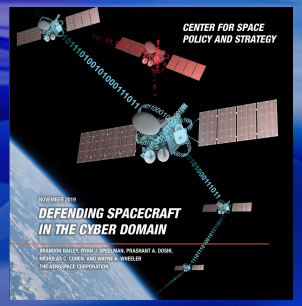
SpaceTech Alumni Symposium 2021
Mitigating Cyber Threats for Space Systems using Defense in Depth

Brandon Bailey
Cybersecurity Subdivision
Cyber Assessment & Research Dept (CARD)
The Aerospace Corporation

July 23, 2021



Paper(s):

https://aerospace.org/paper/defending-spacecraft-cyber-domain

https://aerospace.org/sites/default/files/2020-10/Bailey%20SPD5_20201010%20V2_formatted.pdf

brandon.bailey@aero.org
240.521.4326 (c)

Speaker Bio

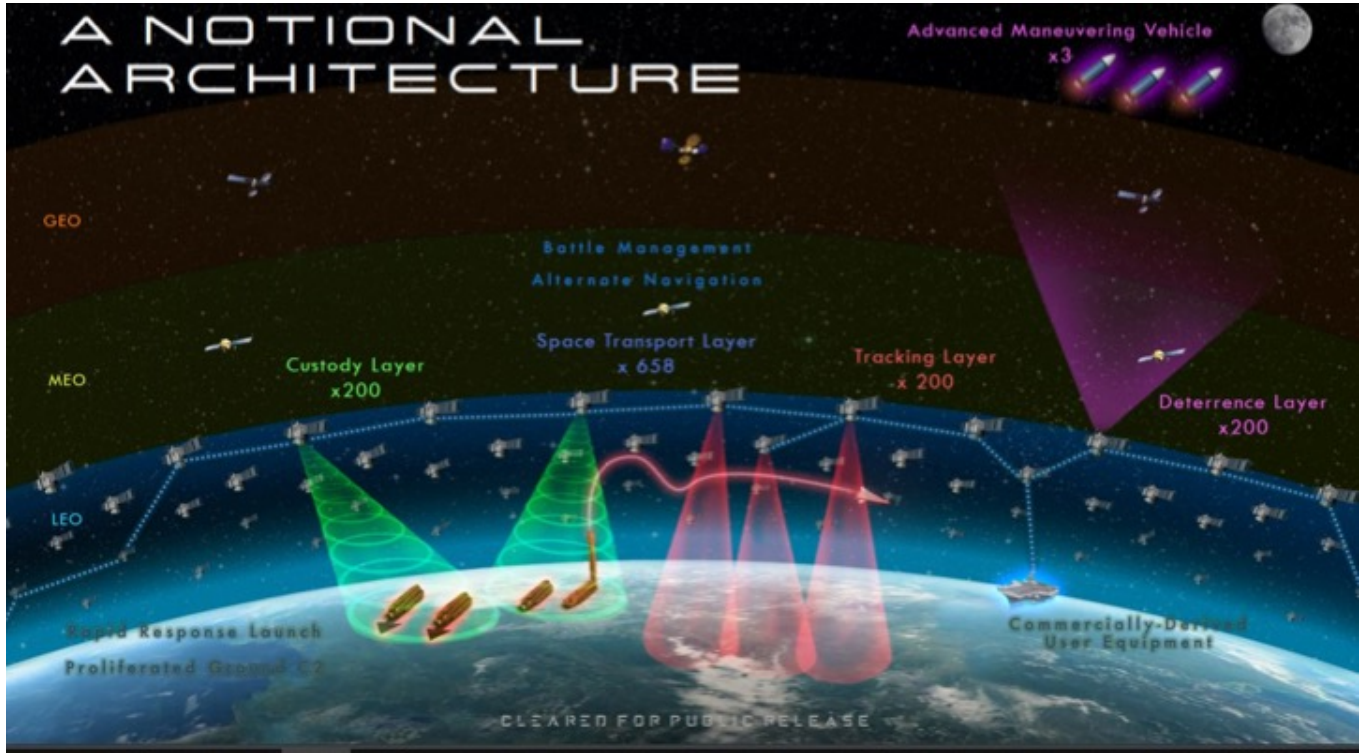
Who Am I and What Have I Done?

Recent Bio & Panel:

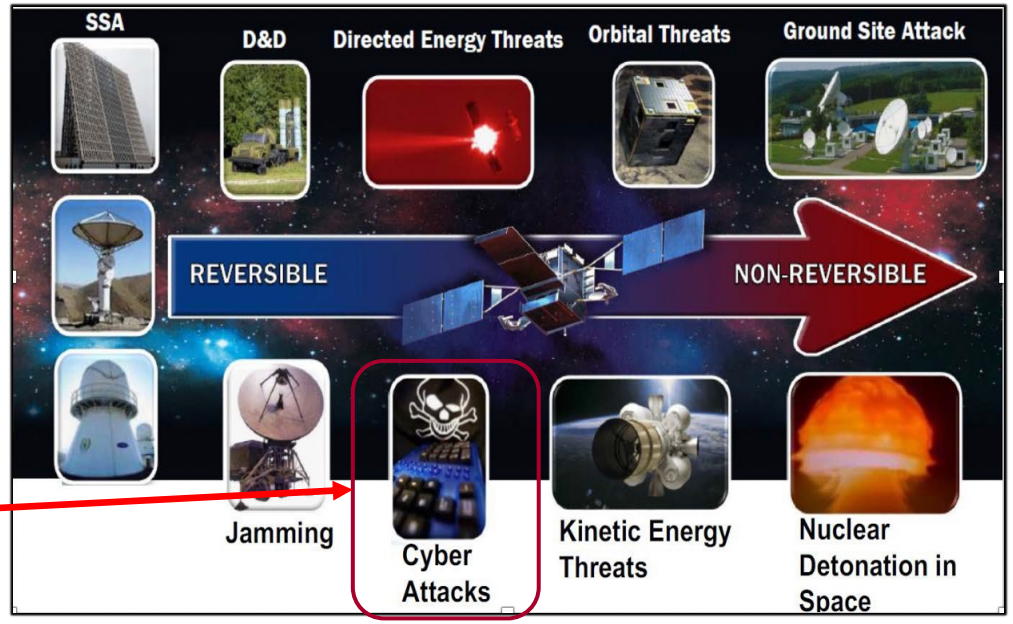
- https://www.wilsoncenter.org/person/brandon-bailey
- https://www.wilsoncenter.org/event/cybersecurity-final-frontier-protecting-our-critical-space-assets-cyber-threats?1626289200

- Works for the Aerospace Corporation within the Cybersecurity Subdivision as a Senior Cybersecurity Project Manager
- Former GS-15 at NASA where he led various cybersecurity efforts and was awarded NASA's Exceptional Service Medal for his landmark cybersecurity work in 2019
- Spent much of his 16-year professional career supporting space
- At Aerospace I have focused on developing a cyber range to support penetration testing training and in-the-lab evaluation of customers' implementations, performing vulnerability assessments and penetration testing activities for multiple customers, and performing cybersecurity research on ground systems and spacecraft systems to better position the federal government with respect to protection our critical space infrastructure
- Presented at DEF CON 2020 on how to exploit spacecraft in addition to being the primary author on two whitepapers on spacecraft cybersecurity Defending Spacecraft in the Cyber Domain & Establishing Space Cybersecurity Policy, Standards, & Risk Management Practices
- In April of 2021, authored a report titled *Cybersecurity Protections for Spacecraft: A Threat Based Approach* which was outlines concepts of defense-in-depth protection necessary to protect spacecraft, and then a threat-oriented approach to space cyber risk assessment. Currently releaseable Distro C (USG and Contractors)

Current State of Security in Space



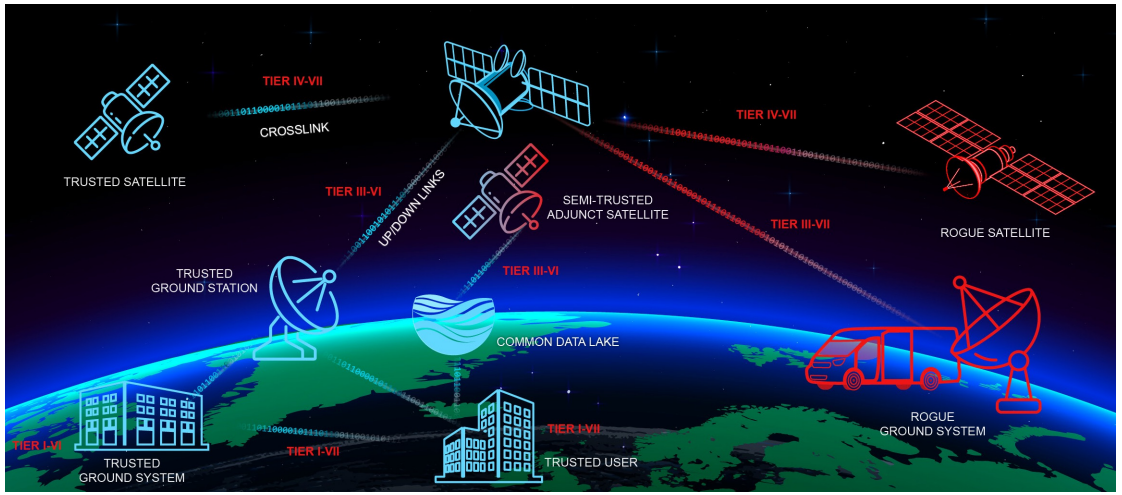
Many believe the single largest vulnerability of space systems today is cyber.



Focus for today

The Cybersecurity in Space Problem

- Traditional spacecraft/payload architectures, sub-systems, and supply chains were developed before current cyber threats were envisioned
- Traditionally, cybersecurity for DoD, civilian and commercial space systems has concentrated on the ground segment with minimal, if any, cyber protections onboard the SV/payload
  - *Encryption/Authentication, TRANSEC, COMSEC, and TEMPEST are typically the only controls (if any)*
    - Not acceptable moving forward giving the threat landscape
      - *Some isolated circles have been working this problem for several years whereas industry and government/international policy is slowing catching up*
- There is needed advancement in cybersecurity for space systems, especially the spacecraft
  - *Many articles/publications identify the cyber problem as a black box (i.e. cyber is an issue), but few are solutions oriented*
    - See links on title slide for two papers from Aerospace Corp
  - *One area is helping mission owners define the "right" requirements backed by proven security principles*
    - New paper (TOR-2021-01333) available upon request that contains example requirements to secure the spacecraft



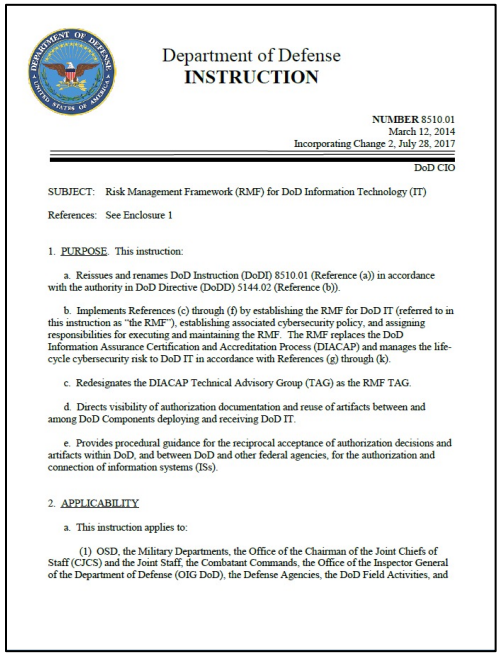
***blue lines** indicate normal expected communications/access*
***red lines** indicate communications from adversary's infrastructure directly*

By defining the right cyber requirements, mission owners will be able reduce cyber risk for the space system

Policy vs Controls vs Requirements

- Cybersecurity can be directed through different levels of detail

Policy



Department of Defense
INSTRUCTION

NUMBER 8510.01
March 12, 2014
Incorporating Change 2, July 28, 2017

DoD CIO

SUBJECT: Risk Management Framework (RMF) for DoD Information Technology (IT)

References: See Enclosure 1

1. PURPOSE. This instruction:

a. Reissues and renames DoD Instruction (DoDI) 8510.01 (Reference (a)) in accordance with the authority in DoD Directive (DoDD) 5144.02 (Reference (b)).

b. Implements References (c) through (f) by establishing the RMF for DoD IT (referred to in this instruction as "the RMF"), establishing associated cybersecurity policy, and assigning responsibilities for executing and maintaining the RMF. The RMF replaces the DoD Information Assurance Certification and Accreditation Process (DIACAP) and manages the life-cycle cybersecurity risk to DoD IT in accordance with References (g) through (k).

c. Redesignates the DIACAP Technical Advisory Group (TAG) as the RMF TAG.

d. Directs visibility of authorization documentation and reuse of artifacts between and among DoD Components deploying and receiving DoD IT.

e. Provides procedural guidance for the reciprocal acceptance of authorization decisions and artifacts within DoD, and between DoD and other federal agencies, for the authorization and connection of information systems (ISs).

