AU/ACSC/BICHLER/AY2015

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

MITIGATING CYBER SECURITY RISK

IN

SATELLITE GROUND SYSTEMS

by

Stephen F. Bichler, Maj, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

MASTER OF OPERATIONAL ARTS AND SCIENCES

Advisor: Lt Col David Hanson

Maxwell Air Force Base, Alabama

April 2015

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

TABLE OF CONTENTS

ABSTRACT

Satellite ground systems represent an often neglected aspect of cyber security when discussing Air Force and Department of Defense cyber vulnerabilities. An increasing amount of cyber security research and attacks focus on space ground systems in the form of satellite control, satellite communications terminal hacking, and GPS spoofing. Public evidence exists demonstrating nation-state adversary willingness and intent for attacking these systems. Ground systems find themselves in a gray area of compliance between the two cyber security risk management regulations DoDI 8510 and Committee on National Security Systems Instruction 1253. Both require compliance to security controls, but neither build in the evaluation or mandatory controls necessary for the mitigation of risk. A further examination of private industry standards and theory shows better methods of mitigating cyber security risk via simplifying the security controls necessary, using time-based methods for analyzing controls, and conducting preventative cyber security engineering on new systems for the provision of information assurance.

INTRODUCTION

For decades space systems provided the United States an unparalleled political and military asymmetric advantage over other near peer states. Similarly the growth of cyber technologies in the United States from the birth of the Internet to today provided an unparalleled information advantage. Coupled together space and cyber technologies emboldened the rapid military successes of the 1990s as space technologies such as satellite communications, Global Positioning System (GPS), space-based intelligence surveillance and reconnaissance, and weather data fused with global data networks and databases allowing the near instantaneous sharing of data. The network-centric warfare models of the late 1990s and early 2000s created a secondary effect as space and cyber technologies coupled together for an unprecedented speed and information processing advantage. The acquisition and operations communities regarded the security of the data, the links, and ultimately the space systems themselves as secondary.

Many of these technologies remain in the United States' inventory today, built using the same insecure cybersecurity model. The ground system and user terminals represents the most vulnerable portion of a space system to cyber security threats. A ground system consists of the network of computers, antennas, and functions commanding and controlling the on-orbit satellite. An example of a ground system is the Air Force Satellite Control Network (AFSCN). A user terminal consists of the devices provided to warfighters for receiving satellite signals. Common user terminals are radios, GPS receivers, satellite phones, satellite communication (SATCOM) terminals. The chokepoint for both cyber and space technologies rests with the ground systems where the transfer and translation of data occurs. Although updated regularly, per Department of Defense (DoD) and Committee on National Security Systems (CNSS) regulations, these ground systems remain vulnerable to cyber-attack. Often times, these systems

receive waivers from security updates due to perceived "performance" issues with the satellite, or operate on slower update schedule due to contracts or operational constraints. All systems technically meet the compulsory guidance for information assurance risk management (DoD 8510.1 and CNSSI 1253) and any risks were accepted by the representative Chief Information Officers within DoD who manage the systems.[1] However, compliance doesn't mean security. There have been several breaches of space ground systems over the last decade and a concentrated effort by adversaries to gain access to American space technology through cyberspace operations. Better methods for identifying and mitigating risk in satellite ground systems will continue as essential tasks in keeping the United States' significant space advantage. The current guidance does not go far enough to mitigate these threats, because adversaries will continue to attack cyber systems and satellite links as these are easier and cheaper to access than the satellites on-orbit.

Although space ground and control systems meet Department of Defense (DoD) compliance policies for cybersecurity, these systems lack an iterative continuing cyber security assessment process for discovery, risk analysis, mitigation and remediation of advanced cyberspace threats throughout the space systems' lifecycle. Space ground and control systems require new methods of risk-based compliance, and frequent evaluation of cybersecurity risk to space operations and a renewed focus on engineering away the weaknesses of systems at their inception; only then will US cyber systems supporting space operations be considered secure and available in conflict.

BACKGROUND

Space Ground and Control Systems Overview

A vast array of components make up satellite ground systems and receivers, as defined in this paper. These include the earth terminals and user receivers, which translate the satellite signal to usable data to the user receiver devices which make up the largest segment of the ground components of satellite. They also include the command and control network the Air Force uses for keeping the satellites operational.

The user terminals and devices represent the most ubiquitous element of a satellite systems. Examples of these devices include major satellite earth terminals which power large military bases or even metropolitan areas with SATCOM signals; the SATCOM tactical radios used in countless military and commercial vehicles, vessels and aircraft; and the wide variety of GPS receiver devices. All of these devices possess some processing and computing power using cyberspace technologies.

Just as important as the technical components of the systems, the command and control (C2) structure for space ground systems aids in their survivability to most attacks as procedural redundancies aid system operations. The preponderance of military space assets receive their C2 from the Joint Space Operations Center (JSpOC) at Vandenberg Air Force Base, while tactical and administrative control falls to the 50th Network Operations Group of the 50th Space Wing at Peterson AFB, Colorado.[2] For NASA space assets, Johnson Space Center and Goddard Space Center possess the ground systems for control of space assets.

Within the 50th Network Operations Group, the Air Force Satellite Control Network (AFSCN) is the ground system responsible for C2 of a large preponderance of DoD satellites. This network consists of a massive, globally connected grid of manned and unmanned sites

which maintain control of satellite actions from earth. Management of AFSCN operations occurs at Schriever AFB in Colorado where AFSCN receives its tasks for satellite operations from the Joint Space Operations Center. The backup communications node is at Vandenberg AFB. There are seven additional tracking sites throughout the world providing control information to satellites when they are overhead. Enabling global operations requires the placement of these sites globally in the Pacific, Greenland, the United Kingdom, and the east and west coasts of the United States. Additionally, AFSCN maintains a number of transportable units in the eventuality that a site goes down or C2 need reestablishment due to a catastrophic event which may occur at both Vandenberg and Schriever AFBs. The AFSCN computer systems vary in their connectivity to the outside world affecting their vulnerability to cyber-attacks at the different sites. Office automation systems connect to the Air Force network for unclassified and classified communications. The Air Force network connects via commercial circuits to the Internet for unclassified communications. The satellite control network operates in conjunction with the other sites and the JSPOC, but does not connect to any open Internet connections; by design it is a closed network. Again the degree of isolation varies by site due to the dependence on commercial circuits within the DoD. Finally, communications with the satellites themselves are isolated communications between the ground station terminal and the satellite receiving the commands; this also represents a closed network. On its face, this seems like a fairly secure design. However, opportunities and precedent have shown cyber penetrations into these closed networks.[3]

The 2nd Space Operations Squadron uses a similar system for the management and monitoring of the GPS constellation. A main control ground station exists at Schriever Air Force Base with a secondary site at Vandenberg AFB and monitoring sites around the world

which are both manned and unmanned. The satellites orbit in the Geosynchronous belt meaning the signal is very low powered requiring many stations throughout the world for monitoring and management. Currently, five manned monitoring sites exist for GPS. GPS sites often co-locate with AFSCN sites and other United States Air Force satellite management and space surveillance ground stations. However, their operations remain separate. [4]

This consolidation effort will likely continue as Air Force budgets constrain further in the coming years. The increased reliance on information systems and automation may power this consolidation meaning a greater reliance on the cyber components of ground stations. The Air Force's Consolidated AFSCN Modernization, Maintenance and Operations or CAMMO contract was recently won by a team including Lockheed-Martin. The number one requirement according to Lockheed's press release and web site was cyber security for the AFSCN during the modernization and consolidation. This acknowledgement by both the Air Force and its largest contractor on the project points to the importance of cyber security at the ground stations.[5]

Cyberspace Components of Satellite Ground System

Like most of the digital world, space systems depend on cyberspace systems. Strategically, the Joint Space Operations Center and the NASA Operations Center use cyberspace technology for space surveillance and monitoring of space objects. Both organizations use cyber technologies in the operation of their satellite systems via large integrated computer networks. The congestion of space requires a robust surveillance information system cataloging thousands of objects. The record-keeping of these objects does not fall in a standalone specialized information system, but in an off-the-shelf data warehouse solution. Space system data represents a gold-mine for potential nation-state adversaries. Whether a government system or a contractor system, space data remains in high-demand among

nations developing space programs, and non-state actors interested in the information on these satellites. There were 15 publicized cyber intrusions into government space systems from 2005-2013, all coming from NASA.[6]

Operationally, satellite ground systems rely on cyberspace technology at every turn. The space operators work off console systems, utilizing computer systems and digital data for the maneuver, control and manipulation of satellites. The AFSCN and GPS control network integrate their respective global communications networks of satellite ground stations, monitoring stations, and satellite links melded together through cyberspace for the overall control of Air Force satellites across the global monitoring of space.[7], [8]

At the tactical level satellite communications, ground terminals exist linking the satellite feed into the communications network of customers. For the military, this includes tactical unclassified and classified networks directly interfaced to satellite terminals for data access. These satellite ground terminals represent a particularly vulnerable point for a satellite system. It is the place where cyber technology and space technology converge at a chokepoint and must speak the satellite's unclassified language for the uplink and downlink of data. This is often an open telecommunications protocol such as Transaction Language 1 (TL1), a common satellite communications protocol used in military SATCOM.[9] Navigation systems also rely on cyberspace technologies for map overlays and integration of position and timing data into usable information. Communications, positioning and timing exist as vital assets to tactical users.

