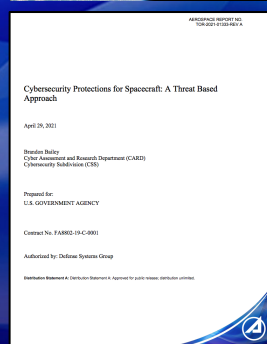




# Using SPARTA to Conduct Space Vehicle Cyber Assessments

**Brandon Bailey**  
**Cybersecurity and Advanced Platforms Subdivision (CAPS)**  
**Cyber Assessment & Research Dept (CARD)**  
**The Aerospace Corporation**



**Papers:**

- [Defending Spacecraft in the Cyber Domain](#)
- [Establishing Space Cybersecurity Policy, Standards, & Risk Management Practices](#)
- [Cybersecurity Protections for Spacecraft: A Threat Based Approach](#)
- [Protecting Space Systems from Cyber Attack](#)

**Presentations:**

- [DEF CON 2020: Exploiting Spacecraft](#)
- [DEF CON 2021: Unboxing the Spacecraft Software BlackBox Hunting for Vulnerabilities](#)
- [DEF CON 2022: Hunting for Spacecraft Zero Days using Digital Twins](#)
- [DEF CON 2023: Building Space Attack Chains using SPARTA](#)

**brandon.bailey@aero.org**  
**240.521.4326 (c)**

Space Cyber  
<https://medium.com/the-aerospace-corporation/space-cyber/home>





# Targeted Audience and Outline

- Audience: experienced in penetration testing or red teaming
- Prerequisite(s) and assumed knowledge
  - *Space system knowledge; specifically, space vehicles*
  - *Has conducted some level of offensive operations on a system*
  - *Understands SPARTA / reviewed SPARTA resources (<https://sparta.aerospace.org/resources/>)*
- Outline
  - *Space 101 (if needed – can skip if space SME)*
  - *Assessments of Space Vehicles*
    - Determining which techniques can have high impact and/or high likelihood
      - *Decomposing the space vehicle, mission, and attack surface*
    - Build procedures to implement the techniques to execute on the SV
    - Determine the actual impact in context of the mission upon execution of the technique(s)
    - Determining risk based on results
  - *Using SPARTA to help with recommendation / countermeasures*
  - *Alternative approach for assessing space vehicles*

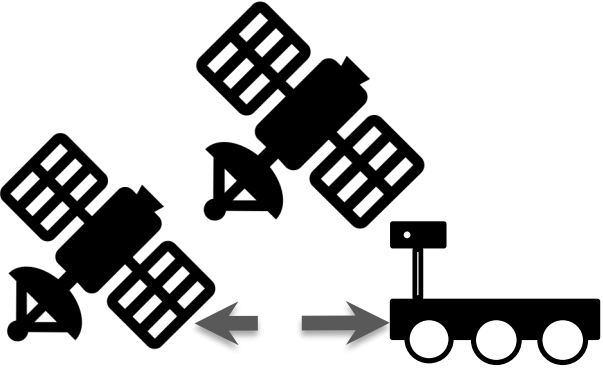


# ***Space 101***

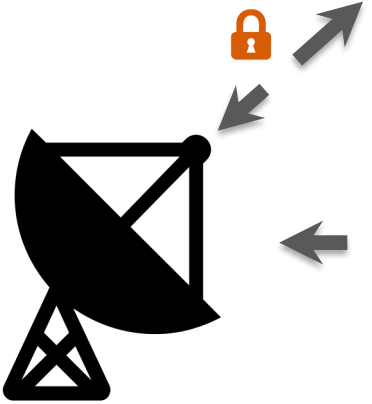


# Components of A Space System

SPD-5<sup>1</sup> 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.”

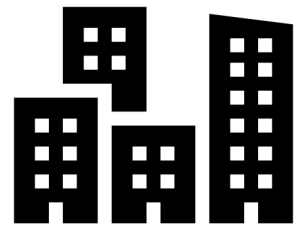


**Space Segment**  
Earth-orbit satellites, planetary probes, deep space



**Link Segment**

Ground-to-space communications, including user devices such as GPS, handhelds, small radio ground stations