2. APPLICABILITY

a. This instruction applies to:

(1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense (OIG DoD), the Defense Agencies, the DoD Field Activities, and

"Program shall implement cybersecurity through RMF as directed in DoD 8510.01"

Control Baseline

Table D-1: NSS Security Control Baselines

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X
AC-2	Account Management	X	X	X	X	X	X			
AC-2(1)	Account Management | Automated System Account Management		X	X		X	X			
AC-2(2)	Account Management | Removal of Temporary / Emergency Accounts		X	X		X	X			
AC-2(3)	Account Management | Disable Inactive Accounts		X	X		X	X			
AC-2(4)	Account Management | Automated Audit Actions	+	X	X	+	X	X			
AC-2(5)	Account Management | Inactivity Logout	+	+	X	+	+	X	+	+	X
AC-2(6)	Account Management | Dynamic Privilege Management									
AC-2(7)	Account Management | Role-Based Schemes	+	+	+	+	+	+			
AC-2(8)	Account Management | Dynamic Account Creation									
AC-2(9)	Account Management | Restrictions on Use of Shared Groups / Accounts	+	+	+	+	+	+			
AC-2(10)	Account Management | Shared / Group Account Credential Termination	+	+	+	+	+	+			
AC-2(11)	Account Management | Usage Conditions			X			X			
AC-2(12)	Account Management | Account Monitoring /	+	+	X	+	+	X			

"Program shall implement CNSSI 1253 Moderate control baseline."

Leaves too much up to interpretation and/or descoping

Specification Requirements

Control Tag	Requirement Text
IA-2(8),IA-2(9)	The SV shall implement relay and replay-resistant authentication mechanisms for establishing a remote connection.
IA-3,IA-4,SI-3(9)	The SV shall uniquely identify and authenticate the ground station and other SVs before establishing a remote connection.
IA-3(1),IA-4,IA-7,SI-3(9),AC-17(2),SC-7(11)	The SV shall authenticate the ground station (and all commands) and other SVs before establishing remote connections using bidirectional authentication that is cryptographically based.
AC-4	The [Program-defined security policy] shall state that information should not be allowed to flow between partitioned applications unless explicitly permitted by the Program's security policy.
AC-4	The SV shall enforce approved authorizations for controlling the flow of information within the SV and between interconnected systems based on the [Program defined security policy] that information does not leave the SV boundary unless it is encrypted.

Actual requirements for program design, development, and testing

Need these

Acquisition Challenges and Lack of Standardization

- 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 (RMF) and Cybersecurity Framework (CSF).
  - *The 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, especially the spacecraft*
    - NIST L-M-H baselines have some applicability on the ground segment but space segment is lacking
      - *Space Overlay does exist (Appendix F CNSSI 1253)*
      - *MDA Software Assurance Overlay Released June 2019*
      - *NIST RMF controls for moderate baseline ~ For SV, 75% N/A while omitting over 80 applicable controls*
        - Time is often wasted on justifications for why not applicable to compliance baseline whereas if tailored baseline was created early on based on applicable threats the "right" requirements would be levied
- While efforts have been made to mold these frameworks for space systems, uniformity is lacking and updated standards and guidelines for space are likely warranted {*see backup for known space security standards*}
- SPD-5 also identified this gap and the need for more collaboration and establishment of standards

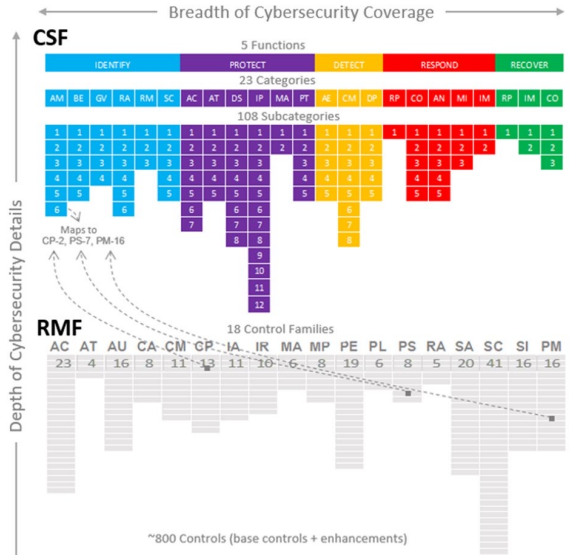
SPD-5 > *"policy of the United States that executive departments and agencies (agencies) will foster practices within Government space operations and across the commercial space industry that protect space assets and their supporting infrastructure from cyber threats and ensure continuity of operations."* SPD-5 goes on to say, *"implementation of these principles, through rules, regulations, and guidance, should enhance space system cybersecurity, including through the consideration and adoption, where appropriate, of cybersecurity best practices and norms of behavior."*

SPD-5 – You May Have Heard of It? - What Does It All Mean?

"Protect space systems from cyber incidents"

- Must secure both the ground and space segments during all phases of development and ensuring risk-based full life-cycle 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*
- Some specific security guidance is recommended
  - *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, calls for basic cyber hygiene but also calls for adherence to NIST guidance*
    - Calls out NIST Cybersecurity Framework (CSF) but can also translate to Risk Management Framework (RMF)

Some, but not all, have been doing this for years

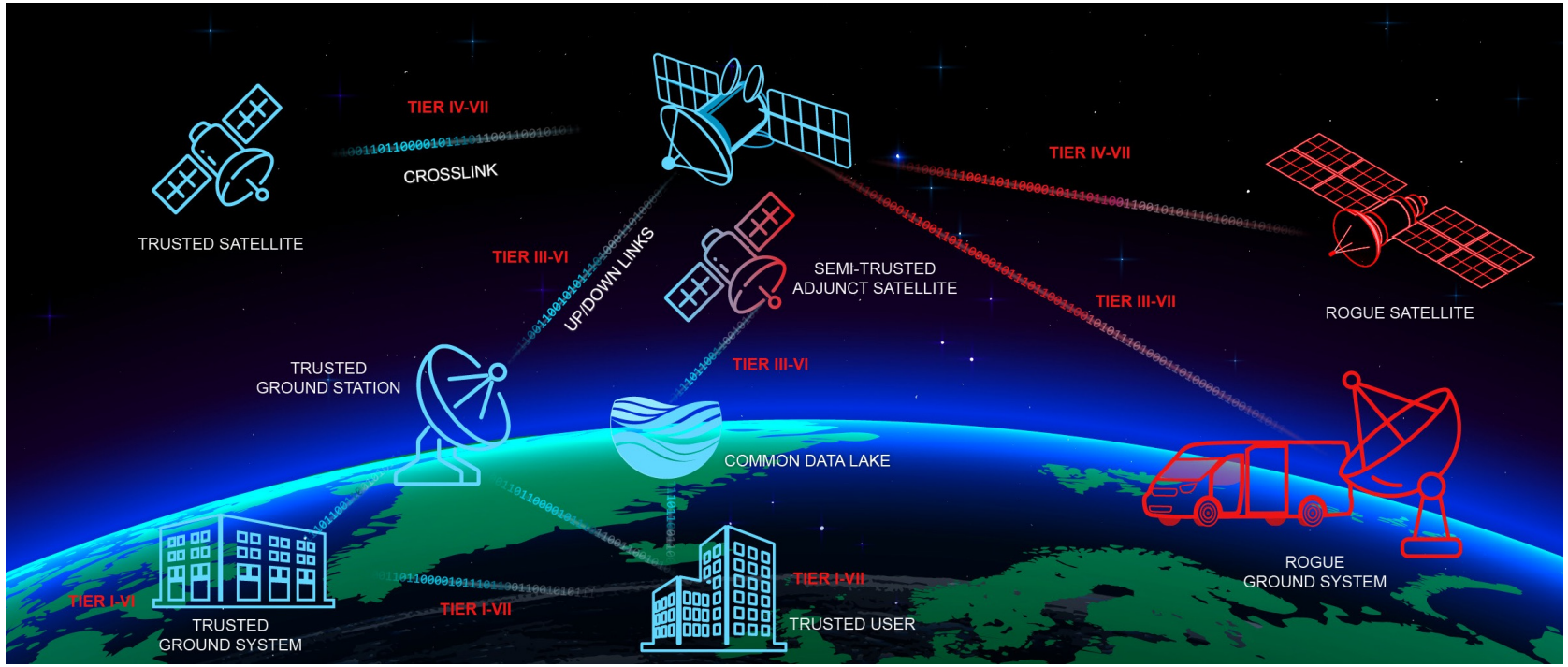


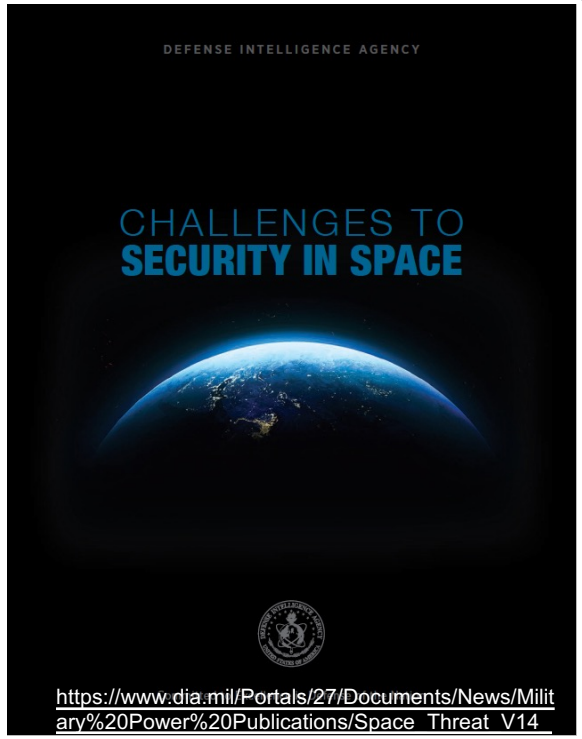
- SPD-5 promotes the establishing of best practices, policies, etc. in addition to sharing the information across the community via ISAC
- Main takeaway is threat informed risk-based engineering should drive security posture of the mission for both the ground and SV to include operational technology (OT) and **all** software – We must go above what SPD-5 calls for in commercial, civil, and national security space to counteract the emerging threats

Motivation for Securing Space Systems

Beyond Policy XYZ Said So….