CYBER THREATS TO SATELLITE GROUND SYSTEMS

Cyber-Based Espionage

The United States' unparalleled advantage in space, particularly in satellite operations, is

due in large part to the massive amounts of research, development, and intellectual property accumulated over the last sixty years of the United States' efforts in space. Unlike in the 1960s, when much of this intellectual property remained locked behind classified fences at government facilities, the distribution of intellectual property through the government, universities and large contractors are much more accessible in digital form.

Nation-states seek this trove of information either for the building of their own space capabilities or the effective countering of US capabilities. From 1997-2013 in open source, there were 12 instances of cyber espionage attacks against NASA networks. These culminated with the arrest of Chinese national and NASA contractor Bo Jiang attempting to flee the United states with "a large amount of information technology he may not have been entitled to possess" in 2013. The Jiang incidente incited the expulsion of 118 Chinese nationals from NASA contract work because of the fear these individuals were acquiring schematics, engineering diagrams, signal schemes and research data for various US space platforms. Additionally, from 2003-2006 a massive Chinese network infiltration campaign dubbed "TITAN RAIN" by law enforcement and intelligence officials targeted DoD, NASA, aerospace contractors and research institutes searching for information on space propulsion systems, solar paneling and fuel systems, as well as other Department of defense acquisition targets.[10] More recently the much publicized Mandiant Technology report exposing "Advanced Persistent Threat (APT) One" on a Chinese People's Liberation Army (PLA) cyber unit showed the aerospace and satellite industries as the second and fourth most targeted industries of just this one particular PLA cyber espionage unit.[11]

China grabs the most headlines with cyber espionage, but they are definitely not alone. Numerous unattributed infiltrations occur at many top space and aerospace firms over the last

several years. A group of Romanian hackers stole sensitive data from both NASA and the European Space Agency in an effort to sell the data on the black market. Eventually, not finding a buyer, they released a majority of the stolen information on the open internet. The Romanian incident shows espionage is not simply a "China" problem.[12]

These incidents of espionage represent the publicized incidents which occurred, because cyber security in government remains shrouded in secrecy. However, using the Defense Operational Test and Evaluation Office's (DOT&E) FY14 report on cybersecurity one grasps the seriousness of the problem. DOT&E reported only 85% of networks in DoD were compliant with the cyber security regulations discussed later in this paper. Not until compliance is near 100% could DOT&E conceive with confidence that DoD networks were safe from adversary intrusion and data exfiltration. One of the key findings of the FY14 DOT&E report dealt with shipboard SATCOM datalink vulnerabilities, indicating again the targeting of space systems. [13]

Cyber Exploitation & Access Operations

In the discussion of cyber espionage the question "how does this happen" should resonate in the reader's mind. Cyber exploitation is the how. Cyber exploitation is the means of gaining and maintain access in a computer network and pre-positioning oneself in the parts of this network which provider the intruder with access to the information they seek. In the United States, cyber exploitation usually coincides with intelligence and espionage missions, but the exploitation of systems is necessary whether the mission of the intruder is theft, interruption, damage or destruction from cyberspace. Access is the key in any cyberspace operation and exploitation represents the means to access.[14]

The most common scenario for a network's exploitation are web page attacks which break up in three categories known as cross-site scripting, cross-site request forgery, and "drive-by"

hacking. These attacks make up three of the Top 10 vulnerabilities according to the Open Web Application Security Project, an independent group studying internet security. In a web page attack, the hacker finds vulnerabilities in a website used by the people they are targeting. These vulnerabilities allow the attacker to redirect the target to another website which downloads a program to the target, commonly known as a trojan horse. Often this secondary website remains invisible to the target, made so by manipulating the user's screen and hiding the nefarious page in one pixels unnoticeable by the human eye. The trojan horse allows the intruder initial access in a network, from there the intruder will move throughout the network attempting to gain the credentials needed to gain further access into the system. [15]

The other common method for network exploitation are phishing attacks. Phishing attacks receive much publicity as they have proven responsible as the initial exploitation in most major commercial and government cyber-attacks of the last decade. In a phishing attack, a target receives an email with a nefarious link to a webpage, often believed a legitimate webpage. This web page downloads the Trojan to the target. Then just like a web page attack the attacker moves on to other portions of the network looking for the information or setting themselves up to persistent on the network if their intent is triggering an attack. [16] According to the DOT&E phishing and web exploitation make up the vast majority of intrusions executed by DoD cyber security evaluation teams and known adversaries. These attack vectors represent the most likely access operations. [17]

The most dangerous method for a space system's exploitation comes through the use of an "air gap" tool, bridging the separation between a space ground system network and the office automation systems and networks. The AFSCN and GPS control networks are mission networks controlling sensitive assets, but they are not classified. Therefore, some of the controls

placed on classified networks do not apply. Therefore, the attachment of an infected storage device (USB thumb drive, external hard drive, infected CD-DVD, or smartphone) could inadvertently allow an adversary access to a space control network. This would be uncontrolled access because the adversary could not access their software once deployed. The precedent for this type of exploitation already exists in the forms of the STUXNET virus in Iran and the agent.btz infection of USCENTCOM networks. In both the incidents the attackers deployed the malicious software to air gapped networks. That software ran its malicious payload. In the case of STUXNET, a destructive payload caused damage to Iran's nuclear reactor.[18] In the case of agent.btz, the results are not widely publicized, but it proved adversary ability to infect classified networks.[19] An air-gapped infection vector against AFSCN or GPS could cripple the Air Force's ability to control its on-orbit satellite resources. Particularly, if the attack occurred at the primary and secondary sites with the malicious software only activating if it recognizes itself being on a satellite control network, similar to how STUXNET worked. [20]

How would an adversary persist and maintain access on space systems? A multitude of weaknesses inherently built into satellite receivers, ground systems, and network components make persistence for a cyber-adversary not only possible but probable. These are not "hacks", but methods built-in by manufacturers and contractors overlooked during the initial build of systems. For example, the Mandiant report discusses in multiple areas how APT1 used built in Windows administrator commands to fortify and expand access in targeted computer networks.[21]

Cyber Attacks on Ground Systems

The targeting of space ground systems increased over the last decade with some extremely sophisticated attacks occurring over the last two years. The following examples chronicle very high-profile cyber vulnerabilities and breaches illustrating the importance of developing adaptive

methods for the security of these ground systems.

