CENTER FOR SPACE POLICY AND STRATEGY

NOVEMBER 2019

DEFENDING SPACECRAFT IN THE CYBER DOMAIN

BRANDON BAILEY, RYAN J. SPEELMAN, PRASHANT A. DOSHI,
NICHOLAS C. COHEN, AND WAYNE A. WHEELER
THE AEROSPACE CORPORATION

AEROSPACE

BRANDON BAILEY

Brandon Bailey is a cybersecurity senior project leader at The Aerospace Corporation. He has more than 14 years of experience supporting the intelligence and civil space arena. Bailey's specialties include vulnerability assessments/penetration testing for space systems and infusing secure coding principles within the software supply chain. Before joining Aerospace, Bailey worked for NASA, where he was responsible for building and maintaining a software testing and research laboratory to include a robust cybersecurity range as well as spearheading innovative cybersecurity assessments of ground infrastructure that support NASA's mission operations. While at NASA, Bailey was honored with several group and individual awards, including NASA's Exceptional Service Medal for his landmark cybersecurity work, NASA's Early Career Achievement Award, and NASA Agency Honor Awards for Information Assurance/Cybersecurity. He has also contributed to teams who have received honorable mention in the 2012 and 2016 NASA's Software of the Year competition. Bailey graduated summa cum laude with a bachelor's degree in electrical engineering from West Virginia University and currently holds multiple certifications in the cybersecurity field.

RYAN J. SPEELMAN

Ryan J. Speelman is the principal director for the Cyber Security Subdivision at The Aerospace Corporation, where he is focused on the security of space-based systems. The organization he leads is involved in many layers of space cybersecurity from legacy system protection to requirements and program development to advanced research and development techniques. Prior to joining the Cyber Security Subdivision, Speelman spent more than a decade in wireless communications, where he worked on many programs focusing on digital signal processing algorithms and radio frequency–based electronic warfare. He holds both a bachelor's degree and a master's degree in electrical engineering from UCLA.

PRASHANT A. DOSHI

Prashant A. Doshi is the associate principal director of the Cybersecurity Subdivision at The Aerospace Corporation. Doshi has spent 15 years of experience supporting the DOD, intelligence community, and civil space programs. Doshi's focus areas are the application of novel computing technologies to challenging space enterprise problems. Doshi holds a bachelor's degree and a master's degree in electrical and computer engineering from Georgia Tech.

NICHOLAS C. COHEN

Nicholas C. Cohen is a member of the Cyber Defense Solutions Department at The Aerospace Corporation. He contributes to national space cybersecurity in a range of areas, including defensive cyber operations, spacecraft cybersecurity, software assurance, and penetration testing. He currently leads a team developing a toolkit called Eirene Sceptre, which provides targeted space system cyber defense. Prior to joining Aerospace, Cohen operated his own Internet service provider and learned how to defend servers against attackers on the Internet. Cohen has a bachelor's degree from Carnegie Mellon University, and a master's degree in electrical and computer engineering from Georgia Tech.

WAYNE A. WHEELER

Wayne A. Wheeler is a senior project leader in the Cybersecurity Subdivision at The Aerospace Corporation. Wheeler has extensive experience leading space architectures development, with a focus on networks and cyber. His recent research focuses on space systems resilience to broad range threats, and advanced cyber protections for spacecraft.

ABOUT THE CENTER FOR SPACE POLICY AND STRATEGY

The Center for Space Policy and Strategy is dedicated to shaping the future by providing nonpartisan research and strategic analysis to decisionmakers. The center is part of The Aerospace Corporation, a nonprofit organization that advises the government on complex space enterprise and systems engineering problems.

Contact us at www.aerospace.org/policy or policy@aero.org

Summary

Space systems comprise many government and commercial components where cybersecurity and space operations are inextricably linked. The vulnerability of satellites and other space assets to cyberattack is often overlooked in wider discussions of cyber threats to critical national infrastructure. Neither space policy nor cybersecurity policy is prepared for the challenges created by the meshing of space and cyberspace, especially for the spacecraft. With the emerging cyber threats to spacecraft from nation-state actors, additional spacecraft defenses must be implemented. Historically spacecraft have been considered relatively safe from cyber intrusions; however, recent emerging threats have brought spacecraft into play as a direct target of an adversary. While space-centric cybersecurity standards and governance are lacking, utilizing defense-in-depth techniques for spacecraft protection will help ensure the spacecraft is resilient to a cyber intrusion. To meet the space cyber challenges, government, industry, and international action is needed. The way forward and potential solutions will include increased cooperation across all sectors and will require a blend of policy and technical solutions. This paper focuses on principles (e.g., onboard intrusion detection and prevention systems, hardware/software supply chain, and onboard logging) that aim to provide decisionmakers, acquisition professionals, program managers, and system designers alike with considerations while acquiring and designing cyber-resilient spacecraft.

Introduction

From commercial markets to militaries, the western world is dependent on space systems. This dependence has led nation-states to develop offensive capabilities targeting those systems.[1] Although many emerging threats to space exist, this paper focuses on cyber for several reasons: the potentially high impact relative to cost, the ability to simultaneously target multiple missions, the difficulty of attribution, and the potential to reduce defensive reaction time. These reasons make a cyberattack on a spacecraft enticing to bad actors. Further complicating the problem is the increasingly intertwined nature of commercial and military assets. Nation-states and non-state actors alike are targeting space systems via cyber. While research and open source intelligence on the vulnerabilities of space systems increases, so are the attacks. In recent years, researchers have published proof of concepts attacking satellite communication and the Iridium satellite network.[2,3] Abstaining from action is not an option, and it is necessary for all national critical space systems to be appropriately hardened against cyber threats.