- Space system cybersecurity threats have grown beyond encryption for perimeter defense
  - *Several nation states emphasize offensive cyberspace capabilities as key assets for multi-domain warfare*
- National space systems must continue operating in cyber contested environments
- Open source doctrine by potential adversaries shows intent to target space assets

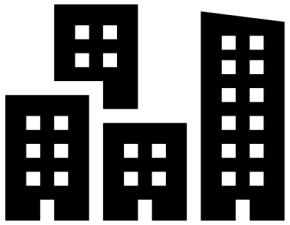




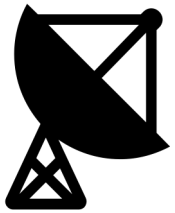
https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_

***blue lines** indicate normal expected communications/access*
***red lines** indicate communications from adversary's infrastructure directly*

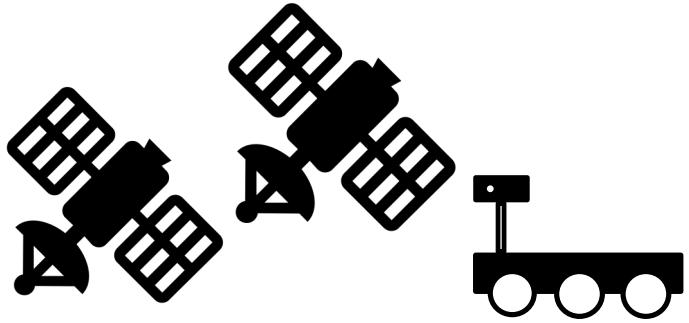
Example Cyber Incidents Against Space Systems



April 2005[4]: A rogue program penetrated NASA KSC networks, surreptitiously gathered data from computers in the Vehicle Assembly Building and removed that data through covert channels.
2011[5]: Cybercriminals managed to compromise the accounts of about 150 most privileged JPL users.
2018[7]: Weaknesses in JPL's system of security controls exploited; attacker moved undetected within multiple internal networks for about 10 months



Since 2007[3] several elite APT groups have been using — and abusing — satellite links to manage their operations — most often, their C&C infrastructure, for example, Turla.
Black Hat 2020[2]: Eavesdropping on Sat ISPs. Basically, ISP not protecting their links and it can be picked up easily.

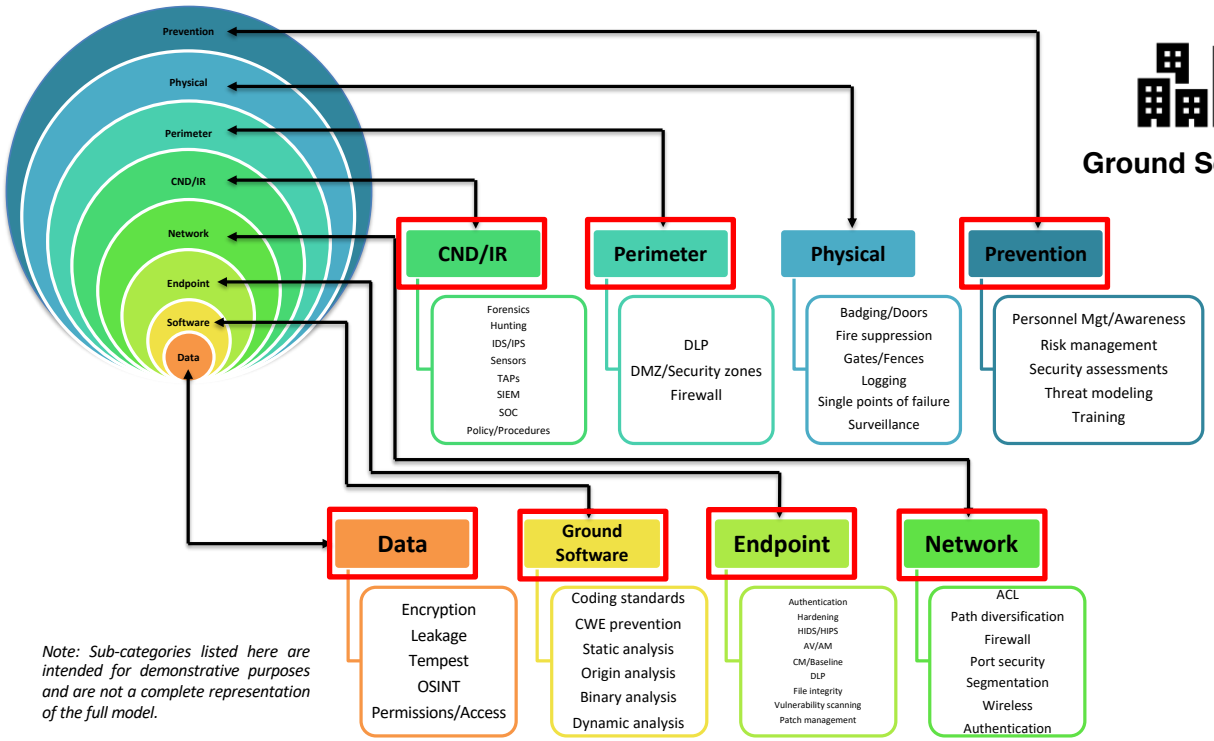


June/July 2008[1]: *Terra EOS AM-1/Landsat-7, a*ttempted satellite hijacking, hackers achieved all steps for remote command of satellite.
2013-2014:[6] UT Austin Radio-Navigation Lab conducts GPS spoofing for UAV control and navigation interruption.

1. SPACE: Cybersecurity's Final Frontier, London Cybersecurity Report, *June 2015.*
2. Black Hat 2020: Satellite Comms Globally Open to $300 Eavesdropping Hack, Threatpost, Aug. 2020
3. Turla APT Group Abusing Satellite Internet Links, Threatpost, Sep. 2015
4. Network Security Breaches Plague NASA, Bloomberg, Nov 2008
5. Hackers Seized Control of Computers in NASA's Jet Propulsion Lab, WIRED, Mar. 2012
6. UT Austin Radio Radionavigation Laboratory
7. 2019 NASA OIG Report

Defense-in-Depth for Space Systems

Many Layers, Many Choices

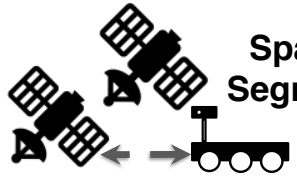


Ground Segment

Note: Sub-categories listed here are intended for demonstrative purposes and are not a complete representation of the full model.

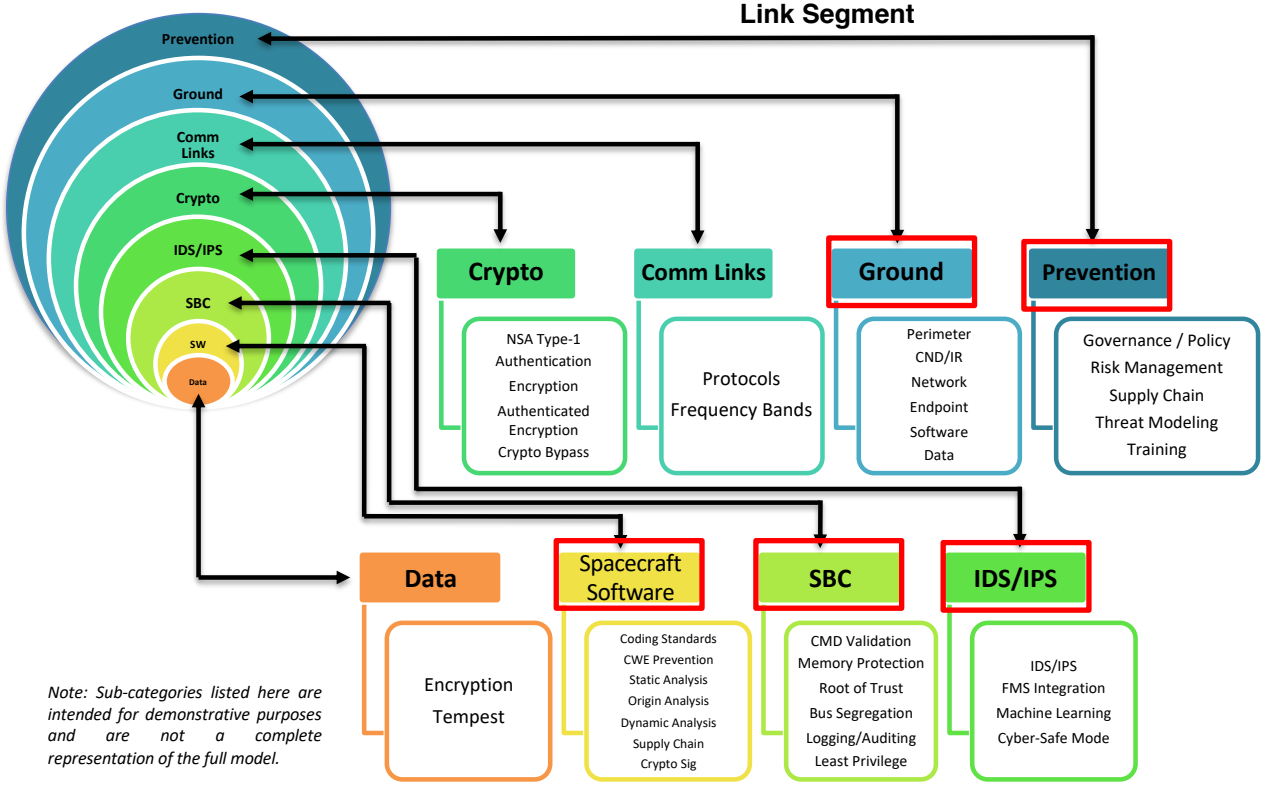
Areas based on Aerospace's experience where the most critical vulnerabilities and cyber gaps reside {see backup for gaps}

Documented cyber threats exists at each layer!



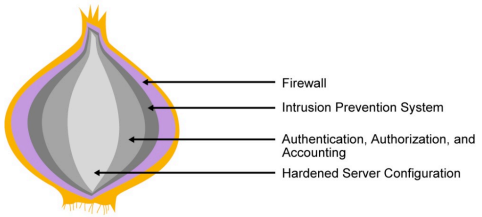
Space Segment

Link Segment

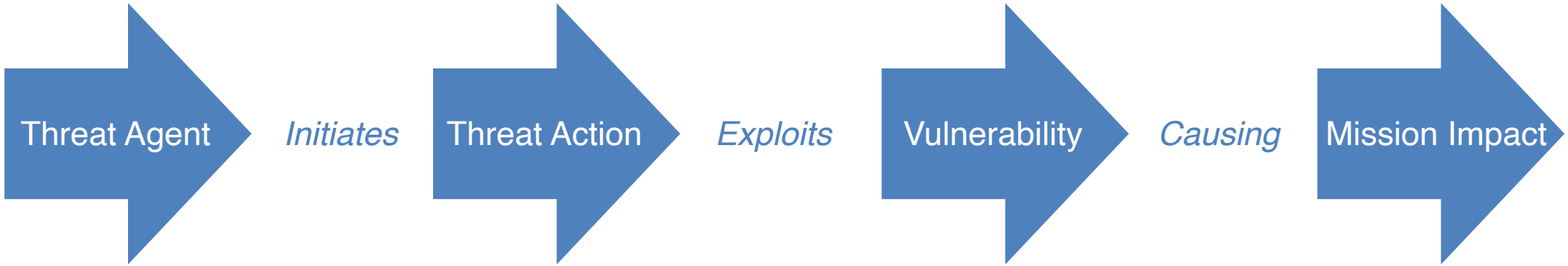


Note: Sub-categories listed here are intended for demonstrative purposes and are not a complete representation of the full model.

