AEROSPACE

OCTOBER 2020

ESTABLISHING SPACE CYBERSECURITY POLICY, STANDARDS, AND RISK MANAGEMENT PRACTICES

Brandon Bailey

Space Policy Directive – 5 (SPD-5) states, "the United States considers unfettered freedom to operate in space vital to advancing the security, economic prosperity, and scientific knowledge of the Nation…Therefore, it is essential to protect space systems from cyber incidents in order to prevent disruptions to their ability to provide reliable and efficient contributions to the operations of the Nation's critical infrastructure." SPD-5 also defines "Space System" as "a combination of systems, to include ground systems, sensor networks, and one or more space vehicles, that provides a space-based service."

Space threats are changing at an incredibly rapid pace. 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.

Our future space systems, to include the spacecraft (and payloads), must be secured and cyber resilient. It is critical to define robust cybersecurity principles and cyber requirements for space systems. We must evolve from the traditional thinking of not engineering in security into the space segment.

Using threat-informed risk-based system engineering and applying defense-in-depth throughout space systems, particularly on the spacecraft themselves, is imperative.

Introduction

SPD-5 defines "Space System" as "a combination of systems, to include ground systems, sensor networks, and one or more space vehicles that provides a space-based service" and it outlines the need for integrating cybersecurity into all phases of development and ensuring that full life-cycle cybersecurity occurs for space systems.

SPD-5 outlines five cybersecurity principles for space systems in section four of the memorandum to serve as the foundation for the United States government approach, which includes working with the commercial space industry and other non-government space operators to further define best practices, establish cybersecurity-informed norms, and promote improved cybersecurity behaviors.

The five principles from section four of SPD-5:

1. Space systems and their supporting infrastructure, including software, should be developed and operated using **risk-based, cybersecurity-informed engineering**

2. Space system owners and operators should develop and implement cybersecurity plans for their space systems that incorporate capabilities to ensure operators or automated control center systems can retain or recover positive control of space vehicles

3. Implementation of these principles, through rules, regulations, and guidance, should enhance space system cybersecurity

4. Space system owners and operators should collaborate to promote the development of best practices, to the extent permitted by applicable law. They should also share threat, warning, and incident information within the space industry, using venues such as Information Sharing and Analysis Centers (ISAC) to the greatest extent possible, consistent with applicable law.

5. Security measures should be designed to be effective while permitting space system owners and operators to manage appropriate **risk tolerances and minimize undue burden, consistent with specific mission requirements**. United States national security and national critical functions, space vehicle size, mission duration, maneuverability, and any applicable orbital regimes.

Principles 1 through 5 essentially supports full lifecycle risk-based cybersecurity engineering and the implementation and sharing of best practices and threats. Subprinciples for item 2 provide the most prescriptive cybersecurity guidance for space systems:

- Protection against unauthorized access to critical space vehicle functions. This should include safeguarding command, control, and telemetry links using effective and validated authentication or encryption measures designed to remain secure against existing and anticipated threats during the entire mission lifetime;

- Physical protection measures designed to reduce the vulnerabilities of a space vehicle's command, control, and telemetry receiver systems;

- Protection against communications jamming and spoofing, such as signal strength monitoring programs, secured transmitters and receivers, authentication, or effective, validated, and tested encryption measures designed to provide security against existing and anticipated threats during the entire mission lifetime;

- Protection of ground systems, operational technology, and information processing systems through the adoption of deliberate cybersecurity best practices. This adoption should include practices aligned with the National Institute of Standards and Technology's Cybersecurity Framework to reduce the risk of malware infection and malicious access to systems, including from insider threats. Such practices include logical or physical segregation; regular patching; physical security; restrictions on the utilization of portable media; the use of antivirus software; and promoting staff awareness and training inclusive of insider threat mitigation precautions;

- Adoption of appropriate cybersecurity hygiene practices, physical security for automated information systems, and intrusion detection methodologies for system elements such as information systems, antennas, terminals, receivers, routers, associated local and wide area networks, and power supplies; and

- Management of supply chain risks that affect cybersecurity of space systems through tracking manufactured products; requiring sourcing from trusted suppliers; identifying counterfeit, fraudulent, and malicious equipment; and assessing other available risk mitigation measures.

What Does it All Mean?

As previously discussed in the paper titled *Defending Spacecraft in the Cyber Domain* from Aerospace's Center for Space Policy and Strategy (CSPS) building in security using defense-in-depth from the beginning is a necessity moving forward. This has been echoed by SPD-5. Many of the themes and principles outlined in SPD-5 overlap from a security perspective but several takeaways can be drawn from the recommended principles.