NASA, by far, represents the most transparent organization in terms of cyber security breaches, with both of the following breaches originated from China. Besides the cyber espionage indicated earlier, NASA also experienced several exploitations and attacks which are concerning for space professionals. In 2007, Goddard Space Flight Center experienced a network penetration leading to data theft regarding earth observation systems. Later that year and in 2008, the earth observation satellite Landsat-7 experienced multiple incidents of interference caused by cyber-attack. In October of 2008, cyber intruders hijacked another earth observation satellite, Terra-EOS AM-1, who not only caused interference, but also achieved all steps necessary for control of the orbiting satellite. The only thing stopping these attackers from commanding the satellite was an understanding of the actual commands for satellite maneuver.[22]

Additionally in 2008, hackers infiltrated the Johnson Space Center's mission control computer network and were able to have the mission control network upload a malicious Trojan horse access program onto computers on the International Space Station disrupting on-board communications, but not endangering the crew or space flight itself. This attack occurred because the ISS computers were not receiving vital software updates to their operating system.[23]

In October 2012, security researchers at Carnegie-Mellon University found several severe vulnerabilities in major government and commercial grade GPS receivers' software which rendered GPS's precision timing invalid. Instead of spoofing or jamming the GPS signal as many other attackers previously conducted, these researchers attacked the inherent weaknesses of GPS's design to disrupt the timing. The attackers falsely set the GPS receiver's location in the software to the center of the earth (i.e. the earth's core), because GPS orients itself off the position of the receiver on the earth's surface in conjunction with the location of the receiver on

the earth's surface. Based on the faulty position, the receivers would either reboot or reject the "middle-of-the-earth" attack data, but this caused permanent corruption of the timing data on the receiver as a secondary effect. Next, the attackers used weaknesses in the operating system software of the receivers to set the date/time of the operating system outside the bounds of the GPS's epheremis timing by 20 years. In so doing, allowed the attackers to reset the timing of GPS at a rate of 40 years per minute, invariably causing the GPS receiver to rollover to a new timing epoch in about 2 days. This desynchronization of timing then flows to the other networked systems and breaks the timing throughout a network using GPS timing. [24] This type of cyber-attack on GPS shows the vulnerability and dependency DoD and other computer networked systems have for precision timing. A most concerning scenario, would be if the GPS control network itself were attacked and this data used to desynchronize timing throughout the satellite system. Although unlikely, it is concerning these issues were found in GPS receivers. It begs the question of whether these issues remain at the satellite control level as well.

At the 2014 major hacker convention DEFCON, security researcher Ruben Santamarta, released a report showing the attack and control by cyber attackers of ten of the top military and commercial SATCOM terminals on the market. Santamarta's research included some technical reverse engineering of SATCOM terminal software, but nearly all of the vulnerabilities found resulted from open-source research in the manuals and documentation of these systems. He discovered weak default passwords, normally left in place by default. Additionally, programmer backdoors from data units which control user communications and control units which control access to the satellite were easily discoverable and left in default modes. Finally, protocols for communications between the satellite control units and the user interface had weak authentication mechanisms, easily guessed or captured by Santamarta's team. Concerning for

the DoD is Santamarta's research included the Harris PRC-119 radio used in most tactical vehicles, the Thuraya IP SATCOM terminal which was used in morale and welfare networks in Afghanistan, and the Cobham Aviator SATCOM terminal used in the C-130J. All were vulnerable to attacks requiring little technical knowledge, but only a good deal of curiosity and access to the network itself. Figure 1 represents the list of vulnerabilities discovered on each type of terminal.[25]

Fig 1 – SATCOM Vulnerabilities from IOActive Whitepaper[26]

Vendor	Product	Vulnerability Class	Service	Severity
Harris	 RF-7800-VU024 RF-7800-DU024	Hardcoded Credentials Undocumented Protocols Insecure Protocols Backdoors	BGAN	Critical
Hughes	 9201/9202/9450/9502	Hardcoded Credentials Undocumented Protocols Insecure Protocols Backdoors	BGAN BGAN M2M	Critical
Hughes	 ThurayaIP	Hardcoded Credentials Insecure Protocols Undocumented Protocols Backdoors	Thuraya Broadband	Critical
Cobham	 EXPLORER (all versions)	Weak Password Reset Insecure Protocols	BGAN	Critical
Cobham	 SAILOR 900 VSAT	Weak Password Reset Insecure Protocols Hardcoded Credentials	VSAT	Critical
Cobham	 AVIATOR 700 (E/D)	Backdoors Weak Password Reset Insecure Protocols Hardcoded credentials	SwiftBroadband Classic Aero	Critical
Cobham	 SAILOR FB 150/250/500	Weak Password Reset Insecure Protocols	FB	Critical
Cobham	 SAILOR 6000 Series	Insecure Protocols Hardcoded Credentials	Inmarsat-C	Critical
JRC	 JUE-250/500 FB	Hardcoded Credentials Insecure Protocols Undocumented Protocols Backdoors	FB	Critical
Iridium	 Pilot/OpenPort	Hardcoded Credentials Undocumented Protocols	Iridium	Critical

In August 2014, the Department of Commerce Inspector General released a scathing report on unpatched security vulnerabilities throughout the ground systems of the Joint Polar Satellite System (JPSS). JPSS is the follow-on weather observation satellite system for both the National Oceanic and Atmospheric Administration (NOAA) and the DoD. The ground system received failing marks in its 2012 cybersecurity audit, but provided several solutions to "get well" before its next evaluation. When the follow-on evaluation finally came two years later not only were the 2012 vulnerabilities not fixed, but several thousand other vulnerabilities were discovered. The findings were so severe a fear existed the entire program could be cancelled. However, NOAA and DoD deemed JPSS too important due to satellites already being on-orbit. The vulnerabilities found in 2012 numbered over 14,000 and numbered over 23,000 after the July 2014 evaluation. The cause determined by the inspectors coupled a complacency in compliance by internal auditors at NOAA with an unwillingness to deviate from scheduled updates by the JPSS contractors. This issue of deviation matches issues DoD space programs experience when trying to address time-sensitive cyber vulnerabilities against an acquisition schedule of a mission-based system.[27] Two months later in November of 2014, NOAA revealed a satellite system breach by nation-state attackers believed to be from China. NOAA discontinued the release of public satellite imagery from its website for over a week due to the attack. [28] An unnamed NOAA source stated "the Chinese are robbing us blind" of satellite technology.[29] This example shows a direct correlation between poor security practices and a breach by a nation-state actor into sensitive satellite systems.

CURRENT CYBERSECURITY RISK MITIGATION FOR GROUND SYSTEMS

Cyber Security Compliance

The cyber targeting of satellite ground systems constitutes an evolving focus of both

commercial security researchers and nefarious nation-state hackers. The basis for government cyber security documentation, since 2012, rests within the National Institute of Standards and Technology's 800-53 Risk Management for Information Systems. Widely lauded in the cyber security industry as the best incorporation of industry best practices into a government policy, the executive branch ordered all departments implementing the process by 2012 to reduce cyber security breaches in government. The six step process in the RMF focuses on moving away from a checklist mindset for evaluating information technology, and moves to an evaluation of risk with continuous monitoring as the goal.[30]

The DoD's guiding documents for cyber security risk management is DoDI 8510.1Risk Management Framework for Information Technology. These document governs the overall, cyber security for IT systems and components throughout the department. In the case of DoD 8510.1, the regulation articulates the evaluation and assessment of risk. However, both documents specifically eliminate "weapons systems." DoD regards its space control systems and communications systems as "weapons systems," and not merely networks. All major satellite systems including GPS and AFSCN do not fall under the DoD 8510.1 guidance. This does not eliminate them from cyber security requirements, but it does allow these systems to circumvent the regulations requirements for periodic evaluation and validation per the regulation. [31]

How then are these systems governed? As weapons systems they fall under the category of National Security Systems and governed by the Committee on National Security Systems (CNSS) which possesses similar guidance on governance and risk management in its CNSSI 1253 with attachments for specialized systems including space. The CNSSI provides a breakdown of cyber security measures which if implemented, properly assessed and re-validated provide a means for setting up a good compliance program. The CNSSI even contains an

attachment specifically on space system controls with concerns for what additional security controls must occur in space systems.[32] However, a huge problem exists as the ground systems associated with the space system remain exempt from the space overlay. Ground systems should "use other appropriate security overlays."[33] Based on the space overlay of CNSSI 1253 the ground system remains covered under other areas. So the security control of space ground systems does not fall under the purview of the space security control regulation because it is terrestrial. However, it also does not count as an IT system.[34] This causes confusion not just for program managers and space operations centers, but also for cyber security evaluators who attempt to judge systems based on the security baselines established.

The CNSS attempted to rectify this situation in May 2014 with the publication of CNSSI 1200, *National Information Assurance Instruction for Space Systems to Support National Security Missions.* This regulation does a better job by specifically addressing minimum requirements for the cyber security of all three segments of the space system: ground, link and space. Unfortunately, the document lacks specifics. The Cyber Defense Annex walks the reader through the steps of the Risk Management Framework with no specifics on timeframes for evaluation, specific methods of evaluation or risk mitigations for cybersecurity. The document focuses on the link layer and space segment crypto security instead of focusing on the ground system's cybersecurity. [35] So space ground systems fall into a vacuum of not quite IT systems governed by DoD 8510.1's Risk Management Framework, not governed by CNSSI 1200 on Space Systems, and governed by CNSSI 1253, but with over 700 controls which for leadership to determine, based on their best guess of what security controls will balance security and operational effectiveness. The guidance lacks specificity, which could lead to assumptions regarding the system's security and its evaluation cycle.