Defense in depth has long been explained by using the 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



Relationship Between Terms

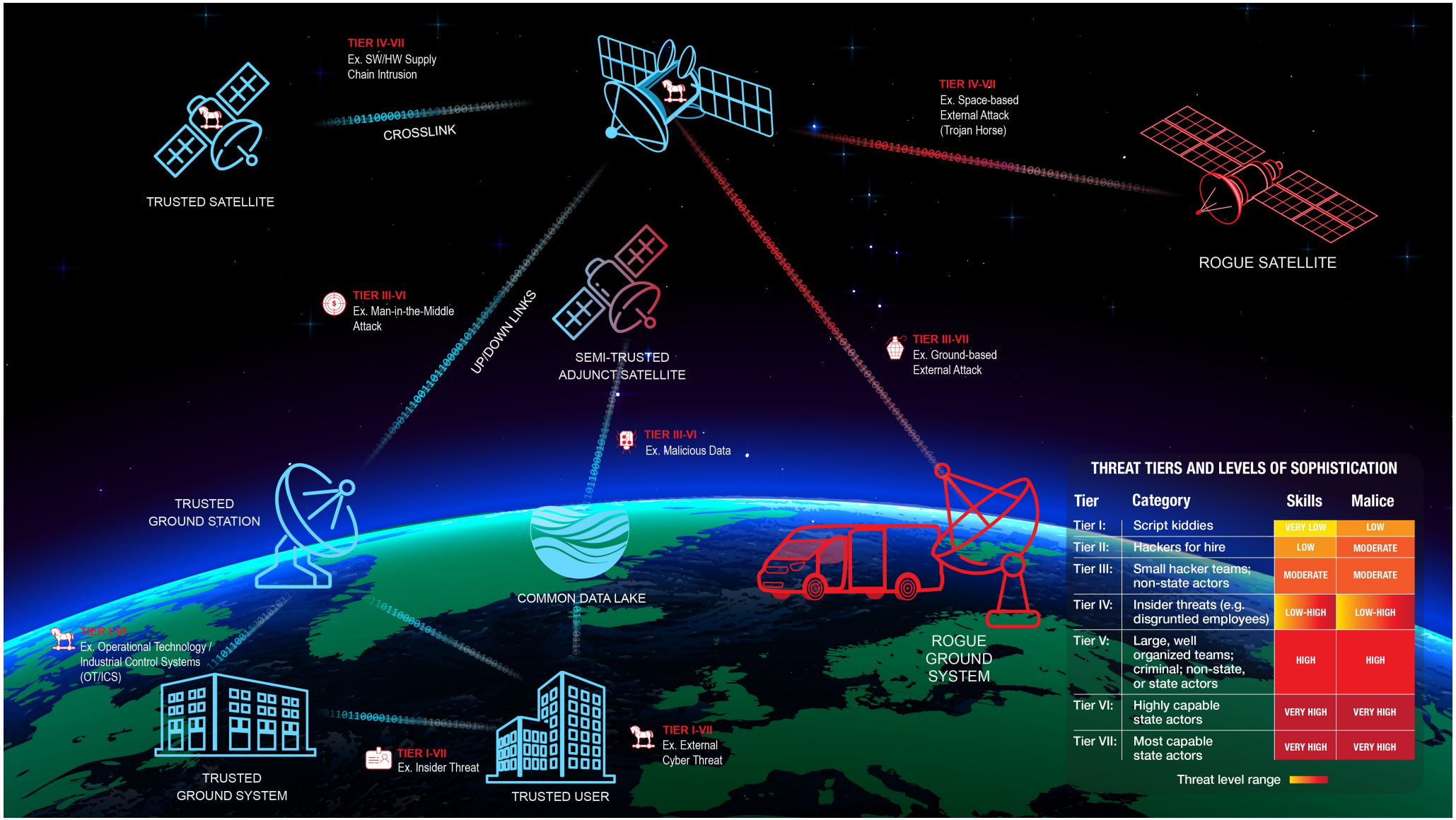


**** Expanded breakdown in backup***

Threat Agents

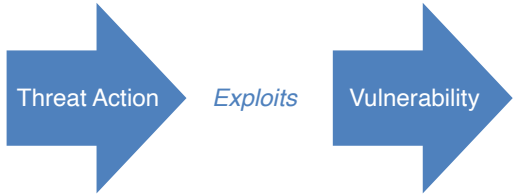
Which tiers affect which system components?

Threat Agent — *Initiates*



Approach for SV Threat Research

Threat & Vulnerability Based



- Reviewed several publications for threats, vulnerabilities, requirements, & security principles

DoD / Government Resources:

CNSSI 1253 Space Overlay
GPS RMF002 Requirements
HPSC Cyber Secure Boot Requirements
MDA Software Assurance Overlay version 19-MDA-10112 (19 Jun 19)
DARPA – System F6 Tech Package (F6TP)

Civil Space:

NOAA ITSM and FIPS documents
NASA Candidate Protection Strategies v4 – November 4, 2019
NASA Software Safety Standard and Handbook – NASA-STD-8719.13

Aerospace Curated Data:

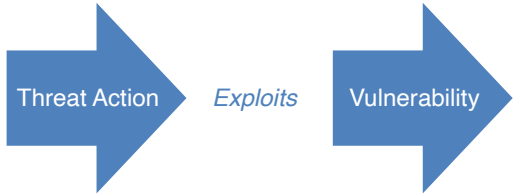
Aerospace CSPS – Defending Spacecraft in a Cyber Domain
Watcher Presentations/Papers
TOR-2019-02178 – Telemetry Security
TOR-2018-02275 – A Need for Robust Space Vehicle Cybersecurity
TOR 2018-01164 – Space-Cyber Requirements for Future Systems
TOR-2019-00506 (ASIC/FPGA Assurance) Rev A Spreadsheet v1-2
Aerospace SCRM TOR (not yet released)

Open Source / Commercial Resources:

CCSDS Threat Green Book (updated draft not yet released)
CENTRA Tech. – Cyber Content of Satellites
CENTRA Tech. – Cyber Threats to Satellite Networks
CENTRA Tech. – Cyber Threats to Satellite-Based IP Networks
CENTRA Tech. – Chinese Research – Satellite Bus Vulnerabilities
CENTRA Tech. – Foreign Satellite Developers Design & Cyber Content
Orbital Security – Space Cyber Guidelines for Commercial Satellites rev-1.0.1
NIST 800-53 Rev 4
Cybersecurity for Space: Protecting the Final Frontier (rel. March2020)

- Develop generic SV threat/vulnerability reference library for use
- Enables threat informed cyber requirements generation
  - *Rank threats/vuln on 5x5 to help drive threats/vuln that need mitigated and thereby driving requirement selection*

Snapshot of SV Threats/Vulnerabilities



ID	Threat/Vulnerability Description	Threat/Vulnerability Source	CAPEC #	Control Tag Mappings	Lowest Threat Tier (I-VII) to Create Threat Event	DiD Graphic Subcategory
SV-AC-1	Attempting access to an access-controlled system resulting in unauthorized access	* CCSDS Threat Green Book * CENTRA Volume I - Cyber Content of Satellites * Cybersecurity for Space: Protecting the Final Frontier	20, 21, 94, 102, 114, 115, 161, 180, 248, 463, 594, 616	IA-5(7),SI-10(3),AC-3(10),AU-3(1),IA-5,IA-7,SC-10,SC-12,SC-12(1),SC-12(2),SC-12(3),SC-13,SC-28(1),SC-7,SC-7(11),SC-7(18),SI-3(9),SI-10,SI-10(5), AC-17(1),AC-17(2)	III	Crypto
SV-AC-2	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	* CCSDS Threat Green Book * CENTRA Volume I - Cyber Content of Satellites	60, 195	AU-3(1),IA-2(8),IA-2(9),IA-3,IA-3(1),IA-4,IA-7,SC-13,SC-23,SC-7,SC-7(11),SC-7(18),SI-3(9),SI-10,SI-10(5),AC-17(1),AC-17(2)	III	Crypto
SV-AC-3	Compromised master keys or any encryption key	* CCSDS Threat Green Book * CENTRA Volume I - Cyber Content of Satellites	20, 97, 474, 485,622	IA-5,IA-5(7),IA-7,SC-12,SC-12(1),SC-12(2),SC-12(3),SC-13,SC-28(1)	III	Data
SV-AC-4	Masquerading as an authorized entity in order to gain access/Insider Threat	* CCSDS Threat Green Book	195, 390, 391, 395, 397, 416	AT-2(2),IR-4(7),PE-3,PM-12	IV	Prevention
SV-AC-7	Weak communication protocols. Ones that don't have strong encryption within it	* CENTRA - Cyber Threats to Satellite Networks	192, 272, 276, 277	SA-4(9),SC-8, SC-8(1), SC-8(2), SC-8(3),SI-7(6)	III	Comms Link
SV-AC-8	Malicious Use of hardware commands - backdoors / critical commands	* NASA Mission Resiliency Protection Program Cyber Protection Strategies	88, 248	SI-10, SI-10(3)	III	SBC
SV-AV-1	Communications system jamming resulting in denial of service and loss of availability and data integrity	* CCSDS Threat Green Book	559, 599, 603, 619	CP-8,AC-18(5),SC-5,SC-40,SC-40(1),SC-40(3),SI-10,SI-10(3)	V	Comms Link

CAPEC helps by providing a comprehensive dictionary of known patterns of attack employed by adversaries to exploit known weaknesses in cyber-enabled capabilities.

Mitigating Controls

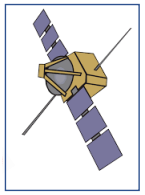
Generic Threat Model Tier

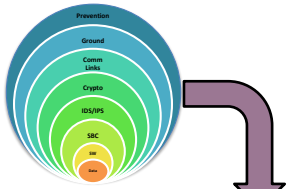
Defense-in-Depth Layer

AC = Access Control
AV= Availability
CF = Confidentiality
DCO = Defensive Cyber Operations.
IT = Integrity
MA = Mission Assurance
SP = Supply Chain
SV = Space Vehicle

= *Space Vehicle Availability Threat ID 1*

Threat Action *Exploits* Vulnerability

SV Cyber  Threats/Vulns



Data

SV-AC-3 Compromised master keys or any encryption key

SV-IT-2 Unauthorized modification or corruption of data

SV-CF-2 Eavesdropping (RF and proximity)

SV-MA-2 Heaters and flow valves of the propulsion subsystem are controlled by electric signals so cyber attacks against these signals could cause propellant lines to freeze, lock valves, waste propellant or even put in de-orbit or unstable spinning

S/C Software

SV-SP-1 Exploitation of software vulnerabilities (bugs); Unsecure code, logic errors, etc. in the FSW.

SV-SP-3 Introduction of malicious software such as a virus, worm, Distributed Denial-Of-Service (DDOS) agent, keylogger, rootkit, or Trojan Horse

SV-MA-3 Attacks on critical software subsystems {AD&C, TT&C, C&DH, EPS}

SV-SP-6 Software reuse, COTS dependence, and standardization of onboard systems using building block approach with addition of open source technology leads to supply chain threat

SV-AV-4 Attacking the scheduling table to affect tasking

SV-IT-5 Onboard control procedures (i.e. ATS/RTS) that execute a scripts/sets of commands

SV-SP-9 On-orbit software updates/upgrades/patches/memory writes.

SBC/Processor/Bus

SV-AC-5 Proximity operations (i.e. grappling satellite)

SV-AV-2 Cyber attack to disrupt timing/timers could affect the vehicle (Time Jamming / Time Spoofing)

SV-AC-6 Lack of bus segregation (e.g. 1553 injection). Things are not containerized from the OS or FSW perspective

SV-AV-3 Affect the watchdog timer onboard the satellite which could force satellite into some sort of recovery mode/protocol

SV-IT-3 Compromise boot memory

SV-IT-4 Cause bit flip on memory via single event upsets

SV-SP-7 Attacking the on-board operating systems. OS has a critical role in the overall security of the system.

SV-AV-8 Clock synchronization attack for Spacewire.