**Ground Segment**

Operations & Support



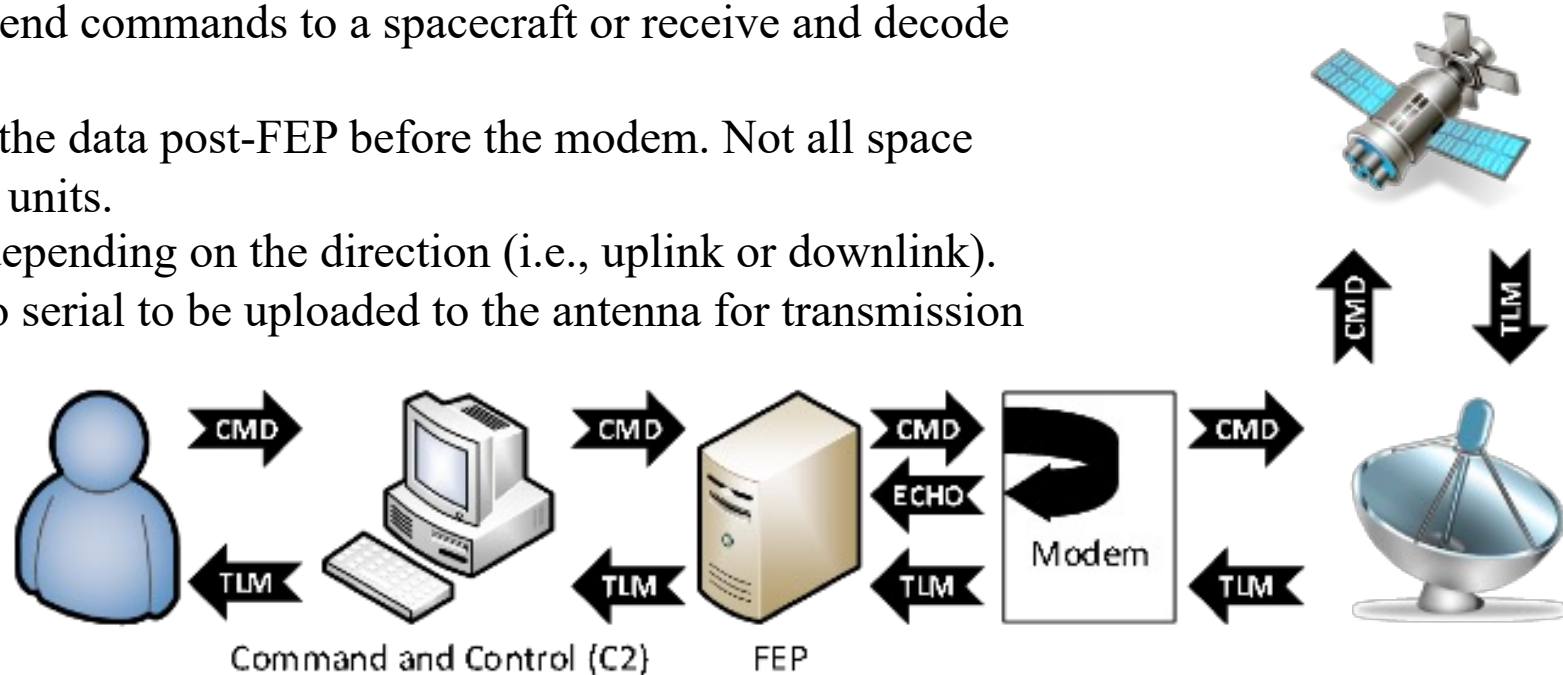


## Basic Terminology – Terms and Definitions

- **Commands (CMD):** Commands are instructions that are sent to the spacecraft. The command database translates text-based commands and parameters to the binary form required by the spacecraft or instrument/payload.
- **Telemetry (TLM):** Data from a spacecraft is telemetry, engineering (housekeeping) or science data
- **Pseudo Telemetry / Derived Telemetry:** Data defined in the telemetry database, not received from the spacecraft, but derived as specified by an Equation=statement. Calculated periodically (~1Hz) or when a telemetry pack is received, event driven pseudo telemetry.
- **Command & Telemetry Database:** Defines the structures for translating packets. These structures are compiled to create the telemetry and command database.
- **Command & Controls (C2):** workstation(s) that relay commands and receive telemetry to and from a spacecraft in a reliable manner
- **Front End Processor (FEP):** encode and send commands to a spacecraft or receive and decode telemetry from a spacecraft
- **Crypto (not always applicable):** encrypts the data post-FEP before the modem. Not all space systems leverage hardware bulk encryption units.
- **Modem:** modulates/demodulates the data depending on the direction (i.e., uplink or downlink). For uplink it translates network packets into serial to be uploaded to the antenna for transmission via Radio Frequency (RF)

- **Packet and APID**

A packet is the basic unit for receipt of telemetry and sending of commands. Every packet type has a unique number called an APID.



# Basic Terminology (cont.)

- A few terms

- *Spacecraft Bus* – usually refers to the fundamental systems of a spacecraft, i.e.

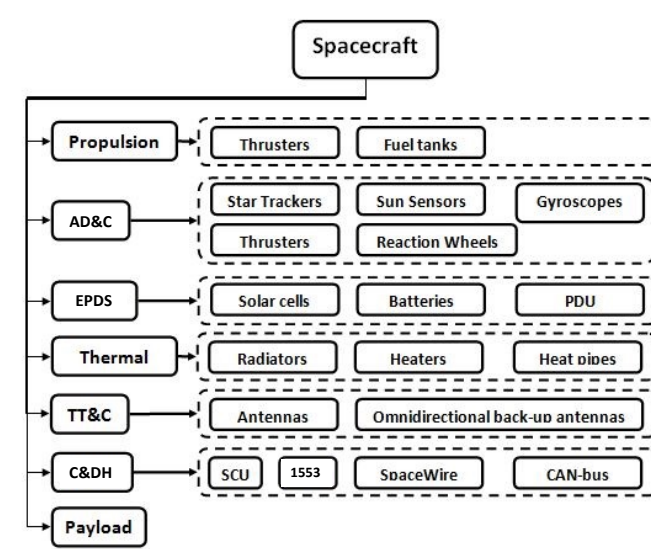
- Mechanical Structure
- Electrical System
- Power System
- Command and Data Handling System (C&DH)
- Attitude Control System/ Propulsion System
- RF System
- Thermal System

- *Payloads* – refers to the instruments on board, i.e.

- Cameras, Telescopes, Radars, etc.

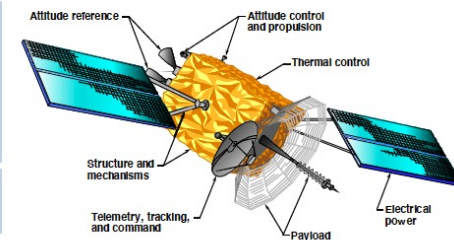
- *Flight Software* is

- Software that flies
- Could be part of the Spacecraft Bus, or an Instrument
- Hosted within flight electronics CPU; e.g., embedded in the C&DH
- Starts when Spacecraft Power is applied to the CPU
- The “Brains” of the on-orbit mission



Subsystem and Descriptions

Attitude Reference and Control	<ul style="list-style-type: none"> <li>▢ Detects satellite orientation relative to onboard measurements or surrounding landmarks</li> <li>▢ Adjusts orientation or position using thrusters, gimbals, or compressed gases</li> </ul>
Command and Data Handling	<ul style="list-style-type: none"> <li>▢ Both onboard and ground operator-sent software commands to be processed</li> <li>▢ Fault detection, health checks, and recovery modes are built in</li> <li>▢ Onboard storage and processing may need encryption or environmental protection</li> </ul>
Power	<ul style="list-style-type: none"> <li>▢ Amount and quality of power, including requirements for duty cycle, average, and peak power</li> </ul>
Structure/Thermal	<ul style="list-style-type: none"> <li>▢ Stable platform for all components</li> <li>▢ Thermal control for all components</li> <li>▢ Location of components with respect to each other</li> <li>▢ Fields of view and movements of antennas, solar arrays, and payloads</li> </ul>
Communications	<ul style="list-style-type: none"> <li>▢ Interaction with ground stations and terminals</li> <li>▢ Interaction with other satellites (e.g., crosslink)</li> <li>▢ Communications security; encryption/decryption</li> <li>▢ Margin for uplink/downlink</li> </ul>
Propulsion	<ul style="list-style-type: none"> <li>▢ Orbit insertion, correction, or repositioning</li> <li>▢ Life-limiting finite resource</li> </ul>