Cyber Security in Acquisition

All the current cybersecurity risk management policies discussed thus far, put a large emphasis on identifying potential cybersecurity issues early in the acquisition process, so the security of these systems is built into the ground systems prior to deployment. Both DoD 8510 and the CNSSIs put a large emphasis on identifying potential risks early in the acquisition process so controls and mitigations become built into the system.[36] CNSSI 1200 provides a program protection plan template for space systems designed for sparking the questions one needs answered for successful pre-identification of security issues. [37] The DoDI 8510.1 risk management framework, although, not strictly applicable, provides a breakdown of assessing cyber security controls in the acquisition process. Both the program protection plan in CNSSI 1200 and the DoD 8510.1 mapping of RMF steps to the acquisition process do not provide the granularity needed for program managers to truly understand the security controls selected early in the process. These program managers cannot be truly certain of the controls protecting the system until testing and implementation. This means often these controls become inadequate or inconsequential at implementation, causing gaps during the monitoring and evaluations required in the RMF. [38]

Cyber Security in Operations

In the operations phase, both the CNSSIs and DoDIs call for continuous monitoring with the general guidance to "continuously monitor the system or information environment for security-relevant events and configuration changes that negatively affect security."[39] This may cause confusion within program offices on what to monitor and what constitutes "security-relevant." Additionally, the CNSSI 1200 calls for risk assessments in each phase of the space system's lifecycle, but does not require follow-on assessments other than one per phase from

acquisition through the testing phases until operations.[40] The great weakness of these risk management methodologies becomes their inability for providing specifics to program manager and cyber security managers on what trade-offs systems require. Nor do they truly identify or assess the absolutely critical nodes in the system which need additional protection. Often the managers of these systems must discover the needed controls based on trial and error due to the lack of knowledge on identifying and examining the new systems in operations. The CNSSI's provide a means for requesting the NSA's Information Assurance Directorate security engineering and assessment help. [41] However, for Air Force space systems these requests must route not only through the Air Force Space Command, but also USCYBERCOM for prioritization. This can cause long lead times resulting in systems not being evaluated for months.

In operations, ground segment monitoring occurs using the best means available, but often the system's configuration prevents very thorough monitoring because space systems do not operate normal TCP/IP protocols and do not operate above the physical and data link layers of the Open Systems Interconnection model, making their communications fairly simple. This means most assessment teams lack the knowledge of the specialized protocols to accurately assess the security of the ground segment communications. [42] Combating this requires the training of additional space control and cyber security personnel capable of assessing the space systems.

Cyber security personnel become a huge limiting factor for the evaluation of space systems in the Air Force. The Air Force maintains one active duty squadron whose mission contains cyber red teaming, but their mission almost exclusively supports the Air Warfare Center's exercises. The Air Force maintains another active duty squadron for cyber blue-

teaming (full knowledge network evaluations and audits), but this team also finds itself responsible for cyberspace incident forensics, taking away time from security evaluations.[43] There are supplemental Guard and Reserve units which augment these missions, but the pool of trained personnel remains small. The promise of CYBERCOM's plus up from the services of 2,000 additional cyber security personnel will alleviate the concern, but these forces will not come immediately trained and prepared for professional grade assessments initially due to the long lead time for developing cyber security professionals. A best estimate for this force puts an FY16 date at best for an operating capability truly supporting the services.[44]

An additional concern for space systems becomes the lack of resources from the space community for augmenting these evaluations. In specialized missions, such as satellite operations and SATCOM, cyber security personnel need augmentation from subject matter experts in the field ensuring the evaluators' assumptions and limitations have a basis in the reality of space operations. Without this space expertise cyber evaluators find themselves in the same position as the hackers who took control of Terra-EOS. Cyber evaluators can affect the cybersecurity of the ground system, but lack the knowledge of satellite operations to take the final steps.[45] There is no doubt an adversary would not make this mistake in wartime and would integrate its space and cyber warfare personnel to counter American space advantage.

NON-DoD RISK BASED EVALUATIONS FOR SPACE SYSTEMS

The current measures for the cyber-security of space systems seem prescriptive and regulation-based instead of adaptive in the highly dynamic cyber threat environment. The CNSSI 1253 provides 774 information security controls and sub-controls for organizations managing space systems to apply and implement.[46] From this list, high-security, and high operationally valuable systems like AFSCN and GPS ground systems must be independently

assessed at least once in each stage of their lifecycle, per CNSSI 1200. [47] Evaluations of long control lists become a tedious auditing process taking the focus off the true nature of the evaluation, assessing risk. The private sector provides excellent methods for analyzing system risk without enduring a heavy bureaucratic cost which can compromise the true intent of implementing a risk management framework.

SANS Institute Top 20 Critical Controls

There are several risk-based evaluation models available, but one of the most common and widely accepted models, due to its simplicity and applicability is the SANS Institute Top 20 Critical Security Controls. The System Administration, Audit, and Network Security (SANS) Institute, is a private research institute on network security and provider of highly technical vendor neutral cybersecurity training. The SANS Top 20 Critical Security Controls takes the 744 security controls of the CNSSI and boils them down to 20 simply controls, evident in all systems and builds an audit model for ensuring the security controls not only exist, but deliver on their security promises. Figure 2 Lists the Controls and maps them to CNSSI's parent document, the NIST 800-53 Risk Management Framework along with several other security frameworks. The SANS Institute maintains the application of these 20 controls eliminates the redundancy in government frameworks in an easily applicable manner.

The model calls for some very simple measures, such as taking inventories of all hardware and software in an organization as well as their configurations and missions (controls 1-3, and 10). The model addresses the need in acquisition for secure designs for systems in the form of security engineering and secure software builds (controls 6, 19). Then the model discusses control of access by individuals to the system in the form of controlled access to information, controlled access to network ports and wireless access points, control of administrative

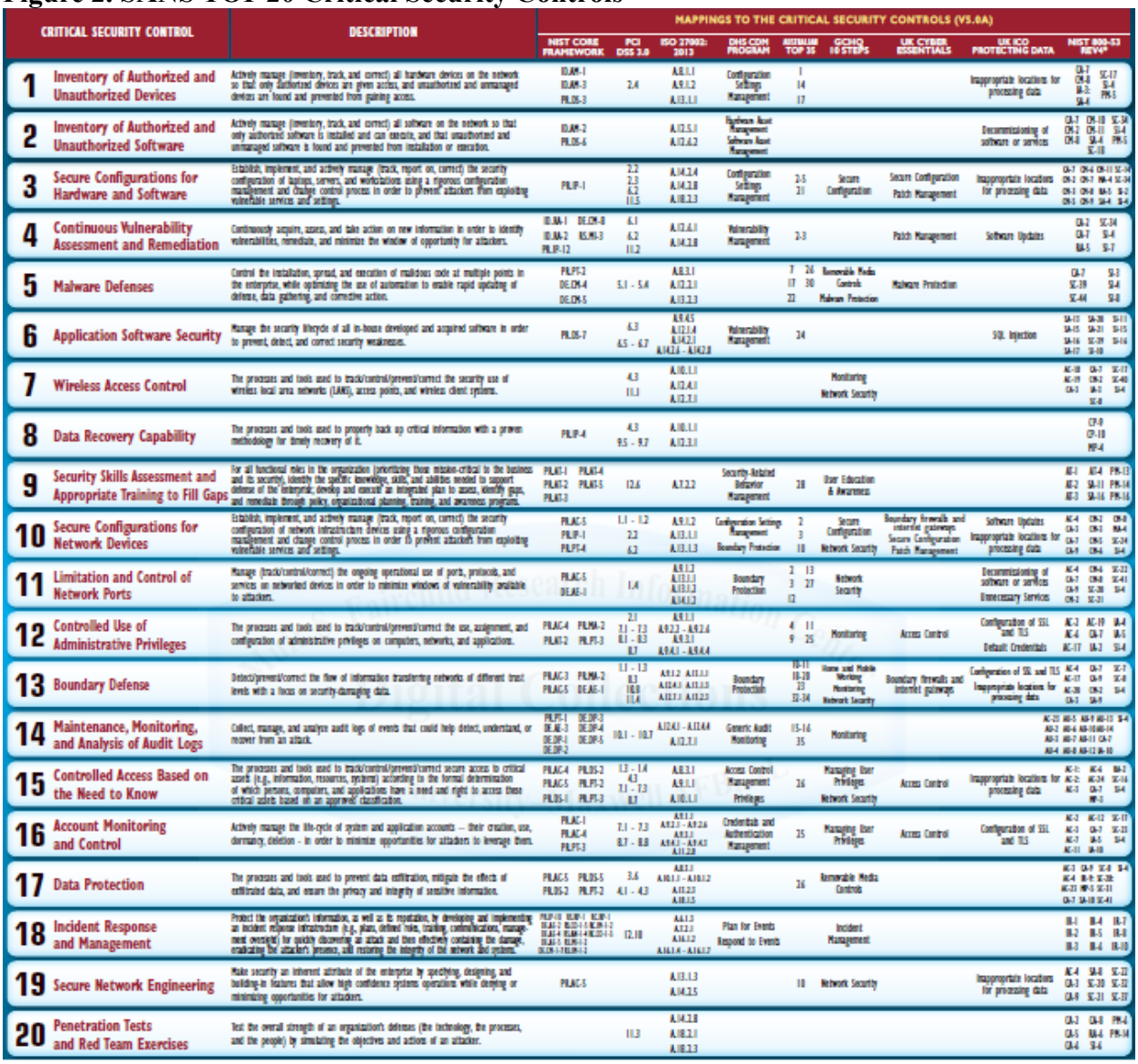
privileges, and "need to know" user access (controls 7, 11-12,15,17). Additionally, the model discusses technical controls used for secure implementation and modeling which include malware defenses, network boundary protection, data recovery capability and system audit log monitoring (controls 5, 8, 13, 14). The model addresses specific procedures needed in operations for ensuring continued cyber security by calling for continuous vulnerability assessment and remediation, incident response, and data recovery (controls 4,16, and 18). Finally, the model addresses the type of people and training needed for a secure system environment calling for security skills assessments and training gaps for all levels of personnel working on the system (control 9). [48] Implementing these measures would surely eliminate some of the confusion regarding the selection and implementation of controls.