The U.S. federal governance structure for general information technology (IT)-based cybersecurity has made strides in recent years with the maturation of the National Institute of Standards and Technology (NIST) Risk Management Framework and Cybersecurity Framework. However, the same cannot be said for the space domain. NIST cybersecurity maturity standards and guidelines help organizations to improve their cybersecurity measures and best practices, but these are not directly applicable to the space domain. While efforts have been made to mold these frameworks for space systems (e.g., Committee on National Security Systems [CNSS] Instruction [CNSSI] 1253F), uniformity is lacking, and updated standards and guidelines for spacecraft are likely warranted. There are pockets of initiatives across the space community that are addressing cybersecurity for space systems. A space system comprises and should have cybersecurity protections applied to all four segments: space, ground, link, and user (see Figure 1); however, most work in this area focuses on the ground segment with little research or guidance on securing the space segment (i.e., spacecraft).

Table 1 outlines some of the known initiatives and standards that have been published relating to cybersecurity within the space domain. Limited published work is available for reference; however, the report *Cyber Enhanced Space Operations* recommends several strategies for more secure space systems and operations.[4] Other nonpublished initiatives are underway within the federal government (e.g., Jet Propulsion Laboratory's Cybersecurity Improvement Project), but at this point all these initiatives are too early to reference as adopted practices and mostly focus on the ground

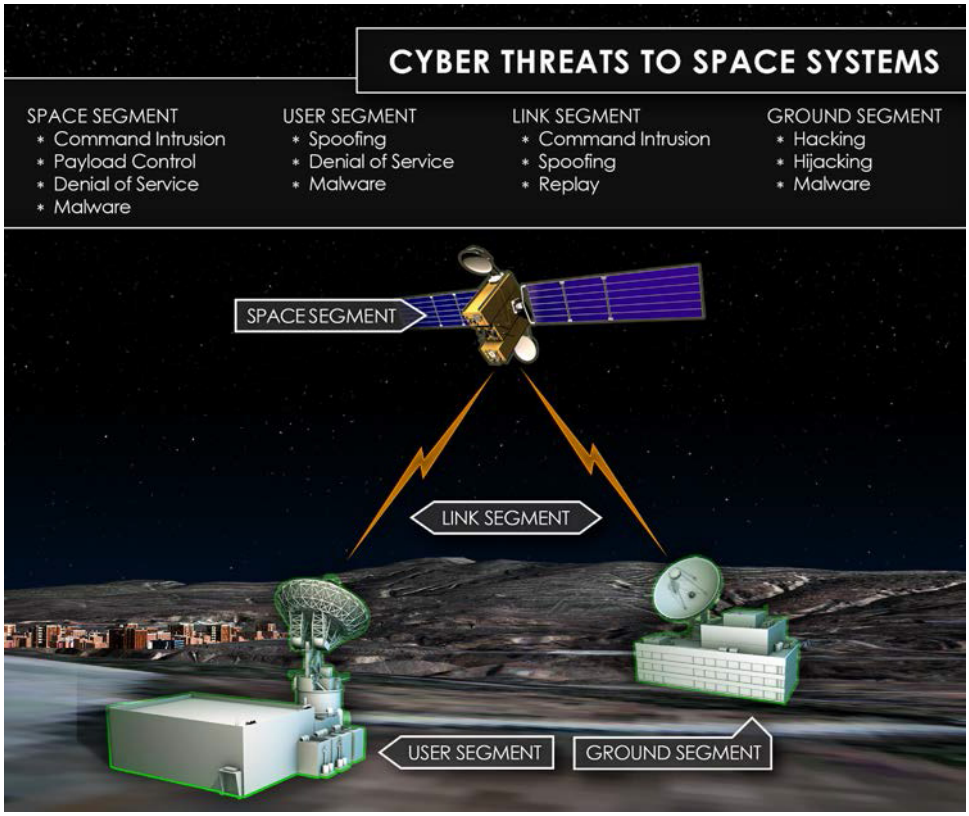

Figure 1: Cyber threats identified by the National Air and Space Intelligence Center (NASIC).[12]

Table 1: Known Cybersecurity Initiatives and Standards				
Organization	**Title of Standard**	**Applicability/ Scope**	**Link to Standard**	**Description of Standard**
CNSS	CNSSI 1200 National Information Assurance Instruction for Space Systems Used to Support National Security Missions	Ground and spacecraft for National Security System (NSS) only	https://www.cnss.gov/CNSS/issuances/Instructions.cfm	This standard elaborates on how to appropriately integrate information assurance (IA) into the planning, development, design, launch, sustained operation, and deactivation of those space systems used to collect, generate, process, store, display, or transmit national security information, as well as any supporting or related national security systems.
CNSS	CNSSI 1253F Attachment 2 Space Platform Overlay	Unmanned spacecraft for NSS only	https://www.cnss.gov/CNSS/issuances/Instructions.cfm	This overlay applies to the space platform portion of all space systems that must comply with CNSS Policy No. 12. The controls specified in this overlay are intended to apply to the space platform after it is launched and undergoing pre-operational testing and during operation. This overlay attempts to mold NIST 800-53 for the space segment.
Consultative Committee for Space Data Systems (CCSDS)	352.0-B Cryptographic Algorithms	Civilian space communications	https://public.ccsds.org/Pubs/352x0b2.pdf	This standard provides several alternative authentication/integrity algorithms that may be chosen for use by individual missions depending on their specific mission environments. It does not specify how, when, or where these algorithms should be implemented or used. Those specifics are left to the individual mission planners based on the mission security requirements and the results of the mission risk analysis.
Consultative Committee for Space Data Systems	355.0-B Space Data Link Security (SDLS) Protocol	Civilian space communications	https://public.ccsds.org/Pubs/355x0b1.pdf	This protocol provides a security header and trailer along with associated procedures that may be used with the CCSDS Telemetry, Telecommand, and Advanced Orbiting Systems Space Data Link Protocols to provide a structured method for applying data authentication and/or data confidentiality at the data link layer.
Consultative Committee for Space Data Systems	356.0-B Network Layer Security	Civilian space communications	https://public.ccsds.org/Pubs/356xb1.pdf	This standard provides the basis for network layer security for space missions utilizing the Internet protocol (IP) and complying with IP over CCSDS space links.
Consultative Committee for Space Data Systems	357.0-B Authentication Credentials	Civilian space communications	https://public.ccsds.org/Pubs/357x0b1.pdf	In the CCSDS space environment, credentials are needed to allow communicating entities to authenticate each other to determine potential authorization and access control actions. CCSDS recommends two types of credentials in this standard: X.509 certificates and protected simple authentication.
Aerospace Industries Association	NAS9933 Critical Security Controls for Effective Capability in Cyber Defense	Department of Defense (DOD) Aerospace contractors enterprise/ground infrastructure	http://www.aia-aerospace.org/wp-content/uploads/2018/12/AIA-Cybersecurity-standard-onepager.pdf	The goal of this standard is to align the fragmented and conflicting requirements that the DOD contracting process imposes on industry. Rather than different DOD organizations using different tools to assess a company's security across different contracts, this standard is designed to apply common and universal elements of cybersecurity across each enterprise.

