2-2008

A Systematic Approach for Securing our Space Assets

Heather Yates
USAF

Michael R. Grimaila
Air Force Institute of Technology

Recommended Citation

Yates, H., & Grimaila, M. R. (2008). A Systematic Approach to Securing our Space Asset. High Frontier, the Journal for Space and Missile Professionals, 4(2), 48–53.

A Systematic Approach to Securing our Space Assets

Maj Heather Yates
Program Manager
Spacecraft Systems Integration
Headquarters National Reconnaissance Office
Chantilly, Virginia

Dr. Michael R. Grimaila
Associate Professor
Graduate School of Engineering and Management
Information Resource Management
Center for Cyberspace Research
Air Force Institute of Technology
Wright-Patterson AFB, Ohio

We are surrounded by the use of space assets, but for the most part are unaware of their impact on our lives. On a daily basis, space assets contribute to our well-being and others around the world. Space activities have enhanced security, monitored the environment, improved and increased information growth and flow, created economic growth, and changed the way people around the world live and work.[1] Since the 1991 Gulf War, we have also come to understand how much the US military depends on space. Military forces use satellite information for communications, intelligence, surveillance, reconnaissance, warning, weather, navigation, and timing. Space has become the ultimate high ground upon which we depend on militarily and as a nation. Because of this dependence, we must ensure our space assets are adequately protected. It is clear that a systematic approach to analyzing the security of our space assets is needed.

In this article, we draw upon the insights gained from the information security domain when developing strategies to secure organizational information assets; consider the application of Pipkin's five-phase information security process in the space operations domain;[2] and focus our discussion on the first phase of Pipkin's process, which is responsible for the identification, valuation, and assignment of safeguards to protect resources.

A Systematic Approach: Pipkin's Five Phases

In his book "Information Security: Protecting the Global Enterprise," Pipkin recognizes that information security is a critical success factor when securing an organization:

> Organizations can no longer regard security as an option, only needed for government contracts. Today's business environment makes security a requirement without which the company will most certainly suffer damaging losses.[3]

While Donald L. Pipkin's book focuses on the protection of business information systems, we believe that the lessons are equally applicable to Department of Defense (DoD) space systems. Military systems operate on the same information architectures as business systems, just with higher stakes if information becomes corrupted, lost, stolen, mismanaged, or unavailable. Just like in business, information is often the key determinate in the success or failure of military operations. Today, commanders rely upon information to make high quality decisions by accessing a greater number of information resources, obtaining more frequent updates from their information resources, and by correlation between, and across, multiple information resources to reduce uncertainty in the battlespace. As a result, we must recognize critical information assets and take steps to insure that they are protected at a level commensurate with their value.

Pipkin describes a cyclic, five-phase process to conceptualize the information security process: *Inspection, Protection, Detection, Reaction,* and *Reflection*. The *Inspection* phase requires the identification, valuation, and assignment of ownership of information assets critical to the organization; the *Protection* phase requires the assignment of the control measures to protect critical information assets commensurate with their value; the *Detection* phase requires the development of robust detection capabilities to insure that any breach of the organization is detected in a timely manner; the *Reaction* phase requires that the organization has developed the resources and capabilities to quickly respond, contain, investigate, and remediate breaches; and the *Reflection* phase requires effective post-incident documentation, reporting, and accountability to assure institutional learning. Neglecting any one of the five phases can expose the organization to excessive losses when they inevitably experience an information incident.

In the remainder of this article, we focus only on the first of Pipkin's five phases: the *Inspection* phase. Based upon our experience, we believe that this phase is the most important and most frequently overlooked. The *Inspection* phase is concerned with the evaluation of the capabilities of the organization; understanding and documenting its security needs; and assessing the current security capabilities to protect its assets. Specifically, we discuss the definition and identification of resources, threat assessment, vulnerability identification, evaluation of potential loss, assigning safeguards, and the evaluation of current status.