## Comms – Ground to Space

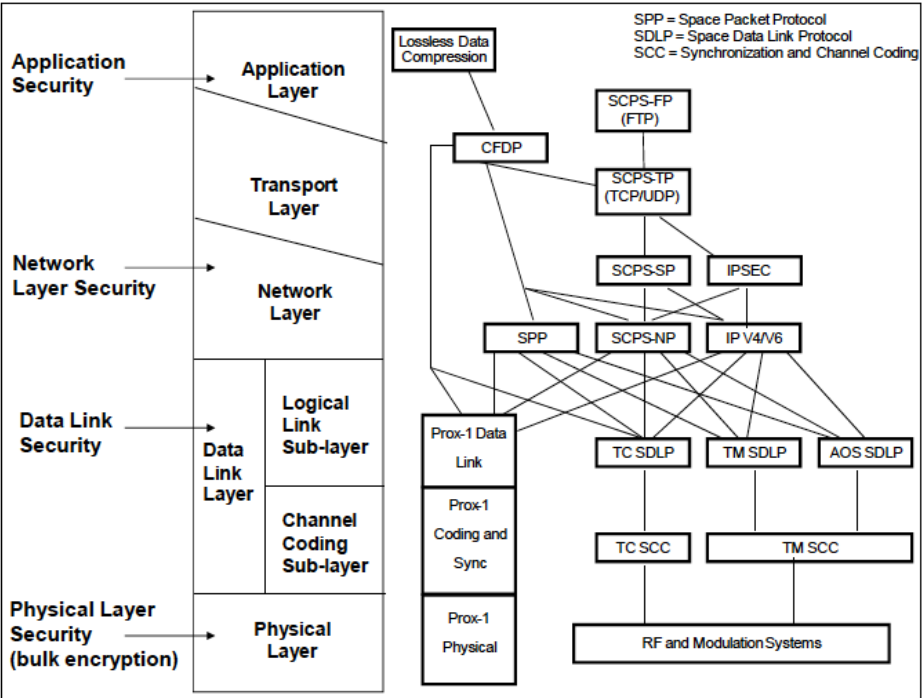


- In the simplest form, a space system is a C2 workstation that is interacted with by some user to communicate to a spacecraft
- The commands are processed by ground software and forwarded to the FEP which formats and frames the messages. From there the data is either sent to a crypto module or if cryptography is not being used it is sent directly to a modem for modulation
- The data is modulated and sent to the antenna for uplink to the spacecraft via RF. For the downlink the reverse occurs where the antenna receives the data via RF, the modem demodulates, the FEP translates the data for delivery to the ground software where the user views the telemetry/data.
- For our purposes, a device on the ground that transmits and/or receives as the “ground system” and referred to the device in space that transmits or receives as the “spacecraft”. The term “payload” refers to the instrument or device onboard the spacecraft performing the mission or collecting data. The ground system includes everything up to the antenna where the spacecraft (and payload) is merely the asset in space.
- Ground system’s antenna may either have a stationary, nondirectional antenna or a movable directional antenna. As an example, when using a directional antenna to communicate with the spacecraft the antenna must slew to be in line with the passing spacecraft. From a cybersecurity perspective, this is often referred to as “cyber physical” and resembles many ICS/OT systems. With directional communications, you communicate to the spacecraft by pointing the ground system’s transmitter receiver in line with the antenna on the spacecraft which will do the same. Doing this enables the utilization of frequencies capable of higher bandwidth to take advantage of each time the spacecraft comes into view in the sky. To maintain directionality with the spacecraft during the pass, the ground station antenna will move in lock with the orbiting spacecraft.

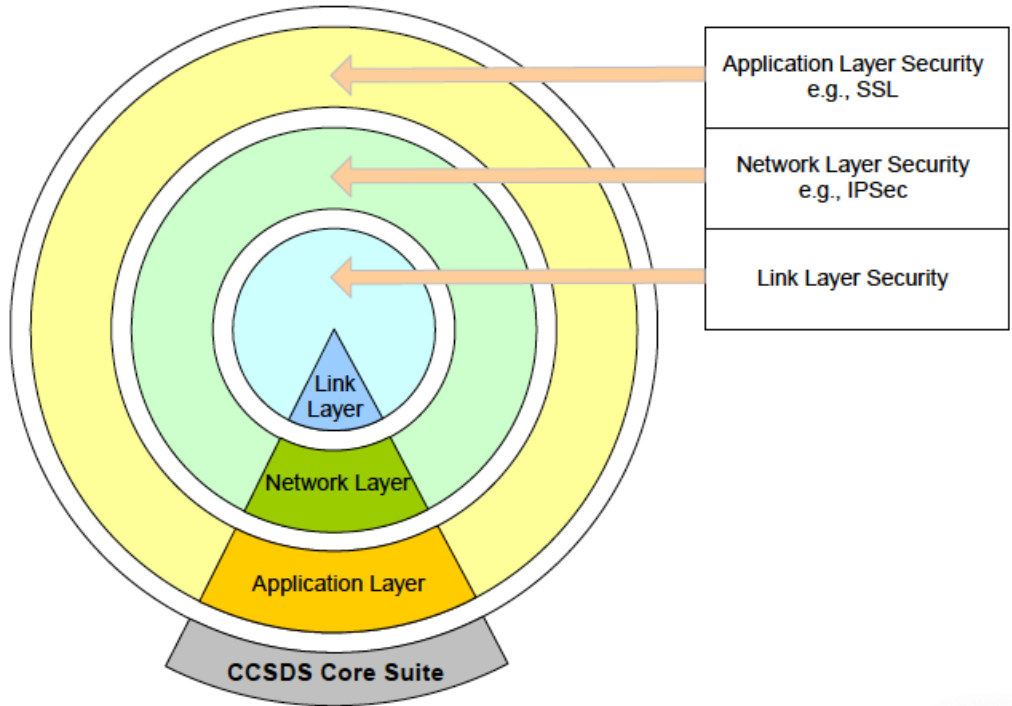


# Space Systems Protocol Overview

- Many systems use CCSDS as the space systems protocol – **Not everyone does!!!**
  - Protocols are created by the Consultative Committee for Space Data Systems ([CCSDS](#))
  - These are recommendations – they are not legally binding
  - These protocols exist to allow for collaboration between international agencies
  - Some protocol differences between commands and telemetry



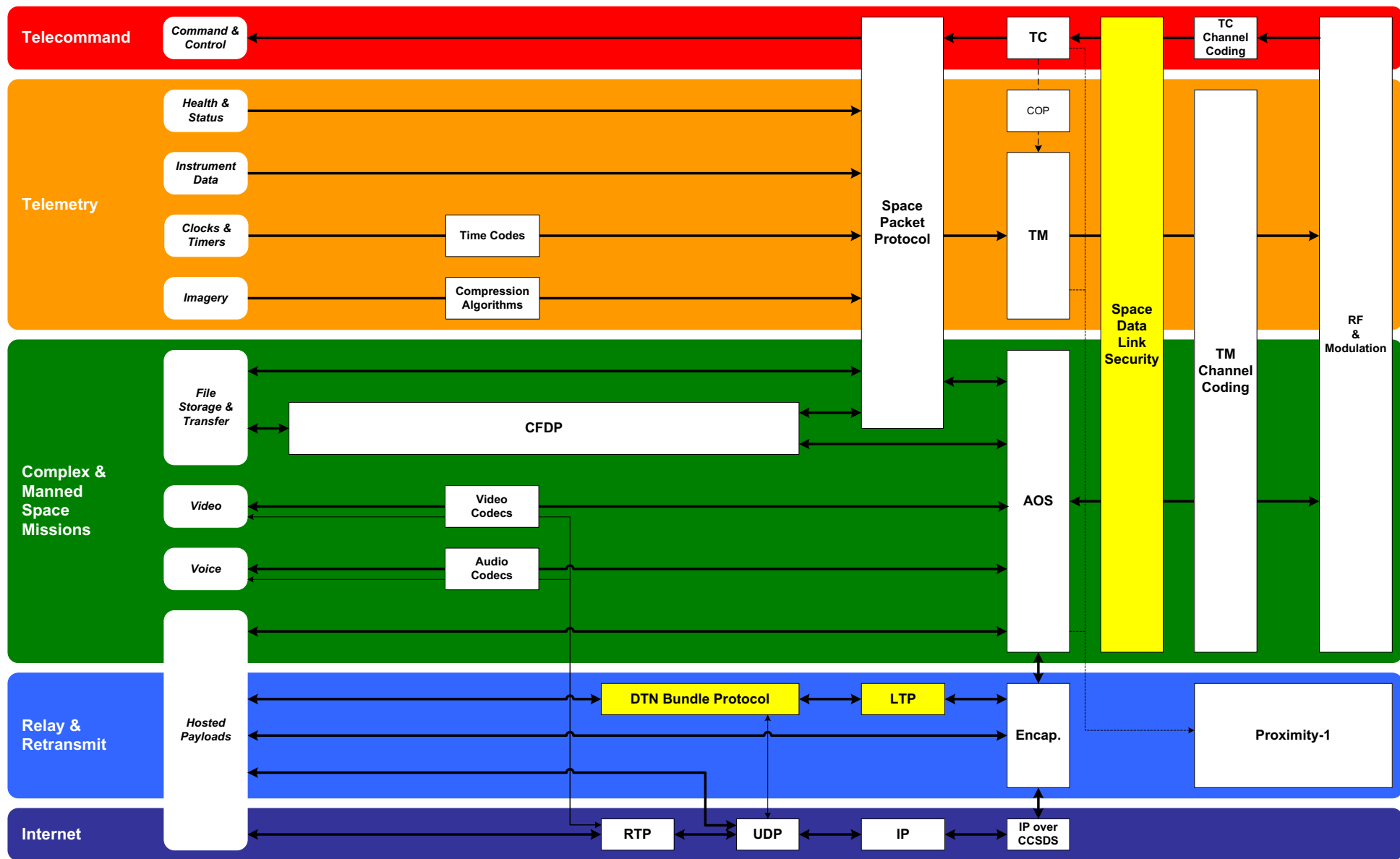
CCSDS Space Mission Protocols and Security Options



