group, February 2010, http://www.hdfgroup.org/release4/HDF4_RM_html/RM_Front.html.

[12] Mirella M. Moro et al., XML: Some Papers in a Haystack, *SIGMOD Record* 38, no. 2 (October 2009): 29-34.

[13] P. Meil et al., National Vulnerability Database (NVD), http://nvd.nist.gov.

[14] Bugtraq vulnerability database, *SecurityFocus.com*, http://www.securityfocus.com/archive/.

[15] Randal E. Bryant, "Graph-Based Algorithms for Boolean Function Manipulation," *IEEE Transactions on Computers* 35, issue 8 (August 1986): 677-691.

Dr. Hamed Okhravi (MS and PhD, Electrical and Computer Engineering, University of Illinois at Urbana-Champaign [UIUC]) is a member of technical staff at the Cyber Systems and Technology Group of MIT Lincoln Laboratory, where he conducts research in the area of cyber survivability and security architectures.

Currently, Dr. Okhravi is developing cyber-attack survivable systems and networks. The current effort focuses on creating a cyber moving target using platform heterogeneity.

Mr. Joshua W. Haines (BS, Electrical Engineering, Union College; MS, Electrical and Computer Engineering, University of Massachusetts at Amherst) is an assistant group leader in the Cyber Systems and Technology Group at MIT Lincoln Laboratory. He is responsible for managing research and development of technology and systems in support of national cyber missions including computer network defense, attack, and exploitation. Focus areas include system analysis, architecture engineering for robustness and security, development of network-centric cyber systems, automated analysis of network vulnerabilities, red-teaming of Department of Defense programs, and development and deployment of traffic generation and test development for test range environments.

Mr. Kyle Ingols (SB and M.Eng., Electrical Engineering and Computer Science, MIT) is a member of technical staff in the Cyber Systems and Technology Group of MIT Lincoln Laboratory. His current work covers a broad spectrum of cyber security, including secure system design, scalable aggregation of network defender data, and protection against physical access to cyber systems.

Winning in Cyberspace: Air Force Space Command's Approach to Defending the Air Force Network

Ms. Jill Baker
Systems Engineer
MITRE Corporation
Headquarters Air Force Space Command
Peterson AFB, Colorado

Mr. Shane Morrison
Principal Systems Engineer
MITRE Corporation
Headquarters Air Force Space Command
Peterson AFB, Colorado

Mr. Jarret Rush
Principle InfoSec Engineer
MITRE Corporation
Cyber Requirements Division
Headquarters Air Force Space Command
Peterson AFB, Colorado

Today's Air Force Network (AFNet) is complex and disparate, a compilation of individual networks that were designed absent an enterprise model or a clear understanding of warfighting and support requirements or constraints, and with an inconsistent approach to identifying or mitigating vulnerabilities. In addition, the segmented approach to network procurement and management created operational and technical seams and information sharing shortfalls, complicating protection of forces and achieving mission assurance while operating in a contested environment.

To provide an available, secure cyberspace enterprise Air Force Space Command (AFSPC), through 24th Air Force (24 AF), is fielding a defensible Air Force network designed to achieve mission assurance. The AFNet's design will be simple, agile, integrated, and interoperable with documented processes for connection, configuration management, reporting, and operational capability assessment.

To shape this mission, the AFSPC Cyberspace Requirements Division (A5J) is implementing a range of actions, including the use of mission area architecting (MAA), improving the net ready key performance parameter (NR KPP), developing a protection KPP, and implementing an operational protection strategy. These measures influence areas where it's felt that adjustment and change will decrease AFNet residual risk and improve the cyber warfighter's ability to gain and maintain cyberspace superiority.

The foundational element of the AFNet strategic improvement strategy, the new plans and requirements (A5) concept of MAA, is the focus of Part One of this article.

Part Two discusses inadequacies in current KPPs and introduces the development of a cyber protection KPP designed to fill the void.

The KPPs will be augmented by development of an operational protection strategy which is also discussed in Part Two.

Part Three considers how these actions are combined into a holistic effort and supplemented by ongoing 24 AF programs to meet cyberspace superiority. These combined efforts are creating an AFNet that is simple, agile, integrated, and interoperable with documented processes for connection, configuration management, reporting, and operational capability assessment.

Part One: Mission Area Architecting

This section discusses how MAA is used to highlight connections and gaps between process and governance, systems analysis, requirements, programs, and funding adequacy. It considers how MAA makes use of Department of Defense Architectural Framework (DoDAF) capability viewpoints to deliver products that identify optimal forces mix, and deployment plans. Finally, it looks at how MAA supports enterprise systems engineering.

AFSPC's mission is to provide an integrated constellation of space and cyberspace capabilities. Consistent with Headquarters (HQ) AFSPC/A5's guidance, AFSPC is taking steps to improve its strategic mission engineering and capability based planning processes using a concept called MAA. The output of these improvements is a strategic analysis plan coupled with a rigorous requirements management process to execute the HQ AFSPC Strategic Plan.[1] MAA provides an analytical foundation for making smarter decisions about what systems are needed to satisfy required capabilities. It supports a broad spectrum of systems engineering and analysis activities such as:

- Mission thread and task analysis
- Capability-based assessment
- Determining an optimized and robust capability mix
- Risk assessments
- Requirements development, analysis, and mapping
- Allocation of requirements to programs
- Evaluation and prioritization of science and technology needs
- Exploration and evaluation of innovative solutions
- Strategic program planning
- Requirements-based justification for the program objective memorandum (POM)

MAA will ultimately provide a tailorable analytic framework and a systems engineering foundation for the development and management of AFSPC-delivered capabilities.

A second benefit of MAA is that it leverages and influences community analytical resources to include the product centers, service research laboratories, and federally funded research and development centers. MAA integrates architectures and analyses into mission area positions that drive explicit, defensible plans and programs in space and cyber. MAA supports the decisions necessary to define and deliver combined space and cyberspace capabilities required to achieve mission objectives.

To accomplish this, MAA captures essential information in a set of strategically useful models and artifacts. The specific artifacts developed are determined by the decisions to be made. For example, figure 1 is used to determine the completeness and traceability of requirement documents needed to inform program development and funding.

MAA will use the strategic capability viewpoints defined in the DoDAF version 2.0.[2,3] These viewpoints, not part of figure 1, include capability hierarchies, capability dependencies, and capabilities mapped to operational activities and services. Combined with project viewpoints these will support products such as optimal forces mix,[4] strategic or campaign level plans, and time-phased force deployment plans.

MAA will help address particular challenges better considered at a more strategic or enterprise level. Currently, MAA is used to address the challenges that are impacting AFSPC's ability to provide dynamic, robust mission capabilities. These challenges include those that result from applying traditional systems engineering when building system-of-systems at increasingly greater scales and those associated with handling change at an enterprise level.

Traditionally, requirements engineering has been stovepiped focusing on specific missions, capabilities, or systems; it did not consistently address the impacts of integrating a system with the systems it operated with or the enterprise infrastructure it operated on. What is missing is an overarching AFNet engineering strategy. As advocated by the HQ AFSPC/A5 and 24 AF, a strategic approach to architecting at an enterprise scale is required. In the case of the AFNet, this includes emphasizing cyber defense and mission assurance as strategic values. Supporting this effort, MAA provides linkages between governance, requirements, programs, and funding establishing connections that highlight gaps and needed developmental work.

Used effectively, MAA will support engineering an AFNet that is defensible and designed to achieve mission assurance. It supports architecting and delivering systems that decrease operational risk, have well defined interfaces and interoperate on the network achieving the AFNet's design, operations, and defensibility goals. MAA's results are helping focus HQ AFSPC's actions to improve the NR KPP and to develop a cyberspace protection KPP and operational protection strategy, described in Part Two.

Part Two: System Design and Requirements Risk Mitigation

MAA ensures that requirements have a validated basis—they are approved, have a validated pedigree, are funded, and part of an acquisition program. However, while critical, MAA in itself does not assure that the fielded capability will integrate and operate on the AFNet without increasing risk. This section of the article considers the NR KPP, a protection KPP, and an operational protection strategy, that will influence the capabilities' early design. They will cause the acquisition program to consider design factors that improve system security and protection architectures and interfaces. The KPPs and protection strategy goals include taking actions that will drive down system risk and minimize AFNet integration risk early in the design process when change is affordable. This will support delivering low-risk systems and fielding a defensible Air Force network designed to achieve mission assurance.

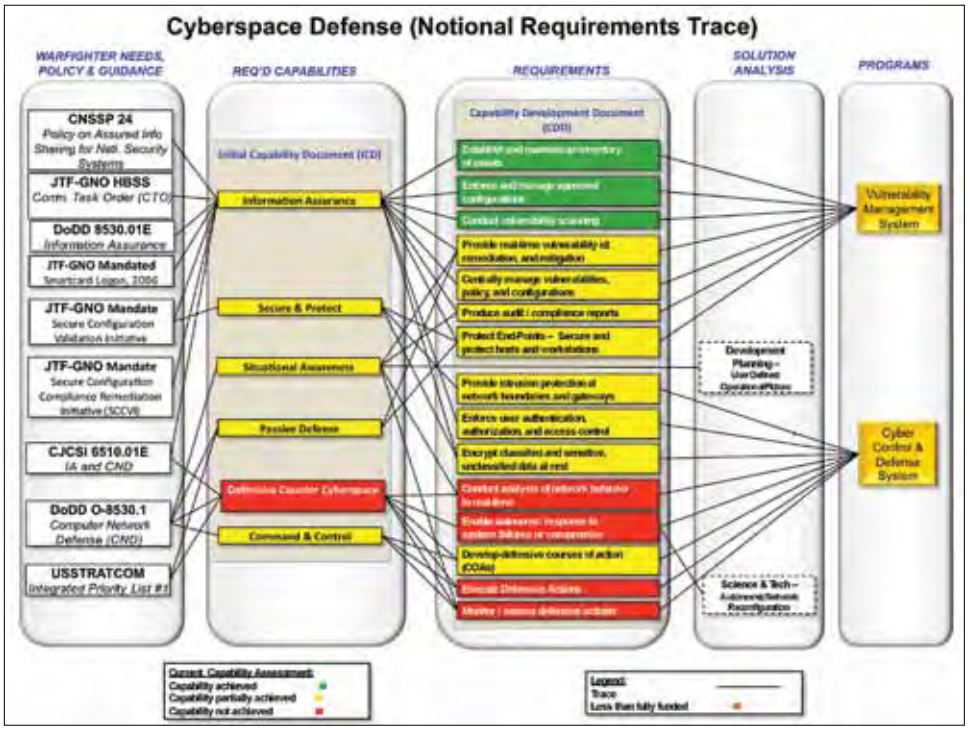

Figure 1. Example mission area architecture product.

Acquisitions specify, field and integrate systems and infrastructure that minimize AFNet operational risk. However, today's acquisition processes are built around the Department of Defense Instruction (DoDI) 5000.2, *Operation of the Defense Acquisition System*. While DoDI 5000.2 provides useful guidance, acquisition processes and KPPs, such as the NR KPP have not kept pace with the evolution of threats or enterprise complexity. As a result, systems designed to meet the NR KPP and other design guidance may not deliver interoperable capabilities that minimize AFNet risk or specified mission capabilities.

The system acquisition process specifies system engineering and development processes and associated artifacts to guide system design and to document and prove correct implementation. For example, acquisitions comply with the

NR KPP, the DoD Information Assurance Certification and Accreditation Process (DIACAP), demonstrate they meet the DoDI 5000.2 specified acquisition milestones, and more. *The acquisition governance is documented in thousands of pages of criteria; documenting the implementation could generate thousands of pages of "proof."* However, in spite of all this guidance, systems are acquired that fail to meet user needs or that negatively impact the network adding risk and decreasing AFNet defensibility.

An example occurred in summer 2009 when a major Air Force mission support system, under development since 2006, attempted a limited release as part of a strategy to dry-run critical subsets of operational capability. Once connected to the AFNet, the system did not perform as anticipated nor as demonstrated in its test environment. After years in development and testing, the system's inability to interoperate with the AFNet prompted the operational decision to terminate the release activities. This instance triggered a wide-scale program review, and many months later, the system has not been reconnected and the system's user continues to accomplish mission activities using resource intensive processes.

Systems, like the example, place system security and operational readiness certifiers in the difficult position of choosing between needed operational capabilities and approving fielding of potential security and performance risks. Within its lead command role for the cyberspace mission, the HQ AFSPC requirements community is involved on several fronts to deliver systems that are interoperable with the AFNet and that minimize operational risk. Some of the key activities include:

- Architecture alignment
- NR KPP revision
- Developing a system protection KPP and key system attributes
- Developing an operational AFNet protection strategy

To be effective and affordable, NR KPP driven requirements and application of a protection KPP need to be done early in the system's development and acquisition lifecycle. Simply put and highlighted by figure 2, early involvement by the requirements, architecture, security, test, and operations communities presents the best opportunity to specify requirements that will minimize system and AFNet integration risk. At some point in the acquisition process system change becomes unaffordable and certifiers end up accepting excessive risk or the certifier refuses to certify the system or connectivity denying the operational community mission capability

Architecture products, such as those generated by MAA, support governance, requirements and funding processes. Other architectures provide the basis for mission capability development, document functional requirements for external interfaces, and help specify technical requirements, including network capacity, performance, and security requirements, for networks over which communications will occur. However, the processes for reviewing, approving, and certifying architectures are not aligned across the acquisition timeline. The lack of synchronization results in missed opportunities for lower-level reviews to feed higher-level reviews and certifications. For example, system and technical design review results for AFNet connectivity should inform higher-level architecture reviews required for Interoperability and Supportability (I&S) Certification.

HQ AFSPC is identifying architecture "lanes in the road" to align processes supporting the definition, evaluation, certification, test, and approval to operate on the AFNet. One outcome will be guidance that defines "required" architecture processes, their inter-relationships, and a notional timeline to support program manager's planning. The guidance will impact information sharing between architectures and processes where architectures impact or contribute, such as DIACAP and the certifier decision process; architecture synchronization should support integration across capabilities and systems and the operational-level configuration management processes. Synchronization will provide AFNet architects and 24 AF warfighters the opportunity to evaluate AFNet technical and security compatibility identifying potential risks before a system is connected to the AFNet in a test or operationally live environment.