Defining DoD Space Resources

The first *Inspection* component requires us to define and identify our resources. Resources are defined as anything that adds value to the organization (or the country in this case) and whose loss would remove value. Information resources typically include all elements of an organization's information infrastructure including the systems, networks, and people. Anything that stores, transports, creates, or uses information in support of organizational objectives is a resource. Space sys-

tems resources include the three segments of space systems: the satellites themselves, the ground stations that operate and process the data, and the communication lines used in the exchange of information. They also include the people, infrastructure, and relationships which are harder resources to categorize and are often the resources that are not properly considered. An adequate identification of resources is required to evaluate risk and apply proper security measures.[4]

After making a formal inventory of DoD space resources, ownership and value must be assigned.[5] In some cases, ownership is an easy answer. In the new US National Space Policy, the secretary of defense and the director of national intelligence are assigned the duty of implementing procedures to "protect, disseminate and appropriately classify and declassify activities" to protect sensitive technologies, sources and methods, and operations.[6] Resource valuation is a much harder problem. Pipkin believes that the owner should determine the value of the resource. For military space systems the owner may be the best person to evaluate the type of investment made or the replacement cost, but not as good at determining the impact on the organization if the information we depend on from space is lost. It is important to note that the value comes not only from understanding how the resource is used in support of the owning organizational mission, but how others outside of the organization value the resource and how the owning organization benefits from the outside organizations use of the information. This is an important and often overlooked contribution to the value of a resource. It is also intimately tied to an understanding of the loss that would occur in the absence of the resource that we discuss below in our discussion of loss analysis.

Assessing Threats

The second inspection component requires us to asses the threats to our resources. A threat can be defined as a potential unwanted or undesirable event. A concise definition from the information technology security realm is given as: "A potential cause of an unwanted incident that may result in harm to a system or organization."[7] Threats can further be characterized by their source: natural, man-made, or technical. Man-made threats can be deliberate or non-deliberate.[8] A deliberate man-made threat can be defined as an expression of intention to inflict evil, injury or damage.[9] While it is possible to pre-emptively address some threats, in many cases threats are out of our control and cannot be totally eliminated. Interestingly, the Space Commission report identified an increase in threats to our space assets:

> The relative dependence of the US on space makes its space systems potentially attractive targets. Many foreign nations and non-state entities are pursuing space-related activities. Those hostile to the US possess, or can acquire on the global market, the means to deny, disrupt or destroy US space systems by attacking satellites in space, communications links to and from the ground or ground stations that command the satellites and process their data. Therefore, the US must develop and maintain intelligence collection capabilities and an analysis approach that will enable it to better understand the intentions and motivations as well as the capabilities of potentially hostile states and entities. An attack on elements of US space systems during a crisis or conflict should not be considered an improbable act. If the US is to avoid a "Space Pearl Harbor" it needs to take seriously the possibility of an attack on US space systems.[10]

Threats to DoD space assets affect the ground segment, communication link, and space segment or a combination of the above. Currently, the most significant deliberate threats to space systems are realized on the ground. These include threats to the physical, electronic, and information exchanges that involve the personnel, facilities, and ground segment equipment and the links to and from the space segment.[11] However due to technology sharing, material acquisitions and the purchasing of space services, threats to the space segment have increased and have started to overshadow the threats to the ground segment.[12] Air Force Doctrine Document (AFDD) 2-2.1, Counterspace Operations outlines some deliberate threats. These threats include:[13]

- Ground system attack and sabotage using conventional and unconventional means against terrestrial nodes and supporting infrastructure.
- Radio frequency (RF) jamming equipment capable of interfering with space system links.
- Laser systems capable of temporarily or permanently degrading or destroying satellite subsystems, thus interfering with satellite mission performance.
- Electromagnetic pulse weapons capable of degrading or destroying satellite and/or ground system electronics.
- Kinetic anti-satellite (ASAT) weapons capable of destroying spacecraft or degrading their ability to perform their missions.
- Information operations capabilities capable of corrupting space-based and terrestrial-based computer systems utilized to control satellite functions and to collect, process, and disseminate mission data.