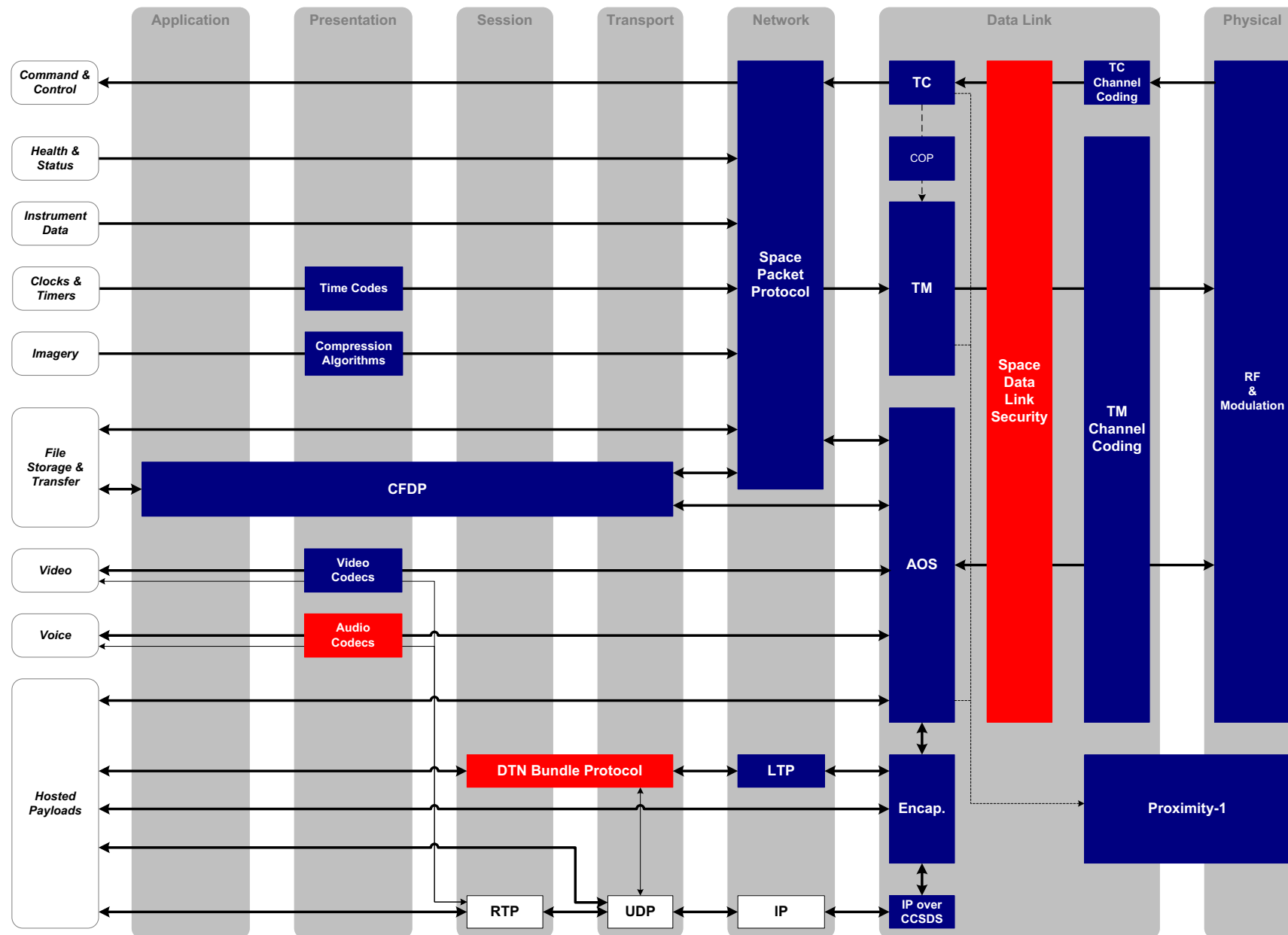
CCSDS Security Core Suite



# Space-to-Ground: Functional View for CCSDS



# Space-to-Ground: OSI Stack View for CCSDS

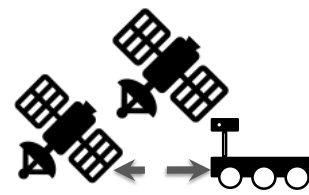


# Space Cryptography Definitions



- AVE – Aerospace Vehicle Equipment
  - *Cryptographic device used on the satellite vehicle to perform secure communications (space crypto)*
- GOE – Ground Operating Equipment
  - *Device located usually within a Space Operations Complex or Mission Control Center that communicates to an on orbit AVE (ground crypto)*
- Red-Side
  - *A network or device that is operating in clear text (No Encryption) considered classified or sensitive data*
- Black-Side
  - *A network or device that is operating with unclassified or encrypted data*
- Algorithm
  - *An encryption algorithm is a component for electronic data transport security. Actual mathematical steps are taken and enlisted when developing algorithms for encryption purposes, and varying block ciphers are used to encrypt electronic data or numbers*
- Block Cipher
  - *A block cipher is a symmetric cryptographic algorithm that operates on a fixed-size block of data using a shared secret. Plaintext is used during the encryption, and the resulting encrypted text is called a ciphertext*
- Electronic Code Book
  - *In cryptography, the simplest mode of operation used with a block cipher to provide the complete encryption algorithm. Each block of regular text (plaintext) is encrypted with the cipher as a unit and turned into encrypted text (ciphertext).*
- OTAR - Over The Air Rekeying
  - *Updating encryption keys by transmitting them via an encrypted communication channel to the device.*
- OTNK – Over the Network Keying
  - *A way to load COMSEC keys using a network instead of a physical workstation.*
- HAIPE - High Assurance Internet Protocol Encryptor
  - *Type 1 encryption device that allows for secure data exchange on an untrusted network by using a shared private key.*

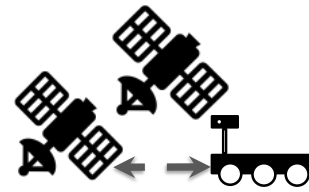
## Comms – Ground to Space (cont.)