- Must secure both the ground and space segments during all phases of development and ensuring risk-based full lifecycle cybersecurity
  - Must include operational technology (ground) and all software (ground and space)
  - Size, Weight, and Power (SWaP) and mission context will be key factors for the security controls to be implemented

- SPD-5 does provide several security controls within the body of the principles:
  - Physical security of TT&C environment
  - TT&C protection using encryption or authentication
  - Jamming and spoofing protections
  - Supply Chain Risk Management
  - Insider Threat
  - Somewhat repetitive but it calls for basic cyber hygiene but also calls for adherence to National Institute of Standards and Technology (NIST) guidance

- SPD-5 recommends using the NIST Cybersecurity Framework (CSF) which is geared toward private industry but can also translate to the Risk Management Framework (RMF) which is what many government space systems are already using for cybersecurity. The RMF is much more prescriptive than the CSF. The RMF's is intended for the entire federal government and the CSF was initially developed for critical infrastructure. The steps in the RMF and the CSF process are different. The RMF process has six steps, and these steps are Categorize, Select, Implement, Assess, Authorize, and Monitor. The CSF process has seven-steps, and these steps are Prioritize and Scope, Orient, Create a Current Profile, Conduct a Risk Assessment, Create a Target Profile, Determine, Analyze, and Prioritize Gaps, and Implement Action Plan. The RMF controls can be used with the CSF, but the CSF does not have its own set of security controls. The CSF maps to a variety of functions titled: Identify, Protect, Detect, Respond, and Recovery. NIST has recommended that the CSF be used to strengthen the RMF. Elements of the CSF can be used to make the RMF more robust.

- SPD-5 promotes the establishment of best practices, policies, etc. in addition to sharing information across the community via ISAC

The main takeaway for SPD-5 is threat-informed risk-based engineering should drive security posture of the mission for both the ground and spacecraft to include operational technology (OT) and **all** software. The risk-based component should take into account mission context, mission requirements, mission duration, SWaP, etc. when selecting security controls.

Drivers for Cyber Hardening Space Systems

SPD-5 and the paper *Defending Spacecraft in the Cyber Domain* acknowledge the need and importance of secured space systems but there are other high-level drivers for securing our space systems.

- National space systems must continue operating in cyber contested environments
- Open source doctrine by potential adversaries shows intent to target space assets
- Current commercial and open source solutions are insufficient to address space cyber threat
  - There are also special challenges to secure legacy systems where upgrading legacy may present higher operational risk than the security vulnerability itself
- For long developmental/acquisition cycles and long on-orbit life of spacecraft
  - Threats will evolve over spacecraft lifespan
  - Cyber defense capabilities must be agile and capable of updating on-orbit

Threat-Based Risk Management

Protecting space systems is a combination of protecting what currently exists (i.e., legacy) as well as protecting future deployments of space-based technology. For legacy systems and future deployments alike, the cyber threat vectors for space systems are visually represented in Figure 1. The green lines indicate normal expected communications/access where the red lines indicate communications from adversary's infrastructure directly. Attacks can occur from the mission's own ground infrastructure, adversaries' ground infrastructure, a visiting spacecraft, or via a hardware or software supply chain implant. While the likelihood of each attack path varies depending on adversaries' capabilities, intent, and the difficulty due to mitigating controls, using defense-in-depth principles alongside risk management strategies will aid in reducing the likelihood and thereby reduce the risk. This approach is supported by SPD-5: "space systems and their supporting infrastructure, including software, should be developed and operated using risk-based, cybersecurity-informed engineering."

Protecting legacy deployments can be difficult, but not impossible and will have to be evaluated on a case-by-case basis. Updating protections of orbiting assets would need to be carefully planned and executed, while enhancing security for ground assets is much easier. On-orbit updates are sometimes risker than the cyber risk itself.