In addition to the above threats, deliberate human acts can threaten the systems we use or the information related to the systems. Examples of deliberate human threats are espionage, sabotage, and information system attacks like worms, viruses or malicious computer attacks.[14] These threats are faced by business information security managers and are not unique to space systems. Private sector organizations must deal with these threats on a daily basis and are charged with protecting their organization from viruses, worms, Trojan horses, social engineering, phising, denial of service, theft of intellectual property, and failure of components. Therefore, we believe it is wise to draw upon the wealth of lessons learned from private sector organizations when securing our space assets.

Besides manmade threats, non-deliberate threats can also affect space assets. Natural threats are unpredictable and include meteor showers, inadvertent collisions of space objects, radio frequency interference, space environment phenomena, and natural destruction to ground systems. Again, just like information systems, space systems are composed of software, hardware, and infrastructure; all of which can fail.[15] A description of the threat and its likelihood assist with risk analysis and are used by the next component of the Inspection phase of security planning.

Identifying Vulnerabilities

The third inspection component requires us to identify vulnerabilities in our resources. A vulnerability can be defined as a weakness in a system that can be negatively affected or be exploited by some threat.[16] The keyword in the definition is "system" in its most general interpretation to include hardware, software, policies, procedures, and individuals. The definition covers flaws in the design of systems and their implementation, lack of rigorous policy and procedure statements, their inadequate implementation, and non-compliance. It is essential to realize that there are both known and unknown vulnerabilities. We can only address the vulnerabilities for which we are aware. For this reason, we must be proactive and continuously work towards the identification of unknown vulnerabilities. Mitigation of risk requires that we identify all potential vulnerabilities so that we can address them commensurate with their value.

Consider satellites which are built to withstand the rigors of launch and the harsh conditions of space. Yet they are relatively fragile objects. They are made of lightweight materials and are packed with sensitive equipment.[17] Our reliance on these complex objects makes us vulnerable to threats. One issue with vulnerabilities is we don't expect them to change or emerge, but they do. Upgrades, configuration changes, and new missions can add or change vulnerabilities. Just as security personnel continuously scan for threats, we must also plan for recurring vulnerability assessments.

For DoD space assets, the dependence upon access to space and the use of space is the biggest vulnerability. This vulnerability creates opportunity for adversaries to negatively impact DoD space capabilities.[18] Complicating this vulnerability is not having complete space situational awareness (SSA). SSA is having the insight into an adversary's space and counterspace operations. SSA requires understanding the current and future conditions, constraints, capabilities, and activities in, from, or through space. It includes understanding the space environment and its effects on our systems so we know if we have a deliberate threat.[19] To improve SSA, the Air Force is focusing on projects to improve our space surveillance capabilities. Projects include a space component, the Space Based Space Surveillance system, upgrading land based space surveillance network, and providing a decision making tool that recognizes attacks on satellites called the Rapid Attack, Identification, Detection, and Reporting System.[20] Former Air Force Chief of Staff, General John Jumper summed up this component of Inspection well:

> Identifying vulnerabilities will allow us to apply our full range of capabilities to ensure space superiority and continued support to joint military operations across the spectrum of conflict. Space superiority is as much about protecting our space assets as it is about preparing to counter an enemy's space or anti-space assets.[21]

Evaluating Potential Losses

The fourth inspection component requires us to evaluate the potential loss of the resources. Our space assets are used by commercial, civil, and military customers. Loss to civil and commercial customers is measured in financial terms; while loss to the military is measured in operational terms. In the case of the military, Mr. Tom Wilson, former Space Commission staff member, states, "as harmful as the loss or degradation of commercial or civil assets would be, an attack on intelligence and military satellites would be even more serious for the nation in time of crisis or conflict."[22] For the Space Commission report, Mr. Wilson came up with five types of losses that could result from an adversary's use of deception, disruption, denial, degradation, or destruction of specific space systems. They include:

- Impairment or elimination of reconnaissance satellites that would reduce SSA and could lead to military surprise, underestimation of enemy strength and capabilities, less effective planning, and less accurate targeting and battle damage assessments.
- Impairment or elimination of missile launch detection satellites that would degrade the US's ability to perform missile launch warning, missile defense, and would increase the psychological impact of the adversary's ballistic missiles.
- Impairment or elimination of satellite communications systems that would disrupt troop command and control problems at all force levels.
- Impairment or elimination of navigation satellites that would make troop movements more difficult, aircraft and ship piloting problematic, and could render many precision-guided weapon systems ineffective or useless.
- Impairment or elimination of Earth resource and weather satellites that would make it more difficult to plan effective military operations.[23]

The impact of possible attack depends on the importance of the resource, the timing, and duration of the loss.[24] Most space systems are truly "one of a kind assets" and as such are critical to mission success and hard to replace. While temporary denial may be worked around, the destruction of our assets would cripple our current capabilities due to the length in production time and response time to launch. In order to adequately provide SSA to commanders, it is essential for each organization to develop an understanding and document critical resource dependencies. This requires identification of all critical resources it relies upon, how and when the resources are used in support of their mission, and how the impact that would result from the loss of one or more resources. In theory, this sounds deceptively simple but in reality is much more difficult to calculate. In many cases, a qualitative assessment can be made by the decision makers who rely upon the resources, but such an estimate is of little value if it is not formally documented. Documentation ensures that the value estimate can be refined over time, provides transparency, reduces the time required to understand the impact of the loss of a resource, and reduces the variance in loss estimation that may occur when there is no documentation. The main idea is that we do not want to wait until we experience a loss to understand what value a resource provided to the organization. In the author's experience, we have seen far too many organizations that neglect to create and maintain this important

documentation. This is not due to ignorance, but instead it is often due to the difficulties in obtaining the required information, lack of personnel to collect and record the information, and fear that if the loss estimation is not properly secured it may be used as a targeting map by an adversary. Each of these impediments can be overcome if we are serious about securing our assets and we are willing to dedicate the time, personnel, money, and technology necessary to address them. Knowing the effects of a loss in military space capability (or our dependence on a resource) assists us in determining our vulnerability to the loss.[25]

Assigning Safeguards

The fifth inspection component requires us to assign safeguards, also known as controls, based upon the information collected during the first four Inspection components: the resources of interest, threats to the resources, the vulnerabilities inherent in the resources, and the loss of capabilities due to the loss of the resources. Assigning safeguards accurately is often difficult because it requires an accurate estimate of the costs to implement the safeguard, the value of the resource, the potential loss incurred if the resource is destroyed or degraded, the size and likelihood of the threats, and the size and likelihood of vulnerabilities. Using poor quality information leads to poor risk decisions and can result a non-optimal protection strategy. It should be noted that a non-optimal protection strategy does not always mean that resources are under protected, it can also mean that certain resources have been over protected at the expense of mitigating other significant risks. The overall goal in assigning safeguards is to identify the optimal protection strategy when constrained by a limited security budget. When assigning safeguards, tradeoffs must be made. Some important guidelines to consider are:

- Protective measures implemented must work together for full effect.
- Protection is only as good as the weakest link.
- Satellite survivability measures must be kept proportional to the value of the satellite's mission.
- Survivability must be kept proportional to the perceived threat.
- Safeguards must be weighed against their operational effects.[26]

Safeguards must be implemented to protect all segments of the resources or space assets. AFDD 2-2.1, Counterspace Operations, identifies Defensive Counterspace operations (DCS) as the ability to "preserve US/friendly ability to exploit space to its advantage via active and passive actions to protect friendly space-related capabilities from enemy attack or interference."[27] Friendly space related capability includes the ground system, communication links and satellites. DCS operations work to protect, preserve, recover, and reconstitute US and Allied space systems before, during and after an adversary attack.[28]

Passive safeguards serve to protect the assets. They are used to limit the effectiveness of the hostile action against the US system. Some passive safeguards identified in AFDD 2-2.1 are:

- *Camouflage, Concealment, and Deception (CC&D).* CC&D is most effective with terrestrial-based nodes. Certain types of ground-based components of space systems may operate under camouflage or be concealed within larger structures. These measures complicate adversary identification and targeting.
- *System Hardening.* Hardening of space system links and nodes allow them to operate through attacks. Techniques such as filtering, shielding, and spread spectrum help to protect capabilities from radiation and electromagnetic pulse. Physical hardening of structures mitigates the impact of kinetic effects, but is generally more applicable to ground-based facilities than to space-based systems due to launch-weight considerations. Robust networks, hardened by equipment redundancy and the ability to reroute, ensure operation during and after information operations attack.
- *Dispersal of Space Systems.* For space nodes, dispersal could involve deploying satellites into various orbital altitudes and planes. For terrestrial nodes, dispersal could involve deploying mobile ground stations to new locations.[29]

These passive DCS measures are layered together to form a defense. Besides passive DCS action, active DCS actions seek to remove or avoid the hostile effects. These active measures rely on early detection and characterization to be effective countermeasures. Active measures include:

- *Maneuver/Mobility.* Satellites may be capable of maneuvering in orbit to deny the adversary the opportunity to track and target them. They may be repositioned to avoid directed energy attacks, electromagnetic jamming, or kinetic attacks from ASATs. Today, maneuver capability is limited by on-board fuel constraints, orbital mechanics, and advanced warning of an impending attack. Furthermore, repositioning satellites generally degrades or interrupts their mission. The use of mobile terrestrial nodes complicates adversarial attempts to locate and target command and mission data processing centers. However, movement of these nodes may also impact the system's capability, as they must still retain line of sight with their associated space-based systems. Though the use of mobile technology is expanding, many of today's ground-based systems are not mobile, making physical security measures essential.
- *System Configuration Changes.* Space-based and terrestrial nodes may use different modes of operation to enhance survivability against attacks. Examples include changing RF amplitude and employing frequency-hopping techniques to complicate jamming and encrypting data to prevent exploitation by unauthorized users.
- *Suppression of Adversary Counterspace Capabilities (SACC).* SACC neutralizes or negates an adversary offensive counterspace system through deception, denial, disruption, degradation, and/or destruction. SACC operations can target air, land, sea, space, special operations, or information operations in response to an attack or threat

of attack. Examples of SACC operations include (but are not limited to) attacks against adversary anti-satellite weapons (before, during, or after employment), intercept of anti-satellite systems, and destruction of RF jammers or laser blinders.[30]

Other active DCS actions include actions that may target an adversary's counterspace capabilities. Such as using conventional and special operations forces to attack and disable an adversary's counterspace capabilities. Having a counterspace capability demonstrates a capability and willingness to counter their efforts deterring an adversary from attacking US/friendly space capabilities. Other safeguards include:

- A single integrated space picture would provide an accessible picture of global and theater space capabilities, threats and operations to commanders, planners, and combat forces, covering the full spectrum of friendly, adversary, and third party space systems. This would provide a comprehensive peacetime and wartime SSA capability, fusing information collected on all space systems, their ground, air, and space links and nodes to include their capabilities, status, vulnerability, and users.
- Physical security systems provide security and force protection for critical ground facilities and equipment. A complementary mix of technology and security forces can effectively and efficiently mitigate specific threats in an ever-changing environment. When properly deployed and utilized, physical security systems can represent an effective deterrent and provide aggressive defense against terrestrial node attack and sabotage.
- Air defense assets are capable of protecting launch and terrestrial nodes from air or missile attack. If threatened, commanders should consider deploying air defense assets such as fighter aircraft, surface-to-air missiles, and/or antiaircraft artillery to protect critical space assets (e.g., facilities and infrastructure). A sound air defense may deter an adversary and most certainly will be instrumental in defending our forces and assets if an attack is attempted.
- Attack detection and characterization systems detect space system attacks and provide information on the characteristics of the attack, especially if the source and/or capability of the attack is unknown or unexpected. These systems will support locating the source of the attack and the type of weapon used in the attack. They may be ground-, air-, or space-based and either integrated with systems they protect or used in a stand-alone capacity. Having our adversaries aware of these capabilities may influence their decision and act as an effective deterrent.
- Survivability countermeasures ensure critical space systems continue to operate both during and after attack. Examples include (but are not limited to): spacecraft system hardening, redundant systems (both on spacecraft and in ground stations), spacecraft maneuverability, ground station mobility, and jam-resistant communication links. Known survivability measures may deter an adversary from attacking our space capabilities.[31]