A source of information used to build system architectures, the NR KPP ensures that programs identify interoperability requirements, that the requirements are designed into the system, and that they are tested. The NR KPP is a mandatory requirement for all systems that exchange information and is implemented through DoD and joint policy to ensure I&S of information technology and national security systems.[5]

Recognizing the need to move the NR KPP into the cyber age, the Joint Staff J6, as the responsible organization for Chairman Joint Chiefs of Staff Instructions (CJCSI) 6212.01E, *Interoperability and Supportability of Information Technology and National Security Systems*, which provides NR KPP guidance,[6] is leading a revision effort with representation from across the joint

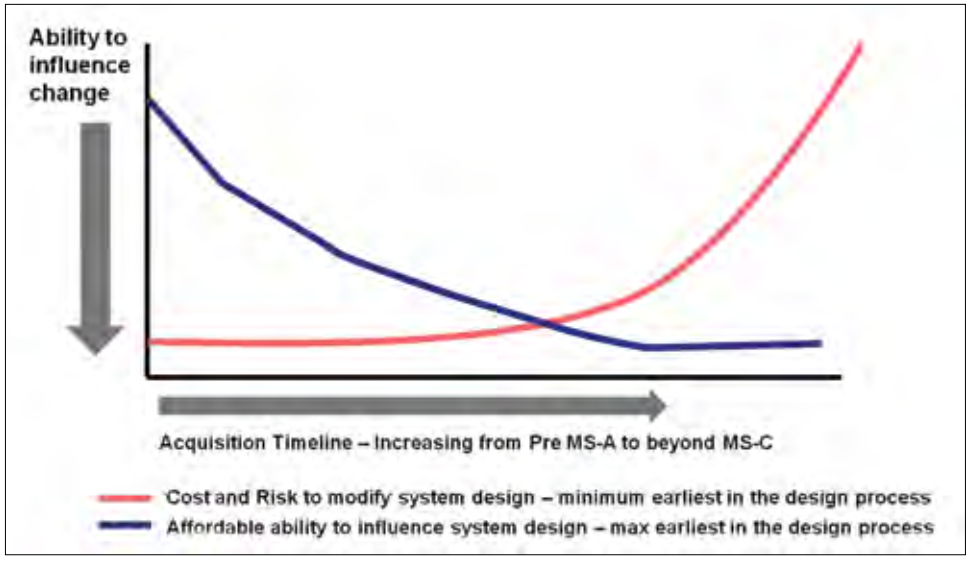

Figure 2. Affordable ability to influence system design.

communities, defense agencies, services, and the defense business system community. The modified NR KPP will be more narrowly-scoped focusing on information exchanges between provider and consumer, including the requirements of the network over which the exchanges will occur. A system's NR KPP will describe required system interfaces and associated measures of effectiveness (MOE) and measures of performance (MOP). These MOEs and MOPs will be the testable criteria used to evaluate KPP's implementation.

The NR KPP revision will increase the relevance of architectures by moving this element forward in the acquisition timeline. Architecture products would be available earlier in order to inform key processes such as formulation of the Capability Development Document, and could be an artifact within the request for proposal. An additional element of the policy revision addresses bandwidth requirements. Under current policy, systems need not identify satellite or terrestrial bandwidth requirements until Milestone C—far too late for service or DoD long-haul communications providers to effectively plan and program capacity impacts to the network. The revision will require bandwidth information beginning as early as the Initial Capability Document; for example, pre-Milestone A.

The updated NR KPP will center on identifying and delivering secure, interoperable, and supportable systems leading to a defensible Air Force network designed to achieve mission assurance. Rigorous evaluation of a program's NR KPP at multiple points across the acquisition timeline should ensure system residual risk is minimized. Validated KPP implementation should be a requisite to any AFNet connection approval. Holistically, the improved NR KPP will be combined with actions such as security service level agreements between the system producer and consumer, a focus on the system-of-systems engineering impacts, and early development and validation of architectures, interface definitions and performance requirements, infrastructure support criteria, and more. When combined with developing a protection KPP and key system attributes (KSA), discussed in the next section, these activities may significantly drive down residual connection and operations risk.

In 2009, then-AFSPC Commander, General C. Robert Kehler, mandated that all AFSPC programs include a threat-based protection KPP and KSAs. Initially only defined for space programs, the KPP ensures that system protection requirements are based on threat analyses, not a set of general threats. HQ AFSPC cyberspace offices are working with their space protection counterparts to adapt the space system process to cyberspace systems. It is anticipated that the cyberspace protection KPP and KSA will function similar to the space protection KPP and KSA; for example, the space process identifies system vulnerabilities by assessing susceptibilities against validated system threats. Countermeasures are then developed and prioritized, and the highest-ranked countermeasures with a materiel solution are converted to a KPP and KSA.

It is foreseeable that a number of AFSPC cyberspace system vulnerabilities identified through this process will be mitigated through implementation of information assurance (IA) controls. This process may also reveal threat-based vulnerabilities whose solutions are not addressed within current IA controls. For example, countering a system-specific advanced persistent threat may not be addressed in the current set of IA controls. In this case, the protection analysis may reveal a system-unique threat that requires a system-unique solution. There will be an ongoing challenge as to how effectively programs can address future, rapidly-evolving cyberspace threats based on today's technology for systems that may not be fielded for months or years.

The protection KPP and KSAs are a low-level design effort that will support fielding a defensible Air Force network designed to achieve mission assurance. To improve its effectiveness, they will be combined with an operational protection strategy. The operational protection strategy, discussed next, is a network enterprise protection framework which the operational community will use to specify capability needs.

The previous discussion presented protection-related initiatives focused on the requirements, acquisition, technical support, and security engineering communities who influence programs on a system-by-system basis. Lacking is an operational perspective on what the network defenders believe are critical enablers to network protection and mission assurance. Not only do the operators continually operate through network defense challenges, they also view AFNet protection from the enterprise and system-of-systems perspectives.

In an effort to address this missing protection element, AFSPC, 24 AF, and other organizations have begun an initiative to capture this critical perspective. The goal is a network enterprise protection framework which the operational community will use to specify capability needs. The means and standards to fulfill these needs will be considered from a system and enterprise view and will be evaluated against existing security and technical standards, such as DIACAP. A vehicle through which to mandate and enforce remaining operational protection needs will then be evaluated. Possible solutions may include modifying existing security standards, mandating measures through the NR KPP or protection KPP, or some other mechanism or process.

The process leading to modification of the NR KPP, developing a protection KPP and KSA and cyberspace protection program should consider operational benefits versus the programmatic impacts of modifying existing structures or creating new mechanisms. Led by HQ AFSPC/A5, the dialog will include all HQ AFSPC directorates, 24 AF, Electronics Systems Center, Air Force Research Laboratory, and others. The improvements should recognize that IA controls are assigned to systems based on the combination of user-defined mission assurance categories (MAC) and confidentiality levels (CL); a result is that the current system protection specification is tiered and that *the user* defines the minimum protection and availability levels that drive the system design process. Since MAC and CL are tiered, there will not be a one-size-fits-all solution. Specified protection criteria should not become too hard and costly to implement. The protection KPP and KSA and protection strategy will balance minimizing risk, meeting user requirements, enabling network operations, management, and sustainment, and ensuring mission assurance is achieved. These actions will then lead towards the goal of fielding a defensible Air Force network designed to achieve mission assurance.

MAA, protection KPP and KSA, and the protection strategy

focus on delivering a defensible network that lends itself to meeting mission assurance. The following discussion looks at mission assurance, actions that 24 AF is taking to improve meeting mission assurance, and connections between the MAA, protection KPP and KSA, and the protection strategy that support the 24 AF efforts.

Part Three: Mission Assurance

Department of Defense Directive (DoDD) 3020.40, *DoD Policy and Responsibilities for Critical Infrastructure*, defines mission assurance as:

> 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. It links numerous risk management program activities and security-related functions, such as force protection; antiterrorism; critical infrastructure protection; IA; continuity of operations; chemical, biological, radiological, nuclear, and high explosive defense; readiness; and installation preparedness to create the synergy required for the DoD to mobilize, deploy, support, and sustain military operations throughout the continuum of operations.

While important as a DoD promulgated mission assurance definition, it does not address early design needs that may impact achieving mission assurance. Casting a wider net, Partha Pal, et al, in their paper, "Managed Mission Assurance - Concept, Methodology, and Runtime Support,"[7] consider mission assurance as "…the guarantee that mission essential functionality (MEF) is continued despite partial failures or changes in the system and its operating environment." They go on to state "Because mission-critical information systems are expected to operate in contested environments (both physical and cyber), "mission assurance"—the guarantee that the MEF is continued despite the compromises and non-catastrophic outages that are inevitable in a contested environment—*must be treated as an engineering and operational goal*."

The MITRE Corporation, in "Operational Mission Assurance,"[8] offers that "Systems engineering for mission assurance is the art of engineering into systems: (1) the capabilities for operators to be aware of different and changing adversarial strategies as well as environmental and system conditions, (2) options and alternatives to accomplish a mission under different circumstances, (3) tools to assess and balance advantages and risks of available response options and alternatives, and (4) the ability to transition to a selected option while simultaneously continuing the mission. Systems engineering for mission assurance extends throughout the entire traditional acquisition lifecycle, from concept development through deployment and beyond, to include supply chain considerations and field operations."

The offered systems engineering centric mission assurance definitions, combined with the DoD definition, supports HQ AFSPC/A5 actions leading to improved acquisition and sustainment processes designed to deliver systems that minimize operational risk and support achieving mission assurance. They articulate a life-cycle view focused on delivering requirements and processes designed to identify and drive down residual risk across a system's lifetime and to field a defensible Air Force network designed to achieve mission assurance.

The 24 AF operates, defends, and sustains the AFNet. They employ the concept, "Strategy Based Architecture,"[9] to achieve mission assurance. The strategy based architecture employs acquisition delivered enablers,[10] such as virtualization, dynamic data protection, multi-level authentication, cross-domain solutions, shared data and storage, and network mobility as well as acquisition program procured operational capabilities such as command and control (C2), situational awareness, and network management to facilitate the strategies' six means—layered defense, secure enclaves, stealth, cyber maneuver, trust management, and simplicity.

The strategy's means are implemented and supported by the operational imperatives of fight through attacks, implement dynamic defense, resilience, and positive C2. Integrated as a single strategy and enhanced by systems designed to minimize residual risk and improve network defense—supported by employment of the functions covered in this article—the strategy enhances mission assurance.

To enable their strategy, 24 AF employs an enterprise and mission view. The "mission view" considers the end-to-end mission thread supporting components and actions that ensure all enterprise components that enable the mission—infrastructure, network services, data sources and sinks, and so forth—are operational, managed, and protected consistent with the criticality of the mission.[11] This approach focuses resources where they have the greatest effect in order to achieve mission assurance.

HQ AFSPC/A5's use of MAA products, adjusting the NR KPP, developing the protection KPP and KSA, and implementing the operational protection strategy are central to decreasing risk and delivering systems that enable network defense. However, there is a need to seek input from the warfighter. Warfighter input identifies specific capabilities required to better enable their ability to defend, operate, and manage the network. Subsequently, AFSPC/A5 uses warfighter feedback to help define the process and KPP adjustments.

Finally, 24 AF and HQ AFSPC are executing a strategy to improve the AFNet's defensibility and increase the probability of achieving mission assurance. Actions include reducing the AFNet's attack surface; simplify the network by "right-sizing" it to meet mission needs; identifying the critical enclaves and mission systems that require increased defense; and defining requirements and implementing solutions designed to improve defensibility. Requirements levied to modify the network and mission systems will take advantage of the MAA and protection changes. As appropriate, HQ AFSPC/A5 will employ rapid cyber acquisition processes, modification of existing acquisition programs, application of Air Force Research Laboratory developed solutions, and militarized commercial solutions to meet the mission requirements.

MAA, the protection KPP, and the protection strategy, combined with the ongoing 24 AF strategy to improve today's AFNet, focus on fielding a defensible Air Force network designed to achieve mission assurance. The efforts are synergistic with de-

livering an AFNet that is simple, agile, integrated, and interoperable with documented processes for connection, configuration management, reporting, and operational capability assessment.

Conclusion

The notions discussed in this article, MAA development and use, adjusting the NR KPP, implementing a protection KPP and KIP and an operational protection strategy are areas where it's felt that adjustment and change will decrease risk. System designs that take advantage of MAA products, the introduction of protection processes, and an understanding of the warfighter's operational strategy based architecture, will decrease system residual risk and lead to a more defensible Air Force network designed to achieve mission assurance.

Looking forward, HQ AFSPC/A5 has entered into a partnership with 24 AF/A3 and A5 focused on defining the requirements and processes and making the architectural and acquisition process changes necessary to implement the 24 AF strategy based architecture. The partnership will generate the requirements needed to "right-size" the AFNet improving the AFNet's defensibility and mission capability. It will specify capability needs that will take advantage of improved architectural processes and protection requirements to deliver safer, more defensible solutions improving the AFNet's ability to achieve mission assurance.

Notes:

[1] General C. Robert Kehler, "2009-2010 Air Force Space Command Strategic Plan," Air Force Space Command, November 2009.

[2] The capability viewpoint articulates the capability requirements, the delivery timing, and the deployed capability.

[3] The DoD Architectural Framework Version 2.0, DoD Deputy Chief Information Officer, is located at http://cio-nii.defense.gov/sites/dodaf20/.

[4] The project viewpoint describes the relationships between operational and capability requirements and the various projects being implemented. The project viewpoint also details dependencies among capability and operational requirements, system engineering processes, systems design, and services design within the Defense Acquisition System process.

[5] Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01G – *Joint Capabilities Integration and Development System*, 1 March 2009

[6] CJCSI 6212.01E, *Interoperability and Supportability of Information Technology and National Security Systems*, provides guidance for NR-KPP development and assessment and defines the five NR KPP elements.