Committee on National Security Systems (CNSS) provides a forum for the discussion of policy issues and is responsible for setting national-level cybersecurity policies, directives, instructions, operational procedures, guidance, and advisories for U.S. government departments and agencies for the security of National Security Systems (NSS) through the CNSS Issuance System.

Consultative Committee for Space Data Systems (CCSDS) develops communications and mission operation standards that support inter- and intra-agency operations and cross support. CCSDS standards include elements of flight and ground systems that are developed and operated by different agencies and organizations. The security working group within CCSDS believes the security risks to both spacecraft and ground systems have increased to the point where CCSDS must adopt existing or develop (as necessary) information security standards in order to protect both flight and ground mission-critical resources and protect sensitive mission information.

Aerospace Industries Association (AIA) represents manufacturers and suppliers of civil, military, and business aircraft, helicopters, UAVs, space systems, aircraft engines, missiles, material, and related components, equipment, services, and information technology in the United States. AIA receives its policy guidance from the direct involvement of chief executive officers of companies of all sizes across all levels of the aerospace industry.

segment. The published security standards listed in the table range from high-level compliance controls to low-level communication protocol standards and are not overarching engineering principles for a spacecraft which is the focus of this paper.

In addition to standards, overarching governance and policies lack the necessary integration between cybersecurity and the space domain. As described by the University of Maryland – School of Public Policy, governance efforts in the space and cyber domains are highly siloed, which may limit meaningful progress.[5] In their research only one strategy document, National Cyber Strategy, published in 2018, provided any mention of improving cybersecurity in the space domain. Similarly, research from Chatham House describes the deficiencies on a global scale in relation to the North Atlantic Treaty Organization (NATO) and how it needs to establish a NATO Space Policy.[6] As these and others have pointed out policy and governance challenges, few publications are solutions oriented as related to reducing cyber risk to space systems, specifically the spacecraft. In lieu of structured governance and standards being available, this paper discusses a threat-based approach to managing cyber risk to spacecraft, including examples of how to apply defense-in-depth (DiD) principles to reduce the risk of cyberattack on a spacecraft. These principles should provide decisionmakers, acquisition professionals, program managers, and system designers alike with considerations while acquiring and designing cyber-resilient spacecraft.

Figure 2 shows the continuum of reversible to nonreversible attack types against spacecraft. Cyberattacks on spacecraft could come in many flavors and depend greatly on the adversary's access and goals. Potential attacks targeting ground stations could result in a breach of the confidentiality or integrity of the downlinked data or potentially the satellite being disabled, destroyed, or deemed unreliable. Attacks against the supply chain could result in a different, more limited set of attacks against the satellites. A range of scenarios exists, and each would have unique impacts on the adversary's options. Some of these scenarios result in irreversible damage while others result in loss of mission time and/or degraded future operations. The more an adversary can sow doubt in our space systems, the greater the impact on our military/economic systems.