- Similar to the ground system's antenna, the spacecraft has to turn the radio frequency signal into a communications stream for processing (i.e., demodulation)
- Once demodulated, there is a computing device that is referred to as the command and data handler which receives the communications from the ground system and directs them as necessary to the embedded flight computer or payload computer
  - *The flight computer is responsible for controlling the functions of the spacecraft with regard to flight*
  - *The payload control computer is responsible for manipulating the payload of the spacecraft. A payload is the portion of the spacecraft carrying out the mission it was designed for (i.e., camera, remote sensing device, etc.). The payload computer would be responsible for telling the camera when to snap pictures, as well as storing those pictures and their metadata for later transmission to the ground.*
- In general, the spacecraft has several required functions, some of which are similar to those of the ground system, such as having to maintain the ability to communicate allowing it to receive tasking. It also has to be able to carry out its mission as well as maintain communications with users on the ground and stay in the correct attitude, on the correct orbit, and achieve necessary positioning. It is necessary to simultaneously satisfy these constraints to maintain communications needs, maintain spacecraft flight requirements, and enable payload operations. The part of the spacecraft responsible for housing and controlling everything needed for the spacecraft to fly is known as the spacecraft bus.



## Comms – Ground to Space (cont.)



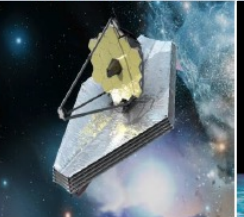

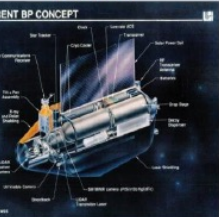


- Like the ground system; the spacecraft needs to make sure its antenna responsible for communications with the ground system is directionally oriented, when necessary, with the ground antenna
  - *The spacecraft therefore must know when and where it is itself in its orbit around the Earth so that it can accurately establish and maintain contact.*
  - *If the spacecraft were to lose its timing or location knowledge, it would essentially become lost and be potentially unable to communicate with the ground or carry out payload tasking. In most situations, to carry out payload tasking, a spacecraft must maintain accurate knowledge of its position, its time, and which way it is facing, otherwise known as its attitude.*
  - *Additionally, the spacecraft must be able to maintain an attitude and position that allows for it to continue to fly as well as carry out its mission. Lastly and most importantly, a spacecraft must do all of these things while keeping enough power stored onboard to continue to do so.*
- A spacecraft may maintain its timing in several ways. It is important to note that spacecraft may go through spans of time where all onboard computing functions are shut off in an attempt to recharge batteries with onboard solar panels. This and other circumstances can cause the computers onboard to lose timing, which is important for the maintaining of communications, encryption, as well as position over the Earth.
  - *It is often not left only to computing devices, and sometimes devices such as atomic clocks can be used to keep track of the passage of time despite the powering off computational devices. Position and attitude knowledge can be tracked via devices such as star trackers or sun sensors. A star tracker is a device that uses knowledge of specific star positions and the reading of stellar lights to identify both where the spacecraft may be in orbit and what its attitude may be. The sun sensor is a less accurate but similar type of device that use the sensing of light from our sun and its strength to make rough determinations of location on orbit as well as general attitude.*



# Payloads

- Payload execution may not seem very power intensive when it is something as simple as capturing a picture, but onboard processing via computer processing units (CPUs), graphical processing units (GPUs), or field-programmable gate arrays (FPGAs) is often very power intensive and can even compete with communication as a top power consumer.
- Payload may be doing long windows of signal collection for a specific type of signal, which might require large amounts of receiving and writing to payload storage device. The payload may also be an emitting payload instead of a sensing one. Where a sensing payload may listen for or monitor a signal or capture a picture, an emitting payload may itself be responsible for radiating a signal of its own which would be more power intensive.
- There are many functions of a spacecraft depending on their payloads and mission. The figure highlights various applications for spacecraft.

Communications	Applications			Special
	Earth-looking sensing	Scientific	Other	
<ul style="list-style-type: none"> <li>• Civil communications</li> <li>• Military strategic</li> <li>• Military tactical</li> <li>• Relay and direct</li> </ul>	<ul style="list-style-type: none"> <li>• Earth resources</li> <li>• Weather</li> <li>• Early warning</li> <li>• Nuclear burst</li> <li>• Oceanography</li> <li>• Boost phase tracking</li> </ul>	<ul style="list-style-type: none"> <li>• Human Exploration – International Space Station</li> <li>• Astrophysics</li> <li>• Heliophysics</li> <li>• Planetary Space Probes</li> <li>• Deep Space Probes</li> </ul>	<ul style="list-style-type: none"> <li>• Navigation</li> <li>• Manufacturing in space</li> <li>• Solar power relay</li> <li>• Tethers</li> <li>• Tugs</li> <li>• Spacecraft repair and maintenance</li> </ul>	<ul style="list-style-type: none"> <li>• Intelligence</li> <li>• Reconnaissance</li> <li>• Jamming</li> <li>• Space surveillance and tracking</li> <li>• Theoretical weapons</li> </ul>
AEHF	SBIRS High GEO	James Webb Space Telescope	GPS III	Brilliant Pebbles Concept
				
Image courtesy of U.S. Air Force	Image courtesy of U.S. Air Force	Image courtesy of NASA	Image courtesy of GPS	Image courtesy of Lawrence Livermore National Laboratory