SV-AC-8 Malicious Use of hardware commands - backdoors / critical commands

SV-MA-8 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.

SV-SP-11 Software defined radios cyber attack

IDS/IPS

SV-AV-5 Using fault management system against you.
Example, safe-mode with crypto bypass, orbit correction maneuvers, affecting integrity of TLM to cause action from ground, or some sort of RPO to cause S/C to go into safe mode;

SV-AV-6 Complete compromise or corruption of running state

SV-DCO-1 Not knowing that you were attacked or attack was attempted

SV-MA-5 Not being able to recover from cyber attack

Crypto

SV-IT-1 Communications system spoofing resulting in denial of service and loss of availability and data integrity

SV-CF-1 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

SV-AC-1 Attempting access to an access-controlled system resulting in unauthorized access

SV-AC-2 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

SV-CF-4 Adversary monitors for safe-mode indicators such that they know when satellite is in weakened state and then they launch attack

Comms Link

SV-AV-1 Communications system jamming resulting in denial of service and loss of availability and data integrity

SV-AC-7 Weak communication protocols. Ones that don't have strong encryption within it

Ground

SV-MA-7 Exploit ground system and use to maliciously to interact with the SV

Prevention

SV-AC-4 Masquerading as an authorized entity in order to gain access/Insider Threat

SV-SP-2 Testing only focuses on functional requirements and rarely considers end to end or abuse cases

SV-SP-4 General supply chain interruption or manipulation

SV-MA-1 Space debris

SV-SP-5 Hardware failure (i.e. tainted hardware) {ASIC and FPGA focused}

SV-CF-3 Knowledge of target satellite's cyber-related design details would be crucial to inform potential attacker - so threat is leaking of design data which is often stored Unclass or on contractors network

SV-AV-7 TT&C in first 10 years leads to most faults; degradation of moving parts follows (gyro, momentum wheels, etc.); then attitude control being other threat

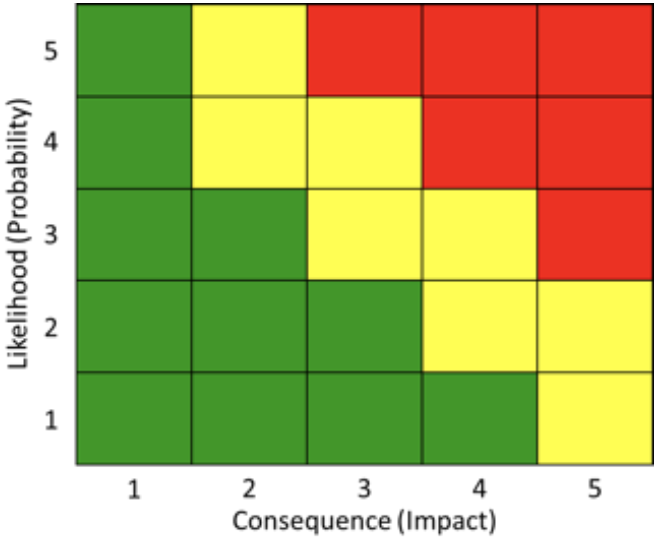
SV-MA-4 Not knowing what your crown jewels are and how to protect them now and in the future.

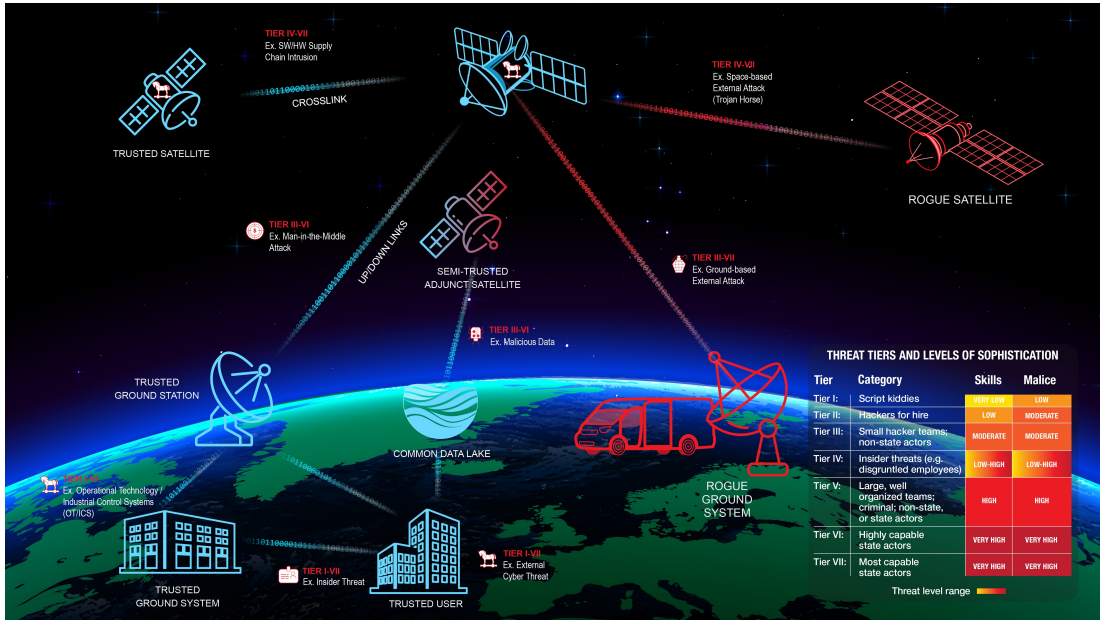
SV-SP-10: Compromise development environment source code (applicable to development environments not covered by threat SV-SP-1, SV-SP-3 and SV-SP-4)

SV-MA-6 Not planning for security on SV or designing in security from the beginning

Risk Management Drives DiD Control Implementation

- Risk management (driven by threats) is a key component when architecting a secure space system or assessing its security gaps. 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





Using adversary threat modeling can help with security control selection.

Must be risk-based engineering and not “compliance” focused

Lenses on Risk

- The Institute for Defense Analysis (IDA) did a study to compare various mission based cyber risk methodologies
  - *Found more than 20 unique methodologies in use*
  - *Most of the models included the same three elements combined in different ways to get to a two-dimensional risk matrix*
- The three common elements are
  - *Criticality (aka, Impact)*
  - *Threat (agent, action)*
  - *Vulnerability*

- ➢ A risk only occurs at the intersection of criticality, threat and vulnerability
  - ➢ But likelihood must be considered
- ➢ You should be able to clearly identify all three in whatever risk method you utilize

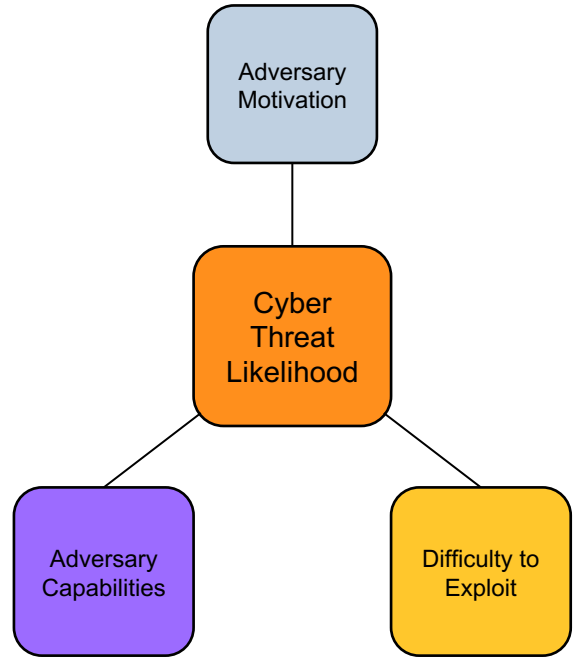
Breaking Down Likelihood

- Probably know the criticality/impact for our mission
- What about how "likely" the threat can exploit the weakness/vulnerability
- Likelihood – a three legged stool
  - *How difficult would it be to exploit accounting for mission design, operational environment, etc.*
  - *Why would threat agent act? What is their motivation?*
  - *What actions are required? What are the capabilities of the threat agent?*
    - Real threat intel (if available) with known adversary capabilities and motivation
    - Can leverage tiered generic threat model when real intel not available

Difficulty to Exploit

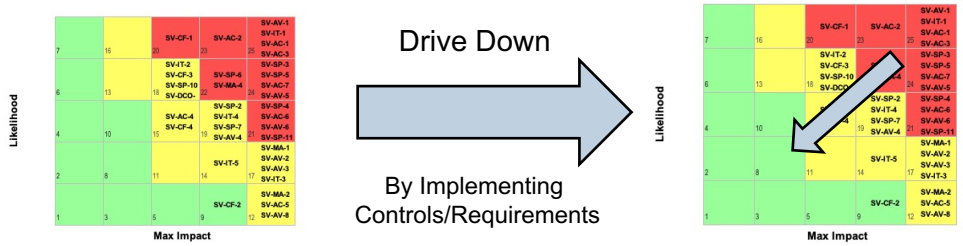
Adversary Motivation

Adversary Capabilities



Risk Based Tailoring using a 5x5

- Evaluate each applicable cyber threat for a mission
  - *Impact on the mission*
  - *Likelihood informed by real threat intel (if available) with known adversary capabilities and motivation*
    - Difficulty to exploit is mission dependent and should be considered
- Once you have threat/vulnerability rating, it can be a starting point for requirements or defense-in-depth principles tailoring, etc. in addition to any compliance baselines
  - *For legacy (existing missions), you identify current security gaps and mitigate if possible*
- The result of the process would be a tailored set of cyber mitigations for the mission to drive down risk



ort	ID	Threat/Vuln Category	Max Impact	Likelihood	Rank	
1	SV-AV-1	TT&C Security	5	5	25	Communications system jamming resulting in denial of service and loss of availability and data integrity
2	SV-IT-1	TT&C Security	5	5	25	Communications system spoofing resulting in denial of service and loss of availability and data integrity
4	SV-AC-1	TT&C Security	5	5	25	Attempting access to an access-controlled system resulting in unauthorized access
6	SV-AC-3	TT&C Security	5	5	25	Compromised master k[illegible] or any encryption key
8	SV-SP-1	Supply Chain	5	5	25	Exploitation of software v[illegible]erabilities (bugs); Unsecure code, logic errors, etc. in the FSW.
18	SV-MA-3	SV Mission Assurance	5	5	25	Attacks on cri[illegible]ware s[illegible]ms * Attitude Determination and Control (AD&C) subsystem determines and co
38	SV-AC-8	SV Access Control	5	5	25	Malici[illegible]s Use c[illegible]har[illegible]commands - backdoors / critical commands
12	SV-MA-7	SV Mission Assurance	5	5	25	Exploit [illegible]und s[illegible]em and use to maliciously to interact with the SV
10	SV-SP-3	Supply Chain	5	4	24	[illegible]duction of m[illegible]icious software such as a virus, worm, Distributed Denial-Of-Service (DDOS) agent, keylogger, roc
14	SV-SP-5	Supply Chain	5	4	24	[illegible]rdware [illegible]s (i.e. tainted hardware) {ASIC and FPGA focused}
29	SV-AC-7	SV Access Control	5	4	24	We[illegible] communication protocols. Ones that don't have strong encryption within it
30	SV-AV-5	SV Availability	5	4	24	sing fault management system against you. Understanding the fault response could be leveraged to get satellite in v
40	SV-MA-5	SV Mission Assurance	5	4	24	ot being able to recover from cyber attack
5	SV-AC-2	TT&C Security	4	[illegible]	[illegible]	Replay of recorded authentic communications traffic at a later time with the hope that the authorized communicatio
21	SV-SP-6	Supply Chain	4	4	22	Software reuse, COTS dependence, and standardization of onboard systems using building block approach with add
36	SV-MA-4	SV Mission Assurance	[illegible]	4	22	Not knowing what your crown jewels are and how to protect them now and in the future.
11	SV-SP-4	Supply Chain	5	3	21	General supply chain interruption or manipulation
20	SV-AC-6	SV Access Control	5	3	21	Three main parts of S/C. CPU, memory, I/O interfaces with parallel and/or serial ports. These are connected via buss
31	SV-AV-6	SV Availability	5	3	21	Complete compromise or corruption of running state
44	SV-SP-11	Supply Chain	5	3	21	Software defined radios - SDR is also another computer, networked to other parts of the SV that could be pivoted to
3	SV-CF-1	TT&C Security	3	5	21	Tapping of communications links (wireline, RF, network) resulting in loss of confidentiality; Traffic analysis to determ
9	SV-SP-2	Supply Chain	4	3	19	Testing only focuses on functional requirements and rarely considers end to end or abuse cases
25	SV-IT-4	SV Integrity	4	3	19	Cause bit flip on memory via single event upsets
26	SV-SP-7	Supply Chain	4	3	19	Software can be broken down into three levels (operating system and drivers layer, data handling service layer, and
27	SV-AV-4	SV Availability	4	3	19	Attacking the scheduling table to affect tasking

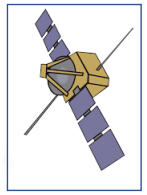
Once threats/vulnerabilities are understood and prioritized, regardless of legacy or future deployment mitigations can be deployed, or risks can be accepted.