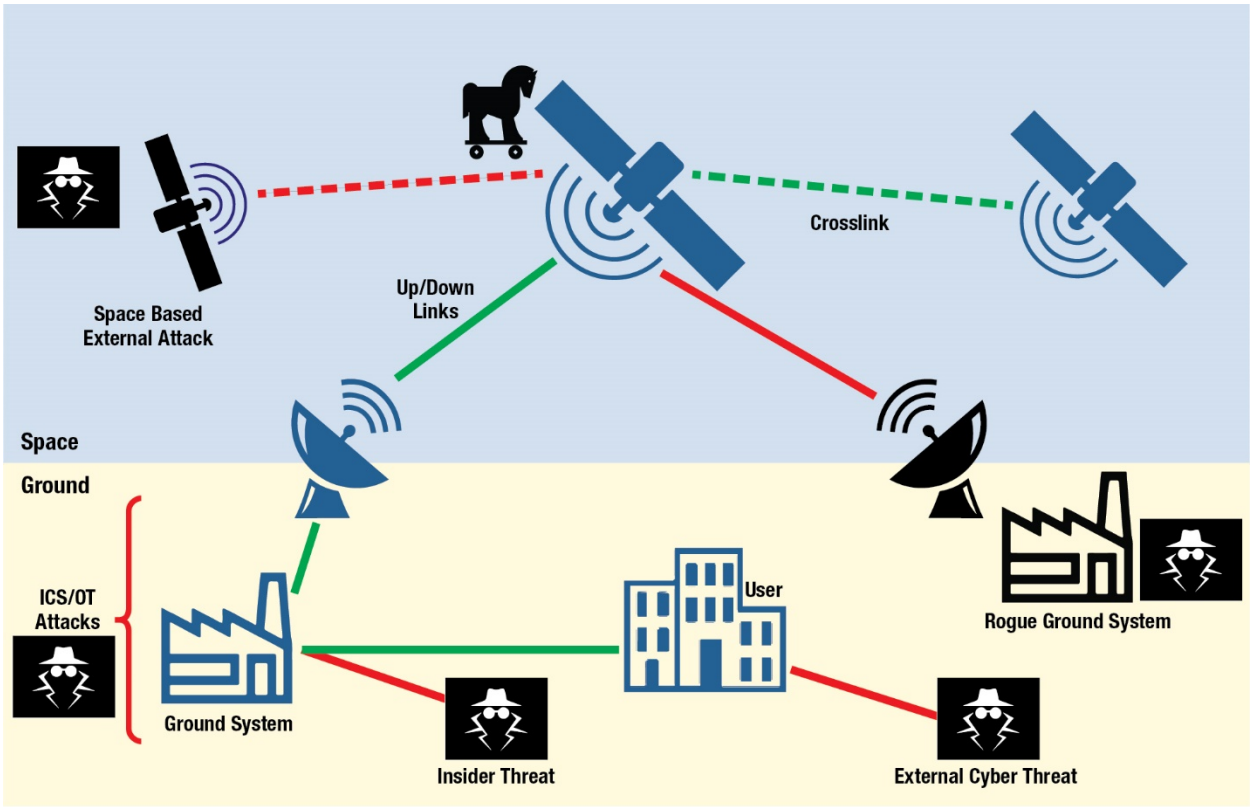

Figure 1. High-level cyber threat vectors.

Cyber Gaps from Past Experience

While the threats continue to evolve, response to those threats in our design and implementation of space systems has not always responded accordingly. The following gaps have been identified across a multitude of space systems over the past 5 to 10 years based on audits, assessments, and public disclosures. These gaps are separated based on their location in the space system architecture (ground vs. space).

Ground

- Insider threats are rarely considered which are compounded with the other gaps below
- Computer Network Defense/Incident Response is lacking in general which affects the ground operator's ability to protect, detect, respond, and recover
- Network design/segmentation is generally lacking which permits lateral movement once the boundary is penetrated
- Lack of encryption east to west (internal to the perimeter boundary) and the usage of many insecure protocols
- Endpoints lack proper hardening; while some systems are "STIG'd" this doesn't protect against many well-known Tactics Techniques and Procedures (TTPs)
- Ground software is the easiest attack vector to include custom developed, COTS, GOTS, and FOSS as secure software development and software assurance is not properly implemented
- ICS/OT environments that support critical ground infrastructure (e.g. dish positioning, data transmission) are extremely vulnerable as these systems were designed and implemented years ago or without many cyber protections
  - Ground based ICS/OT environments have similar trends as more traditional ICS/OT environments where they struggle to implement many of the best practices promoted by ICS-CERT (i.e., Seven Strategies to Defend ICSs, Improving ICS Cybersecurity with Defense-in-Depth Strategies, etc.)

Space

For the spacecraft, most security is geared around cryptography on the command link, Transmission Security (TRANSEC), and some Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions (TEMPEST) controls but the identified gaps include:

- Insider threats are rarely considered which are compounded with the other gaps below
- Ground systems are vulnerable and are the mostly likely entry point
- Spacecraft software can be vulnerable if secure design and coding principles are not applied and software assurance is not properly implemented
- Due to the autonomy of a spacecraft, software resilience and availability is critical

- Supply chain compromise of hardware and software could go undetected due to insufficient policies and procedures as well as absence of on-board monitoring
- Lacking on-board monitoring, logging, and alerting capabilities
- Safe mode features can put spacecraft in more vulnerable state (i.e., crypto bypass mode)

Protecting the Space System (Ground to Space) Space System Defense-in-Depth

One of the fundamental problems with space system design is an assumption that protection at the boundaries will be enough. For space, the boundary is often thought to be the communications link (i.e., radio frequency link) and/or the ground system in general. 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 risk-based defense-in-depth principles. Similarly, current and future space system designs must overcome the risk of an adversary breaching the boundary and operating unhindered inside the system.