Evaluating the Current Status

Currently there are more than 450 active foreign spacecraft in orbit, and that number is expected to reach 600 by 2010.[32] With this increase in foreign satellites, there will be new imaging, environmental and even navigational satellites entering the mix. "Many countries are developing advance satellites for remote sensing, communication, navigation, imagery, and missile warning. The increase in the number and capability of these satellites enhances a country's command, control, communication, and computers intelligence, surveillance, and reconnaissance capabilities and in turn their warfighting capability" which changes the environment we operate in.[33] As this mixture changes, we must monitor this environment and our security, which is the last component of inspection. Evaluating the effectiveness of current processes requires periodic analysis of procedures and testing. If possible a complete evaluation of the system needs to be done from the perspectives of satellite to the communication links to the ground station and finally the deployment of the information. An evaluation is required on the physical security, personnel policies and practices, business processes, backup and recovery measures, and network controls to include our operations security and information assurance, as noted in AFDD 2-2.1:

> Operations security (OPSEC) and information assurance (IA) protect our space systems by limiting the availability of information on their operations, capabilities, and limitations to our adversaries. IA protects critical computer systems from intrusion and exploitation. Guiding adversaries' actions can successfully deter effects on our space services, but OPSEC and IA operations are primarily focused on defending our assets from attack.[34]

Along with a review of our procedures, testing must be done to identify additional resources, threats, and vulnerabilities. We currently test only individual aspects of DoD space systems. We have inspections that test the security of certain bases or facilities but not the system as a whole. This is an area that could be improved—the integration and testing of our space capabilities across the complete space spectrum. A representative of the Langfang Army Missile Academy has said, "In future space wars, the main operations will consist of destructive satellite attacks and counterattacks, as well as jamming and antijamming operations."[35] In other words, the threat is real and will continue to grow making it necessary to continuously monitor the situation.

Conclusion

Inspection is just one aspect of a robust security program. We have found that while we do a good job at protection, detection, and reaction to security incidents; we often fail to do well during the first phase *Inspection* and the last phase *Reflection*. There has been a significant amount of research in the individual components of *Inspection*—resource definition, threat assessment, loss analysis, vulnerabilities identification, safeguard assignment, and evaluating the current status that can be applied to DoD space assets. But we think it is vital to look at the whole picture to ensure there are no security gaps. President George W. Bush believes our top goal is to "strengthen

the nation's space leadership and ensure that space capabilities are available in time to further US national security, homeland security, and foreign policy objectives and to enable unhindered US operations in and through space."[36] The first step in ensuring DoD space superiority is a systematic inspection of DoD space assets.

Notes:

[1] *US National Space Policy,* Authorized on 31 August 2006 and supersedes Presidential Decision Directive/NSC-49/NSTC-8, National Space Policy, 14 September 1996.

[2] Donald L. Pipkin, *Information Security Protecting the Global Enterprise,* Hewlett-Packard Company, 2000.

[3] Ibid., 17.

[4] Pipkin, *Information Security.*

[5] Ibid.

[6] *US National Space Policy,* 9.

[7] ISO/IEC 13335:1996, "ISO/IEC Information technology—Guidelines for the management of IT Security – Part 1: Concepts and models for IT Security." ISO/IEC 13335, 1996.

[8] Pipkin, *Information Security.*

[9] *Merriam-Webster's Collegiate Dictionary,* Tenth Edition, 2002.