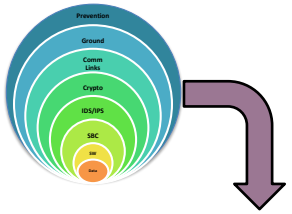
Key is to perform the necessary risk-based cyber analysis for each critical mission/capability.

Remember: Goal of 5x5 can be to identify tolerance and establish "essential" security controls

Threat Action *Exploits* Vulnerability

Essential for Generic Space System

SV Cyber  *Threats/Vulns*



Data

SV-AC-3 Compromised master keys or any encryption key

SV-IT-2 Unauthorized modification or corruption of data

SV-CF-2 Eavesdropping (RF and proximity)

SV-MA-2 Heaters and flow valves of the propulsion subsystem are controlled by electric signals so cyber attacks against these signals could cause propellant lines to freeze, lock valves, waste propellant or even put in de-orbit or unstable spinning

S/C Software

SV-SP-1 Exploitation of software vulnerabilities (bugs); Unsecure code, logic errors, etc. in the FSW.

SV-SP-3 Introduction of malicious software such as a virus, worm, Distributed Denial-Of-Service (DDOS) agent, keylogger, rootkit, or Trojan Horse

SV-MA-3 Attacks on critical software subsystems {AD&C, TT&C, C&DH, EPS}

SV-SP-6 Software reuse, COTS dependence, and standardization of onboard systems using building block approach with addition of open source technology leads to supply chain threat

SV-AV-4 Attacking the scheduling table to affect tasking

SV-IT-5 Onboard control procedures (i.e. ATS/RTS) that execute a scripts/sets of commands

SV-SP-9 On-orbit software updates/upgrades/patches/memory writes.

SBC/Processor/Bus

SV-AC-5 Proximity operations (i.e. grappling satellite)

SV-AV-2 Cyber attack to disrupt timing/timers could affect the vehicle (Time Jamming / Time Spoofing)

SV-AC-6 Lack of bus segregation (e.g. 1553 injection). Things are not containerized from the OS or FSW perspective

SV-AV-3 Affect the watchdog timer onboard the satellite which could force satellite into some sort of recovery mode/protocol

SV-IT-3 Compromise boot memory

SV-IT-4 Cause bit flip on memory via single event upsets

SV-SP-7 Attacking the on-board operating systems. OS has a critical role in the overall security of the system.

SV-AV-8 Clock synchronization attack for Spacewire.

SV-AC-8 Malicious Use of hardware commands - backdoors / critical commands

SV-MA-8 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.

SV-SP-11 Software defined radios cyber attack

IDS/IPS

SV-AV-5 Using fault management system against you. Example, safe-mode with crypto bypass, orbit correction maneuvers, affecting integrity of TLM to cause action from ground, or some sort of RPO to cause S/C to go into safe mode;

SV-AV-6 Complete compromise or corruption of running state

SV-DCO-1 Not knowing that you were attacked or attack was attempted

SV-MA-5 Not being able to recover from cyber attack

Crypto

SV-IT-1 Communications system spoofing resulting in denial of service and loss of availability and data integrity

SV-CF-1 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

SV-AC-1 Attempting access to an access-controlled system resulting in unauthorized access

SV-AC-2 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

SV-CF-4 Adversary monitors for safe-mode indicators such that they know when satellite is in weakened state and then they launch attack

Comms Link

SV-AV-1 Communications system jamming resulting in denial of service and loss of availability and data integrity

SV-AC-7 Weak communication protocols. Ones that don't have strong encryption within it

Ground

SV-MA-7 Exploit ground system and use to maliciously to interact with the SV

Prevention

SV-AC-4 Masquerading as an authorized entity in order to gain access/Insider Threat

SV-SP-2 Testing only focuses on functional requirements and rarely considers end to end or abuse cases

SV-SP-4 General supply chain interruption or manipulation

SV-MA-1 Space debris

SV-SP-5 Hardware failure (i.e. tainted hardware) {ASIC and FPGA focused}

SV-CF-3 Knowledge of target satellite's cyber-related design details would be crucial to inform potential attacker - so threat is leaking of design data which is often stored Unclass or on contractors network

SV-AV-7 TT&C in first 10 years leads to most faults; degradation of moving parts follows (gyro, momentum wheels, etc.); then attitude control being other threat

SV-MA-4 Not knowing what your crown jewels are and how to protect them now and in the future.

SV-SP-10: Compromise development environment source code (applicable to development environments not covered by threat SV-SP-1, SV-SP-3 and SV-SP-4)

SV-MA-6 Not planning for security on SV or designing in security from the beginning

Defense in Depth for Ground Segment

Defense is needed at all layers

Ground Segment

Data Encryption (DAR, DIR, Transport), Leakage, OSINT, Tempest, Permissions/Access

Software CM/Build Environment, Secure Coding Standards, CWE Prevention, Documentation/Diagrams, Dynamic Testing, SW Component/Origin Analysis, Static Code Analysis, Threat Modeling, WAF

Endpoint App Whitelisting, Auditing, Authentication, AV/AM, Backups, CM/Baseline, Device SoD, DLP, File Integrity, FW, Hardening, HIDS/HIPS, Logging, Memory Protection, Patch Mgmt, Permissions, Remote Access, Service Configuration, User Least Privilege, Vulnerability Scanning

Network Reverse Proxy, ACLs, Authentication, CM, Device Hardening, Diversification of Paths, Documentation/Diagrams, FW, Logging, NAC, NOC, NTP, Port Security, Segmentation, SNMP, Trunking, Remote Management, Web Proxy, Wireless

CND/IR Forensics, Hunting, Threat Intelligence, IDP/IPS, IR Policy/Procedures, Sensors, SIEM, SOC, TAPs

Perimeter VPN, Remote Access, DLP, DMZ/Security Zones, FW

Physical Badging/Doors, Fire Suppression, Gates/Guards, Logging, Mission Security Personnel, Infrastructure Diversity, Surveillance

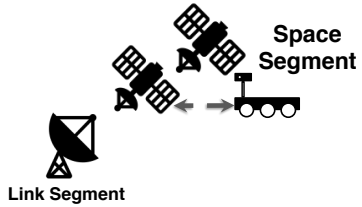
Prevention Personnel Awareness, Insider Threat, Security Assessments, Threat Analysis, Training, Supply Chain

RED: example of mission specific analysis to derive DiD principles (every mission should do given their environment/threats)

**** Expanded breakdown in backup***

Defense in Depth for the Space Segment

Defense is needed at all layers



Data Encryption (DAR, DIR, Transport), Tempest

S/C Software CM/Build Environment, Secure Coding Standards, CWE Prevention, Documentation/Diagrams, Dynamic Testing, SW Component/Origin Analysis, Static Code Analysis, Threat Modeling, Crypto Sig/Code Signing

SBC CMD Validation, Memory Protection, Root of Trust, Bus Segregation, Logging, Auditing, Least Privilege

IDS/IPS Intrusion Detection and Prevention, Fault Management System Integration, Machine Learning, Cyber-Safe Mode

Crypto NSA Type-1, Authentication, Encryption, Authenticated Encryption, Crypto Bypass

Comms Link Protocols, Frequency Bands

Ground Physical, Perimeter, CND/IR, Network, Endpoint, Software, Data

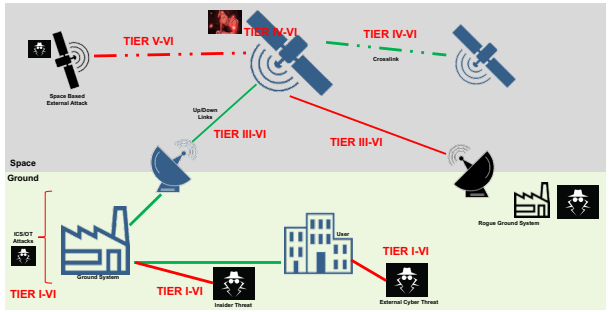
Prevention Governance/Policy/Acquisition, Risk Management, Supply Chain, Threat Analysis, Training, Insider Threat

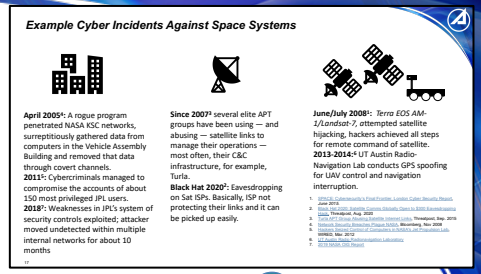
RED: example of mission specific analysis to derive DiD principles (every mission should do given their environment/threats)

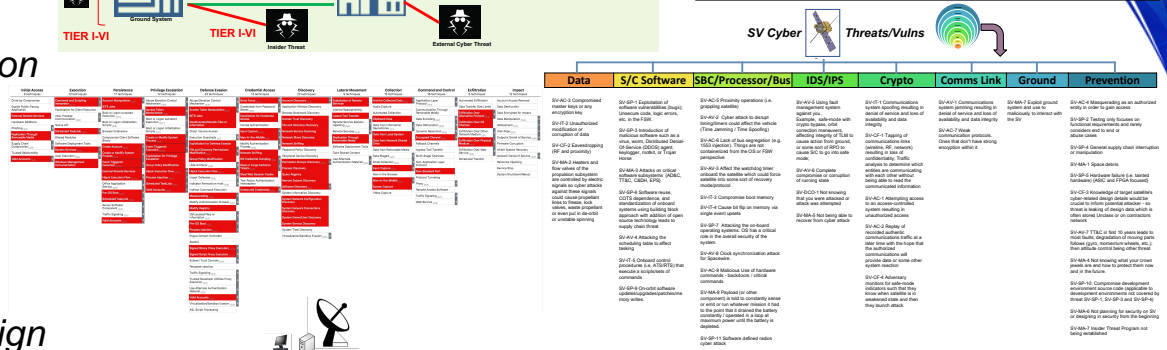
**** Expanded breakdown in backup***

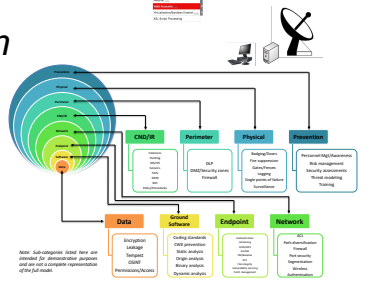
Summary

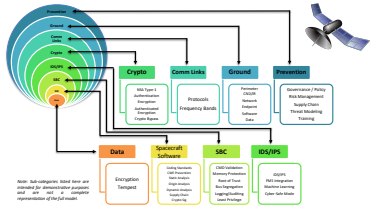
- Given the lack of critical space system failures it is convenient to ignore security
  - *Not an option moving forward as space systems are too critical for our nation and we have evidence of attacks*
  - *Understanding the threat vectors and adversary TTPs*
- Risk-based defense in depth is a big part of the solution
  - *Needs to be designed in at the beginning of our programs*
  - *Proper requirements are key!!! – w/o them we run the risk of unsecure design*
    - Inadequate cyber requirements and governance has led to the gaps around 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.)
- Using threat modeling and mission characteristics a ranking (5x5) for each cyber threat for the mission can aid in understanding cyber risk
  - *Criticality/Impact, Threat, & Vulnerability w/ Likelihood – not an exact science!*
    - Adversary tiers and/or real threat intel helps with this analysis
- Throughout the development lifecycle, including operations, robust defense-in-depth assessments are key in understanding gaps and high risk area
  - *Cannot be solely compliance process & requires in-depth technical analysis*