[7] Partha P. Pal et al., "Managing Mission Assurance - Concept, Methodology and Runtime Support," IEEE International Conference on Privacy, Security, Risk, and Trust, 2010, 159-1164.

[8] The MITRE Corporation, Operational Mission Assurance, MITRE Systems Engineering Guide, Colorado Springs, Colorado, 2011.

[9] HQ 24th Air Force, 24th Air Force Concept for a Strategy-Based Network Architecture, San Antonio, Texas, 2010.

[10] The strategy based architecture takes advantage of operational enablers, such as network management, operational planning, command and control and situational awareness, and intelligence feeds. However, this article's focus is acquisition related issues.

[11] "Components" includes infrastructure, hosts, servers, communications systems, weapon systems, and their software, etc., needed to execute the mission.

Ms. Jill M. Baker (BS, University of Wisconsin-Superior; MBA, Chapman University) is a systems engineer for the MITRE Corporation, Colorado Springs, Colorado. Supporting Headquarters, Air Force Space Command (HQ AFSPC), Requirements Directorate, Cyberspace Requirements Division, her current areas of focus include requirements support to the AFSPC Cyberspace Operations and Defense Capability Team and analysis of cyberspace protection capabilities as delivered through formal acquisition programs. Previously, Ms. Baker supported AFSPC and Electronic System Center in the definition and acquisition of space command and control and situational awareness capabilities for joint warfighters, including commander, joint forces component commander-space. Prior to this, Ms. Baker led the effort to revise the information operations condition under the then-newly-formed computer network defense mission for US Space Command (USSPACECOM). As a US Air Force Reservist (retired), Ms. Baker supported Space Defense and Space Control planning and operations for USSPACECOM and HQ AFSPC.

Mr. Shane Morrison (BA, Mathematics and Cell Biology, University of Colorado, Boulder; MS, Computer Science, Santa Clara University) is a principal systems engineer with the MITRE Corporation since 1990. He currently leads MITRE's Cyberspace Requirements Team and Space Systems Engineering Group supporting Air Force Space Command (AFSPC). He supports cyber integration and leads the Cyberspace Mission Area Architecture and strategic analysis effort. His interests include cyber control, real-time analytics, complex adaptive systems, and resilient computing. He previously served as MITRE's chief engineer to the AFSPC/A6 and advised on studies on cloud computing and predictive analytics. Over the last decade, Mr. Morrison led several AFSPC technical studies and requirements development for future space control, networking, and computing capabilities. Mr. Morrison has advised AFSPC, Air Force Research Labs, and the Electronic Systems Center (ESC) on space command and control strategic technology planning. He was the ESC certified test director for strategic missile warning and Ground-base Electro-optical Deep Space Surveillance.

Mr. Jarret B. Rush (BS, Computer Science, University of Nebraska; MS, Systems Engineering, University of Virginia; MS Information Assurance, Norwich University) is a principle InfoSec engineer with the MITRE Corporation. Currently supporting the HQ AFSPC Requirements Directorate, Mr. Rush's efforts includes articulating requirements and capabilities for future cyber warfighting systems, accomplishing long-term cyber system architecture development, and supporting science and technology development. Mr. Rush has supported the Advanced Extremely High Frequency and Transformational Satellite space programs; worked on the Joint Tactical Radio System; information assurance and architecture development support to the airborne network; and a number of other high interest networking and communications systems. Other areas where Mr. Rush has worked include network engineering, Internet protocol, tactical data links, and others, for command and control systems such as the Air Operations Center, the Control and Reporting Center, and the Air Support Operations Center.

Single Integrated Network Environment: The Strategy for Air Force Network Integration

Lt Col Patrick B. Dunnells, USAF
Deputy Director, Plans and Programs
Air Force Network Integration Center
Scott AFB, Illinois

As the nation becomes increasingly dependent on information technology (IT) to conduct economic, social, and military functions, the Air Force Network (AFNet) has become a key component of national military power. To reach our full potential in the cyberspace domain, it is critical we ensure cyber defense without negatively impacting mission assurance (MA). The Department of Defense (DoD) defines MA as a process designed to ensure that tasks and duties can be performed as intended.[1] MA enables the DoD to carry out the national military strategy by ensuring availability of required capabilities and infrastructures to accomplish the mission. The AFNet today is complex and disparate, characterized by air, space, and terrestrial networks functioning within separate command and control (C2), battlespace awareness, and net-centric paradigms. This segmented approach to network procurement and implementation complicates our ability to defend the network. Further, it hinders the ability to share information, defend critical assets, and enable decision superiority which directly impacts MA. The Air Force Network Integration Center is leading the effort to build a Single Integrated Network Environment (SINE): an agile, integrated, defensible, and interoperable Air Force network environment operationally commanded and controlled as a single entity focused on joint force commander and warfighter needs.[2] For this concept to succeed, it requires a mature and robust information enterprise architecture that's dynamic, configurable, and responsive to commanders' needs.

Current Environment

Whether operating on land, air, or space, joint and US Air Force operations depend on a trusted and reliable exchange of information in and throughout the cyberspace domain. This dependency is increasingly at risk as cyberspace exploitation and attacks have grown more sophisticated and more serious in this persistent, global, and highly contested domain. Our cyberspace infrastructure is a national asset and defending it is a national security priority.[3]

Our nation's adversaries are constantly targeting IT through exploitation, disruption or destruction.[4] These adversaries are developing technical capabilities enabling them to challenge US military superiority. These threat actors are fielding sophisticated systems and developing asymmetrical strategies to attack, degrade, and deny the ability to operate in and through the cyberspace domain.[5] Their strategies are designed to circumvent our core strengths, exploit our weaknesses, and constrain our freedom of action.

Issues and Concerns

The Air Force's networks are a heterogeneous conglomeration pieced together without adequate consideration of the security implications of the resulting architecture. This resulted in a terrestrial network infrastructure that, in many cases, has grown without a clear understanding of all the network dependencies and vulnerabilities. Likewise, with space systems, the "DoD is now facing a situation where satellites with advances in capability will be residing in space for years without users being able to take full advantage of them because investments and planning for ground systems, user and space components were not well coordinated."[6]

The current terrestrial AFNet, in addition to the aerial and space network environments, can be characterized by shortfalls identified by the GIG 2.0 initial capability documents (ICD), Joint Aerial Layer Network (JALN) ICD, Joint Space Communications Layer ICD, and AFNet capability development document. These shortfalls include, but are not limited to the following:

- The network continues to focus on performance and service delivery at the expense of defensibility and MA.
- Many Air Force C2 systems are incapable of directly sharing information which creates stove-pipes, burdens operating forces, and hampers warfighter situational awareness.
- The mission system-centric approach to building networks and the obstacles created between multiple networks that handle information of different classifications, results in the inability to meet the information needs of the warfighter.
- Programs acquire their own network infrastructure, resulting in nonstandard solutions, unnecessary duplication of infrastructure, and waste of resources.
- Piecemeal approaches to technical connectivity and interoperability make it difficult to achieve rapid and dynamic information sharing.
- The AFNet lacks cohesion, agility, and versatility due to differing authorities, processes, policies, and standards that focus on mission system-centric solutions rather than on supporting joint warfighter requirements.
- A static and inconsistent posture with time-delayed response and defense that hinders network defense and ability to operate in a contested cyberspace environment.
- The existing Air Force networks do not support an adequate C2 structure, network defense, a common operating picture, or meet the warfighter capacity, connectivity, information sharing, and network security requirements.

Desired Effects

The desired effect of SINE is full-spectrum decision superiority, achieved through assured system and network availability, assured information protection, and assured information delivery. This includes providing the warfighter with robust network opera-

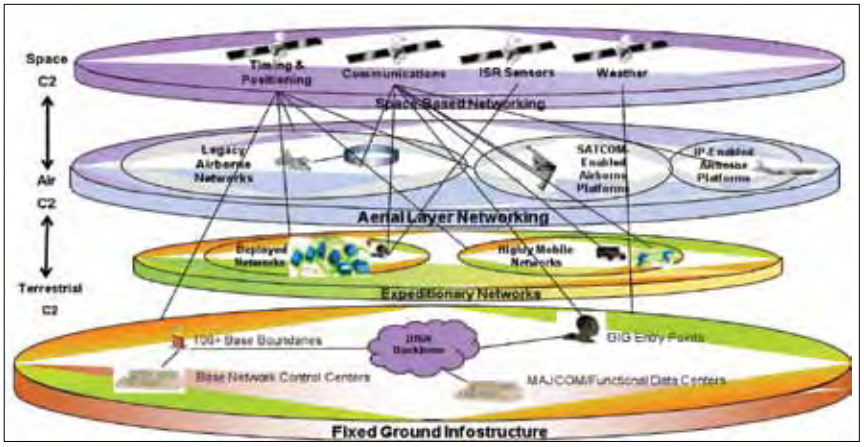

Figure 1. The Air Force's networks are a heterogeneous conglomeration of different networks pieced together, resulting in a number of shortfalls that make security and mission assurance difficult to achieve.

tions and network defense capabilities based on seamless and secure network connectivity and information systems access across terrestrial, airborne, and space networks. Common attributes inherent to a single integrated network include layered defense, secure data discovery and access, cyber maneuverability, standardization, global connectivity and availability, secure enclaves, speed of need operational capabilities, dynamic configuration, and dynamic architecture. The primary objective of SINE is integrating air, land, and space layers to improve warfighter effects throughout cyberspace.

A unified approach to network C2 and management with dynamic layered-defense capabilities is required to achieve the SINE objective. In addition, SINE will require migration of existing stovepipe networks into an integrated environment to optimally and dynamically meet prioritized mission requirements in support of Air Force and joint communities. Additional SINE effects include unified network C2, secure environment, efficiency, and MA. These effects are consistent with the goals of the DoD's Network Operations Strategic Vision:[7]

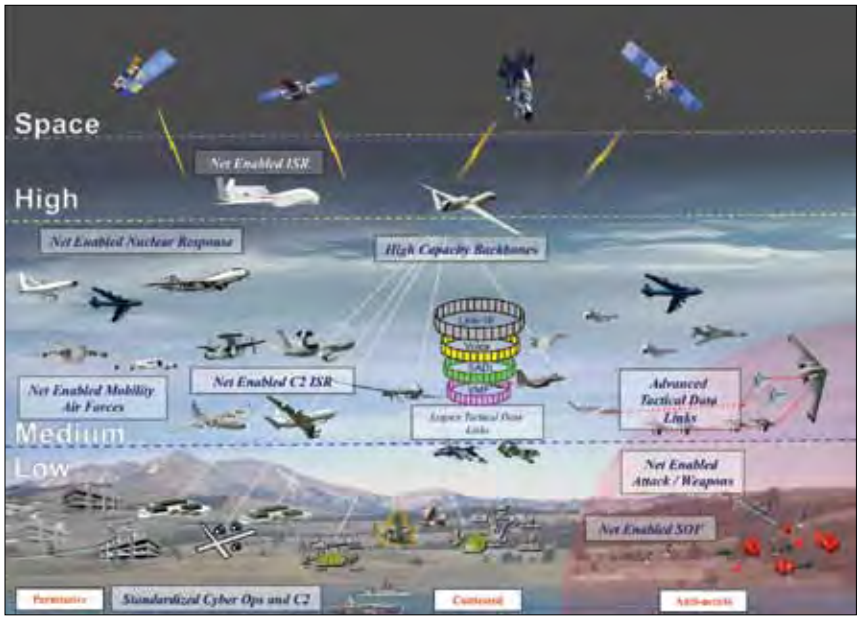

Figure 2. The future AFNet 2025 features a fully integrated, layered joint cyber battlespace across the full range of military operations.

Unified cyberspace C2 will greatly enhance our ability to react and operate through cyberspace events while providing a single interface to the operational and joint community. Currently, multiple communications organizations (i.e., Air Force Intelligence, Surveillance and Reconnaissance Agency; 624th Operations Center; Major Command (MAJCOM)/ Air Force Communications Coordination Center; squadrons, etc.) work in parallel to ensure required networks and IT services are available to support Air Force missions. During cyberspace events such as system failures or denial of service attacks, the lack of a unified cyberspace C2 structure creates a focus on individual system/network availability vice overall MA. The Air Force needs an ability to dynamically reprioritize cyberspace resources holistically to meet mission objectives. Achieving this goal will be made possible through shared situational awareness for cyberspace and mission operations centers, enforcing C2 authority for 24 AF to ensure the best of centralized control/decentralized execution practices, and by defusing legacy-focused thinking.

To ensure the most defendable battlespace possible, the AFNet architecture must enhance our ability to conduct missions in a highly contested environment. If a system is compromised, the mission should be able to continue and information should remain secure. The AFNet should also ensure the infrastructure is secure, functioning as expected, and will remain available. An integrated network environment must provide maximum protection for Air Force mission critical systems while safeguarding other systems. SINE will operate under the assumption that key segments of the network have already been penetrated, or that a threat is actively working to penetrate it. This requires a prioritization for employment of defensive capabilities and a prioritization of assets to be defended. In other words, there are some mission critical systems that the Air Force cannot allow an adversary to compromise. These could include space assets; key intelligence, surveillance, and reconnaissance assets; and C2 capabilities. On the other end of the spectrum, there are Air Force systems that need to interact with unsecure entities on the Internet. As such, SINE will take several approaches to ensuring a secure network environment. These approaches include:

- ***Secure Enclaves:*** Layered enclaves will offer varying levels of protection based on mission requirements. One enclave may contain the systems and data that are critical to Air Force missions. Systems, networks, and data within this enclave should receive the highest level of protection. The next enclave may contain the Air Force's core systems. This includes systems, data, and networks that support day-to-day business. The outer enclave may contain systems that regularly interconnect with untrusted systems on the Internet. These systems cannot be protected without an inordinate amount of effort, and these connections to the AFNet must be closely monitored and controlled.

- ***Trust Management:*** SINE will need to implement automated verification of actions against security policies. By authenticating access credentials, we can protect missions and secure operations within and across enclaves.
- ***Stealth Systems:*** SINE will ensure a level of security through obscurity. The concept is a cloaked network that secures data and hides servers and clients in plain sight.