Both large traditional developments and more modern rapidly developed space systems should ensure that they have a cyber-hardened design with risk-based defense-in-depth throughout. A space system should have cybersecurity protections applied to both the ground and space segments. Cybersecurity in general has been overlooked for many space systems, but when protections have been deployed, the focus has been on the ground segment with little research or guidance on securing the space segment (i.e., spacecraft). Defense-in-depth has long been explained by using an onion as an example of the various layers of security. The outer layer contains the border protection (e.g., firewall). Middle layers contain various controls. The data is in the center. Figure 2 and Figure 3 depict a visual representation of the layers where defenses can be applied to ground and space segments. Starting at the outer layer, prevention is where governance, supply chain protection, and risk management occur. The inner layers are where the mission data and the flight software reside, which are where encryption, coding standards, static and dynamic analysis are used to reduce risk. Also, the areas circled in red are where the most critical vulnerabilities and cyber gaps reside.

Ground Defense-in-Depth Principles

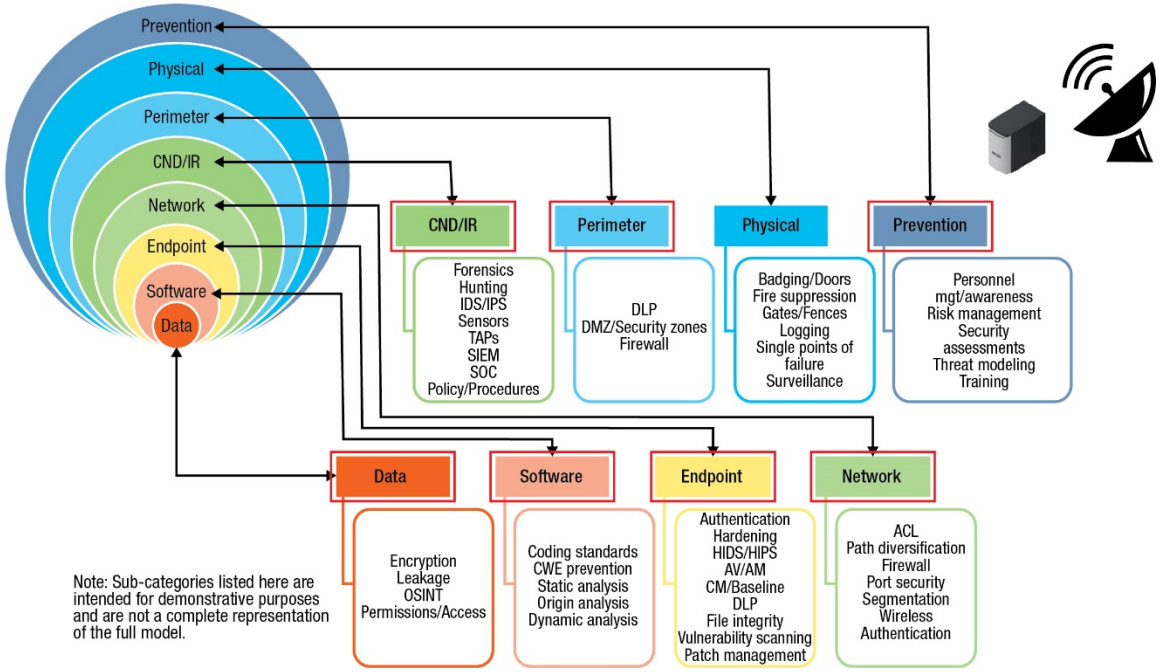

Figure 2. Ground defense-in-depth principles.