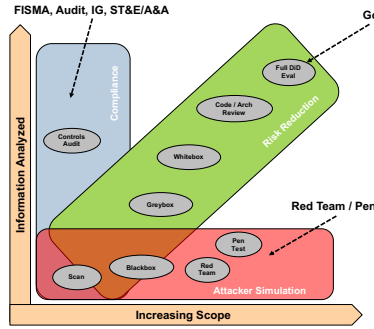












Backup Slides

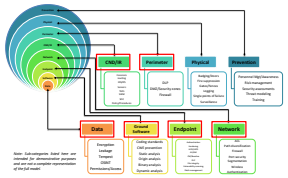
Known Space System Standards

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 & Spacecraft for National Security System (NSS) only	https://www.cnss.gov/CNSS/issuances/Instructions.cfm	Elaborates how to appropriately integrate Information Assurance 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	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 SP 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	Provides several alternative authentication/integrity algorithms which may be chosen for use by individual missions depending on their specific mission environments. 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	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	CCSDS credentials are needed to allow authentication between communicating entities for 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	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.
NASA	Space System Protection Standard	Applicable to all NASA programs and projects (starting in 2020)	https://standards.nasa.gov/sites/default/files/standards/NASA/PUBLISHED/Baseline/nasa-std-1006.pdf	Establishes Agency-level protection requirements to ensure NASA missions are resilient to threats and is applicable to all NASA programs and projects starting in 2020.

Cyber Gaps from Past Experience

Ground

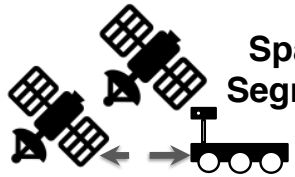
Ground Segment

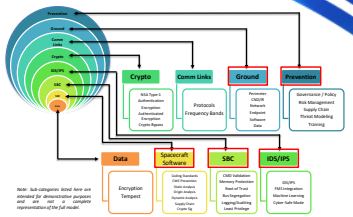


- Insider threats are rarely considered which are compounded with the other gaps below
- Computer Network Defense/Incident Response is lacking in general which affects the ground operator's ability to protect, detect, respond and recover
- Network design/segmentation is generally lacking which permits 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.)

Spacecraft

Space Segment





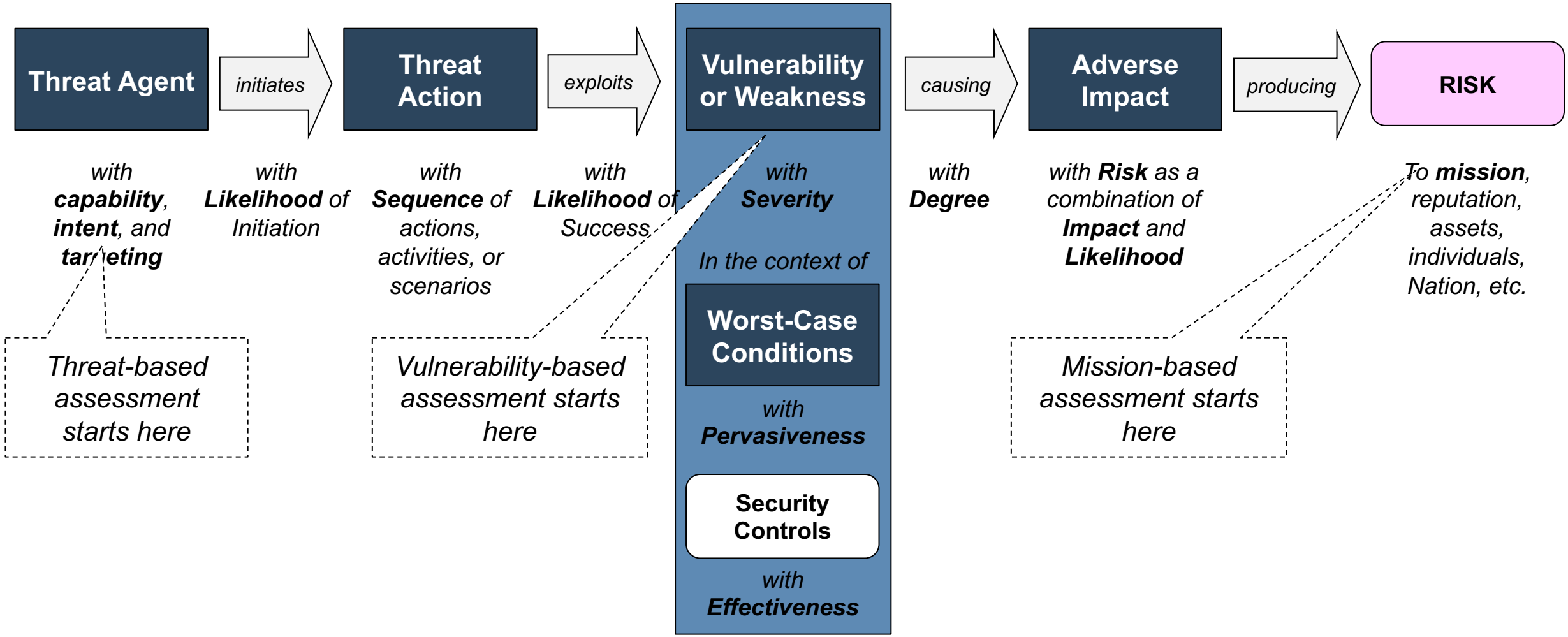
For the spacecraft, most security is geared around cryptography on the command link, Transmission Security (TRANSEC), and some Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions (TEMPEST) controls but the current gaps include:

- Insider threats are rarely considered which are compounded with the other gaps below
- Ground systems
- 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 in on-board monitoring, logging, and alerting capabilities
- Safe mode features can put spacecraft in more vulnerable state (i.e. crypto bypass mode)

Link Segment

N/A for most NSS, but some Commercial and Civil do not implement TRANSEC and/or COMSEC (authentication & encryption + key mgmt)

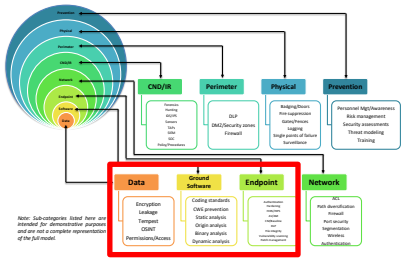
Generic Cyber Risk Model



https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Implementation of Ground Defenses

Some Examples



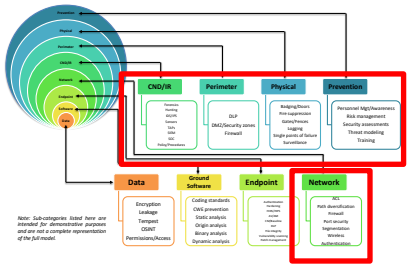
Category	Sub-Category	Implementation Goal
Data	Encryption (DAR, DIT, transport, etc.)	Ensures full disk encryption on all critical assets and for data in transit.
	Permissions/Access (sensitive) *	No iTAR / SBU / CUI / Sensitive / Classified data exposed and accessible with people who have no need to know. File servers/ Web server's security implemented.
Ground Software	Secure Coding Standards*	Secure coding standards identified in policy AND standards are enforced during implementation (e.g. violation alerts in IDE, manual code review, etc.).
	Common Weakness Enumeration (CWE) Prevention*	Performs their own system-specific CWSS scoring of CWEs for prioritization. This establishes which weaknesses will have the highest impact on the spacecraft given how the software operates.
	Dynamic Testing*	Performs continuous dynamic testing throughout application development, operations, and maintenance.
	Origin Analysis*	Maintains a software bill of materials. AND tracks all associated vulnerability information for the components. AND Regularly updates vulnerable third-party components.
	Static Code Analysis*	Performs static analysis scans with a complimentary combination of tools AND has a defined process for prioritization/remediation of security related findings.
	Threat Modeling*	Adheres to an exhaustive formal software threat modeling process following an established framework (or custom developed equivalent).

Endpoint	Application Whitelisting	Application whitelist exists and is properly used.
	Auditing	Security audits of logs are part of the security plan/policies AND security audits are efficient and executed as planned.
	Authentication	Utilizes multifactor authentication for endpoints.
	Anti-virus (AV)/Anti-malware (AM)	Anti-virus or Anti-Malware are deployed, and procedures exist to keep efficient and up to date.
	Backups	Standards, solutions, and procedures for system's backups are implemented securely and efficiently AND the process and data are routinely tested and verified.
	Configuration Management (CM)/Baseline*	CM/baseline standards/solution are properly implemented and efficient.
	Device Separation of Duties	Standards for permissions on device services and features are properly applied.
	File Integrity	A solution for file integrity checking is used efficiently (keywords, sensitive files, etc. are identified).
	Firewall (all interfaces)	Host-based firewalls are properly configured and routinely verified.
	Hardening	Security hardening standards are implemented and routinely verified as exceeding 80%.
	Host-based Intrusion Detection System (HIDS)/Host-based Intrusion Prevention System (HIPS)	HIDS/HIPS are configured, updated, and routinely verified.
	Logging	The logging process/solution is central, efficient, and reviewed frequently.
	Memory Protection	Memory protection solution is efficiently used and properly configured.
	Patch Management	Patch management program/standards is efficient, up-to-date, and properly configured for all software (OS/apps).
	Permissions	Documented application or procedure for permissions on files, directories, applications, or accounts/groups are applied correctly.
	Remote Access	Policies for remote access to systems are properly implemented using secure communication protocols.
	Service Configuration	Documented application or procedures for services' security configuration are properly implemented.
	User Least Privilege	Individual users separated by roles AND users have to reauthenticate for all elevated privileges.
	Vulnerability Scanning*	A vulnerability assessment process exists where tuned scan profiles are used for all systems AND administrative credentials are used for more than 90% of scans.