The integration of separate mission and common user networks will provide a more effective and efficient means to support Air Force missions. Moving from a series of stovepiped mission-specific networks to a shared standardized capability will be a more efficient means to support the operational community but will improve information sharing support. SINE will move the Air Force to a consolidated environment which can more efficiently and effectively manage the IT assets, provide cyberspace protection, and interface with the Air Force and joint operational communities. These efficiencies will be gained through standardization (i.e., networks, processes, policies) and promoted through SINE socialization.

As noted earlier, MA enables the DoD to carry out the national military strategy by ensuring availability of required capabilities and infrastructures to accomplish the mission. The cornerstone of MA is establishing and defending physical and logical pathways. It addresses risks in a uniform, systematic, and standardized manner across the entire enterprise thereby making progress toward normalizing cyberspace. The Air Force's ability to set and maintain current mission priorities and the cyberspace community's ability to dynamically support those priorities are critical. SINE will ensure MA through the use of prioritization methodology, layered defense (i.e., enclaves) in accordance with Air Force and joint priorities, access policies, socialization towards a mission-oriented common/shared solution vice dedicated networks/system, and a dynamic and agile infrastructure that allows for rapid recovery from an incident to avoid mission failure.

Next Steps

The SINE effort has made significant strides toward achieving their desired effects. There are several activities currently under way including the AFNet migration, the JALN analysis of alternatives, and socializing the SINE strategy.

Migrating user accounts from their legacy MAJCOM domains to a single network environment is key to achieving the effect of having a network that is commanded and controlled as a single entity. To date, more than 136,000 user accounts have been migrated of the 845,000 planned. This consists of 29 bases spread across five MAJCOMs (Air Education and Training Command, Air Force Reserve Command, Air Mobility Command, Air Force Space Command, and Air National Guard). With an additional 113,000 user migrations planned in fiscal year 2011 and full migration planned by the end of 2013, this effort is making great progress.

With respect to JALN, while we currently have effective airborne communications via tactical data links, the ability to extend the Internet Protocol (IP)-enabled AFNet to our airborne platforms is still in relative infancy. Initial stages have mainly involved incorporating limited aerial network capability into selected wide body platforms. In the future, implementation of persistent aerial network backbone communications with intra-network gateways will improve communications to IP-enabled aircraft and munitions. The AFNet will be fully integrated with DoD networks and leverage capabilities delivered by JALN. Net-enabled aircraft will be free to enter and leave aerial networks seamlessly, or form ad-hoc networks as required. High capacity airborne backbone craft will bring connectivity where it's needed.

Concurrent with these initiatives, the SINE strategy is being socialized and vetted through Air Force senior leaders, and the SINE vision is being staffed through Air Force Space Command. Currently in draft, the SINE Integration Plan and Enabling Concepts are expected to be completed by mid-2011. Achieving the effects of SINE will require a considerable amount of socialization. Through briefings, point papers, articles, and discussions, we are continuously working to share the intent of SINE. These efforts are essential in setting the groundwork for an integrated network environment.

Conclusion

Given the global nature of cyberspace and the intricacies of missions cyberspace supports, SINE is critical to achieving a mature operational cyberspace capability. As the Air Force strategic direction in cyberspace matures, the focus will remain on ensuring a MA focused and defensible Air Force network environment operationally commanded and controlled as a single entity focused on Joint Force commander and warfighter needs. Ultimately, this plan's influence on cyberspace requirements and investment decisions will ensure the Air Force's cyberspace capabilities remain flexible, agile, and defendable against all adversary activities.

Thanks to Mr. Edgard I. Zamora, associate, Booz Allen Hamilton for his assistance in writing this article.

Notes:

[1] Maj Gen Richard Webber and Col Mark E. Ware, "Cyberspace Mission Assurance: A New Paradigm for Operations in Cyberspace," *High Frontier* 6, no. 4:3.

[2] The US Air Force Blueprint for Cyberspace, 2 November 2009, 5.

[3] National Security Strategy, May 2010, 27.

[4] AFSPC Functional Concept for Cyberspace Operations, 14 June 2010, 9.

[5] Ibid., 14.

[6] Senate, GAO-10-447T, *Space Acquisitions: Testimony Before the Subcommittee on Strategic Forces, Committee on Armed Services*, 14.

[7] DoD NetOps Strategic Vision, 11 December 2009, 7-11.

Lt Col Patrick B. Dunnells (BS, Mathematics, University of North Carolina Greensboro; MS, Systems Management, Golden Gate University, California) is the deputy director, plans and programs, Air Force Network Integration Center, Scott AFB, Illinois. He manages and orchestrates the integration of plans, programs, and policy to achieve cyber capabilities that maximize mission and operational effectiveness; manages training and professional development; manages the manpower, financial and personnel resources portfolio to achieve greatest mission efficiencies.

Defending the Cyber Alamo: An Indefensible Position in Cyberspace

Mr. Leander J. Brandt, IV
Tactics Development Director
23d Information Operations Squadron
Lackland AFB, Texas

In the most famous battle of the Texas Revolution, a heavily outnumbered group of volunteers fought to the death to defend the Texas Army garrison at the Alamo. The Texians fought gallantly, but their position was indefensible because the Mexican Army assaulted from all sides and the Alamo was never designed to withstand a siege against a large force armed with artillery. Like the Alamo, today's Air Force Network (AFNet) is under siege but was not designed to withstand the determined attacks of sophisticated adversaries.

Viewing a network as a fortress with a defended perimeter but unprotected interior is an inadequate security model, which is why the defense-in-depth model has been adopted. Although we have added security enhancements such as the Host Based Security System, the Air Force has not taken defense-in-depth as far as it needs to go. The standard desktop configuration (SDC) and standard server configuration (SSC) consist of commercial-grade software that was produced for the mass market and never intended by its designers to operate in a contested military environment. The AFNet presents a large attack surface to the adversary because our software was not designed for a cyber siege. Thus the AFNet remains indefensible; it is as if the Air Force has built a cyber Alamo.

The purpose of this article is to present a plan for rebuilding the AFNet using a hardened, customized operating system and suite of applications that were designed for military use. The key to this is gaining control over our software by only running programs built to military requirements and certified for military use through a source code auditing and testing process. Replacing commercial-grade software with weapons-grade software will give Air Force network defenders the maximum advantage against attackers by raising the bar of difficulty for successfully penetrating the AFNet. Airmen currently lack the tools they need to detect, react, and recover from cyber intrusions at acceptable rates, but using security software built to meet Air Force requirements will give cyber defenders critical capabilities to detect and remediate intrusions. Once the Air Force has control over its own software, then command-and-control over the AFNet itself becomes a tractable problem.

The Air Force has fielded the SDC/SSC in an attempt to standardize software across the network. However, standardization does not equate to control when the standardized software is all produced by commercial vendors who design it with the goal of maximizing profit and market share. The military defines requirements and performs tests for most other military equipment, and software should be no exception. For example, humvees proved vulnerable to improvised explosive device (IED) attacks, so the US Army and Marine Corps began fielding mine resistant ambush protected vehicles. When the military needed a new combat vehicle, it did not purchase a sport utility vehicle from a large auto manufacturer simply because many people drive sport utility vehicles (SUV). Instead, the military developed requirements and acquired a combat vehicle designed with the adversary threat in mind.

Similarly, when the Air Force needed a new cargo aircraft, we did not simply purchase a popular civilian cargo plane, nor did we blindly accept whatever plane the biggest aircraft manufacturer decided to sell at the time. It took an extensive acquisition process to identify the C-17 as the plane that best met Air Force requirements, and it is unlike aircraft built for commercial air cargo use. The Air Force has learned that cyberspace is not so different from the kinetic world. Cyberspace has been recognized as the fifth warfighting domain, and the new Air Force mission is to "fly, fight, and win ... in air, space, and cyberspace." The Air Force has been saying for years that the network is a weapon system, so just like military vehicles, planes, ships, and guns, the software used on the AFNet should be specially built for the military to operate in a combat environment.

In cyberspace, the threat is real and the adversary is an overwhelming force, so the Air Force should field desktop and server software designed with the cyber threat in mind. In cyberspace, Airmen are being asked to fight through cyber IED attacks while driving an SUV, when they should be driving a cyber MRAP. Instead of a C-17, Airmen are now flying a Spruce Goose in cyberspace. The F-22 has raised the bar for America's adversaries and has given the Air Force a critical advantage in aerial combat. We should do the same thing in cyberspace by fielding a hardened cyber warfighting platform that raises the bar for adversaries who attempt attacks on the AFNet. If parity is not acceptable in the air, then defeat should not be acceptable in cyberspace. In order to "fly, fight, and win" in cyberspace, the Air Force needs a a dedicated defensive cyber weapon system to replace the mass-market software of today's SDC/SSC.

Rebuilding the AFNet with hardened software is not a popular solution, but the Air Force should take a serious look at the reasoned arguments for this approach to cyber defense. First, we must assume that nothing is 100 percent when it comes to cyber security, so a hardened cyber platform should never be billed as a "secure system" because security is always relative in cyberspace. Safer software is not only possible, but it already exists and much of it is freely available from the open source community. Many cyber professionals argue that alter-

native software only has "security by obscurity" because the software has not yet had enough market share to motivate hackers to exploit its vulnerabilities. As the story goes, adversaries would soon exploit the new software just as they did the legacy software. That argument makes the faulty presumption that all software is equally vulnerable, that is, nothing could be more secure than our SDC/SSC. More importantly, that argument fails to consider that source code auditing and minimizing software functionality can dramatically improve software security. Besides, the past 15 years have operationally proven the insecurity of mass-market commercial software.

As proof that code audits are a practical way to improve software security, the OpenBSD team has produced a general-purpose operating system and suite of server applications that are renowned for their excellent security track record. The OpenBSD team did not start out writing a new operating system (OS) and server suite; they took existing software and began a process of code reviews, fixing bugs as they found them. As a result, the default installation of OpenBSD has had only two remotely exploitable vulnerabilities in over 10 years,[1] a claim that SDC/SSC software vendors cannot make. Thus the hardened cyber platform would not achieve security by obscurity, rather, it is improved security by code quality and minimalistic design. If the system contains fewer vulnerabilities and the ones that remain are more complex, it will be much more difficult (and therefore expensive) for attackers to find and exploit them.

Detractors of the hardened software concept assert that auditing source code would be too costly. However, the OpenBSD team audited their code with only six to 12 members who fixed thousands of bugs during the first year alone.[2] Auditing the code for a hardened platform may take a few more bodies, since a multitude of office automation programs, hardware drivers, browser plugins, and miscellany such as PDF readers must all be audited. Considering how many personnel are dedicated to cyber defense across the AFNet enterprise, it is not unrealistic to say that the Air Force could afford perhaps 30 programmers to audit the hardened cyber platform source code. Auditing source code would be an ongoing task, because subtle and complex bugs will continue to be discovered in code that has already been reviewed, and new programs and patches will provide steady work for the auditing team. The effort will be well worth it, considering the untold cost of exfiltrated data and the cost of being held at risk by persistent intruders who can cross the fine line to network attack at a time and place of their choosing.

Over the years, Microsoft Windows has become entrenched as our default operating system, not because of its superior quality or military utility, but because of Microsoft's successful licensing strategies in the commercial market. However, historical circumstances alone should not dictate the direction that Air Force cyber takes in the future. We no longer have to accept the default software; superior alternatives are available now. The hardened cyber warfighting platform will most likely have a Unix-like OS in order to leverage many Unix technological advantages like kernel-level mandatory and discretionary access controls. Just like the Air Force does when it evaluates new aircraft, we should conduct a "fly-off" and pick the system that best meets Air Force needs. There are several Linux and Berkeley Software Distribution (BSD) Unix distributions that are good candidates, and we would customize the chosen distribution for our own needs. Even Solaris should be considered because now it is open-source and it runs on commodity hardware. Unix is modular so the Air Force can choose what components it wants without being forced to accept anything we do not need. The large number of Linux and BSD distributions produced by companies and independent volunteer teams proves the relative simplicity of customizing Unix for a particular purpose, so nobody can say that a customized Unix system is beyond the capability of the US Air Force.

It should be emphasized that the Air Force would not be creating its own system from scratch; that is clearly not our function. This new software acquisition model would give the Air Force the flexibility to use open-source or proprietary software as long as it, (1) meets military requirements and (2) has had a code audit to find and fix bugs that can result in vulnerabilities. The Air Force should bring open-source code in-house, audit the code, and either fix the bugs or require a vendor to fix them. Very little code would be written by Air Force personnel; they would focus mainly on integrating software components into approved baselines and managing system configurations. The process of auditing source code and integrating the system should be done in-house so that the Air Force can control the quality of the personnel working on the project through background investigations. This would also avoid continuity and communication problems associated with external vendors. In the case of proprietary software, companies can keep their code closed-source—Air Force personnel will sign the nondisclosure agreements—we just need to be able to audit the code and the vendor needs to be responsive in fixing the bugs that the Air Force finds.

Lastly, the issue of user and administrator training must be addressed. Air Force cyber operators already receive Unix instruction during their training pipelines. Most users do not know how or are not allowed to administer Windows systems, so migrating to Unix will not make any difference to them. Since we will control what the software is and what it does, we can make it look very familiar to users accustomed to Windows. The old clunky UNIX workstations have given way to very user-friendly Unix graphical interfaces that provide many nice features that Windows still cannot offer. Many programs like Adobe Reader and Mozilla Firefox are already ported to Unix, and a lot of today's Air Force systems are web-based. Many other government off-the-shelf programs are based on Java or Oracle, both of which will run on Unix systems. Applications that cannot be ported to Unix can continue to run on Windows terminal servers, virtual machines, or full Windows installations. Simply reducing the number of legacy systems will bring the noise level on the network down to the point that sensors will be more effective with fewer false positives and missed alerts.