The final control and probably the most important for space ground systems is penetration tests and red teaming (control 20). These consist of independent threat assessments of the entire environment with the goal of mimicking an attack from a known threat vector. Not to be confused with a risk assessment or an audit, a penetration test requires a certified team of cybersecurity and space experts breaking into the system. These testers will assess the network through other network connections, inserting their own malware, or social engineering their way to system access and gaining some level of control of the ground system, i.e. mimicking the attack on the Terra-EOS to gain control of satellite operations may be a penetration test goal. The level of effort and time this requires provides a good indication to a commander of how much cyber security risk the ground system contains. There are two unfortunate aspects of penetration tests. First, they are not fun for a system owner. The certified DoD Red Teams and penetration testing teams are extremely thorough, chaining disparate security flaws together into system access and greater intelligence on how the system operates than what system owners

thought was exposed.[49] Second, penetration testing, as discussed above, teams are a scarce DoD resource. As CYBERCOM stands up its Cyber Protection Teams, the penetration testing capabilities in DoD will increase, but the skills gap currently makes a long wait for penetration testing services of DoD space systems.[50]

The SANS Top 20 model applies very easily over the AFSCN and GPS control networks. The controls apply very well to how the systems are engineered and applied. Without getting bogged down in the details of the individual control numbers within the CNSSI 1253 and CNSSI 2000, the SANS Top 20 provides both space leadership and operators simple axioms for building cyber security into the system that the regulations themselves do not provide. Leadership can build metrics off this simple list, while the operators can develop their programs as robustly as they need to meet the overall intent. No doubt, this model would also lower the administrative overhead of selecting, tracking, and maintaining the security control program mandated in CNSSI 1253. This simplification would aid in overall compliance and security.

Figure 2. SANS TOP 20 Critical Security Controls[51]



CRITICAL SECURITY CONTROL	DESCRIPTION	MAPPINGS TO THE CRITICAL SECURITY CONTROLS (V5.0A)								
		NIST CORE FRAMEWORK	PCI DSS 3.0	ISO 27002: 2013	DHS CDM PROGRAM	AUSTRALIA TOP 35	GCHQ 10 STEPS	UK CYBER ESSENTIALS	UK ICO PROTECTING DATA	NIST 800-53 REV4*
1 Inventory of Authorized and Unauthorized Devices	Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.	ID.AM-1 ID.AM-3 PR.DS-3	2.4	A.8.1.1 A.9.1.2 A.13.1.1	Configuration Settings Management	1 14 17			Inappropriate locations for processing data	CA-7 CM-8 IA-3 SA-4 SC-17 SI-4 PM-5
2 Inventory of Authorized and Unauthorized Software	Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.	ID.AM-2 PR.DS-6		A.12.5.1 A.12.6.2	Hardware Asset Management Software Asset Management				Decommissioning of software or services	CA-7 CM-2 CM-8 CM-10 CM-11 SA-4 PM-5 SC-34 SI-4
3 Secure Configurations for Hardware and Software	Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.	PR.IP-1	2.2 2.3 6.2 11.5	A.14.2.4 A.14.2.8 A.18.2.3	Configuration Settings Management	2-6 31	Secure Configuration	Secure Configuration Patch Management	Inappropriate locations for processing data	CA-7 CM-2 CM-3 CM-6 CM-8 CM-9 MA-3 MA-4 SA-4 SC-34 SI-2
4 Continuous Vulnerability Assessment and Remediation	Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.	ID.RA-1 ID.RA-2 PR.IP-12 DE.CM-8 RS.MI-3	6.1 6.2 11.2	A.12.6.1 A.14.2.8	Vulnerability Management	2-3		Patch Management	Software Updates	CA-2 CA-7 RA-5 SC-34 SI-4 SI-7
5 Malware Defenses	Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.	PR.PT-2 DE.CM-4 DE.CM-5	5.1 - 5.4	A.8.3.1 A.12.2.1 A.13.2.3		7 17 22 26 30	Removable Media Controls Malware Protection	Malware Protection		CA-7 SC-18 SC-44 SI-3 SI-4 SI-8
6 Application Software Security	Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.	PR.DS-7	6.3 6.5 - 6.7	A.9.4.5 A.12.1.4 A.14.2.1 A.14.2.6 - A.14.2.8	Vulnerability Management	34			SQL Injection	SA-11 SA-15 SA-16 SA-17 SC-39 SI-10 SI-16
7 Wireless Access Control	The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANs), access points, and wireless client systems.		4.3 11.1	A.10.1.1 A.13.4.1 A.13.7.1			Monitoring Network Security			AC-18 AC-19 CA-3 CA-7 CM-2 SA-9 SC-8 SC-40 SI-4
8 Data Recovery Capability	The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.	PR.IP-4	4.3 9.5 - 9.7	A.10.1.1 A.12.3.1						CP-9 CP-10 MP-4
9 Security Skills Assessment and Appropriate Training to Fill Gaps	For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.	PR.AT-1 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5	12.6	A.7.2.2	Security-Related Behavior Management	28	User Education & Awareness			AT-1 AT-2 AT-3 AT-4 SA-11 SA-16 PM-13 PM-14 PM-16
10 Secure Configurations for Network Devices	Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.	PR.AC-5 PR.IP-1 PR.PT-4	1.1 - 1.2 2.2 6.2	A.9.1.2 A.13.1.1 A.13.1.3	Configuration Settings Management Boundary Protection	2 3 10	Secure Configuration Network Security	Boundary firewalls and internet gateways Secure Configuration Patch Management	Software Updates Inappropriate locations for processing data	AC-4 CA-3 CA-7 CA-9 CM-2 CM-6 CM-8 MA-4 SC-24 SI-4
11 Limitation and Control of Network Ports	Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.	PR.AC-5 DE.AE-1	1.4	A.9.1.2 A.13.1.1 A.13.1.2 A.14.1.2	Boundary Protection	3 13 27 12	Network Security		Decommissioning of software or services Unnecessary Services	AC-4 CM-6 CM-7 CM-8 SC-20 SC-21 SC-32 SC-41 SI-4
12 Controlled Use of Administrative Privileges	The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.	PR.AC-4 PR.AT-2 PR.MA-2 PR.PT-3	2.1 7.1 - 7.3 8.1 - 8.3 8.7	A.9.1.1 A.9.2.2 - A.9.2.6 A.9.3.1 A.9.4.1 - A.9.4.4		4 9 11 25	Monitoring	Access Control	Configuration of SSL and TLS Default Credentials	AC-2 AC-4 AC-17 AC-19 CA-7 IA-2 IA-5 SI-4
13 Boundary Defense	Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.	PR.AC-3 PR.AC-5 PR.MA-2 DE.AE-1	1.1 - 1.3 1.4 8.3 10.8 11.4	A.13.1.2 A.13.1.3 A.13.2.1 A.13.2.3 A.14.1.2 A.14.1.3	Boundary Protection	10-11 18-20 23 32-34	Home and Mobile Working Monitoring Network Security	Boundary firewalls and internet gateways	Configuration of SSL and TLS Inappropriate locations for processing data	AC-4 AC-17 AC-18 CA-3 CA-7 CA-9 CM-2 SC-7 SC-8 SI-4
14 Maintenance, Monitoring, and Analysis of Audit Logs	Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.	PR.PT-1 DE.AE-3 DE.DP-1 DE.DP-2 DE.DP-3 DE.DP-4 DE.DP-5	10.1 - 10.7	A.12.4.1 - A.12.4.4 A.12.7.1	Generic Audit Monitoring	15-16 35	Monitoring			AC-23 AU-2 AU-3 AU-4 AU-5 AU-6 AU-7 AU-8 AU-9 AU-11 AU-12 IR-4 IR-5 IR-8 CA-7
15 Controlled Access Based on the Need to Know	The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.	PR.AC-4 PR.AC-5 PR.DS-1 PR.DS-2 PR.PT-2 PR.PT-3	1.3 - 1.4 4.3 7.1 - 7.3 8.7	A.6.2.1 A.9.1.1 A.10.1.1	Access Control Management Network Privileges	26	Managing User Privileges Network Security	Access Control	Inappropriate locations for processing data	AC-1: AC-2: AC-3 AC-4 AC-6 CA-3 CA-7 IA-2 IA-4 SC-7 SC-16 SI-4 MP-3
16 Account Monitoring and Control	Actively manage the life-cycle of system and application accounts -- their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.	PR.AC-1 PR.AC-4 PR.PT-3	7.1 - 7.3 8.7 - 8.8	A.9.1.2 A.9.2.1 - A.9.2.6 A.9.3.1 A.9.4.1 - A.9.4.3 A.11.2.8	Credentials and Authentication Management	25	Managing User Privileges	Access Control	Configuration of SSL and TLS	AC-2 AC-3 AC-7 AC-11 AC-12 IA-5 IA-10 SC-17 SC-23 SI-4
17 Data Protection	The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.	PR.AC-5 PR.DS-1 PR.DS-2 PR.PT-2	3.6 4.1 - 4.3	A.8.3.1 A.10.1.1 - A.10.1.2 A.11.2.7 A.18.1.5		26	Removable Media Controls			AC-3 CA-7 IA-3 MP-2 MP-3 MP-4 MP-5 SC-8 SC-28 SC-31 SI-4 CA-7 IA-10 SC-41
18 Incident Response and Management	Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.	PR.IP-10 RC.RP-1 RC.IM-1 RC.IM-2 DE.AE-2 DE.AE-4 DE.AE-5 RS.MI-1 RS.MI-2 DE.CM-1 DE.DP-4	12.10	A.6.1.3 A.7.2.2 A.16.1.2 A.16.1.4 - A.16.1.7	Plan for Events Respond to Events		Incident Management			IR-1 IR-2 IR-3 IR-4 IR-5 IR-8 IR-10
19 Secure Network Engineering	Make security an inherent attribute of the enterprise by specifying, designing, and building-in features that allow high confidence systems operations while denying or minimizing opportunities for attackers.	PR.AC-5		A.13.1.3 A.14.2.5		10	Network Security		Inappropriate locations for processing data	AC-4 CA-3 CA-9 SA-8 SC-20 SC-21 SC-22 SC-32 SC-37
20 Penetration Tests and Red Team Exercises	Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.		11.3	A.14.2.8 A.18.2.1 A.18.2.3						CA-2 CA-5 CA-8 PM-6 PM-14 SI-6