*The sub-categories denoted with * could be controls implemented during development/sustainment in addition to an operational control*

Implementation of Ground Defenses

Some Examples



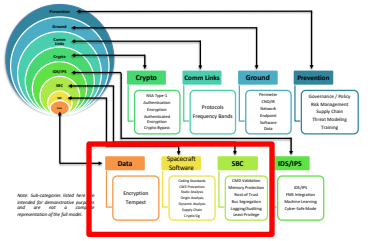
CND/IR	Hunting	Personnel are trained and tasked to continuously monitor logs/traffic
	Threat Intelligence*	Collaborates with threat intelligence sources both internal and external to the organization and integrates into tools where appropriate.
	IDS/IPS	IDS/IPS has insight to all critical areas of network AND staff is in place to monitor alerts 24/7.
	Incident Response Policy/Procedures*	Has fully documents IR procedures. AND performs self-assessments via tabletop exercises.
	Sensors	Sensors are deployed in-line to monitor critical data flows OR sensors are place at aggregation points.
	Security Information & Event Manager (SIEM)	SIEM is present in and customized alerts are configured. AND performs 24/7 monitoring of events (on-site or remote alerting).
	Security Operations Center (SOC)	Has a local dedicated SOC with insight into all the necessary critical data flows.
	Test Access Points (TAPs)	Full deployment of TAPs in-line of all critical data flows OR TAPs are deployed in an aggregation style deployment where all critical data flows are captured.
Perimeter	Virtual Private Network (VPN)/Remote Access	VPN, multi-factor authentication, and host verification required for access to internal system resources.
	Demilitarized Zones (DMZs)/Security Zones	Services hosted for external consumption are properly protected by DMZ/security zoning AND proper limitations placed on internal network access and authentication.
	Firewall	Firewalls are configured with highly refined rulesets AND firewall configurations are routinely verified AND firewall configurations are routinely verified.
Physical	Badging/Doors	Badging in & out with pin is required.
	Infrastructure Diversity	All critical components have geographically dispersed (300 miles) redundancies.
Prevention	Personnel Awareness*	Insider threat training required.
	Security Assessments	ATO granted and yearly A&A occurs with security assessments on critical infrastructures.
	Threat Analysis*	Has ability to implement controls / intel into infrastructure based on classified threat intel and how it applies to their system.
	Training*	Regular role-based cyber training with hands on training occurs at least yearly AND performs ongoing social engineering campaigns to reinforce security awareness (e.g. phishing/vishing campaigns).

Network	Access Control Lists (ACLs)	Tailored ACLs with near complete system coverage (this ties into segmentation as well).
	Authentication	Central authentication used by default (RADIUS/TACACS) with local as backup for network devices.
	Device Hardening	No Telnet or HTTP enabled, secure hash algorithms are used, no cisco smart install. AND Unused ports are disabled (i.e. shutdown) and in a suspended VLAN.
	Diversification of Network Paths	Fault tolerant pathways established on network Core, Distribution, and Access.
	Firewall (internal network boundaries)	Firewalls are configured with highly refined rulesets AND firewall configurations are routinely verified.
	Logging (on devices and ACLs)	Tailored logging is performed and is stored in a common central location.
	Network Access Control (NAC) - Device Authorization	Complete 100% coverage of NAC.
	Network Operations Center (NOC)	Full time NOC operated 24/7.
	Port Security	Utilizing sticky MACs with 3 or less reservations per port for all ports.
	Segmentation	Micro segmentation (separation of duties in network segmentation form) exists AND proper VLAN'ing with unique VLAN IDs is followed in the entire environment.
	Simple Network Management Protocol (SNMP)	Uses SNMPv3 with proper configuration (auth, server, alert settings).
	Wireless (Could play in with Security zones really only practical for Guest)	No wireless networks in mission operations environment OR wireless networks utilize 802.1x authentication with WPA2 OR wireless networks feature Active Directory integration with WPA2 Enterprise and device level authentication.

*The sub-categories denoted with * could be controls implemented during development/sustainment in addition to an operational control*

Implementation of Defenses for Space Segment

Some Examples

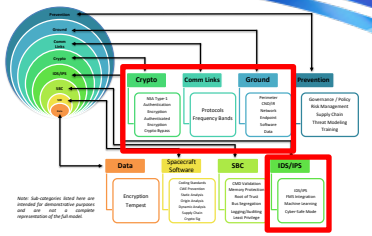


DiD Layer	DiD Sub-Layer	Implementation Goal
Data	Encryption (DAR, DIT, transport, etc.)	Ensures confidentiality and integrity at rest or in transit (within the spacecraft) for all critical data.
	Tempest	Shielding sensitive equipment from emanating electromagnetic radiation that may carry sensitive information. Applied to prevent the information from being intercepted by outside entities.
S/C Software	Configuration Management (CM)/Build Environment*	Build environment is reproducible and verifiable (e.g., software bill of materials validation) throughout the build process. Stringent source code control with strong authentication (e.g., multi-factor) on software commits. Build system needs to be deterministic where the source code always produces the same resulting build.
	Secure Coding Standards*	Secure coding standards identified in policy. AND Standards are enforced during implementation (e.g., violation alerts in IDE, manual code review, etc.).
	Common Weakness Enumeration (CWE) Prevention*	Performs own system-specific scoring of CWEs for prioritization of which weaknesses will have the highest impact on the spacecraft given how the software operates.
	Documentation/Diagrams (deployed location, I/O, data types, etc.) *	Maintains high-level documentation of software architecture with data flows defined. AND Maintains lower-level diagrams of input/output modules with data types handled by each.
	Dynamic Testing*	Performs continuous dynamic testing throughout flight software development, operations, and maintenance.
	Software Component Analysis (i.e., Origin Analysis) *	Maintains complete knowledge of software components utilized in flight software (e.g., software bill of materials). AND Tracks all associated vulnerability information for the components.
	Static Code Analysis*	Performs static analysis scans with a complimentary set of tools. AND has a defined process for prioritization/remediation of security related findings.
	Threat Modeling*	Adheres to a formal software threat modeling process following an established framework (or custom developed equivalent).
	Crypto Signatures/Code Signing	Lightweight cyber protection functions implemented (e.g., hashes), and best practices applied in subsystems/firmware throughout the spacecraft to assure the software author and guarantee that the code has not been altered or corrupted since it was signed. Software and firmware updates verified with cryptographic signatures/code signing. Cryptographic signatures provide the means to protect the integrity of the content and to verify its authenticity.
SBC/Bus/ Processor	CMD Validation	All received commands have authentication and validation. Appropriate counters are used for both valid and invalid commands.
	Memory Protection	Memory monitoring and protection solution is efficiently used and configured.
	Root of Trust (RoT)	RoT trusted computing module implemented on radiation tolerant burn-in (non-programmable) equipment. RoT functions, such as verifying the device's own code and configuration, must be implemented in secure hardware.
	Bus Segregation	Communication buses which bridge critical and non-critical spacecraft systems should either be separated or explicitly protected. Shared bus communication between components that cannot be separated should have countermeasures applied at each component's interface (e.g., encryption, authentication, babble protections).
	Logging	Collection and storage of data over a period of time to analyze events/actions of the system, such as interactions through which data, files, or software is stored, accessed, or modified. The spacecraft should independently perform command logging and anomaly detection of command sequences for cross validation.
	Auditing	Security audits of logs are part of the mission's security plan/policies/procedures. AND Security audits are efficient and executed as planned.
	Least Privilege	OS tasks run in the context of least privilege and a zero-trust approach is used with flight processor software.

*The sub-categories denoted with * could be controls implemented during development/sustainment in addition to an operational control*

Implementation of Defenses for Space and Link Segments

Some *Examples*



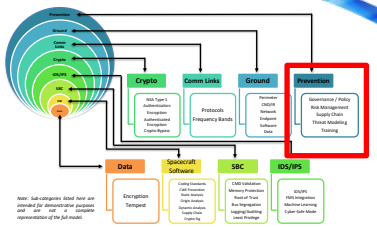
IDS/IPS	**Intrusion Detection and Prevention**	Continuous monitoring of telemetry, command sequences, command receiver status, shared bus traffic, and flight software configuration and operating states. Implementation of both signatures based and algorithm/machine learning-based anomaly detection techniques.
	Fault Management System Integration	IDS and fault management systems should be integrated as they are performing similar functions but looking for different anomaly signatures. Consideration should also be included to avoid conflicting actions between the two systems.
	Machine Learning	Automation should be trained on a data set that includes a variety of typical system operations and undergoes adversarial attack methods. Space operations are highly structured and in general lend themselves well to machine learning for anomaly detection.
	Cyber-Safe Mode	The spacecraft IPS and the ground should retain the ability to return spacecraft critical systems to a known cyber-safe mode where all non-essential 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 enabled by the RoT hardware.
Crypto	**NSA Type-1**	A Type 1 product is a device or system certified by the NSA for cryptographically securing confidentiality of classified U.S. Government information. Type-1 is usually only applicable to National Security Space missions. The term "Type 1" also refers to any cryptographic algorithm (or "Suite," as NSA refers to them) that has been approved by NSA for use within Type 1 equipment.
	Authentication (w/o Encryption)	Authentication, integrity, and the anti-replay function on the space communication link when data confidentiality is not required. Authentication for spacecraft commands provides assurance that the spacecraft can only be controlled/commanded by an authorized control center.
	Encryption (non-Type-1 w/o Authentication)	Provides data confidentiality but no authentication or integrity. Encryption primitives transform a block of plaintext data into ciphertext data. Encryption-only for a particular use case does not protect against malicious manipulation of data.
	Authenticated Encryption (non-Type-1)	Combination of encryption and authentication, thus, providing data confidentiality, data integrity, authentication, and anti-replay function. Authenticated encryption algorithms combine authentication and encryption algorithms with a single cryptographic key and algorithm.
	Crypto Bypass	Crypto bypass is completely disabled. All communication is properly encrypted.

Comms Link	**Protocols**	Communications protocol designed to be used over a space link, or in a network that contains one or multiple space links. A space link is a communications link between a spacecraft and its associated ground system or between two spacecraft. Protocols should include the capability to support security principles like authenticated encryption within the protocol.
	Frequency Bands	Having resilient communication uplink methods such as multiple paths, frequency hopping, or spread spectrum.
Ground	**Physical**	Traditional physical security controls for a physical location, such as badge control, fire suppression, guards/gates/guns with proper surveillance.
	Perimeter	Ground infrastructure has proper firewall configurations, data loss prevention, and security zones for external interactions (i.e., DMZ).
	Computer Network Defense/Incident Response (CND/IR)*	Robust architecture is established with threat hunting, intrusion detection/prevention, targeted sensor placement with TAPs and SIEMs. Security operations center functions with documented procedures and policies to detect, respond, and recover.
	Network	Employment of least-trust principles with protection such as access control lists, segmentation, port security, and communication authentication.
	Endpoint*	Hardening of endpoint devices such as two-factor authentication, host-based intrusion detection/protection, anti-virus/malware, patching and vulnerability scanning.
	Software*	Utilization of software assurance methods for all ground system software. Procedures and tools are available to prevent CWEs and eliminate CVEs as well as tracking software bill of materials. Dynamic analysis in space-centric cyber test beds is performed.
	Data*	Data-at-rest and data-in-transit encryption is utilized, TEMPEST is deployed, Operations Security (OPSEC) is practiced, permissions and access control are applied to all sensitive data.

*The sub-categories denoted with * could be controls implemented during development/sustainment in addition to an operational control*

Implementation of Defenses for Space and Link Segments

Some *Examples*



Prevention	**Governance / Policy / Acquisition***	Cybersecurity requirements are established in overarching policies and flow down into acquisition for contractors to implement.
	Risk Management*	Integration of cyber threat risk assessment with overall concepts of risk management during requirements creation. Infusion of cyber resilience and concepts into the initial stages of concept development enables trades of possible mitigations or alternative architectures. Leverage adversary simulation and digital twin technologies to perform technical security testing at the system level. More technical analysis and testing should be included in the risk management and approval process.
	Supply Chain*	Establish supply chain risk management program for hardware and software suppliers. Critical components and subsystems should be identified and handled with prioritization to mitigate primary impacts to the system.
	Threat Analysis*	Ability to gather and analyze threat intelligence against the system.
	Training*	Regular role-based cyber training occurs at regular intervals. For example, mission operators need to perform threat hunting or red versus blue events where defensive cyber operators learn how to detect, respond, and recover from cyberattacks.
	Insider Threat*	While defense-in-depth will aid in mitigating insider threat to a degree, a formalized insider threat program is warranted in many cases to ensure dedicated resources and training are available.

*The sub-categories denoted with * could be controls implemented during development/sustainment in addition to an operational control*