The days are gone when a commander who had been notified of a network infiltration would reply, "So what? It's just

unclassified data." Momentum is now growing in the Air Force to secure the AFNet by any means necessary because securing our network is not only a matter of national security, it's a matter of national honor. The AFNet is sovereign US territory, and we should be committed to defending it as such. The Air Force prides itself that no enemy aircraft has attacked US ground troops in over 50 years.[3] Unfortunately, the same thing cannot be said about cyberspace since the AFNet is presently being held at risk by persistent adversaries. While there are many approaches to cyber defense, nobody seems to be talking about implementing a weapons-grade OS and application suite as the next logical step toward defense-in-depth and operationalizing the AFNet. This article is intended to spark discussions and raise questions about our traditional network defense and software acquisition models in the Air Force cyber community. The Air Force is already leading the way in standardization since our SDC has become the federal desktop configuration, but the pressing need for a hardened cyber platform still extends across the services and indeed the entire federal government. Like it did with the global positioning system program, Air Force Space Command once again has the opportunity to take the lead and provide a solution that can be used to great advantage by a great many people in the military and the federal government.

Notes:

[1] OpenBSD 4.8, *OpenBSD.org*, http://www.openbsd.org.

[2] OpenBSD Security, *OpenBSD.org*, http://www.openbsd.org/security.html.

[3] The US Air Force Posture Statement 2004, Secretary of the Air Force, Chief of Staff, Washington DC, 21, http://www.posturestatement.af.mil/shared/media/document/AFD-070717-047.pdf.

Mr. Leander J. Brandt IV (BA, History, Southwest Texas State University, San Marcos, Texas; BS, Computer and Information Science, University of Maryland University College, Adelphi, Maryland) is the tactics development director, 23rd Information Operations Squadron, Lackland AFB, Texas. He is responsible for delivering relevant, validated tactics to Air Force cyberspace warfighters.

Mr. Brandt received his commission through the Air Force Reserve Officer Training Corps in 1999, and has previously served on active duty as a communications officer at the Pentagon and Goodfellow AFB, Texas. He continues to serve in the Air Force Reserves as a cyberspace operations officer assigned as an individual mobilization augmentee at the 92nd Information Operations Squadron. His previous Reserve assignment was at the Joint Information Operations Warfare Center, Lackland AFB, Texas.

Air Force Cyberspace Strategic Planning Factors

Mr. John D. Wright
Senior Cyberspace Strategic Planner
Strategic Plans Branch
Directorate of Plans, Programs, and Analysis
Headquarters Air Force Space Command
Peterson AFB, Colorado

Following combat operations in the Persian Gulf War, and the war in Iraq, the tools and tactics of how military strategists plan and engage in conflict have evolved—influenced by accelerating and exponential technological change. The pace of technology advancement is penetrating developing world arenas. While providing new opportunities to many, the connection of systems via networks also raises the risk of effects against the US national security mechanisms and critical infrastructures.[1] These features affect the capabilities and risk that are brought to the battle space and the nature of the environment in which conflicts occur—more than ever in the domain of cyberspace comprised of networks, telecommunications, and associated systems.[2]

The US is recognizing cyberspace as a center of gravity and elements of national power depend upon interconnectedness and technology infrastructures.[3] Cyberspace is a domain in which the US military faces growing risk. Information technology pervades core aspects of its operations,[4] from logistics and command and control (C2) to targeting and guidance. As this dependence has grown, revealed are vulnerabilities to potential effects like delays of battle networked information to US forces. The development of new micro-machines may offset some risks with defense mechanisms, as might nano-technology, super-automation, and artificial intelligence. These technology strengths could enhance support to the US military and advance data analyses and information assurance but may deliver new threats in the hands of adversaries.[5] Therefore, the US military must further engage in understanding technology use, inter-dependencies, vulnerabilities, and in strategic planning account for risk factors to defend, support, or apply force in, through or from cyberspace—relying on this domain in conflicts. The objectives of Air Force cyberspace superiority are: (1) control elements of cyberspace while protecting information from adversary action, (2) exploit control of information to employ cyberspace capabilities against adversaries, and (3) enhance Air Force and joint forces by cyberspace integration and mission assurance essential for strategic-to-tactical operations in other domains. Moreover, the Air Force must assess plans, programming, initial structures, manning, and visions to fulfill cyberspace capabilities while balancing risks for the future. Air Force strategic priorities in cyberspace must deliver operational advantages by: integrating cyberspace capabilities into normal operations accounting for risks; fielding information structure(s) that are protected; and denying adversaries information. The thrust of this article is to provide broad strategic factors that influence the determination of Air Force cyberspace planning, objectives, capabilities, and actions pertinent to risk and priorities. These strategic factors are provided in a *staff (or commander's) multi-part estimate format*, outlining several Air Force courses of action (COA), culminating with a risk management COA and tenets for *defense in cyberspace*.

It is always wise to look ahead, but difficult to look farther than you can see. ~Winston Churchill

Strategic Factor One – Visioning for Air Force Cyberspace

Towards 2030, envisioned is a future fundamental change in force structure and doctrine within the US military. A more technologically proficient military force emerges, readily networked by sophisticated command, control, communications, computers, intelligence, surveillance, and reconnaissance. Air Force cyberspace superiority evolves to advanced information superiority as primary warfare objective (like air superiority) and enhances precision application of force across a wide range of operations from military conflict to peace keeping.[6, 7] Strategic forces will continue to serve as one of the elements of the US security policy, but they are supplemented more as a national and theater deterrent force by cyberspace operational capabilities nominally dependent on global-to-local information structures. Air Force cyberspace forces support multi-lateral and coalition operations—protected by dynamic, risk-based processes (detailed later within this article). Cyberspace forces further support national indications, warning, and coordination centers, providing early notification and mitigation for adversary attempts to effect defense and national information, data, networks, systems, and processes.

Strategic forces will continue to serve as one of the elements of the US security policy, but they are supplemented more as a national and theater deterrent force by cyberspace operational capabilities nominally dependent on global-to-local information structures.

Our adversaries already recognize the US's dependence on cyberspace as a national center of gravity and are actively seeking ways to exploit our reliance on the domain to further their own interests.

Strategic Factor Two – The End State

From the visioning for Air Force cyberspace (strategic factor one) an end state is such that cyberspace *operations* will have matured into a formalized warfare discipline at the service and joint command levels, and support national policy; its concepts have caused changes in doctrine, strategy and organization, resulting in a more capable and agile information and data secure force. Air Force cyberspace *forces* are *integrated* to mutually support one another, other operations, and produce coherent effects whether in defensive, exploitive, or offensive modes. Common terminology and principles are accepted conventions; service and national war colleges educate military leadership in its principles while military (and civil) schools develop personnel with advanced cyberspace knowledge and skills. Air Force cyberspace *military* operations *strategies* are developed across a *virtual* network of *centers*, and are exercised by component and joint forces, continually evolving innovative concepts and tactics, techniques, and procedures. Cyberspace operations *forces* and tools provide the national and theater command authorities with a wide range of non-lethal or augmentation options from the tactical-to-strategic in operations, and significantly enhance the effectiveness of limited use of force. Air Force advanced information *superiority*, as well as the enabling integrated information structures, are *viewed strategically*.

Strategic Factor Three – Situation and Considerations

Characteristics of the area(s) of operation. Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[8] The US remains dependent on the use of cyberspace to maintain its way of life and to employ select instruments of national power. The rapid development and use of networks, telecommunication systems, and other technologies that use electronics have led to the recognition of cyberspace as a domain for warfighting. Our adversaries already recognize the US's dependence on cyberspace as a national center of gravity and are actively seeking ways to exploit our reliance on the domain to further their own interests. The previously-mentioned definition of cyberspace leads to two divergent uses of cyberspace as a military domain: (1) as a war fighting domain that provides sovereign options and (2) as an enabling domain for superiority in the other domains of land, sea, air, and space. The warfighting and enabling aspects of the cyberspace domain set the stage for strategic planning factors in today's Air Force mission tasks—to fly and fight in air, space, and cyberspace.

Adversary forces. Pervasive and sustained computer-based (cyberspace) attacks against the US and others continue to pose a potentially critical impact to systems, operations and the infrastructures they support. Knowing the identity and motivations of the actors is a key dimension in characterizing the cyberspace threat. Of the many cyberspace actors, those of concern to the Air Force, based on the potential impact on US military operations, are: (1) nation-states and state sponsored hackers, (2) foreign and insider espionage threats, (3) potentially well-financed terrorist groups, and (4) criminal elements. Cyberspace attacks, like conventional military operations, are conducted against objectives or select targets. These attacks may be conducted against the network or through the network. Targeting against the network includes disrupting C2 or other communications to deny US military capabilities. Targeting through the network includes striking traditional military targets, as well as manipulating data on a network. In short, today can be characterized largely as peacetime in the cyber domain, with some continuous level of activity occurring, including both probing and ex-filtration. It is clear, however, that there is a potential for cyberspace warfare to rapidly enter a pre-hostilities phase, and for the evolving capabilities of nation-states, and eventually terrorist organizations, to escalate the level and precision of attacks as an adjunct to other military activities. Thus, the prewartime and military use of cyber warfare is a growing threat that a global US military must be able to defend against. This was illustrated by the reported Russian cyberspace attacks on Estonia and Georgia, in that lack of cyberspace defense can significantly affect elements of national power.[9]

Friendly priorities, guidance, and missions. Friendly strategic factor elements entailing priorities, guidance, and missions are outlined below to ensure linkage from the national to the Air Force cyberspace planning. The *National Strategy to Secure Cyberspace* is the comprehensive strategy for the US to secure cyberspace, and spells out three *strategic priorities*:[10]

- Prevent cyberspace attacks against America's critical infrastructure.
- Reduce national vulnerability to cyberspace attacks.
- Minimize damage and recovery time from cyberspace attacks.

Next the National *Military Strategy for Cyberspace Operations* (NMS-CO)[11] is the comprehensive strategy for the US Armed Forces to ensure US superiority in cyberspace. The four *strategic priorities* of the NMS-CO are:

- Gain and maintain initiative to operate within adversary decision cycles.
- Integrate cyberspace capabilities across the range of military operations.
- Build capacity for cyberspace operations.
- Manage risk for operations in cyberspace.

Strategically aligning with the national security priorities as a service—*three* Air Force Cyberspace Superiority Core Function Master Plan missions have emerged as below:

- ***Cyberspace defense.*** Cyberspace defense is the passive, active and dynamic employment of capabilities to respond to imminent or on-going actions against Air Force or Air Force-protected networks, Air Force's portion of the Global Information Grid or expeditionary communications assigned to the Air Force.[12]
- ***Cyberspace force application.*** Cyber force application is combat operations in, through, and from cyberspace to achieve military objectives and influence the course and outcome of conflict by taking decisive actions against cyber-vulnerable, military-approved targets.
- ***Cyberspace support.*** Cyberspace support is foundational, continuous or responsive operations in order to ensure information integrity and availability in, through or from Air Force controlled infrastructure and its interconnected analog and digital portion of the battle space.

Air Force Capabilities. In planning for the above three cyberspace missions sets, the Air Force must pursue capabilities for superiority in an environment of complexity, risk, change, vulnerability, and low barriers to entry to create military employment advantages in the face of such trends. The Air Force must provide for operations where the employment of cyberspace capabilities is to achieve objectives in, from, or through cyberspace. Such Air Force operations can include network or computer activities to operate and defend Air Force mission information, networks, and communications supporting other military missions. High-level Air Force cyberspace capabilities shall involve:

- Gaining and maintaining an asymmetric advantage over adversaries to defend, exploit, and conduct force application.
- Gaining and maintaining cyberspace superiority, while executing a range of military operations at the time and domain of our choosing.
- Maintaining situational awareness in cyberspace to globally plan and command forces for assurance of missions.
- Assuring freedom of action for Air Force missions in, through and from cyberspace, including the freedom from attack and the ability to fight through attacks.

Assumptions. The Air Force will have to cope with uncertainty in the future regarding the threats, requirements, rapidly evolving capabilities, and changes in military structures:[13]

- The Air Force reliance on networks and cyberspace operations will drive software intensive programs and systems, while engaging a highly skilled force.
- Cyberspace assets and forces operate continuously (24 hours a day, 365 days a year) providing global and theater effect options throughout the spectrum of conflict with commensurate situational awareness.
- Combatant commanders will identify new mission needs in cyberspace for their areas of responsibility.
- C2 for cyberspace missions will require leading-edge planning and assessment technology to stay ahead of adversaries.
- Air Force acquisition processes will be refined to provide timely and responsive fielding of cyberspace capabilities for Air Force component and joint force needs.
- Essential intelligence, surveillance, and reconnaissance (ISR) and intelligence requirements are established for the defined battle space. Lack of timely, accurate and predictive ISR for cyberspace will affect Air Force's ability to understand and shape domains to achieve and/or maintain cyberspace superiority.
- Military operations will continue to depend upon select cyberspace civil, allied, and commercial systems and infrastructure, warranting levels of protection.

Strategic Factor Four – Courses of Action

The following elements comprise a *foundation necessary* for Air Force courses of action at the strategic levels to offset Air Force mission risks. Elements below are not listed in priority to reflect the need to further engage in these COAs in parallel:

- Provide an operating *environment to support cyberspace* operations, and protect associated systems and networks that transport, store, retrieve, and process friendly information.
- Develop robust *network security* operations to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction from adversaries.
- Provide *passive defense measures* to deter, deny and degrade adversary network *exploitation* while also serving to preserve, protect, recover, and reconstitute friendly cyberspace capabilities.
- Employ *active countermeasures* to rapidly respond to threats by *affecting adversary* forces or reducing their effectiveness in, through, or from cyberspace.
- Enable operations *centers* to plan, direct, coordinate, and control cyberspace forces—*integrated* with other operations.

[T]he Air Force must pursue capabilities for superiority in an environment of complexity, risk, change, vulnerability, and low barriers to entry to create military employment advantages in the face of such trends.