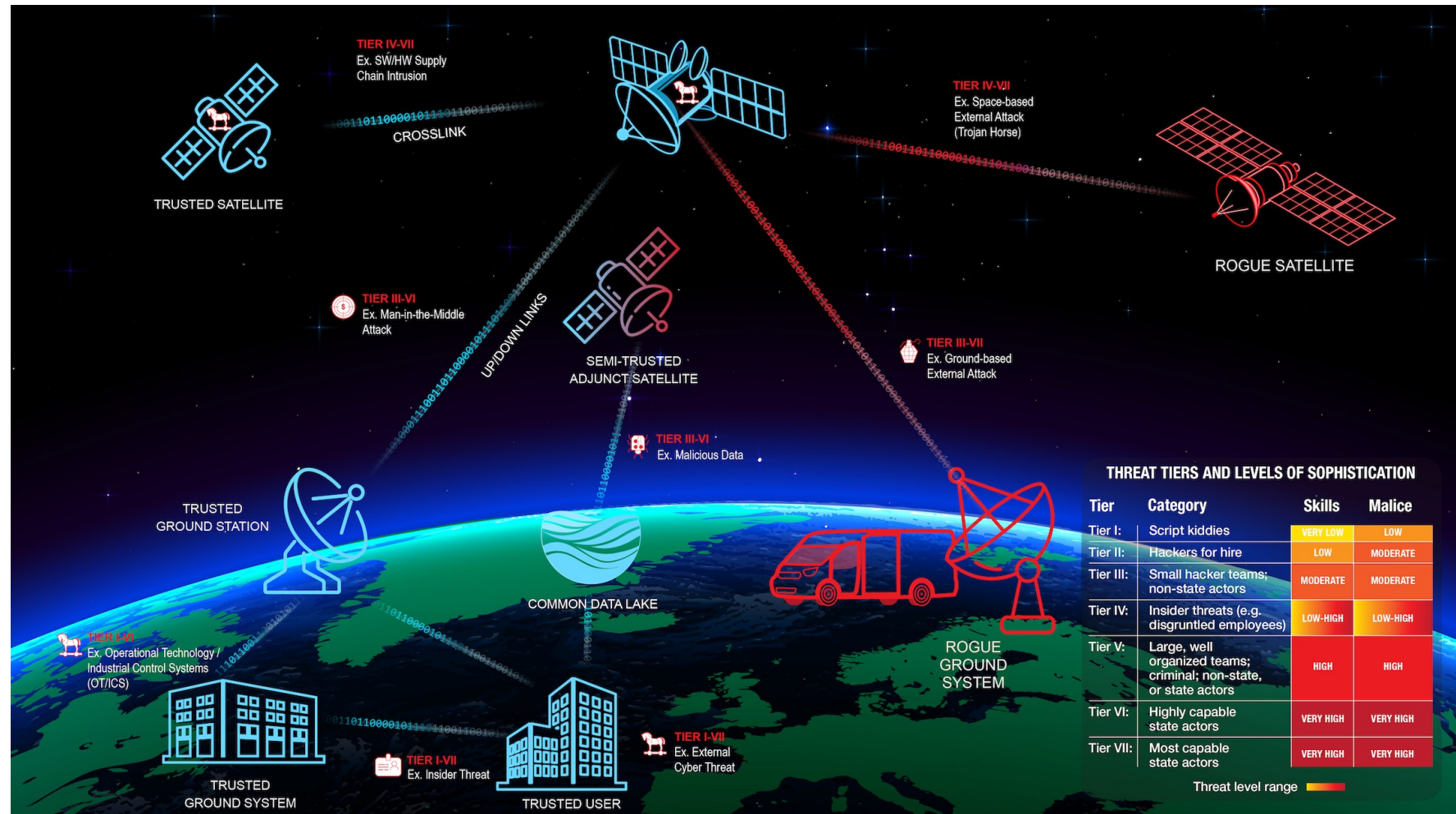
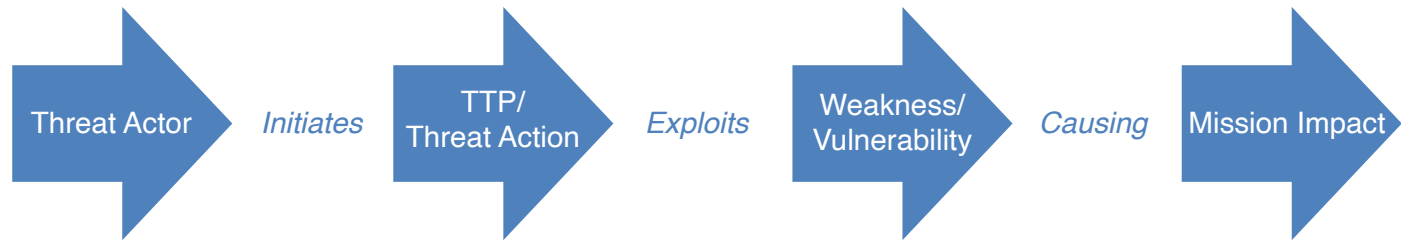
# Attacks/TTPs

Attacks / TTPs can occur across all segments within a space system {i.e., ground, link, and space} to achieve the desired impact for the threat actor

TTP= Tactics, Techniques, & Procedures

A vulnerability assessment against a space vehicle involves the systematic identification, analysis, and evaluation of potential weaknesses or vulnerabilities in the space vehicle's design, components, systems, and operational procedures.

**Goal:** Identify TTPs that could be used by adversaries leading to potential risks or compromises in the space vehicle's mission success, safety, or functionality.







# ***Vulnerability Assessment vs Penetration Testing vs Red vs Purple***

## *Know the Difference in Terminology*

- **Vulnerability Assessment:** Identify and assess vulnerabilities in a system, network, or application. It aims to provide a comprehensive overview of potential weaknesses without actively exploiting them.
- **Penetration Testing:** Simulate a real-world attack by actively exploiting vulnerabilities to determine the extent to which an attacker could compromise the system's security. Penetration testing goes beyond identifying vulnerabilities; it involves attempting to exploit them to assess the impact on the system.
- **Red teaming** is distinct from both vulnerability assessment and penetration testing but shares some similarities. Red teaming involves a broader and more holistic approach than traditional penetration testing and it is often unannounced. It often goes beyond technical vulnerabilities to include social engineering, physical security, and other aspects of an organization's defenses. Red teaming aims to provide a realistic simulation of an advanced and persistent adversary.
- **Purple teaming** involves coordination and communication between the offensive (red team) and defensive (blue team) security teams to enhance the overall security posture of an organization. The term "purple" is derived from the combination of "red" and "blue," symbolizing the integration of offensive and defensive security activities.
  - Regular and ongoing communication between the red and blue teams is a central aspect of purple teaming. This collaboration allows for the sharing of insights, findings, and lessons learned. Purple teaming facilitates the transfer of knowledge between offensive and defensive teams. Blue team members gain insights into the tactics, techniques, and procedures (TTPs) used by attackers, while red team members gain a better understanding of defensive measures and the organization's security architecture.
- Space missions would likely benefit the most from purple teaming as it will help the blue, which could be the engineering team in lieu of a blue team as many space missions do not have operational blue teams.



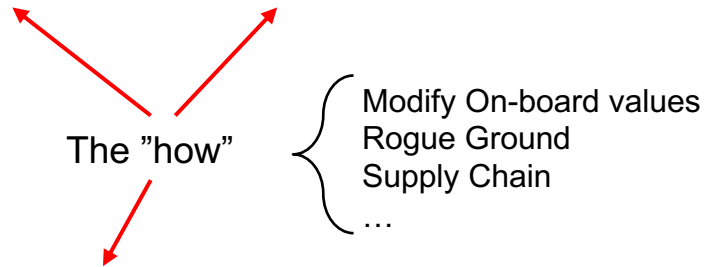
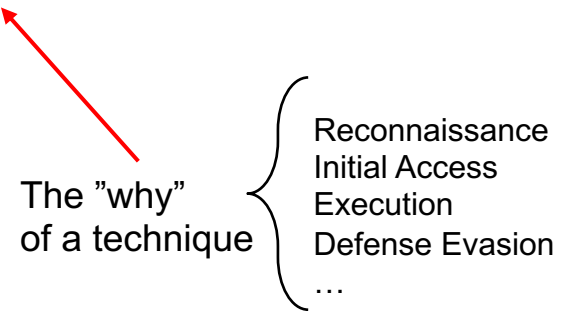