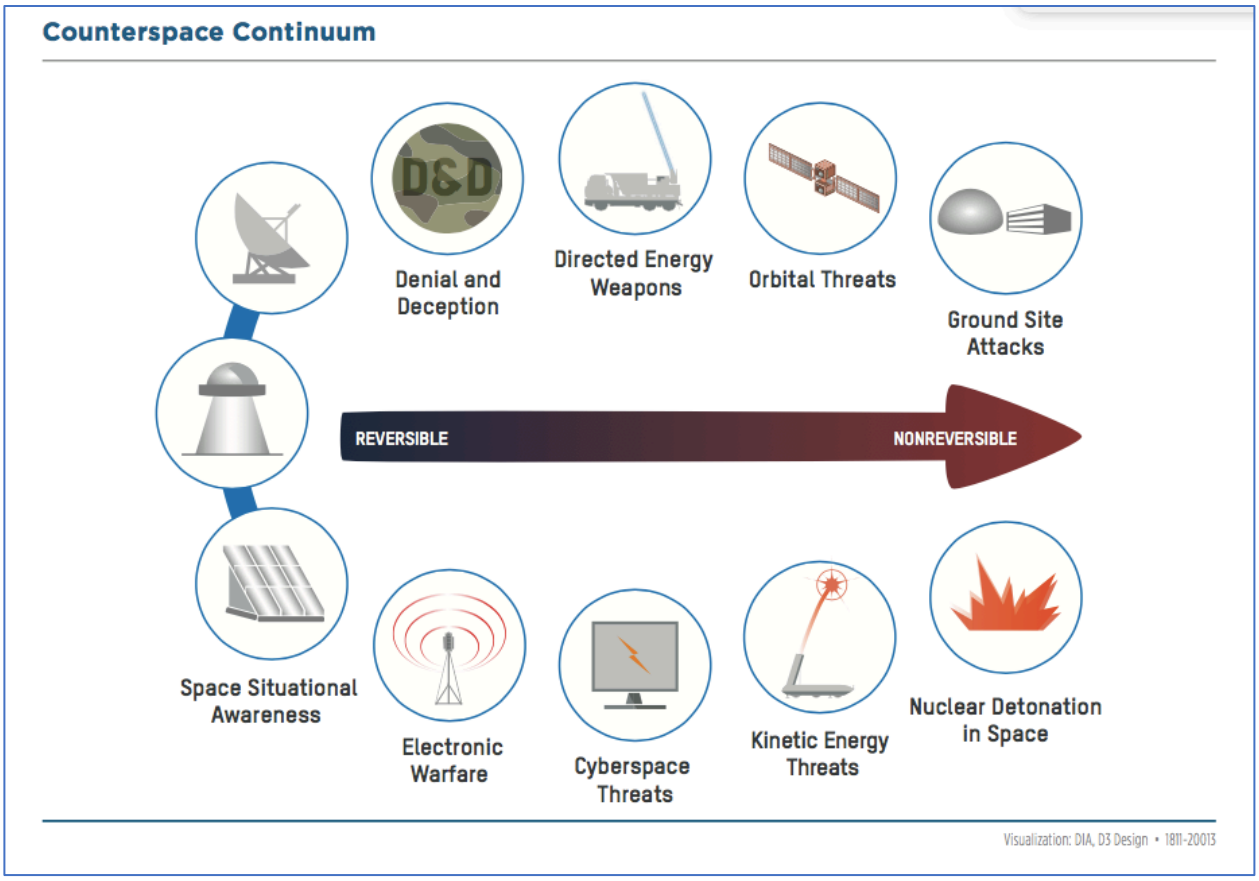

Figure 2: Counterspace continuum showing range of attacks to spacecraft including cyberspace attacks.[1]

Traditional View and Current Design Practices

Many assume that DOD satellites are generally well protected against cyberattacks (depending on their age, orbit, and access). In the commercial satellite world, this is thought to not be the case, even though increasingly they are being used for military purposes.[7] Commercial satellites do not require the same level of governance as satellites in the DOD and civilian sectors, and they do not have standardized security. Traditionally within the DOD, civilian, and commercial space sectors, complacency and misunderstandings about cyber vulnerabilities for spacecraft are widespread. In all three sectors, spacecraft have been built assuming a very limited range of cyber threats. Furthermore, most spacecraft architectures, subsystems, and supply chains were developed before current cyber threats were envisioned. Traditionally, cybersecurity for space systems has concentrated on the ground segment with minimal, if any, cyber protections onboard the spacecraft. There are several reasons why spacecraft themselves have been assumed off limits for cyberattacks:

- Spacecraft architectures are built using unique hardware/software that is not susceptible to common computer malware.
- Spacecraft have communications only with protected ground infrastructure that is "air gapped" from the commercial Internet, so they cannot be cyberattacked by external adversaries.

- Physical access to spacecraft once launched is highly unlikely.

- DOD spacecraft are developed, manufactured, and launched by cleared defense contractors, with closed supply chains presumed to be inaccessible to potential adversaries. Additionally, strong National Security Agency (NSA)-approved encryption on DOD spacecraft uplinks/downlinks means that data cannot be exposed to or manipulated by adversaries.

Due to these factors, cyber concerns have historically focused mostly on electronic warfare threats such as jamming, which is a classic denial of service attack; spoofing, where adversaries attack sensors and/or position receivers; or replay attacks, where a valid command or telemetry sequence is recorded and replayed to cause an effect. Jamming can be partially mitigated by such techniques as hardening the physical layer communication waveform or increasing the link margin. Spoofing and replay attacks, on the other hand, have been traditionally dealt with by utilizing proper authentication.

Better understanding of cyber threats has led to a realization that systems may be vulnerable despite the traditional assumptions. For example, motivated adversaries may develop highly targeted malware, assumptions about isolated networks may be invalid, and adversaries may breach development environments and supply chains.

Similar misconceptions with cyberattacks were made with industrial control systems (ICSs). An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, and pneumatic) that act together to achieve an industrial objective (e.g., manufacturing and transportation of matter or energy). ICS environments were thought to be unsusceptible to cyberattacks due to some of the same reasons as spacecraft: closed supply chains, unique embedded hardware/software systems, "air-gapped," and physical protections. These same misconceptions have resulted in vulnerabilities in ICS, which have documented intrusions using similar attack vectors that are mentioned in subsequent sections of this paper. These ICS cyberattacks have not only resulted in millions of dollars in physical damages, they have also resulted in the loss of life. Compromising the hardware and software supply chains, jumping air-gapped networks, and compromising cryptography have been successfully executed in the ICS-embedded world, and space systems could fall victim to similar attacks if proper protections are not taken.[8]

"There is a clear trend toward lower barriers to access, and widespread vulnerabilities coupled with reliance on relatively unsecured commercial space systems create the potential for non-state actors to carry out some counter-space cyber operations without nation-state assistance. However, while this threat deserves attention and will likely grow in severity over the next decade, there remains a stark difference at present between the cyber attacks capabilities of leading nation-states and other actors."