- Develop strategic and operational planning *analytical tools* to further provide timely and accurate information, enhanced decisions, and assessment.
- Develop an Active Duty, Guard, Reserve, and civilian force that is sourced and shaped to match defined skills, competencies, and grades based on requirements to provide a healthy future force.
- Conduct continuous cyberspace training, exercises, and mission rehearsals to improve mission readiness and operational effectiveness.
- Provide cyberspace mission requirements into a refined and responsive acquisition process.
- Ensure that select cyberspace systems and related equipment support continued and enhanced inter-operability with other services, agencies and coalition partners as appropriate.
- Explore advanced technologies, conduct flexible research and development, and test responsive to the needs of cyberspace missions.
- Infuse cyberspace specific perspectives, ideas and risk thinking into military processes, concepts, and doctrine.

Air Force cyberspace risk management mitigation for defense.[14] A culminating strategic factor COA: Our Air Force must re-energize and focus on risk management actions in operations and acquisition for defense of specific cyberspace information, data, and processes to remediate and mitigate threats and vulnerabilities. This cyberspace defensive risk-based strategy establishes a baseline of critical data and information (see figure 1) on the top left side of figure 1 and identifies the associated essential and dependent networks and systems. Next, on the right side of the diagram, the threat is assessed and concomitant risk determined based on the vulnerability assessment of essential networks and systems. Then the aggregation of the risk management process and a cost/benefit analysis yields a cyberspace defense program strategy in the center of the diagram. Subsequent modification to processes, procedures, and system solutions or associated changes based on technology, design, testing, exercises, and operational employment enables the strategy implementation. The process is dynamic and continues to integrate and refine the strategy and solutions.

Figure 1. Air Force cyberspace defensive risk management strategy.

This Air Force cyberspace defensive strategy (in figure 1) is a process to manage risk of loss or assurance of information, data, and associated processes. It is impossible to pay the operational and the financial price of total risk avoidance. Risk management provides appropriate protection based on capabilities planning and operational priorities as well as effectiveness and efficiencies. This risk management process and resulting mitigation strategy must address the interests, capabilities and information, data, and processes critically supporting the Air Force, elements of Department of Defense and government, and non-government elements in these complex activities. This strategy will yield a consistent approach and economies of scale in the protection and defense of the highly inter/intra-connected cyberspace and operational forces. These rapidly evolving and highly complex processes and systems require proactive measures to ensure integration, capabilities, and efficiencies.

Risk Tenents for Air Force Cyberspace Defense

The following tenets will anchor this Air Force defensive cyberspace risk-based strategy and guide subsequent implementation:

1. Air Force cyberspace information, data, information-dependent systems, components, and advanced cyberspace systems shall be identified and evaluated through risk mitigation processes.

2. Air Force cyberspace forces shall prepare to operate successfully in degraded information and communications environments.

3. C2 of Air Force cyberspace forces shall be planned and exercised to operate with the minimum amount of critical information and data required for direction and application of force, while taking full advantage of the availability of other information and data to enhance C2 functionality.

4. Air Force cyberspace defensive assessments and mitigation actions (vulnerabilities to trade-offs) shall be integrated into all information and cyberspace system acquisition program(s) processes.

5. Continuous integration and interoperability among Air Force cyberspace command, control, communications, computers, and associated intelligence, surveillance, and reconnaissance activities shall be incorporated in the requirements, research and development, acquisition and operational processes.

6. The acquisition process shall engage in innovative ways of fielding defensive technologies, cost-effectively and expeditiously consistent with a refined development time

line while addressing inherent risks to retain Air Force readiness and operational capabilities.

7. War gaming and exercises shall be used to create realistic cyberspace environments for Air Force training, exercise planning, and acquisition purposes. War games and exercises should simulate cyberspace wartime stresses to ensure commanders understand and are prepared to operate/exploit information, data, system, and process capabilities with some vulnerability.

8. Air Force cyberspace core competencies shall be sustained and enhanced, while integrating policy, personnel, technologies, systems architectures, programs, plans, and budget aspects.

The inclusion of these tenets and aforementioned COAs in Air Force cyberspace policy and directives shall provide strategic foundational conditions towards not only cyberspace superiority, but a future end state of advanced information superiority—superiority for users and systems to securely exchange critical information in seconds, and operate together more securely and advantageously in the face of man-made or natural effects. In summary, attainment of advanced information superiority warrants accounting for the strategic factors outlined in this article to reduce operational and acquisition risk—critical to cyberspace defense for Air Force missions.

Notes:

[1] DoD Strategy for Defense Critical Infrastructure, March 2008. Articulates the approach required for ensuring the availability of assets deemed essential to the successful completion of DoD missions in an all-threat and all-hazard environment. DoD Directive 3020.40, *Defense Critical Infrastructure Program (DCIP) Management*, in August 2005 called for the identification and prioritization of all defense critical infrastructures.

[2] Chairman of the Joint Chiefs of Staff (CJCS) memo (CM) 0363-08, July 2008. Cyberspace is defined as: A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

[3] The Comprehensive National Cybersecurity Initiative (CNCI) was adopted as national policy as part of National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23). The CNCI addresses current cyber security threats, anticipates future threats and technologies, and develops a framework for creating in partnership with the private sector, 2007.

[4] DoD Directive, 8000.01, *Management of the DoD Information Enterprise*, February 2009. Information. Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

[5] Information assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities, DoD Directive 8500.01E, April 2007.

[6] Air Force Doctrine Document (AFDD) 3-12, *Cyberspace Superiority*, 15 July 2010, 2. Cyber superiority. The operational advantage in, through, and from cyberspace over adversaries to defend, exploit and conduct offensive operations at a given time and place, without effective interference.

[7] Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 17 October 2008. Information Superiority. The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

[8] Cyberspace definition, Chairman of the Joint Chiefs of Staff (CJCS) Memorandum, Definition of Cyberspace Operations, 18 August 2009.

[9] Susan Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State* (USA: Oxford University Press, 2009); and Franklin D. Kramer, Stuart Starr, and Larry Wentz, eds., *Cyberpower and National Security* (Potomac Books Inc, 2009).

[10] "The National Strategy to Secure Cyberspace," White House, February 2003, http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf. Covers the necessity for vigilance in cyberspace, many defensive aspects of cyberspace operations, and the general principles that should guide national response to a cyberspace—crisis.

[11] Department of Defense, Chairman of the Joint Chiefs of Staff, National Military Strategy for Cyberspace Operations, December 2006, http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf. The NMS-CO describes the cyberspace domain, articulates cyberspace threats and vulnerabilities, and provides a strategic framework for action. The NMS-CO is the US Armed Forces' comprehensive strategic approach for using cyberspace operations to assure US military strategic superiority in the domain. The integration of offensive and defensive cyberspace operations, coupled with the skill and knowledge of our people, is fundamental to this approach.

[12] DoD Directive 8000.01, *Management of the DoD Information Enterprise*, February 2009. GIG. The globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to war fighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. Non-GIG IT includes stand-alone, self-contained, or embedded IT that is not connected to the enterprise network.

[13] Adapted from DRAFT CAF Strategic Plan Annex C Cyberspace Superiority Way, March 2009.

[14] Adapted from Vision and Strategy For Defending Information, Lt Col John D. Wright, 19 June 00, *Air & Space Power Journal*, digital archives, http://www.airpower.maxwell.af.mil/airchronicles/cc.html.

Mr. John D. Wright (MS, National Security Strategies; MA, Human Resource Development) is a Senior cyberspace strategic planner in the Strategic Plans Branch, Directorate of Plans, Programs, and Analysis, Headquarters AFB Command, Peterson (AFSPC) AFB, Colorado. In this capacity he is responsible for cyberspace planning for AFSPC and supports Headquarters Air Force and joint cyberspace planning efforts. Mr. Wright previously served as a senior Air Force officer for 27 years, with assignments in multiple specialties, as an intelligence, space (operations/control), and information operations officer, in the field in Kosovo during Operation Joint Guardian, Enduring and Iraq Freedom and other operational positions in the Air Intelligence Agency, Air Force Information Warfare Center, Air Combat Command, US Air Forces Europe, Electronic Security Command, National Security Agency, and US Space Command. He has commanded at the group, squadron, center, and detachment levels. As a joint specialty officer, he has held transformational joint positions on a combatant command, and on the Office of the Secretary of Defense staff. Mr. Wright is a graduate of Squadron Officer School, Air Command and Staff College, and Industrial College of the Armed Forces.

The Air Force Network Architecture

Mr. Steven L. Stoner
Chief
AFNet Architecture Development Branch
Air Force Network Integration Center
Scott AFB, Illinois

The Air Force Network, (AFNet) is the official name for the Air Force provisioned portion of the Department of Defense's (DoD) Global Information Grid. The desired effect of the AFNet is full-spectrum decision superiority for the warfighter, achieved through assured system and network availability, assured information protection, and assured information delivery. This includes providing the warfighter with robust network warfare capabilities based on seamless and secure network connectivity and information systems network access across the terrestrial, airborne, and space domains.

The AFNet Architecture describes common information technology and net-centric capabilities. Evolving Air Force policy will mandate the use of AFNet capabilities by all US Air Force mission and support systems in lieu of program-unique solutions whenever possible. Many system-unique information technology (IT) and net-centric capabilities that power today's mission and support systems will transform into the AFNet IT and net-centric capabilities described in this architecture.

The architecture is being developed following the service oriented architecture (SOA) methodology. A SOA is a method for constructing and organizing systems which greatly facilitates information sharing between systems. Rather than hard-coding connections between applications, a services-oriented architecture exploits more flexible mechanisms such as eXtensible Markup Language and web services to exchange data. The advantage for the US Air Force of this "loosely coupled" approach is that an individual system can be modified without having a negative impact on the systems with which it is integrated.

The AFNet Architecture is structured in five domains to align to the Defense Information Enterprise Architecture:

- Communications
- Computing infrastructure
- Data and services
- Secured availability
- Network operations

Required capabilities are mapped to Joint Capability Areas, the DoD Net-Centric Operational Environment, and combatant commander's required capabilities.

The AFNet Architecture provides standard "taxonomies" for Air Force capabilities, operational activities, and systems functions and "grouping" of semantically related concepts into the following clusters:[1]

- *Performers*. Things that perform activities such as service performers, systems, personnel, and organizations.
- *Resource Flows*. The interaction between performers that is both temporal and results in the flow or exchange of objects such as information, data, materiel, and even other performers.
- *Information and Data*. Representations (descriptions) of things of interest and necessary for the conduct of activities.
- *Activities*. Activities are work that transforms (changes) inputs into outputs or changes their state.
- *Capability*. Views the need to perform a set of activities under certain conditions and standards to achieve desired effects and the way in which those needs are satisfied.
- *Services*. Business and software services, what they do for what effects, by what measures and rules, how they are described for discovery and use, and how and where they can be accomplished.
- *Rules*. How rules, standards, agreements, and constraints are related and are relevant to architectures.
- *Measures*. All form of measures (metrics) applicable to architectures including needs satisfaction, performance, interoperability, organizational, and resources.

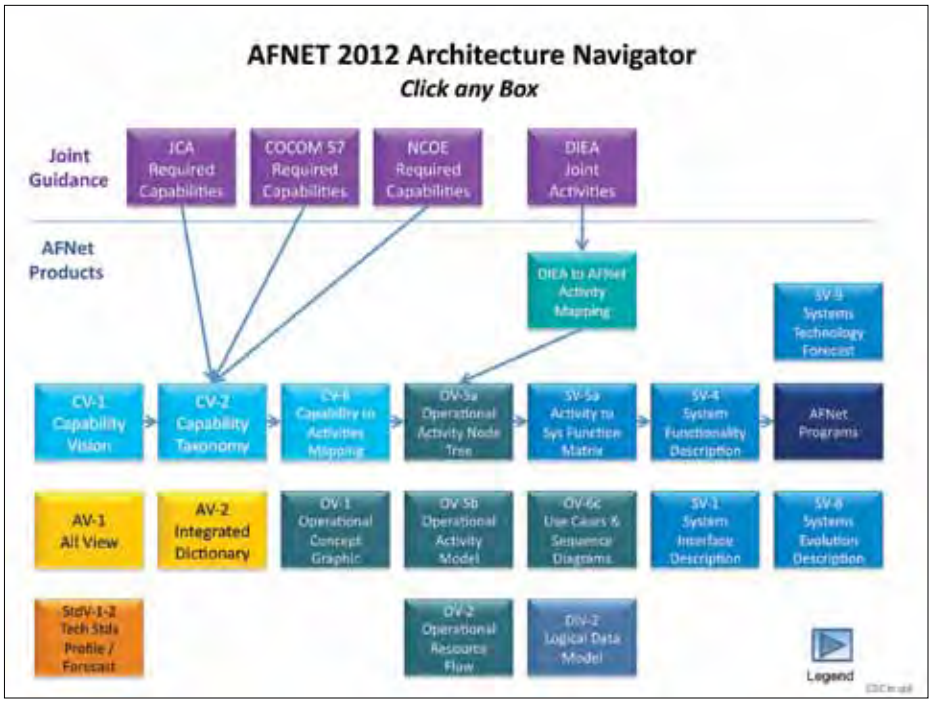

Figure 1. AFNet 2012 Architecture navigator tool.

- *Locations*. All forms of locations including points, lines, areas, volumes, regions, installations, facilities, and addresses including electronic addresses (e.g., uniform resource locator's) and physical (e.g., postal).

The AFNet 2012 Architecture consists of thirty DoD Architecture Framework (DoDAF) Version 2.0 compliant documents. These documents are designed to support the senior-level decision-making process on a broad basis. As such, they are not designed or intended to target a single or limited set of decisions. These architecture products are at a level consistent with the level of detail required for senior decision makers to establish strategy, validate requirements, allocate resources, and provide program oversight. They provide sufficient detail required to define relationships with other sub-enterprise architectures, describe high-level capabilities and system functionality, support analysis of alternatives and guide solution definition.

The AFNet Architecture includes a "navigator" tool (figure 1) that provides key linkages to required Air Force and joint capabilities and activities, enabling AFNet-supported programs which map to the AFNet Architecture to inherit traceability to appropriate governing guidance and documentation.

Summary

The size and scope of the AFNet environment requires cyber warriors to mature planning and design, create current solutions and execute operations using fielded systems in a simultaneous, orderly fashion. Waiting for the perfect design, or moving forward without a design would be mistakes. Use of architecture is the best method to achieve managed change.