[10] *Report of the Commission to Assess United States National Security Space Management and Organization,* Space Commission, Pursuant to Public Law 106-65, 11 January 2001, 8.

[11] Adolfo J. Fernandez, *Military Role in Space Control: A Primer,* Congressional Research Service Report to Congress, 23 September 2004.

[12] National Air and Space Intelligence Center (NASIC)-1441-3894-05, *Challenges to US Space Superiority,* March 2005.

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

[14] Pipkin, *Information Security.*

[15] Ibid.

[16] ISO/IEC 15947:2004, "ISO/IEC Information technology—Security techniques - IT intrusion detection framework." ISO/IEC 15947, 2004.

[17] Paul Stares, *Space and National Security,* The Brooking Institution, 1987.

[18] Maj Gen Shelton, 14AF CC, speech, briefed to IDE class at AFIT, 15 November 2006.

[19] AFDD 2-2.1, *Counterspace Operations.*

[20] John A. Tirpak, Securing the Space Arena, *Air Force Magazine,* July 2004.

[21] AFDD 2-2.1, *Counterspace Operations,* 1.

[22] Tom Wilson, *Threats to United States Space Capabilities,* Space Commission Staff Member, http://www.fas.org/spp/eprint/article05.html, section V.

[23] Ibid.

[24] Pipkin, *Information Security.*

[25] Ibid.

[26] Stares, *Space and National Security.*

[27] AFDD 2-2.1, *Counterspace Operations,* 31.

[28] Ibid.

[29] Ibid., 26.

[30] Ibid., 27.

[31] Ibid., 28.

[32] NASIC, 10.

[33] Ibid.

[34] AFDD 2-2.1, *Counterspace Operations,* 29.

[35] National Air and Space Intelligence Center, 16.

[36] Mark Kaufman, "Bush Sets Defense As Space Priority: US Says Shift is Not a Step Toward Arms, Experts Say It Could Be," *Washington Post,* 18 October 2006.

Maj Heather H. Yates (BS, Applied Mathematics, University of Virginia; MS, Management, Troy State University; MS, Systems Engineering, Air Force Institute of Technology (AFIT)) is program manager, Spacecraft Systems Integration, Headquarters National Reconnaissance Office, Chantilly, Virginia. She directs the technical activities of a major contractor systems engineering team building advanced spacecraft and subsystems components.

Major Yates was commissioned through ROTC at the University of Virginia in May 1994. She has served a variety of space/missile operations and acquisition positions. Her initial assignment was to Malmstrom AFB, Montana where she served as a Minuteman III combat crew commander, evaluator, and instructor. At the 11th Space Warning Squadron, Major Yates was responsible for all contract issues for the Attack and Launch Early Reporting to Theater (ALERT) system and was qualified as a theater warning crew commander. Major Yates transitioned from operations to acquisition at the Space and Missile Systems Center, where she was responsible for the Space-based Infrared Satellite System (SBIRS) International Affairs, SBIRS Mission Processing Development and was the SBIRS and Military Satellite Communication staff director for the Program Executive Officer (Space). Prior to her current assignment, Major Heather Yates completed Intermediate Development Education at AFIT and earned the "Distinguished Graduate" award.

Dr. Michael R. Grimaila (BS, Electrical Engineering; MS, Electrical Engineering; and PhD, Computer Engineering, all from Texas A&M University) is an associate professor and a member of the Center for Cyberspace Research at the Air Force Institute of Technology, Wright-Patterson AFB, Ohio. He is a CISSP, CISM, GSEC, and holds the NSA IAM and IEM certifications. He teaches and conducts research in the areas of information assurance, information warfare, and information operations. Dr. Grimaila serves on the Editorial Advisory Board of the ISSA Journal, on the ISACA Security Program Metrics Project, and is a member of the DoD/NII Information Assurance Best Practices and Security Metrics Working Groups. He is also a member of the ACM, IRMA, ISACA, ISC2, ISSA, ISSEA, the SANS Institute, and is a senior member of the IEEE.