The Quantitative Model: Time Based Security

The SANS Top 20 matches well against the risk management framework regulations, but like many security control models it only addresses the presence of controls first and does not quantify what those controls provide. The assessment of risk in the model remains qualitative. The risk in the Top 20 model becomes a subjective measure.[52]

A private-sector information security model, whose origins coincidentally reside in the DoD in the early 1990s, fixes the subjectivity issue of security controls by using a universal measure to quantify risk, time.[53] *Time-Based Security* by Winn Schwartau develops the idea of a simple mathematic formula for the evaluation of every security measure a system puts in place:

$$\mathbf{Protection_{time} > Detection_{time} + Response_{time}}$$[54]

Protection represents the time a security measure will provide before it becomes compromised, circumvented or destroyed. Detection represents the time it takes for the people monitoring the system to realize a compromise occurred. Response time represents the time it takes those people monitoring the system to do something about the compromise. So protection measures from every security control should provide more protection time than it takes for the people managing the system to detect and respond to what is happening. [55] Schwartau contends any system protection must test against this formula or it is useless.

For those who system owners looking for modernization like AFSCN and GPS who may not know what protections they need for an upgraded system, Schwartau recommends they assume there are no protections and determine against a live test how long detection and response take. From there building a protection scheme becomes easier and process improvements in detection and response also become easier. However, without quantitative data on how well security controls work against the specific expected threats there is no security.[56] Additionally the model provides a method for evaluating multiple controls in succession. For example, if the satellite control console is the target then each successive control preventing access to it is judged. A high-level example could test the time it takes attackers to: access to the base network, access to the satellite control network, and finally access of the console. Commanders then can make true risk-based decisions on whether they can afford additional

protections.

The major issue of a quantitative time-based model becomes the requirement for granular testing of every security control on an existing system. The importance of independent red teamers and network penetration testers becomes a limiting factor in this model. However, the promises of CYBERCOM's influx of trained personnel via Cyber Protection Teams may alleviate this human capital concern.[57]

The time-based method applies to new systems, but the selection of security controls becomes a tedious process if the system designers do not consider security at the outset of design. Then the selection of security controls in the time-based model may overwhelm system designers. Without an idea of what to protect in a new or modernized ground system the quantitative model only provides best guesses. The quantitative models work best in existing systems.

Preventative Security

A final model for risk-based evaluation of space ground systems comes from the leadership of the Air Force Laboratory which advocates a preventative mission assurance model. Dr. Kamal Jabbour advocates for a mission assurance model based on redefining cyberspace as anything processing a signal and then using the six steps of the information lifecycle: generation, processing, storage, communication, consumption, and destruction in evaluating the risk to the system. Unlike the other models which focus on detection and often the threat vector. Dr. Jabbour's model focuses on the vulnerability. Dr. Jabbour contends if one can build a system with no vulnerabilities of risk to the system in operation than one can maintain security. His "Science of Mission Assurance" reflects his background in engineering, which means his model works best for the initial build of systems and the acquisition model. [58]

For existing systems, this preventative model requires the re-engineering of communication channels. It does not provide adaptive methods for dealing with existing cyber security channels as those found in existing space systems. The preventative model in the future will become extremely viable for the modernization and re-engineering of the AFSCN ground station network architecture.[59] In the short term, though, Jabbour's model does little to address the security of systems currently in operation.

ANALYSIS AND RECOMMEDATIONS

Although DoD touted the implementation of the Risk Management Framework for its information technology and national security systems the effect on space systems is minimal. Unfortunately, CNSSI 1253 and CNSSI 2000 both make assumptions about the space segment being less vulnerable to cyber-attack and minimize the amount of controls necessary. These regulations make the governance of the ground segment much more difficult, by not specifically calling out a basic framework for satellite ground systems. Without a doubt, a cyber-attack on AFSCN or GPS during time of war would deny or delay the United States' access to satellite communications, imagery, or navigation and timing would eviscerate strategic advantage over an adversary. The CNSS should revisit both documents and assist system owners by base lining the requirements for satellite ground control stations and satellite receiver terminals ensuring maintenance of integrity in the ground stations.