Notes:

[1] The entire set of AFNet 2012 architecture products is available from any .mil address in the AFNet Architecture's folder on the Air Force Knowledge Now web site at: https://afkm.wpafb.af.mil/AFNet. This folder contains the Microsoft Word document which provides the aforementioned "navigator" capability to help readers select and access documents of interest.

Mr. Steven L. Stoner (BS, Electrical Engineering, Indiana Institute of Technology) is chief, AFNet Architecture Development Branch at the Air Force Network Integration Center, Scott AFB, Illinois. He has served in a number of engineering and management positions in the Department of Defense and private industry and holds patents for a high explosive mine testing apparatus and a two-way radio communications system.

Preparing the Air Force for Computer Network Operations

SSgt Andrew T. Jones, USAF
Instructor
39th Information Operations Squadron
Hurlburt Field, Florida

Cyberspace

The name alone conjures up all manner of things. Through practical experience though, the most common is the 35-year-old guy surrounded by monitors and keyboards in his mom's basement. In today's rapidly-changing world, quite often the one with the most cyber know-how is among the youngest. To that end, one can easily see that the Air Force is realizing that, but even the most tech-savvy kid in one discipline is not going to be fully-competent across all domains. And that's where the 39th Information Operations Squadron (39 IOS), located at Hurlburt Field, Florida, comes into play. What began at the 39 IOS as Undergraduate Network Warfare Training (UNWT) has laid the foundation for what is now Undergraduate Cyber Training (UCT). UCT is the technical school for brand-new officer and enlisted cyber defense operators at Keesler AFB, Mississippi.

An Evolving Mission

As the move was made, the 39 IOS switched the focus from teaching basic network warfare training to developing the next level of training, Intermediate Network Warfare Training (INWT). INWT takes the concepts from UNWT/UCT and builds upon them. Like its predecessor, INWT is pay-grade neutral: the class is open to enlisted, officers, and civilians who have proved they have a need, such as filling a combat mission ready position, and the proper clearance. With that shift in focus, the 39 IOS also saw a shift in intensity as classes are being held more often and with more students. Along with the network warfare, the squadron will still be teaching the other courses they have traditionally offered as well: the Information Operations Integration Course, Signature Management Course, an instructor methodology course, and various mission qualification training courses.

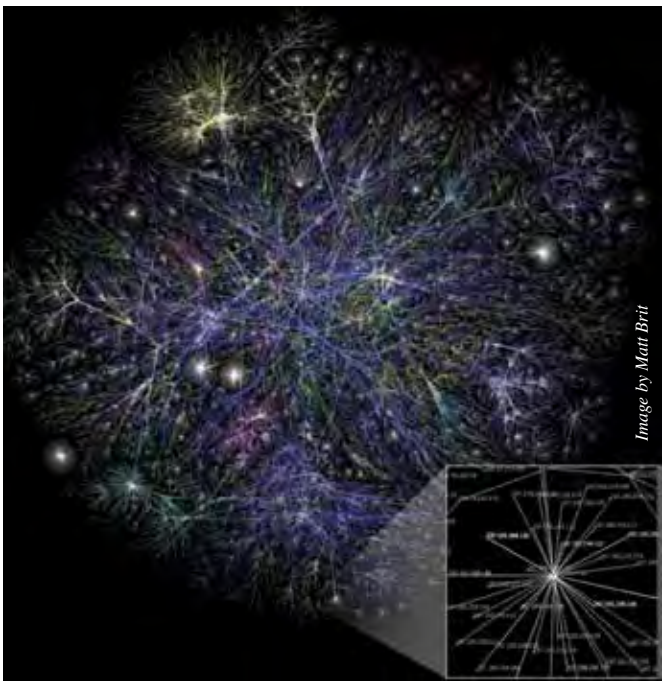

Figure 1. Partial map of the Internet based on the 15 January 2005 data found on www.opte.org. Each line is drawn between two nodes, representing two IP addresses.

The People

The 39 IOS's instructor cadre members are among the best and brightest in the Air Force and the support staff that makes sure the classrooms work is second to none. It truly is a result of all of those people working together that they have been able to develop and start teaching INWT in such a short time span. These people spent many long hours working to make this course possible and fulfill the service's need for cyberspace and information operations training.

The Expertise

As the members of instructor cadre can attest, raw talent is important, but in the operational environment, that will only go so far. The cyber domain is constantly changing, and when teaching operators to fly, fight, and win in cyberspace, continuous training is key. The cadre maintains their expertise by keeping abreast of current events, following the development of new capabilities and maintaining contacts on the outside. Most of the cadre maintains qualification currency for Air Force mission systems. Some of them attend conferences such as Black Hat and DEF CON or participate in major Air Force and joint exercises to stay on the tip of the sword, or continue to teach in these challenging environments. The subject matter of 39 IOS courses is unique in that what is taught one week could be rendered obsolete and utterly-inconsequential the following week. Curriculum review and update cycles are measured in days and weeks—new techniques are not saved for future classes.

The Domain

Cyberspace is unique. Unlike air, land, water, and space, cyberspace is man-made and in cyberspace, even the very fabric of the domain can be manipulated. Cyberspace is everywhere, and nowhere: you cannot just point in a direction and say, "that's cyberspace." Cyberspace, by its very nature, also poses some very unique challenges.

The Challenges

In cyberspace, there are no geographical or easily definable political boundaries. Borders and distances mean nothing when information travels at the

In cyberspace, there are no geographical or easily definable political boundaries. Borders and distances mean nothing when information travels at the speed of light.

speed of light. No longer does mounting an attack mean flying planes, sailing ships, and landing troops. Now all one needs is an internet connection and the right combination of ones and zeros. Programs to conduct these activities are easily available from a number of different websites. Whole packages of these programs, meant for use by security testing professionals, are made free under public use licenses. At the 39 IOS, the team follows the development of the latest tools of the trade and where possible, incorporates their use and familiarization into the courses. For those tools not able to be used in the training environment, the courses teach the capabilities applicable to the Air Force missions.

The Event

One word: Stuxnet ... a game changer. Disclaimer first: this is not the time or forum for a "whodunit" debate. What cannot be ignored is the wide breadth of reporting in the news media that Stuxnet showed the world that targeted cyber weaponry, "precision guided munitions" if you will, is possible. Not only is it possible, it exists. Even scarier though is that by all accounts, even though Stuxnet's existence was made public in summer 2010, it was reportedly "fired" sometime in 2009.[1] This means that for about a year, this worm quietly spread globally and eventually to an industrial control system in Iran. While other computers around the world were infected, they were not the target and therefore were not harmed by the infection. To top all that off, even after being discovered, it continued on its mission by being very difficult to remove from the system. Imagine if something like that, with a different end target, infiltrated our power control systems, water, sewer, pipelines, and air traffic control systems. The effects could be catastrophic from military, political, economic, or even societal standpoints. At the 39 IOS, this concern, and the understanding of how these processes work, drives the faculty and inspires the students to think about these things in a different light, a "how can we prevent this" light.

The Revolution

As seen in recent news, uprisings in the Middle East, starting with Egypt then spreading to other countries, have all had several things in common. Civil unrest may be the most glaringly common factor, but more notable from a cyberspace perspective is that many of the embattled governments tried to curb demonstrators from organizing by cutting off internet access. In Egypt's case, companies around the world responded by providing alternative ways for Egyptians to make their voices heard. Methods included dial-up connections, satellite phones, and proxy servers. One company even set up a phone number where voice mails left would be converted into Twitter messages. This onslaught of alternative means to access meant that the Egyptian people were still able to plan and organize and in light of that, the Egyptian government reversed their decision and turned the Internet back on.[2]

The Way Forward

The mission as described in layman's terms is very simple: secure cyberspace. The execution is more complex. In this ever-changing, ever-evolving domain, the 39 IOS takes their mission very seriously and will continue to change and evolve themselves to meet the new needs and remain on the cutting-edge for the students, the Air Force, and the nation.

Those wishing to become a part of the 39 IOS, as instructors, support staff, or students, can call the 39 IOS at DSN 579-3939 (Commercial [850] 884-3939) to describe their intentions and they will be directed to the appropriate personnel.

Notes:

[1] Gregg Keizer, "Is Stuxnet the 'best' malware ever?," 16 September 2010, http://www.infoworld.com/print/137598, "At the time, researchers believed Stuxnet—whose roots were later traced as far back as June 2009..."; CN, Computing Now, blog excerpt, "Symantec: Stuxnet Infections Started in 2009," IEEE Computer Society, 15 February 2011, http://www.computer.org/portal/web/news/home/-/blogs/3784583; jsessionid=ad94fde9c397967912af7259f430, "Stuxnet was launched in June 2009."

[2] Shereen El Gazzar, et al., Fox Business, "Egypt Communications Cut As Protests Continue," 28 January 2011, http://www.foxbusiness.com/markets/2011/01/28/egypt-communications-cut-protests-continue/; John D. Sutter, "Internet access returns in Egypt," *CNN Tech*, 2 February 2011, http://www.cnn.com/2011/TECH/web/02/02/egypt.internet/index.html?iref=allsearch#; Alexei Oreskovic, "Google launches Twitter workaround for Egypt," *MSNBC online*, 1 February 2011, http://www.msnbc.msn.com/id/41360089/.

SSgt Andrew T. Jones (AAS, Computer Science Technology, Community College of the Air Force) is an instructor at the 39th Information Operations Squadron (IOS), Hurlburt Field, Florida. The squadron provides qualification training to over 450 students annually, teaching courses spanning from tactical cyber mission skills through major command-level information operations planners. In this capacity, Sergeant Jones teaches and develops courses in, among other things, network warfare operations (NW Ops) concepts and operational functions, law and ethics in NW Ops, network fundamentals and NW Ops employment; this includes mission coordination and employment of network data extraction, manipulation, nodal vulnerability assessment, and engineering.

Sergeant Jones entered the Air Force in 2005 as a communications – computer systems programmer. He served four and a half years at the 554th Electronic Systems Group at Maxwell AFB – Gunter Annex in Montgomery, Alabama, before accepting a cyber instructor position at the 39th IOS. Sergeant Jones is a graduate of Undergraduate Network Warfare Training and converted to the Cyberspace Defense Operator Air Force Specialty Code upon receipt of his 7-level.

Rethinking Cyber Defense

Mr. David W. Aucsmith
Senior Director
Institute for Advanced Technology in Governments
Microsoft Corporation
Redmond, Washington

Computer systems have been under attack almost from the beginning of computers themselves.[1, 2] Over the years we have developed many tools and processes for keeping them secure. Arguably, we have not been very successful. We have now reached the stage that the cyber environment has become a unique war fighting domain. A war fighting domain in this sense is defined by the unique tactics, techniques, and procedures needed to defend or attack computer systems in military enterprises. We have not been able to create computer systems that are immune to the attack weapons (malicious computer code, malicious network communications, or social engineering) of our adversaries. Years of failure suggest that we must rethink how we protect computer systems.

Microsoft products and customers have been a part of cyber-attacks since the first personal computer was connected to the Internet. Over this time, we have developed insights into how and why cyber-attacks succeed or fail.

Why Systems are Not Secure

When I first started working at Microsoft, my Department of Defense (DoD) colleagues would frequently ask a question that was roughly framed as, "Why don't you guys just write better software to begin with then we would not have these problems." Obviously the problem is more complicated than that question suggests. The reasons that it is more complicated are important to understanding how computer systems might be made more secure in the future. The answer depends on two factors.

First, we have adversaries. Anytime that one has adversaries—who are adapting their weapons, tactics, and deployment to the development of your technology—one has a classic arms race. I would respond to my DoD colleagues with, "I will create a computer system that will remain secure as soon as you build an airplane that cannot be shot down." This is the dynamic of adversarial relationships. However, adversarial relationships in cyberspace are further exacerbated due to the highly asymmetric nature of cyber engagements; the significant mobility afforded the attacker, and the difficulty of attribution.

The second factor in building secure computer systems is that we are building incredibly complicated systems. We are building computer systems that are far more complex than our ability to completely model or understand their functionality, in a formal sense. Indeed, as computer systems become more multi-threaded, multi-processor enabled, and data driven, they will become more non-deterministic and less able to be modeled or completely understood.

The reality is that we are building incredibly complex computer systems, which we have no formal way to analyze, and we are placing them in front of experienced, resourceful, and determined adversaries. This set of circumstances guarantee that vulnerabilities will be found in the computer system, weapons and tactics will be developed to exploit those vulnerabilities, and that the computer system will be successfully compromised at some point in the future.

Why Security Testing is Only Part of the Answer

The traditional approach to achieving secure computer systems has been to develop computer security evaluation and testing criteria. Over the years, there have been numerous attempts to create certifications for computer security. These include the DoD trusted computer system evaluation criteria, better known as the Orange Book, published in 1985.[3] More recently, there has been the Common Criteria (International Standard Organization/International Electrotechnical Commission Standard 15408).[4] These certification methodologies, and others like them, specify a set of security features and assurances and then rely on compliance testing and analysis.

These types of methodologies identify where the computer system as built does not meet the criteria as specified. The problem with this approach is that very frequently vulnerabilities occur because the computer system as built has additional functionality not specified by the criteria. A buffer overrun is an additional entry point not in the specification. The failure of the certification-based approach is that it is impossible to create a systematic way to find all such vulnerabilities. This can easily be verified by asking, "How do you know when you have found them all?"

This is not to say that security certifications are useless. They are essential for confidence in identifying those features which do not meet standards. They are necessary but not sufficient. Where they do not work well, where a computer system has additional functionality not specified, we need a different methodology, one that allows one to approximate a search for additional functionality. One way to do this is to at least ask the question, "Of all the bad things I know about, are there any

[A]s computer systems become more multi-threaded, multi-processor enabled, and data driven, they will become more non-deterministic and less able to be modeled or completely understood.

present in the system?" We call this *threat modeling*.[5]

Threat modeling, in this context, is a methodology where we characterize the code constructs that lead to vulnerabilities and successful attacks. We search for and remove those constructs. What makes threat modeling particularly valuable is that it is not static. As new code constructs that lead to vulnerabilities are identified, we can add them to the threat model database for use in analyzing future systems or even for reanalyzing past systems. As useful as threat modeling is, even in conjunction with classic certification methodologies, it cannot alert you to vulnerabilities that have never before been seen or imagined.