—Global Counterspace Capabilities:
An Open Source Assessment[10]

The Emerging Threat in Cyberspace

Cyber capabilities of nation-states have increased in recent years.[1] Cyber threats pose a significant and complex challenge due to the absence of a warning and speed of an attack by an adversary, the difficulty of attribution, and the complexities associated with carrying out a proportionate response.[6] The "2019 Global Threat Report" from CrowdStrike® says, "Nation-state adversaries were continuously active throughout 2018—targeting dissidents, regional adversaries and foreign powers to collect intelligence for decisionmakers." In terms of sheer speed, Russian hackers are now able to complete a major system breach in less than 19 minutes, 8 times faster than their nearest competitors in North Korea.[9] While this data is not space system-specific, it points to the fact of increasing speed and capabilities. With the adversaries' increasing desire and capabilities to disrupt our space systems accompanied with our dependence on space for critical capabilities, spacecraft cybersecurity protections should be a high priority. In fact, various open source reports exist suggesting that nation-states and other actors are already attempting cyber intrusions into government spacecraft assets.[1,11] Government assets are not alone in being a target; given the reliance of the military on commercial satellites to augment bandwidth, cyberattacks on commercial space systems are also a concern. As stated by Secure World Foundation, "A growing number of non-state actors are actively probing commercial satellite systems and discovering cyber vulnerabilities that are similar in nature to those found in non-space systems. This indicates that manufacturers and developers of space systems may not yet have reached the same level of cyber hardness as other sectors."[10] With the expanding list of threat actors and increase in awareness of vulnerabilities and adversary capabilities, all sectors of the space domain need to invest in improving the cybersecurity of space systems, especially onboard the spacecraft. Figure 1 (presented earlier) provides an overview of the current cyber threat landscape for space systems. Although this paper focuses on the spacecraft, it is important to understand the broader context and attack vectors.

With the everchanging threat landscape within the space domain, it is important to rethink the assumptions that civilian, commercial, and DOD spacecraft are safe from cyberattacks. Spacecraft being developed today need to be resilient to attacks 10 to 20 years in the future.[13]

In the supply chain alone, several potential entrance points exist. For example, spacecraft may utilize third-party intellectual property and/or open source software or firmware with unknown vulnerabilities or implants. As spacecraft become more complex and timelines for development shrink, less attention and scrutiny may be applied to the software supply chain. It is true that spacecraft are not flying and will not fly traditional commercial IT components such as servers and Ethernet switches and, therefore, are not susceptible to most forms of malware. However, nation-state actors have the motivation and means to fund development of specially designed malware to target the components that are flown on spacecraft. Nation-state actors have already demonstrated this in the ICS realm with the malicious computer worm called Stuxnet, which targeted Iran's nuclear program. It was specially crafted malware for a particular embedded logic controller that was connected to uranium centrifuges.

The hardware supply chain is another high-probability entrance point for an adversary. Due to the economy of silicon manufacturing, hardware fabrication has been outsourced overseas with little oversight. Inserting a backdoor into a part or parts is a significant threat to space systems. In the best case, an adversary will only know a part is military grade and may not know exactly what system or subsystem it will end up on. In the worst case, they may have access to a developer's supply chain and be able to place a part into a critical subsystem,

knowing the interfaces in great detail. Regardless, the hardware supply chain must be protected and "trojan" backdoors must be mitigated. Fortunately, some research and development is already underway to address this problem as outlined in *ASIC/FPGA Trust Assurance (AFTA) Framework*.[14]

Additionally, insider threat is a significant concern. Several other mechanisms exist that could potentially be utilized to breach a space system, such as a replay attack as discussed in *Mitigation of Command-Link Replay Attacks against Satellites*.[15] In addition to various known entrance points, spacecraft are often operated with lifecycles spanning a decade or two, and it is impossible to predict all offensive cyber techniques many years in the future. Systems must be resilient to threats that have not yet been considered.

As large constellations composed of relatively inexpensive and networked small satellites are considered as an alternative to traditional large exquisite spacecraft, further cyber concerns emerge. To keep manufacturing speeds high and costs low, small satellites will rely on more commercial parts as opposed to military grade. Taking steps to ensure a safe supply chain is advisable, but development schedules may not allow for a perfect supply chain scrub. Because various non-cyber threats (e.g., kinetic and electronic warfare) to space systems are largely mitigated by many small satellite constellations, adversaries may look for offensive cyber as a mechanism to attack a large constellation. A cyber vulnerability could affect all nodes in a constellation if they share the same design, which could render that whole constellation unreliable.

Defense in Depth

The fundamental problem for space systems is that they are designed assuming protection at their boundaries will be enough. Little internal protection exists if the boundary is breached. Similar schools of thought existed in the beginning days of traditional cybersecurity, where border firewalls were providing the only protection from intrusion. This approach proved to be faulty, and well-protected IT systems are now designed with DiD principles. Similarly, current and future space system designs must overcome the risk of an adversary breaching the boundary and operating unhindered inside the system using these principles. Both large traditional developments and more modern rapidly developed space systems should ensure that they have a cyber-hardened design with DiD throughout.

For a space system, a DiD strategy relies on multiple layers of security to protect mission-critical assets. This approach arches over acquisition, secure supply chains, space system hardening and monitoring, secure software development, intrusion detection and prevention, culture, people, etc. to create multiple layers as a security control. Recalling the earlier NASIC graphic in Figure 1 and applying a DiD strategy, security controls would need to be applied at the user segment, ground segment, link segment, and space segment to ensure the space system has a robust security architecture. The next section outlines how to apply DiD on the space segment only. Ground and wireless link architectures are out of scope of this paper, though a secure spacecraft is dependent on secure ground and wireless security.