Space Defense-in-Depth Principles

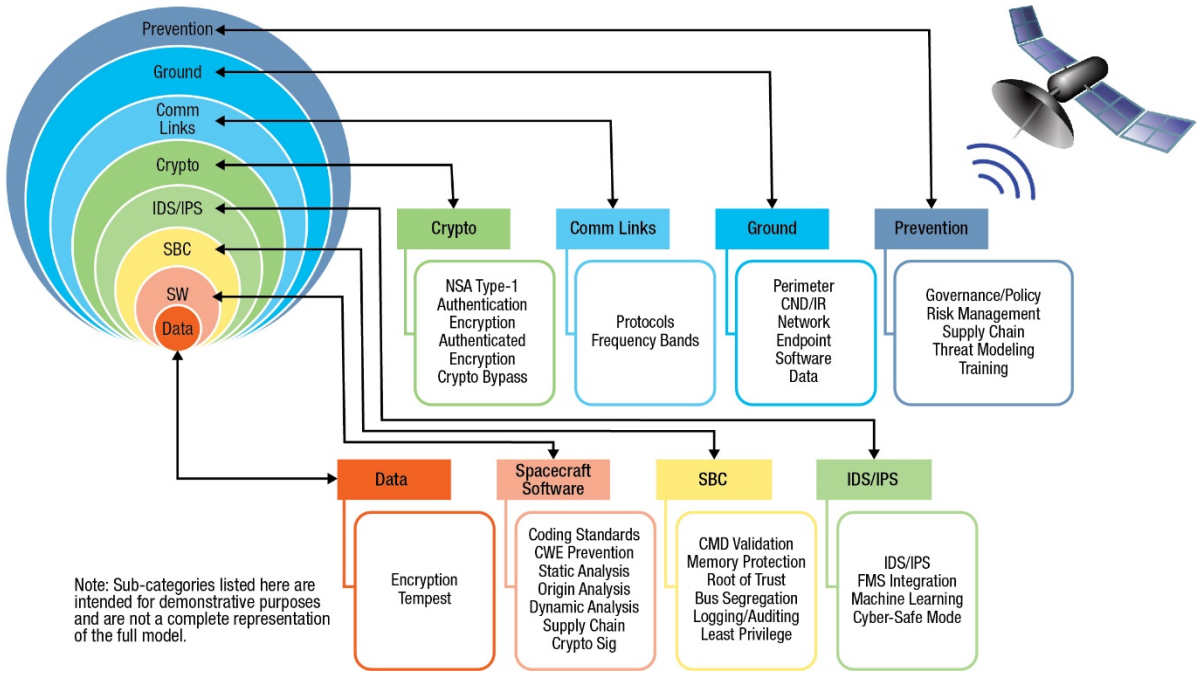

Figure 3. Space defense-in-depth principles.

Translating Security Principles for Space Systems to Existing Standards

Government programs and/or organizations have attempted to take portions of NIST governance and apply it to space systems. The most notable attempt at this was with CNSSI 1253 and the generation of the space overlay. The space overlay was an attempt to take an existing control set and create an overlay specific for the spacecraft as well as the launch vehicle. Overlays take something that exists (CNSSI 1253 / NIST 800-53) and determine what applies and does not apply. The space overlay takes the existing control set and articulates what **could be** applicable to the spacecraft. The important distinction in this approach is the approach is not risk or threat-informed and is very generic in nature. The space overlay has a purpose, but a better approach which aligns with the direction NIST is moving toward in revision 5 of 800-53 is creating a spacecraft baseline.

The baseline approach starts from a clean sheet of paper and establishes a specific baseline. With this approach, designers/engineers will take the master catalog (i.e., CNSSI 1253 / NIST 800-53 and all the enhancements) and generate their Program/Mission baseline. While baseline generation can be labor intensive, it will result in tailored controls/requirements for a particular mission. In an effort to promote a threat-informed baseline approach, the engineers need to understand the applicable threats to aid in control derivation. To accomplish this, a generic threat library can be used to help identify the threats needing mitigated. Figure 4 establishes a library of threats per layer applicable to a space system that need mitigated during design and/or operations. The items circled in red are deemed essential for any space system to implement mitigations, which are further broken out in Figure 4. The intent of these graphics is to depict generic cyber threats across all layers of the space system but also to highlight the most essential items to mitigate.

Every threat/vulnerability identified can loosely be translated to guiding principles as articulated by NIST or CNSSI. The key is understanding the underlying security principles and how they correlate to existing guidance. There is a bit of translation needed but as described in Aerospace's *Protecting the Space System* presentation, it can and has been done. An example of this translation can be seen with jamming protection which also aligns with one of the referenced security principles in SPD-5. An example requirement would be that the spacecraft shall be resilient against communications and positioning jamming attempts. This security principle is translatable to NIST RMF controls CP-8, AC-18(5), SC-5, SC-40, SC-40(1), SC-40(3), SI-10, and SI-10(3). Additionally, it correlates to the NIST CSF Identify {ID.BE-4}, Protect {PR.DS-4}, and Detect {DE.CM-1}. When security is handled as an engineering problem and not a compliance exercise, the overarching security principles defined with NIST RMF/CSF can be beneficial, but translation is necessary.