Without specific regulatory guidance on the frequency of evaluations commanders and space ground system owners determine their own level of evaluation of their system. No one likes their practices, procedures and security being evaluated. Particularly, if those evaluations go poorly, it could cost an officer their career. This paradigm must change. Cyber evaluations need not be an "inspection" event. They can be a collaborative endeavor which builds on the

security of the overall network being evaluated. The United States Army does a good job of this with its regionally-based cyber assistance teams. These teams evaluate networks for a set period of time, then stay on-site with the system owners to come up with remediations and fixes for the system itself. [60] In its FY2014 annual report DOT&E reported this "find-and-fix" approach as a more successful approach to cyber security evaluations providing greater overall effectiveness in closing network security vulnerabilities. [61]

Highly critical ground systems, such as AFSCN and GPS must be the highest priorities for evaluation not just by the Air Force's cyber security evaluation teams, but also at the DoD level. The Air Force and CYBERCOM should alternate the evaluation of these systems each year, ensuring evaluation of ground systems on an annual basis. Space personnel should assist the teams as a "white cell" to provide insight on how the space components operate. One would much rather see an evaluation team break into a satellite and control its operation with a qualified satellite operator available, as opposed to the NASA Terra-EOS incident of 2008.[62] Finding these concerning vulnerabilities before a conflict is imperative in securing the US space advantage.

SATCOM terminals should receive far more rigorous evaluation prior to fielding. The Air Force and DoD should return these devices to the contractor upon discovery of glaring vulnerabilities built into the receivers. It is unacceptable for military personnel to use devices which are so easily manipulated through open-source research of the technical manuals on the devices.[63] One cannot underscore the importance of SATCOM in wartime for US advantage. Without properly evaluating the security of these devices, adversaries could leverage critical holes at the point of intersection between military data networks and satellite communications for espionage or worse disabling of communications on the battlefield.[64]

When evaluation teams measure the security of existing systems they must measure the security controls in place against time. The time-based security model allows system owners to measure their existing controls and evaluate their processes in improving the detection and response. The argument against time-based metrics contends that cyber intrusions happen in a matter of seconds. This may be true, but the intrusion itself may not truly hurt the system's operational effectiveness. A true implementation of time-based security measures how long it takes an adversary's intrusion onto a ground system network to actually affect the space asset's operational effectiveness or siphon data from the network.[65] This timeline typically could be much longer than the initial intrusion. Measuring time against the operational effects instead of network effects will focus the evaluation of the system to a more meaningful metrics assessing the risk to a system and the information therein. If it takes a penetration testing team two days of attempts, but three seconds to enter a system the protections worked for two days and three seconds. The question then becomes, how come the detection didn't see the attempted penetrations for the two days prior and the response time has to somehow reduce itself down to three seconds or less when the intrusion occurs. This requires extra work and thought by both cyber security evaluators and the responsible network operations personnel working with the space systems. However, one cannot argue the granularity provided by time-based measures in determining true risk.[66]

Finally, for modernization of existing space operations networks and the build out of new networks, AFSPC and DoD should use Dr. Jabbour's Mission Assurance model focusing on the removing vulnerabilities before they occur in systems.[67] This will require additional time in the design and testing phases of an already long acquisition process for space systems. However, the long-term benefit of space operations and satellite communications networks impervious to

cyber-attack will sustain the United States' space advantage going forward.

CONCLUSION

The cybersecurity of the United States' space ground systems should be a growing concern for the Air Force and DoD as a whole. The targeting of space ground systems by adversaries and independent security researchers increases each year. The vectors for initial cyber-attack remain constant, while the advanced targets evolve in sophistication when aimed at space systems. Unfortunately, the compliance culture of DoD and CNSS's Risk Management Framework for cyber security often exempts relevant controls or allows too much self-analysis of these critical systems. The unwieldy nature of the acquisition system means the contracts for space ground systems networks often did not consider cyber security, making updates much more difficult. Looking at the private sector one sees risk-based cyber security evaluation models which apply well to existing space systems simplifying the process and providing true quantitative evaluations of security. At least one model exists for the proper acquisition and engineering of cyber security into systems from the beginning.

The need exists for implementing the SANS Top 20 for reducing the overhead on security compliance and the time-based model for assessing the new controls for ensuring critical information and systems are protected. By implementing these measures with more frequent independent evaluations from integrated space and cyber security evaluations teams, and taking security engineering much more seriously on new and modernizations of ground systems the Air Force will assure the space advantage exists when the United States needs it most…wartime.

1. Department of Defense Instruction 8510.1, *Risk Management Framework for DoD Information Technology.* 12 March 2014. & Committee on National Security Systems Instruction 1200, *National Information Assurance Instructions for Space Systems Used to Support National Security Mission,* 7 May 2014.
2. Major Edward Chatters et al. *AU Space Primer* (AU Press, 2010). 153-155, 164
3. Air Force Satellite Control Network Program Office. *Air Force Satellite Control Network v5.1* (provided by Lt Col David Hanson, December 2014).
4. Lt Col David Hanson (Assistant Dean of Operations, Air Command and Staff College, former AFSCN site commander). Information provided to author via questions.
5. Lockheed Martin Homepage. "AFSCN CAMMO." http://www.lockheedmartin.com/us/products/space-ground-solutions/satellite-control-network-support-consolidation.html (accessed on 10 Jan 2014).
6. Jason Fritz, "Satellite Hacking Perplexed," *The Bulletin of the Centre for East-West Cultural and Economic Studies* 10, no. 1 (May 2013), 31-40
7. Air Force Satellite Control Network Program Office. *Air Force Satellite Control Network v5.1* (provided by Lt Col David Hanson, December 2014).
8. Lt Col David Hanson (Assistant Dean of Operations Air Command and Staff College, former AFSCN site commander). Information provided to author via questions.
9. The author evaluated cyber security ground system networks as part of his military experience and draws from these experiences in this reference. CW3 Anthony Hall, a SATCOM operator assisted in the translation during the months of March-April 2014.
10. Jason Fritz, "Satellite Hacking Perplexed," *The Bulletin of the Centre for East-West Cultural and Economic Studies* 10, no. 1 (May 2013), 32
11. Mandiant. *APT1: Exposing One of China's Cyber Espionage Units.* 18 Feb 2013. www.mandiant.com (accessed 1 Oct 2014), 24
12. Jason Fritz, "Satellite Hacking Perplexed," *The Bulletin of the Centre for East-West Cultural and Economic Studies* 10, no. 1 (May 2013), 33.
13. Director of Operational Test and Evalution, *FY2014 Annual Report.* http://www.dote.osd.mil/pub/reports/FY2014/ (accessed on 28 Jan 2015) 331, 335, 336.
14. Mandiant. *APT1: Exposing One of China's Cyber Espionage Units.* 18 Feb 2013. www.mandiant.com (accessed 1 Oct 2014),
15. The Open Web Application Security Project. *OWASP Top Ten 2013: Ten Most Critical Security Flaws on the Web*, 6, 9, 14.
16. Mandiant. *APT1: Exposing One of China's Cyber Espionage Units.* 18 Feb 2013. www.mandiant.com (accessed 1 Oct 2014), 28-30.
17. Director of Operational Test and Evalution, *FY2014 Annual Report.* http://www.dote.osd.mil/pub/reports/FY2014/ (accessed on 28 Jan 2015), 335
18. David Kushner. "The Real Story of STUXNET," *IEEE Spectrum*, 26 Feb 2013. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (Accessed on 20 Mar 2015).
19. Ellen Nakashima. "Defense Official Discloses Cyberattack," *Washington Post*. 24 Aug 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/08/24/AR2010082406495.html (Accessed on 20 Mar 2015).
20. David Kushner. "The Real Story of STUXNET," *IEEE Spectrum*, 26 Feb 2013.

http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (Accessed on 20 Mar 2015).
21. Mandiant. *APT1: Exposing One of China's Cyber Espionage Units.* 18 Feb 2013. www.mandiant.com (accessed 1 Oct 2014), 24-36
22. Jason Fritz, "Satellite Hacking Perplexed," *The Bulletin of the Centre for East-West Cultural and Economic Studies* 10, no. 1 (May 2013), 33
23. Ibid, 32-33
24. David Brumley et al. *GPS Software Attacks*. Association of Computing Machinery: Computer and Communication Security Conference 2012, 16-18 October 2012 (accessed 25 Feb 2015). 7-9
25. Ruben Santamarta, *SATCOM Terminals: Hacking by Air, Sea, and Land*. IOActive Security Services. August 2014, 8, 10-12, 16, 19-21.
26. Ibid, 8.
27. Department of Commerce, *OIG-14-027M: Expedited Efforts Needed to Remediate High-Risk Vulnerabilities in the Joint Polar Satellite System's Ground System.* Office of the Inspector General's Report (Washington DC, 21 September 2014) 2-5.
28. Mary Pat Flaherty, Lisa Rein , and Jason Samenow. "Chinese Hack U.S. Weather Systems, Satellite Network", *Washington Post*, 12 November 2014. http://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html (Accessed 17 January 2015).
29. Ibid.
30. Department of Defense Instruction 8510.1, *Risk Management Framework for DoD Information Technology.* 12 March 2014, 16.
31. Department of Defense Instruction 8510.1, *Risk Management Framework for DoD Information Technology.* 12 March 2014, 4,6.
32. Committee on National Security Systems Instruction 1253, *Security Categorization and Control Selection for National Security Systems – Space Platform Overlay,* 27 March 2014, Attachment 2 to Appendix F, 1-33.
33. Ibid, 1 (Footnote 2).
34. Committee on National Security Systems Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, 27 March 2014. 3-7.
35. Committee on National Security Systems Instruction 1200, *National Information Assurance Instructions for Space Systems Used to Support National Security Mission,* 7 May 2014.
36. Department of Defense Instruction 8510.1, *Risk Management Framework for DoD Information Technology.* 12 March 2014. & Committee on National Security Systems Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, 27 March 2014.
37. Committee on National Security Systems Instruction 1200, *National Information Assurance Instructions for Space Systems Used to Support National Security Mission,* 7 May 2014. D-1, D-2.
38. Department of Defense Instruction 8510.1, *Risk Management Framework for DoD Information Technology.* 12 March 2014, 12, 13, 25, 37.
39. Department of Defense Instruction 8510.1, *Risk Management Framework for DoD Information Technology.* 12 March 2014, 37.