Cyberspace as Maneuver Warfare

Since we must place highly complex computer systems in the presence of adversaries—computer systems that cannot be definitively tested—we need to approach computer security in a new way. We must acknowledge that we cannot build computer systems that are secure and will remain so in perpetuity. Rather, we must build computer systems that are adaptable, configurable, and give us the ability to anticipate and respond to our adversary's behavior. It is the difference between the Maginot Line and maneuver warfare. We need to create the equivalent of maneuver warfare in cyberspace.

To make systems adaptable, we need to be able to change their behavior to input or change their attack surface.[6] One of the ways we do this is by patching the software of the computer system. Patching and defensive updates, such as anti-virus signature updates, are how we achieve maneuver warfare in cyberspace. We should not view patching as a failure, but rather, as successfully maneuvering the software baseline against an attack by an adversary. We need to strive to make patching frequent, quick, and transparent.

As it is likely that an adversary will, at some time, identify and exploit a previously unknown vulnerability, we must approach the problem differently. We must make the use of an unknown cyber weapon prohibitively expensive, in a broad sense, for our adversary to use. While we have no choice but to allow our adversary the use of a new weapon, we should immediately sense the attack and then rapidly adapt every other computer system in the enterprise to be immune to the weapon's future use. Our adversary can use the weapon only once after which it is useless (assuming computer systems are patched, updated, and configured correctly).

This change in philosophy implies a level of sensors, communications, and what is now called *active defense* that is rarely found today. However, it is obtainable with current technology.

Sensors and Intelligence

I use the term sensor here in its broadest context. It is some mechanism, software, or process, which provides information about the state of the system in which it is deployed. This information is then used to generate indications and warnings—that is, to generate intelligence. Ultimately, intelligence is derived from a rich and diverse population of sensors and is aggregated and correlated for maximum usefulness.

When organizations develop a cyber-situational awareness capability, typically they instrument their information technology environment as a sensor. Usually this includes the deployment of intrusion detection systems, anti-virus systems, network traffic analysis systems, and the like. What we have found over time is that these sensors are our worst sensors for situational awareness. They give no indication of what our adversary is planning, sometimes they can show that we are under attack, and they are excellent for forensics after an attack has occurred. To put this into a military metaphor, this is akin to not knowing you are under attack until your adversary is in the foxhole with you. This is a little too late. In no other war fighting domain would we accept this level of situational awareness.

The question then is how to develop and deploy sensors that can give us indications and warnings of our adversary's intentions and actions. That is, provide intelligence. While this may seem like an impossible task, there are practical sensors that have some of these characteristics. Honeypots are one such sensor.[7] If placed in desirable locations, they may provide information about attack tools and weapons. If they are designed to be immune to known attacks then the only successful attacks will be ones that are hitherto unknown. They can capture new tools and techniques and send that information to analyst or analysis machines where patches, signatures, settings, and/or heuristics can be developed. The goal would be to rapidly disseminate the patches, signatures, settings, and heuristics to all other enterprise components to make them immune from the same attack. Thus, the only successful attack using a new weapon would be the attack on the honeypot.

Traditional intelligence methods, when targeted against the cyber domain, may also be good sensors. For example, collecting open source intelligence about cyber-attack tool development could identify potentially unknown weapons. Again, the point is to identify a new weapon by any means available and then rapidly immunize the enterprise against it. Other potential sensors include heuristics-based anti-virus software, network scanners, configuration monitors and such—as long as they are tied to an automated processing capability that can use that intelligence to develop suitable counter measures.

In order for a sensor to be used for automated defense at scale, it must have a very good signal to noise ratio. False positives must be rare. Most network-based sensors do not have this property. Network-based sensors have difficulty knowing which specific traffic is from legitimate processes and which is from malicious processes. End point (or host-based) sensors, such as anti-virus software, honeypots, and the like are able to disambiguate traffic to their hosts because malware must "reveal" itself to take control of the system.

Hygiene

To be effective, sensors must have a high signal-to-noise ratio. There are two ways to do this. We can develop sensors that have a very high selectivity or we can reduce the background noise. One of the ways to reduce the noise is to improve the security posture of the enterprise as a whole. Out of date or unpatched computer systems succumb to attacks from weapons which have long since been identified and for which immuniza-

tion is available. That is, if they had been patched or brought up to the current version of that software, they would not have been compromised. If computer systems easily succumb to known attacks, it is superfluous to protect them from unknown attacks. This implies a minimum level of hygiene that must be present in the enterprise as a precondition for effective defense.

There are other issues besides being unpatched or out-of-date systems that contribute to security vulnerabilities, such as, poor system administration or incorrect system settings. Indeed, dynamic modification of system setting may be an effective way to counter an attack, For example, dynamically disabling auto-execute of universal serial bus (USB) storage devices would have immunized computer systems from the attacks utilizing USB storage as an attack vector. This level of hygiene is technically easy to do but rarely attained in practice in most enterprises. It requires tools and processes for distributing patches and configuration changes quickly and it requires a willingness to upgrade systems to new versions of software and hardware.

Implications

The traditional view of computer security has not lead to secure systems. We must rethink how we approach cyber defense. Computer systems cannot be made permanently secure in an adversarial environment. If we accept that premise, then we are forced to make computer systems adaptable and resilient. To do so, we must have knowledge on which to base our adaptations and we must have a process for handling that knowledge at a speed that out paces our adversary's ability to exploit the vulnerability. This requirement leads to the conclusion that we need sensors that can detect the first use of a cyber-weapon and the tools, processes and mechanisms to communicate the resultant knowledge to the entire enterprise.

Also inherent in this argument is that we must ensure that the enterprise can only be attacked by unknown weapons else there is little incentive for the adversary to deploy new or more sophisticated weapons. Why should an adversary use new weapons against an enterprise when old ones work sufficiently well?

Achieving cyber defense then requires three things:

- Enterprise wide hygiene—up to date, correctly configured, and patched systems.
- Sensors that can detect the first use of a new weapon—preferably outside of the enterprise.
- Processes for using the knowledge of a new weapon to immunize the enterprise—at speeds greater than the reaction time of the adversary.

There are working examples of each of these requirements deployed in enterprises today. No new or revolutionary technology is required to achieve this. It simply requires the will to do so.

Notes:

[1] Computer systems in this context mean any computational device including desktop computers, servers, routers, and firewalls.

[2] Brian Kerbs, "A Short History of Computer Viruses and Attacks," *The Washington Post*, 14 February 2003.

[3] Department of Defense (DoD) 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, Assistant Security of Defense, Command, Control, Communications, and Intelligence, 26 December 1985.

[4] Joint Technical Committee, ISO/IEC 15408-1:1999, JTC1, "Information Technology – Informational technology – Security techniques – Evaluation criteria for IT security," International Organization for Standardization, 1999.

[5] Frank Swiderski and Window Snyder, *Threat Modeling*, (Redmond, Wash: Microsoft Press, 2004).

[6] Michael Howard and David LeBlanc, *Writing Secure Code* (Redmond, Washington: Microsoft Press, 2003).

[7] Honeynet Project, *Know Your Enemy: Learning About Security Threats* (Boston: Addison-Wesley, 2004).

Mr. David W. Aucsmith (BS, Bio-Chemistry, University of Georgia; MS, Physics, Naval Postgraduate School; MS, Information and Computer Sciences, Georgia Institute of Technology) is the senior director of Microsoft's Institute for Advanced Technology in Governments. He is responsible for technical relationships with US and other government agencies, as well as on select special projects. He is also currently a special government employee, SES grade, with the Department of Defense (DoD).

Before joining Microsoft in August 2002, Mr. Aucsmith was the chief security architect for Intel Corporation from 1994 to 2002. He has worked in a variety of security technology areas including secure computer systems, secure communications systems, random number generation, cryptography, steganography, and network intrusion detection. Mr. Aucsmith is a former officer in the US Navy and has been heavily involved in computer security and cybercrime issues for more than 20 years. He is, or has been an industry representative to numerous international, government, and academic organizations including the technical advisory boards of both the National Security Agency and the National Reconnaissance Office. He is on the National Academy advisory board on survivability and lethality analysis and the Directorate Advisory Council for the National Security Directorate of Pacific Northwest National Labs. He is co-chairman of the FBI's Information Technology Study Group, a member of the Secret Service Task Force on computer aided counterfeiting, a member of the President's Task Force on national defense and computer technology and a member of the DoD's Global Information Grid Senior Industry Review Group. Mr. Aucsmith was also US industry representative to the G8 Committee on organized, transnational, and technological crime where he participated directly in the G8 summits in Paris, Berlin, and Tokyo.

Aucsmith holds 33 patents for digital security technology and is an editor for the *IEE Journal of Information Security*, and a member of the advisory board for the College of Computing at the Georgia Institute of Technology. Additionally, he has a Certificate in Fine Arts Photography from the University of Washington.

Book Review

Surviving Cyber War

Surviving Cyber War. By Richard Stiennon. Lanham, Maryland: Government Institutes, 2010. Bibliography. Notes. Index. Pp. x, 170. $65.00 Hardcover ISBN: 978-1-60590-674-1; $39.95 Paperback ISBN: 978-1-60590-688-1; $39.95 Electronic ISBN: 978-1-60590-675-1

The number of books, not to mention journal articles and web pages, devoted to cyber terrorism, cyber warfare, or cyber defense has grown steadily during the past few years. Indeed, the proverbial trickle has become a literary flood of biblical proportions, which threatens to inundate even the most skillful cyber-savvy readers. Anyone attempting to become intimately familiar with all that is being written would, in all probability, suffer the same mental and physical consequences as someone who foolishly tries to outrun the Bay of Fundy's rising tide. Even a less venturesome soul—one simply dabbling at the water's edge to become better informed about cyber threats—might end up gasping for breath.

For those anxious to plunge into the most recently published books about cyber warfare, Richard Stiennon's *Surviving Cyber War* offers a suitable springboard. Using historical examples and drawing from personal experience, this founder of the independent analyst firm IT-Harvest and author of the "ThreatChaos.com" security blog has constructed a valuable primer on the evolution of cyber conflict and a basic guide for governments, commercial enterprises, and others interested in defending themselves. Far less intimidating than Edward Amoroso's more technical *Cyber Attacks: Protecting National Infrastructures* or Jeffrey Carr's moderately sophisticated *Cyber Warfare*, Stiennon's book offers both a substantive challenge to neophytes and a refreshing tutorial for experts. It complements, in both content and style, Richard Clarke's and Robert Knake's *Cyber War: The Next Threat to National Security and What to Do About It*.

To introduce his topic, Stiennon recounts Shawn Carpenter's story—the tale of a cyber warrior who discovered in 2004 that Chinese hackers had infiltrated Sandia National Laboratories and, consequently, stepped into the middle of an FBI investigation dubbed Titan Rain. The author backtracks to explore the beginning of Chinese cyber threats to the US. He explains the techniques and tools of cyber espionage, and he enumerates some of the countermeasures. For anyone contemplating how to design a response to a cyber threat, he spells out a simple trio of security maxims: (1) good network security assumes endpoints are hostile; (2) good endpoint security assumes the network is hostile; and (3) secure data assumes the user is hostile. From there, Stiennon proceeds to a historical analysis of e-mail assaults and distributed denial of service (DDOS) attacks, which he describes as among the most common forms of cyber warfare. As a defense against DDOS attacks, he touts as the phased techniques—communication, network response, and hardening server infrastructure—Estonia employed after Russia's "crowd sourcing" attacks in 2007.

Stiennon suggests that just as the weapons and tactics introduced during the Battle of the Somme nearly a century ago signaled a new era in human conflict, so do the present day's rapidly evolving attacks on and across cyber networks. Indeed, the latter are "poised to become the defining innovation of twenty-first-century warfare" (77). Reflecting further on World War I history, he describes T. E. Lawrence's guerilla warfare concept—"a hardened interior defended by its natives at the fine level of a square mile"—as a "close parallel" to an "appropriate model for information security" (113). While some might be tempted to focus on cyber offensive investments, Stiennon argues that creation of a carefully crafted "distributed defense" should be the primary goal for mitigating cyber risk.

For so slim a volume, *Surviving Cyber War* contains a weighty amount of substantive material. Pondering the lessons learned from Russia's cyber attacks on Georgia in 2008, for example, Stiennon acknowledges the difficulty of finding and training a corps of cyber warriors. He proposes immediate creation of cyber "research functions, even establishing separate labs on the order of Sandia, Livermore, and Oak Ridge" (102). Furthermore, he stresses the need for new treaties and international arrangements to curtail the use of cyber weapons. Stiennon debunks most recent think-tank studies on cyber war or cyber defense, including those by Cato Institute, Hoover Institute, Heritage Foundation, and National Research Council, because they do not exhibit a technical understanding of the issues; he suggests think tanks "broaden their research capability by incorporating security technologists from industry" (153).

Based on the assumption that gaining total information dominance is the objective, Stiennon contends that success in cyber war depends on the strength of four pillars: intelligence, technology, logistics, and command. In his elaboration on the "paramount importance" of mastering each pillar, he especially emphasizes eleven areas of development in offensive technology. Beyond mastering the four pillars, Stiennon asserts that any nation expecting to survive future wars must reorganize its current military and "the way in which it is guided by General HQ and ultimately the state leaders" (130). For the US and most other nations, the question of how best to organize remains unanswered and open to debate.

By the time this review appears in print, anyone rushing out to purchase *Surviving Cyber War* might want to look for a copy of Stiennon's second book. Scheduled for release in June 2011, its title is *Cyber Defense: Countering Targeted Attacks*. Stiennon has characterized it as "more like a textbook," which will categorize all types of cyber attacks and identify the tools needed to defend against each type of attack.

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) 554-3731
Fax: (719) 554-6013

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