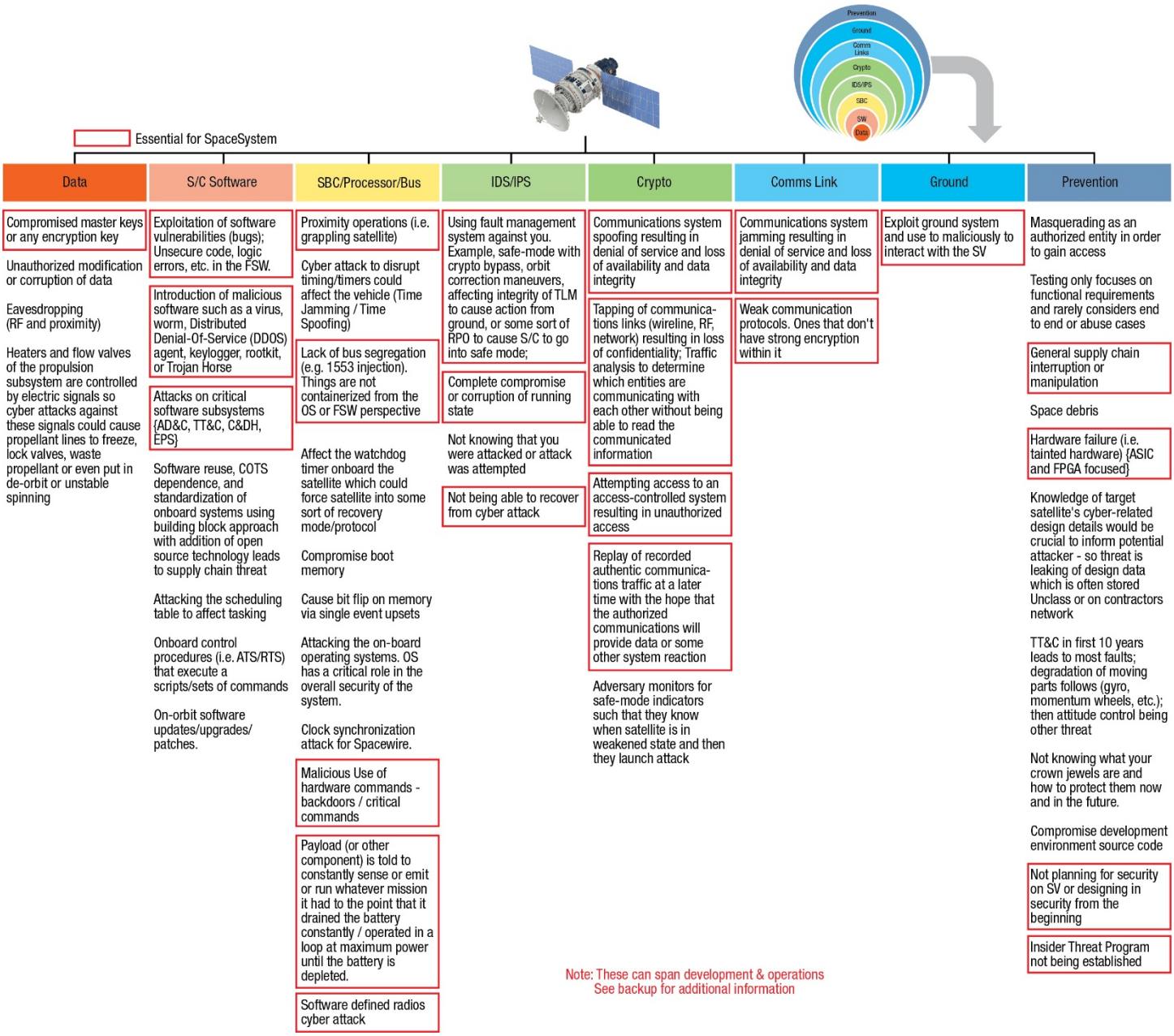

Figure 4. Library of threats.

Category	Essential Threats / Vulnerabilities to Mitigate for Space
Data	Compromised master keys or any encryption key. Encryption is great but self-defeating if key management is not properly implemented.
S/C Software*	Exploitation of software vulnerabilities (bugs); Unsecure code, logic errors, etc. in the flight software. Due to autonomy of spacecraft and increased usage of software on-board, software attacks can be mission ending.
	Introduction of malicious software such as a virus, worm, Distributed Denial-Of-Service (DDOS) agent, rootkit, or Trojan Horse. Outside of unintentional vulnerabilities with on-board software, malicious compromise of the software supply chain is a substantial threat and can be difficult to detect and prevent depending on the sophistication. Malicious logic embedded in software is difficult to detect due to the novel nature of it which can't be detected using signatures.
	Attacks on critical software subsystems {AD&C, TT&C, C&DH, EPS}. Many critical components on the spacecraft are controlled by software and adversaries would target these mission critical sub-systems.
SBC/Processor/ Bus	Lack of bus segregation (e.g. 1553 injection). Things are not containerized from the operating system or flight software perspective. Generally, the on-board architectures rely on trust and segregation is often not implemented. While this is a default security principle in traditional IT, it is lacking in most spacecraft architectures.
	Malicious use of hardware commands - backdoors / critical commands. Some spacecraft components have built in backdoor commands which can be exploited if discovered. Only enable the required backdoor commands or disable all commands that are not authenticated and encrypted.
	Payload (or other component) is told to constantly sense or emit or run whatever mission it had to the point that it drained the battery constantly / operated in a loop at maximum power until the battery is depleted. Power is a critical commodity on the spacecraft and the availability of the spacecraft is directly dependent on power. If not properly implemented, a compromised payload could drain spacecraft power.
	Software Defined Radios (SDRs) cyberattack. SDRs are gaining in popularity and capability, these minicomputers are vulnerable to attacks like any other computational component.
IDS/IPS	Using fault management system against you. Example, safe mode with crypto bypass, orbit correction maneuvers, affecting integrity of telemetry to cause action from ground, or some sort of proximity operation to cause spacecraft to go into safe mode. Understand your safing procedures and not putting the spacecraft in a more vulnerable state is key to building a resilient spacecraft.
	Complete compromise or corruption of running state can be possible if not engineered properly. High integrity controls need to be in place to revert to safe and secure state.
	Not being able to recover from cyberattack. Autonomy is required for spacecraft and a well-designed fault management strategy accompanied with the high integrity safe/secure state is crucial.
Crypto	Communications system spoofing resulting in denial of service and loss of availability and data integrity.
	Tapping of communications links (wireline, RF, network) resulting in loss of confidentiality; Traffic analysis to determine which entities are communicating with each other without being able to read the communicated information.
	Attempting access to an access-controlled system resulting in unauthorized access (i.e. command link intrusion).
	Replay of recorded authentic communications traffic at a later time with the hope that the authorized communications will provide data or some other system reaction.
Comms Link	Communications system jamming resulting in denial of service and loss of availability and data integrity.
	Weak communication protocols. Ones that don't have strong support for encryption and authentication within it.
Ground*	Exploit ground system and use to maliciously to interact with the spacecraft. This is a generalized threat which can be broken down to many different TTPs as described in Table 2 of paper.
Prevention*	General supply chain interruption or manipulation. This affects both the hardware and software for both ground and spacecraft.
	Hardware failure (i.e. tainted hardware). On-board the spacecraft ASICs and FPGAs are heavily used and at due to outsourcing the supply chains that can be compromised.
	Not planning for security on spacecraft or designing in security from the beginning which is needed to properly build a cyber resilient space system.
	Insider Threat Program not being established.