# Conducting the Cyber Assessment

- Understanding the scope and rules of engagement is key (ground, SV, or both?)
  - If it is a vulnerability assessment – then technically no exploitation should be performed
  - Penetration testing, red teaming, or purple teaming would include some level of exploitation and execution of TTPs against the in-scope assets
- Regardless of if exploitation is in scope – the process for identifying the TTPs to be executed or theorized is the same
  - If TTPs are not executed, the exercise is more theoretical and is limited in truly understanding impact on the mission
- For space systems, there are several resources to help with TTP development and execution
  - Ground Segment and User Segment – [ATT&CK](#)
  - Link Segment – [SPARTA](#)
  - Space Vehicle – [SPARTA](#)

• These frameworks use Tactics, Techniques, and Procedures in a tabular format

– Tactics across the top row of the matrix, with techniques and sub-technique(s) listed underneath



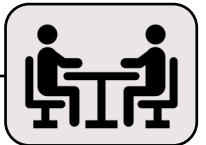
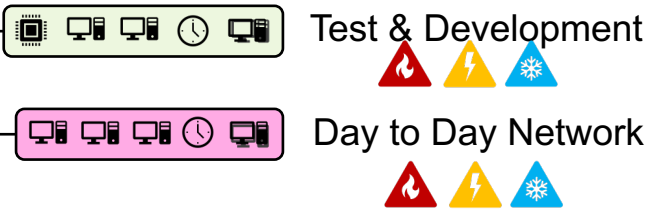
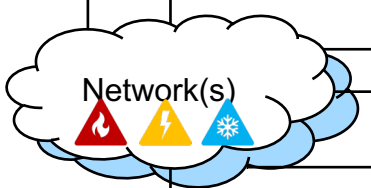
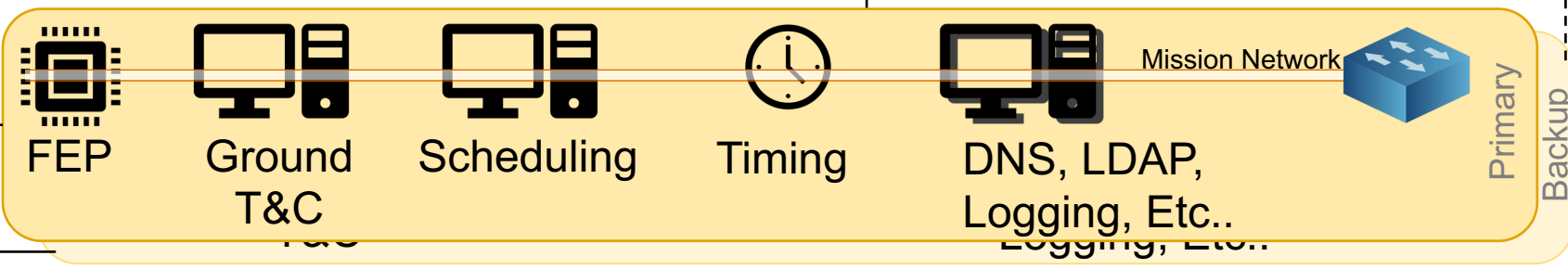
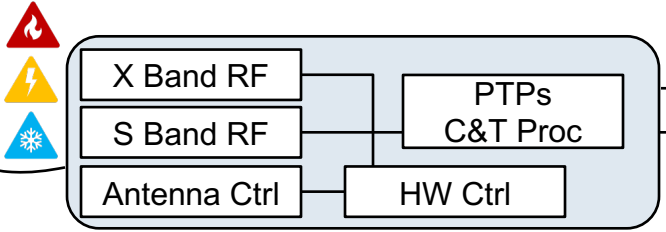
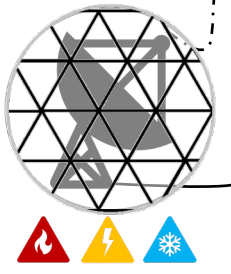
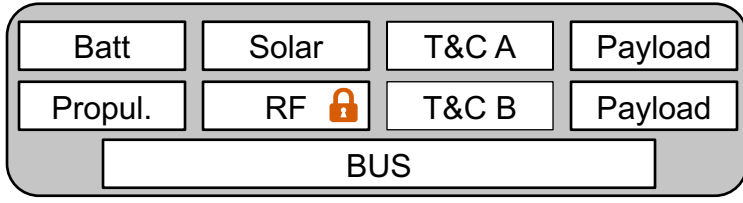
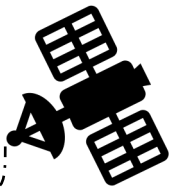
Techniques can likely apply across multiple SVs

Procedures will differ

*Procedures* would be detailed implementation of a *technique* or *sub-technique* being executed by threat actor (i.e., step by step). Likely differ for each SV.



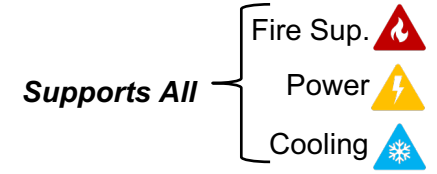
# Space Systems – Large Attack Surface (IT,OT,SV)



Mission Partners



Science

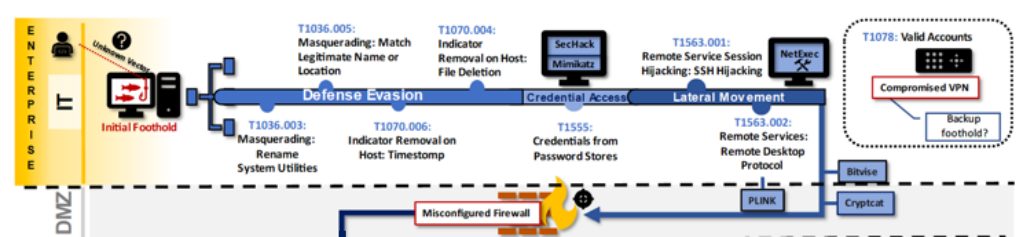
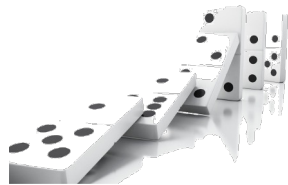


# TTP / Adversary Emulation

- Stringing together Tactics, Techniques and Procedures (TTPs) or exploitation of weaknesses is how Advanced Persistent Threats (APTs) operate
- Typically use multiple TTPs to satisfy objectives of attacker
  - No one vulnerability was the downfall, but multiple tied together to have impact on mission
  - One missing patch or one password discovery can start the attack chain

- Deny ground telemetry and mission data processing
- Deny all communications to the space vehicle
- Execute commands on the space vehicle
- Deny ground commanding
- Compromise mission data integrity
- Degrade confidence in system health tools
- Exfiltrate mission data
- Identify any weaknesses and vulnerabilities that could negatively impact operations