40. Committee on National Security Systems Instruction 1200, *National Information Assurance Instructions for Space Systems Used to Support National Security Mission,* 7 May 2014. 7,J-1.
41. Committee on National Security Systems Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, 27 March 2014. 1, 7, D-1, J-1 & Committee on National Security Systems Instruction 1200, *National Information Assurance Instructions for Space Systems Used to Support National Security Mission,* 7 May 2014, 1.
42. Committee on National Security Systems Instruction 1200, *National Information Assurance Instructions for Space Systems Used to Support National Security Mission,* 7 May 2014, 7.
43. Osborne, Casey. "The Skulls of the 92nd: Defending the front lines of cyber warfare." http://www.24af.af.mil/news/story.asp?id=123307567 (accessed 20 March 2015).
44. Maj Gen Brett Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly,* 73, 2nd Quarter 2014, 15-17.
45. Jason Fritz, "Satellite Hacking Perplexed," *The Bulletin of the Centre for East-West Cultural and Economic Studies* 10, no. 1 (May 2013), 32-33.
46. Committee on National Security Systems Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, 27 March 2014. D-1- D-35.
47. Committee on National Security Systems Instruction 1200, *National Information Assurance Instructions for Space Systems Used to Support National Security Mission,* 7 May 2014, 6.
48 SANS Institute. *SANS Top 20 Critical Security Controls version 5.* Fall 2014. https://www.sans.org/critical-security-controls/ (Accessed 15 December 2014).
49. Director of Operational Test and Evalution, *FY2014 Annual Report.* http://www.dote.osd.mil/pub/reports/FY2014/ (accessed on 28 Jan 2015), 332-335.
50. Maj Gen Brett Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly,* 73, 2nd Quarter 2014, 14.
51. SANS Institute. *SANS Top 20 Critical Security Controls version 5.* Fall 2014. https://www.sans.org/critical-security-controls/ (Accessed 15 December 2014).
52. SANS Institute. *SANS Top 20 Critical Security Controls version 5.* Fall 2014. https://www.sans.org/critical-security-controls/ (Accessed 15 December 2014).
53. Winn Schwartau, *Time Based Security* (Interpact Press, Seminole, FL, 1999), v-vii.
54. Ibid, 41.
55. Ibid, 33-39.
56. Ibid, 41-53.
57. Maj Gen Brett Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly,* 73, 2nd Quarter 2014, 14-17, 19.
58. Kamal Jabbour, "The Science of Mission Assurance," *Journal of Strategic Security* IV, 2 (2011), 64, 66-71.
59. Kamal Jabbour, "The Science of Mission Assurance," *Journal of Strategic Security* IV, 2 (2011), 62, 66-67.
60. The author's experience working network evaluations on Army networks noted an apparent desire for "Find-Fix" teams. The author juxtaposes this against his experience on Air Force networks which was adversarial due to the impression of the evaluation team as inspectors providing a report.
61. Director of Operational Test and Evalution, *FY2014 Annual Report.* http://www.dote.osd.mil/pub/reports/FY2014/ (accessed on 28 Jan 2015), 335, 337.

62. Jason Fritz, "Satellite Hacking Perplexed," *The Bulletin of the Centre for East-West Cultural and Economic Studies* 10, no. 1 (May 2013), 33.
63. Ruben Santamarta, *SATCOM Terminals: Hacking by Air, Sea, and Land*. IOActive Security Services. August 2014, 1-26.
64. Major Bryan Eberhardt et al. *AU Space Primer* (AU Press, Maxwell AFB, AL, 2010). 183, 186-187
65. Winn Schwartau, *Time Based Security* (Interpact Press, Seminole, FL, 1999), 55-60.
66. Ibid, 5-76
67. Kamal Jabbour, "The Science of Mission Assurance," *Journal of Strategic Security* IV, 2 (2011), 60-71.

BIBLIOGAPHY

Air Force Satellite Control Network Program Office. *Air Force Satellite Control Network v5.1* Diagram.

APT1: Exposing One of China's Cyber Espionage Units. Mandiant Security Services Whitepaper, 18 Feb 2013, www.mandiant.com (accessed 1 Oct 2014).

Brumley, David et al. *GPS Software Attacks*. Association of Computing Machinery: Computer and Communication Security Conference 2012, 16-18 October 2012 (accessed 25 Feb 2015).

Cateledge, Burton, Chatters, Edward, Eberhardt Bryan et al. *AU Space Primer* Maxwell AFB: AU Press, 2010.

Committee on National Security Systems Instruction 1200, *National Information Assurance Instructions for Space Systems Used to Support National Security Mission,* 7 May 2014.

Committee on National Security Systems Instruction 1253, *Security Categorization and Control Selection for National Security Systems – Space Platform Overlay,* 27 March 2014.

Committee on National Security Systems Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, 27 March 2014.

Department of Defense Instruction 8510.1, *Risk Management Framework for DoD Information Technology.* 12 March 2014.

Director of Operational Test and Evalution, *FY2014 Annual Report.* Washington D.C.: Department of Defense, http://www.dote.osd.mil/pub/reports/FY2014/ (accessed on 28 Jan 2015).

Flaherty, Mary Pat, Rein, Lisa, and Samenow, Jason. "Chinese Hack U.S. Weather Systems, Satellite Network", *Washington Post*, 12 November 2014. http://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html (Accessed 17 January 2015).

Fritz, Jason. "Satellite Hacking Perplexed," *The Bulletin of the Centre for East-West Cultural*

and Economic Studies 10, no. 1 (May 2013).

Jabbour, Kamal. "The Science of Mission Assurance," *Journal of Strategic Security* IV, 2, 2011.

Kushner, David. "The Real Story of STUXNET," *IEEE Spectrum*, 26 Feb 2013. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (Accessed on 20 Mar 2015).

Lockheed Martin Homepage. "AFSCN Consolidation (CAMMO)," http://www.lockheedmartin.com/us/products/space-ground-solutions/satellite-control-network-support-consolidation.html (accessed on 10 Jan 2014).

Nakashima, Ellen. "Defense Official Discloses Cyberattack," *Washington Post*. 24 Aug 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/08/24/AR2010082406495.html (Accessed on 20 Mar 2015).

Office of the Inspector General. *OIG-14-027M: Expedited Efforts Needed to Remediate High-Risk Vulnerabilities in the Joint Polar Satellite System's Ground System.* Washington D.C. : Department of Commerce, 21 September 2014

Osborne, Casey. "The Skulls of the 92nd: Defending the front lines of cyber warfare." http://www.24af.af.mil/news/story.asp?id=123307567 (accessed 20 March 2015).

OWASP Top Ten 2013: Ten Most Critical Security Flaws on the Web, Open Web Application Security Project.

SANS Institute. *SANS Top 20 Critical Security Controls version 5.* Fall 2014. https://www.sans.org/critical-security-controls/ (Accessed 15 December 2014).

Santamarta, Ruben. *SATCOM Terminals: Hacking by Air, Sea, and Land*. IOActive Security Services, August 2014.

Schwartau, Winn. *Time Based Security.* Interpact Press, Seminole, FL, 1999.

Williams, Brett. "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly,* 73, 2nd Quarter 2014.