Principles of a Cyber-Resilient Spacecraft

When designing a cyber-resilient space system, many different security control implementations exist that will improve civilian, commercial, and DOD space systems' security. However, this paper focuses on the following DiD principles: onboard intrusion detection and prevention systems, hardware/software supply chain, and onboard logging. Additionally, other considerations will be mentioned to complement these main three principles, which will also bolster the spacecraft's cyber protections. Selection of which DiD

principles to employ should be driven by sound risk management processes. To manage risk, decisionmakers should assess the likelihood and potential impact of a cyberattack against the spacecraft and then determine the best approach to deal with the risks: avoid, transfer, accept, or mitigate. To mitigate risks, decision makers must ultimately determine what kinds of DiD principles (i.e., security controls) to apply. Not all risks can be eliminated, and no decisionmaker has unlimited budget or enough personnel to combat all risks.

Intrusion Detection and Prevention Systems

The backbone of a cyber-resilient spacecraft should be a robust intrusion detection system (IDS). The IDS should consist of continuous monitoring of telemetry, command sequences, command receiver status, shared bus traffic, and flight software configuration and operating states. From a telemetry monitoring perspective, several parameters exist that have the highest likelihood of indicating a cyberattack against a spacecraft and should be actively monitored on the ground and looking into the future onboard the spacecraft with the IDS.[16]

The IDS should implement both signatures- and machine-learning-based anomaly detection techniques, an approach recommended by NIST.[17] Signatures should be derived from known threat information and weaknesses in the system, which have been identified by analysis. Machine-learning algorithms should be trained on a dataset that includes a variety of typical system operations. Space operations in general lend themselves well to machine-learning approaches for anomaly detection. Space operations tend to be highly structured and predictable: operators rarely deviate from vetted procedures and scheduling is performed well in advance.

Responses to detected events may vary depending on the nature of the threat. Violating nonsevere rules or crossing a low-scoring threshold will trigger an alert in telemetry to the ground operator with the violation, the raw data that caused it, and a recommended course of action. If a severe rules violation occurs or a higher threshold is crossed, the spacecraft's intrusion prevention system (IPS) will take automated actions, which may include swapping to a redundant side, quarantining command sequences, reloading flight software, and/or halting suspect units. An example of the first scenario may be a command receiver locking up when the spacecraft is not in view of a valid ground station. If the potential intrusion does not pass the decryption and authentication stage, immediate action is not needed, but the ground should be notified with relevant log data as soon as possible. An example where an immediate and automated response would be required is a known malware behavior being detected in the memory contents of the flight computer.

The IPS system should be integrated into the existing onboard spacecraft fault management system (FMS) because the FMS has its own fault detection and response system built in. Typically, the FMS is a relatively simple system looking for specific conditions and taking specific prescribed actions. Some of the rules-based detection techniques of the IPS may be similarly simple. The machine-learning techniques do not necessarily need to be overly complicated; relatively simple techniques can look for command sequences, which are far out of line with what has been previously seen in operations. The reason that both the IPS and FMS systems should be integrated is that they are essentially performing the same functions but are looking for different anomaly signatures. In fact, there may be scenarios where each of them detects an anomalous condition and attempts to take an action. Having them integrated ensures they do not take conflicting actions.

The spacecraft IPS and the ground should retain the ability to return critical systems on the spacecraft to known cyber-safe mode. Cyber-safe mode is an operating mode of a spacecraft during which all

nonessential systems are shut down and the spacecraft is placed in a known good state using validated software and configuration settings. The default cyber-safe mode software should be stored onboard the spacecraft in memory with hardware-based controls and should not be modifiable.

Supply Chain

It is critical that spacecraft developers implement a supply chain risk management program. They must ensure that each of their vendors handles hardware and software appropriately and with an agreed-upon chain of custody. Critical units and subsystems should be identified and handled with different rigor and requirements than noncritical units and subsystems. Parts should be sourced from reputable vendors and checked for signs of counterfeiting. Proper configuration management must be implemented for all software and firmware residing in any system on a spacecraft.

All software on the spacecraft should be thoroughly vetted and properly handled through the configuration management and secure software development processes. Leveraging secure coding standards or principles will aid in the reduction of nonintended weaknesses. For example, software developers for safety-critical software at the Jet Propulsion Laboratory follow the *Power of Ten – Rules for Developing Safety Critical Code*.[18] Additionally, others follow coding standards from the Software Engineering Institute or adhere to government regulations for avionics (e.g., DO-178C, "Software Considerations in Airborne Systems and Equipment Certification").[19] While standards are important during development, verification and validation are equally important. Both static and dynamic source code analysis tools should be run on flight-critical software.

Static code analysis is a method of debugging by examining source code against a set (or multiple sets) of coding rules. This type of analysis addresses weaknesses or nonconformance to coding standards in source code that might lead to vulnerabilities. This may also be achieved through manual code reviews, but using automated tools is much more effective. Another option is dynamic analysis, which is the testing and evaluation of a program by executing data in realtime. The objective is to find security errors in a program while it is running versus autonomously analyzing source code. These analysis tools should be a part of the development pipeline and should automatically run on a regular basis. Issues are much less costly to fix if they are discovered quickly, and feedback from the tools encourages developers to be security minded.

When performing static analysis, a multitude of static code analysis tools should be used to maximize the ability to detect security defects. Static analysis tools, like many other security tools, have strengths and weaknesses and by applying multiple tools the likelihood of detecting defects is increased.[20] However, not all defects (i.e., buffer overflows, race conditions, and memory leaks) can be discovered statically and require execution of the software. This is where space-centric cyber testbeds (i.e., cyber ranges) are imperative as they provide an environment to maliciously attack components in a controlled environment to discover these undesirable conditions. Technology has improved to where digital twins for spacecraft are achievable, which provides an avenue for cyber testing that was often not performed due to perceived risk to the flight hardware.[21]

Software often leverages third-party code, which may introduce vulnerabilities into the system. The prime integrator must take responsibility for all security weaknesses introduced via the use of third-party code. At a minimum, that means obtaining the code via trusted means and updating to new versions that fix security weaknesses and ideally includes scanning and testing third-party software for security weaknesses.