*Threats/vulnerabilities that have mitigations needed during development in addition to operations

Figure 4. Library of threats. (Cont.)

Risk Management Drives DiD Control Implementation

The above prioritization and items marked essential were not selected by chance. These were selected using an example threat-informed risk management strategy. Risk management is a key component when architecting a secure space system or assessing its security gaps (Figure 5). Not all security controls can be implemented due to resources (or even technology) and schedules.

When trying to establish which cybersecurity controls should be employed by a mission or set of missions, it should be a risk-based decision and not solely driven by compliance. Not only should it be risk from what threats and vulnerabilities could manifest themselves within the system and their impact to that system, but it should also be risk to the overall mission(s). The operational environment needs to be considered when classifying the threats and vulnerabilities which would be within the likelihood calculation.

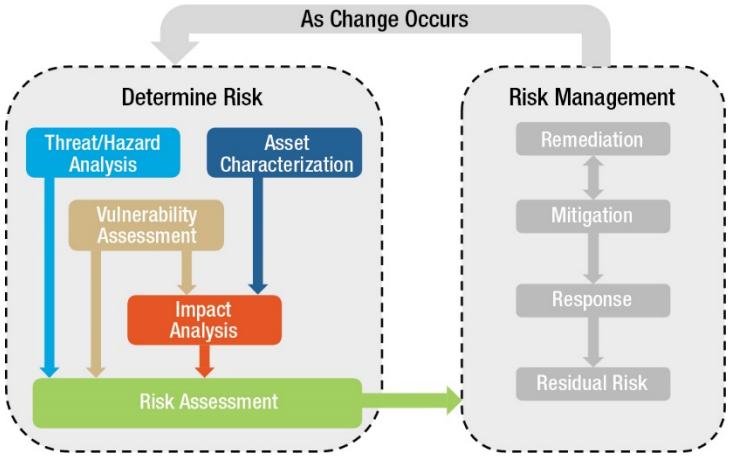

Figure 5. Risk management process.

Adversary threat modeling can help with security control selection. As described in SPD-5, it must be risk-based engineering and not "compliance" focused. The aforementioned essential threats/vulnerabilities to mitigate were prioritized using a generic increasing tiered threat model where Tier I adversaries are classified as "script kiddies" and Tier VI are the most capable nation state actors. When overlaying these threat tiers onto the previous threat vector figure, the result is displayed below. Where Tier I adversaries can operate on the ground via cyber means, the higher tiered adversaries are the ones operating with their own ground infrastructure or using space-born cyberattacks. The tiered modeled helps calculate the likelihood when determining which risks to mitigate. Cyber threat likelihood includes difficulty to exploit (i.e., access), motivation, and adversary capabilities. The motivation and difficulty would be Program/Mission dependent, but the adversary capabilities can be analyzed using a generic approach. The generic approach outlined below resulted in the aforementioned essential items in Figure 4.

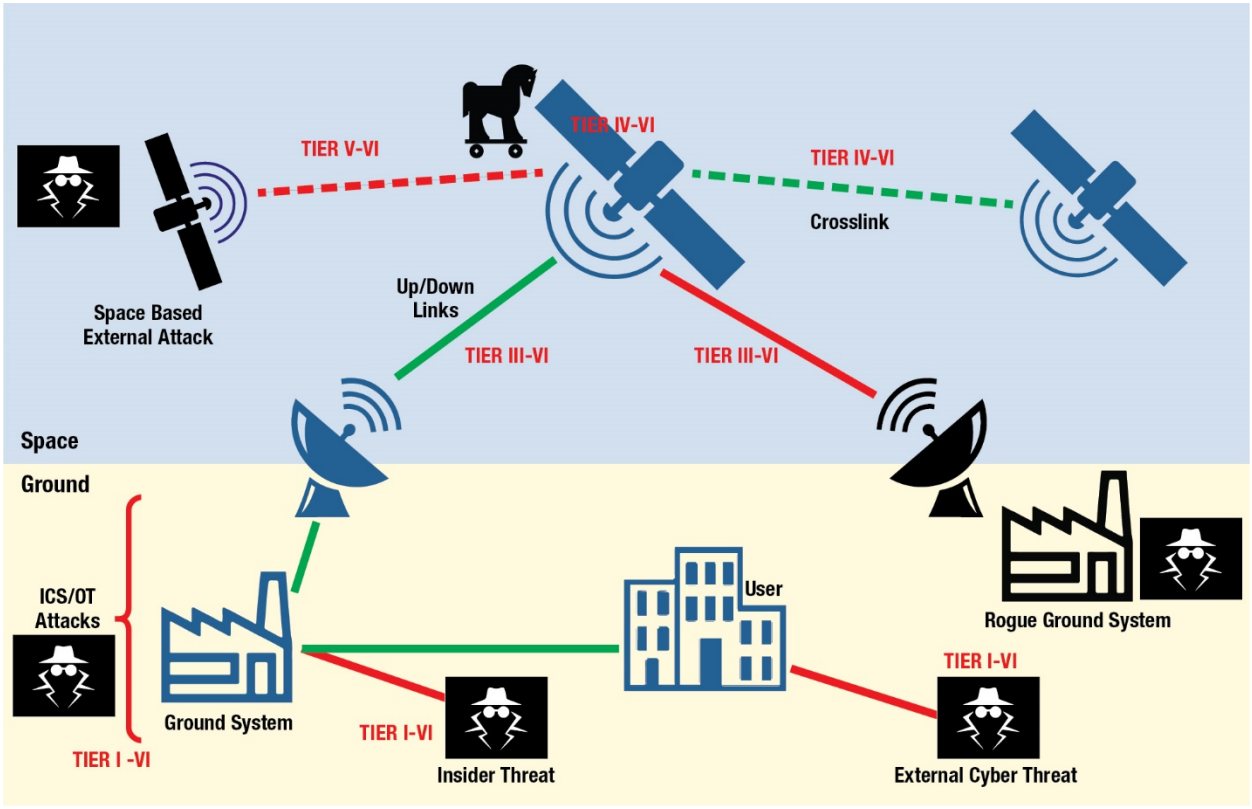

Figure 6. Overview of cyber threat vectors for space systems.

Summary

Given the lack of critical space system failures it is convenient to ignore security. This is not an option moving forward as space systems are too critical for our nation particularly since the barrier to entry into space has been drastically reduced with smallsats, commercial ground, and launch. Many of our nation's critical space infrastructure are in sustainment phases which translates to limited resources for security risk mitigation. Often upgrading legacy space systems is a higher operational risk than the security vulnerability itself and decision makers must be willing to accept the risk in either direction. Moving forward the following recommendation can be made:

- Risk-based defense-in-depth must be part of the solution
  - Needs to be designed in at the beginning of our programs as supported by SPD-5
- Using threat modeling and mission characteristics, a ranking (i.e., 5x5) for each cyber threat for the Program/Mission can aid in understanding cyber risk
  - This approach will likely result in many of the same controls supported by SPD-5 (i.e., TT&C security, physical, SW etc.)
- Inadequate cyber requirements and governance has led to the following being the largest cyber risk areas for space systems
  - Insider threat, supply chain (hardware and software) for both ground and spacecraft, crypto/comms area (as not everyone secures the comm links, including key management), situational awareness (e.g., threats, cyber monitoring, response, recovery) on both ground and spacecraft, and cyber best practices for the ground systems (e.g., software, ICS/OT, monitoring, segmentation, etc.)

SPD-5 aims to close these current gaps. It establishes a set of principles to protect the nation's valuable space assets from an increasing number of cyber threats. Its principles are designed to enable the protection of critical capabilities from communications to weather monitoring that Americans rely on every day. In combination with risk management and defense-in-depth principles for space systems outlined in this paper, SPD-5 can provide a whole-of-government framework and commercial approach to safeguard space assets and critical infrastructure.

About the Author

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.