Logging

Logging is the process of collecting and storing data over a period of time in order to analyze events/actions of the system. It enables the tracking of all interactions through which data, files, or software is stored, accessed, or modified. Both the spacecraft and ground should independently perform command logging and anomaly detection of command sequences for cross validation. Commands received may be stored and sent to the ground through telemetry and automatically checked to verify consistency between commands sent and commands received. Alternatively, command sequence hashes can be used to verify consistency if telemetry link bandwidth is a concern.

Logging of other onboard indications of an intrusion attempt should be performed as well and may be spacecraft design specific. For example, parameters at the input to the command receivers may be of use for anomaly investigations. Legacy spacecraft have not traditionally kept logs of the fidelity needed for forensic analysis. Often, onboard anomalies do not have sufficient logging to make a determination, especially if the anomaly occurs between passes and the data has been lost due to a side-swap. Experimenting with the creation or adoption of a security information and event management tool for space vehicles would be prudent.

Other Standard Cyber Protections

In addition to the three main principles previously mentioned, several other complementary considerations can bolster spacecraft cyber protections.

It is important for the computing module to be able to access a set of functions and commands that it trusts; that is, that it knows to be true. This concept is referred to as root of trust (RoT) and should be included in the spacecraft design. The RoT serves as a separate compute engine controlling the trusted computing platform cryptographic processor. The RoT computing module should be implemented on radiation-tolerant burn-in (nonprogrammable) equipment. With RoT, a device can always be trusted to operate as expected. RoT functions, such as verifying the device's own code and configuration, must be implemented in secure hardware (i.e., field programmable gate arrays). By checking the security of each stage of power-up, RoT devices form the first link in a chain of trust that protects the spacecraft.

Wherever possible, lightweight cyber protection functions should be implemented and best practices applied in subsystems/firmware throughout the spacecraft. Software and firmware updates should be verified with cryptographic signatures. Cryptographic signatures provide the means to protect the privacy of the content and to verify its integrity and authenticity.

Communication buses that bridge critical and noncritical spacecraft systems should either be separated or explicitly protected. Within government spacecraft, the commonly used military standard 1553 (MIL-STD-1553) was designed before the term *cybersecurity* was invented, and the concern is that this bus, which was designed with no infiltration protection, could be easily corrupted or manipulated if any unintended data made it onto the data bus. Therefore, if the MIL-STD-1553 bus is used to communicate between the flight computer, attitude control system, thrusters, and various payloads, the payload communication should be separated or encryption, authentication, and anti-babble protection should be applied in front of each unit.

Small Satellite Considerations

Due to the increased usage and capabilities of smaller satellites, both the complexity and availability of satellite technology are growing, making the space infrastructure even more vulnerable.[7] The future of the space enterprise is moving toward large constellations of small satellites in low Earth orbit. As designs are being

developed, several considerations should be made. Many of the aforementioned DiD principles apply to small satellites, but with these new technologies come new security considerations.

These smaller vehicles impose additional weight and size constraints as compared to traditional space vehicles. NSA hardware-based cryptography has been a cornerstone for protecting the command link on DOD missions; however, utilizing software cryptography should be considered as an acceptable solution moving forward for all spacecraft. This paradigm shift will require proper approvals for DOD missions as NSA hardware type-1 encryption has been a long-standing requirement.

As previously described, onboard intrusion detection and prevention should be deployed on traditional spacecraft; for smallsats, cyber monitoring functions, such as flight software memory monitoring, may be co-resident with the flight processor. As depicted in Figure 3, architectures leveraging systems on a chip are particularly well suited for this application because they contain both core processors as well as programmable logic. Note that these platforms typically are not radiation hardened but may be seen in small and low-cost spacecraft designs of the future.

As the smallsat marketplace matures alongside the embedded security community, commercial and open source solutions will be developed that can bolster the security implementations of smallsat constellations for commercial and government use. As capabilities mature, the space community will need to be agile in its verification, validation, and acceptance to reap the benefits. Hardening smallsats, using a variety of methods and technologies, will be possible as long as the space community is willing to be agile and shift their mindset from the traditional ways of thinking.

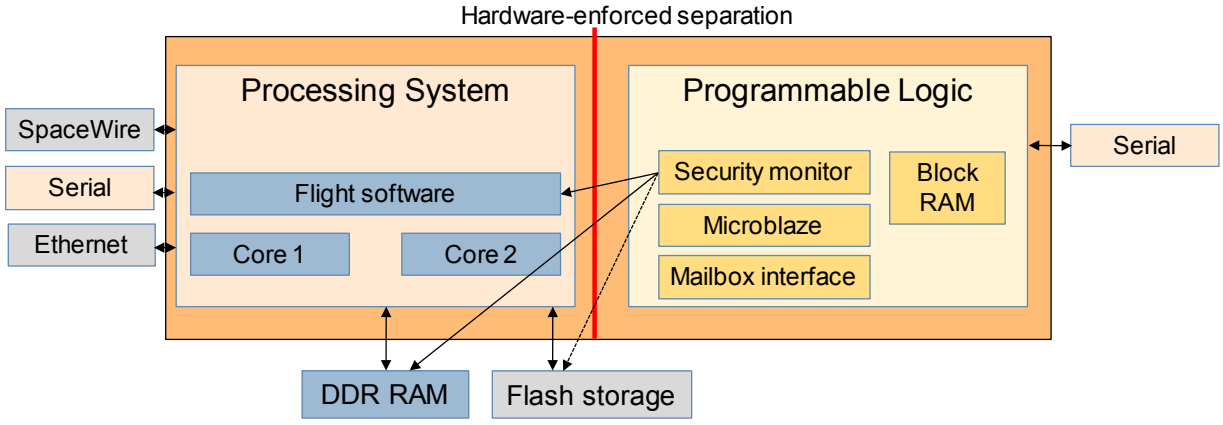

Figure 3: Example architecture.

Conclusions

The vulnerability of satellites and other space assets to cyberattack is often overlooked in wider discussions of cyber threats to critical national infrastructure. Neither space policy nor cybersecurity policy is prepared for the challenges created by the meshing of space and cyberspace, especially for spacecraft. In the absence of formal policy and regulations, industry and government alike can begin to apply defenses at all segments within the space system to build a more robust security posture. To mitigate risks, decisionmakers must ultimately determine what kinds of DiD principles to apply. Not all risks can be eliminated, and no decisionmaker has unlimited budget or enough personnel to combat all risks. However, decisionmakers, acquisition professionals, program managers and system designers can consider the following key principles when acquiring or designing a cyber-resilient spacecraft:

- Intrusion detection and prevention leveraging signatures and machine learning to detect and block cyber intrusions onboard spacecraft
- A supply chain risk management program to protect against malware inserted in parts and modules
- Software assurance methods within the software supply chain to reduce the likelihood of cyber weaknesses in flight software and firmware
- Logging onboard the spacecraft to verify legitimate operations and aid in forensic investigations after anomalies
- RoT to protect software and firmware integrity
- A tamper-proof means to restore the spacecraft to a known good cyber-safe mode
- Lightweight cryptographic solutions for use in smallsats

References

[1] Defense Intelligence Agency; *Challenges to Security in Space,* February 11, 2019, pages 9, 20, 29, and 36, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf.

[2] Porup, J; "It's Surprisingly Simple to Hack a Satellite", August 21, 2015, https://www.vice.com/en_us/article/bmjq5a/its-surprisingly-simple-to-hack-a-satellite.

[3] Eddy, M; "Satellite Communications Hacks Are Real, and They're Terrifying", August 9, 2018, https://www.pcmag.com/news/363004/satellite-communications-hacks-are-real-and-theyre-terrify.

[4] Ewart, R; Wheler, W; Betser, J; Cohen, N; Knobbe, R; Horejsi, J; Gonce, J; *Cyber Enhanced Space Operations from Frameworks to Enterprise Evolution,* September 2016, https://arc.aiaa.org/doi/pdf/10.2514/6.2016-5474.

[5] Symonds, E; *Comparing and Contrasting Space and Cyber Governance in Multilateral Forums and U.S. Policy Initiative,* May 2019, page 2, https://swfound.org/media/206442/symonds_space_cyber_governance_may2019.pdf.

[6] Unal, B; *Cybersecurity of NATO's Space-based Strategic Assets,* July 2019, pages 4 and 20, https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf.

[7] Livingston, D; Lewis, P; *Space, the Final Frontier for Cybersecurity?,* September 2016, page 21, https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf.

[8] Ginter, A; "The Top 20 Cyberattacks on Industrial Control Systems," January 25, 2018, https://waterfall-security.com/blog/top-20-cyberattacks-ics.

[9] Crowdstrike; *2019 Global Threat Report*, March 2019, pages 2 and 15, https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/.

[10] Weeden, B; Samson, V; *Global Counterspace Capabilities: An Open Source Assessment,* April 2018, page 7-1, https://swfound.org/media/206118/swf_global_counterspace_april2018.pdf.

[11] London Cyber Security LTD; *Space Cybersecurity's Final Frontier,* June 2015, pages 18–23, https://static1.squarespace.com/static/56d0212027d4bded627db544/t/56deb84c3c44d8eb68c68083/1457436755011/LCS+June+Report-web.pdf.

[12] National Air and Space Intelligence Center; *Competing in Space,* December 2018, page 18, https://media.defense.gov/2019/Jan/16/2002080386/-1/-1/1/190115-F-NV711-0002.PDF.

[13] Harrison, Todd; Johnson, Kaitlyn; Roberts, Thomas; Bergethon, Madison; Coultrup, Alexandra; *Space Threat Assessment 2019*, April 2019, page 5, https://aerospace.csis.org/wp-content/uploads/2019/04/SpaceThreatAssessment2019-compressed.pdf.

[14] Rao, V; *ASIC/FPGA Trust Assurance (AFTA) Framework,* The Aerospace Corporation, El Segundo, California (August 20, 2019). Restricted Distribution.

[15] Martin, Jon; *Mitigation of Command-Link Replay Attacks against Satellites,* The Aerospace Corporation, El Segundo, California (August 2019). Restricted Distribution.

[16] Martin, Jon; *Satellite Telemetry Indicators for Identifying Potential Cyber Attacks*, Aerospace TOR-2019-02178, The Aerospace Corporation, El Segundo, California (August 16, 2019). Approved for Public Release; Distribution Unlimited.

[17] Scarfone, K; Mell, P; *Guide to Intrusion Detection and Prevention Systems,* February 2007, page 2-4, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

[18] Holzmann, G; *The Power of Ten – Rules for Developing Safety Critical Code*, June 2006, http://spinroot.com/gerard/pdf/P10.pdf.

[19] "SEI CERT Coding Standards," Software Engineering Institute, last modified February 5, 2019, https://wiki.sei.cmu.edu/confluence/display/seccode.

[20] Center for Assured Software National Security Agency; *CAS Static Analysis Tool Study – Methodology,* December 2011, page 24, https://samate.nist.gov/docs/CAS_2011_SA_Tool_Method.pdf.

[21] Glaessgen, E; Stargel, D; *The Digital Twin Paradigm for Future NASA and U.S. Air Force Vehicles* April 2012, page 1-2, https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20120008178.pdf.