Don't Get Hung on Initial Access



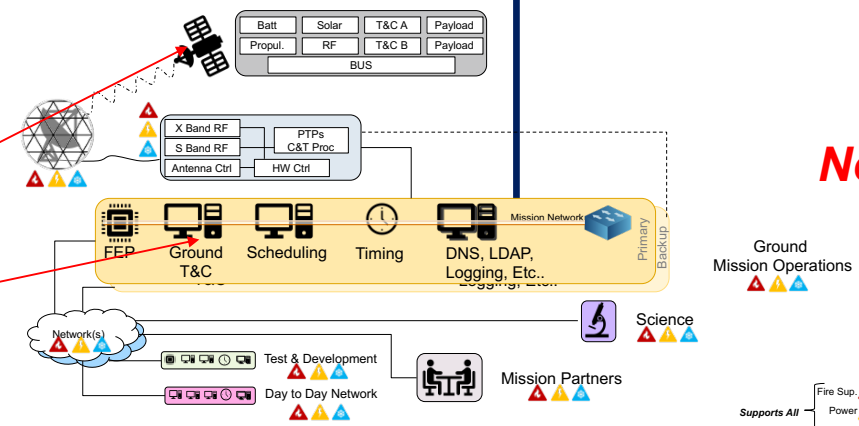
Tactics to attempt for SV

- Execution
- Persistence
- Defense Evasion
- Lateral Movement
- Exfiltration
- Impact

ATT&CK<sup>®</sup>  
Notional Attack Chain

**SPARTA**  
SPACE ATTACK RESEARCH & TACTIC ANALYSIS

Initial Access	Execution	Defense Evasion	Credential Access	Lateral Movement	Impact
IA-0009	EX-0006	EX-0012.03	EX-0009.01		





# Focusing on TTPs for the SV

- If penetration testing or just assessing SVs vulnerabilities, SPARTA can be leveraged in various ways

1. *Determining which techniques can have high impact on MISSION and/or high likelihood*

- Decompose the MISSION to determine impact

- *Develop test objectives to drive impact*
  - Is only theoretical until executed/confirmed
- *Examine attack surface*

2. *Build procedures to implement the techniques to execute on the SV*

- Inject malware onboard, malicious commanding, exploit software weakness, etc.

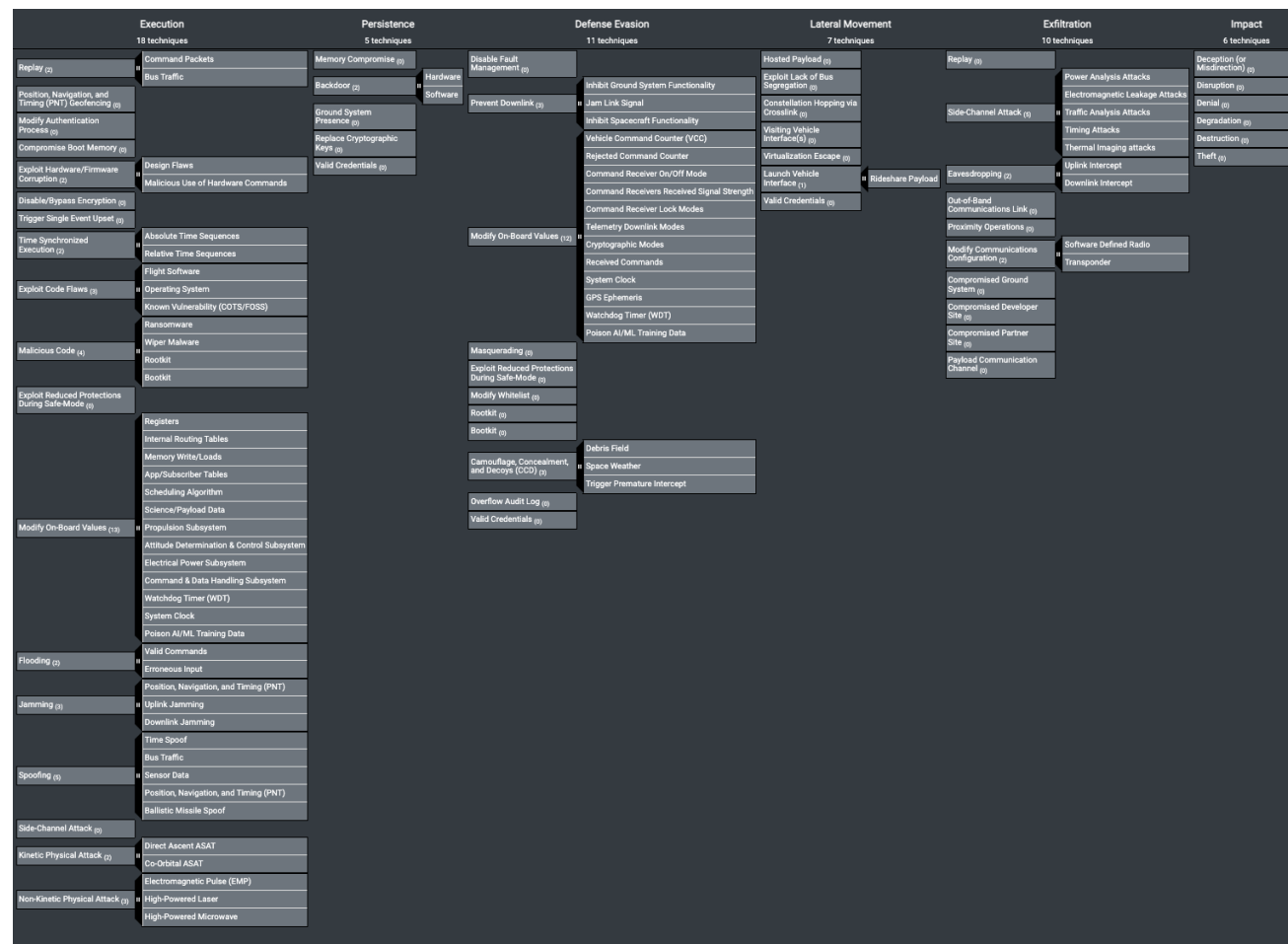
3. *Determine the actual impact in context of the mission upon execution of the technique(s)*

- Ex: Deception (or Misdirection), Disruption, Denial, Degradation, Destruction, or Theft

• Or -->

- Deny all communications to the space vehicle
- Execute commands on the space vehicle
- Compromise mission data integrity
- Degrade confidence in system health tools
- Exfiltrate mission data

- Then, potentially could analyze end to end attack chain to determine risk to the SV if desired







***Step 1.***

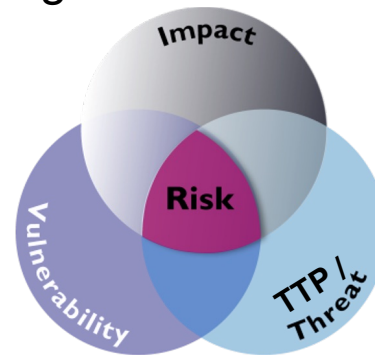
***Determining Techniques High Impact and/or High Likelihood***



# 1. Determining Techniques High Impact and/or High Likelihood

*Initially Ignore Initial Access Tactic – Assume Breach*

- Assumed Breach is a cybersecurity strategy that acknowledges the likelihood of a security breach and operates with the assumption that a breach has / will occur
  - *Verifies that protection, detection and response mechanisms are implemented properly — even reducing potential threats from “knowledgeable attackers”*
- For SVs, too much focus is often placed on Initial Access which prevents discovery of vulnerabilities on the space vehicle
  - *I got COMSEC so if you didn’t defeat my crypto ...*
  - *I’m air gapped ...*
  - *I accept the risk of insider threat ...*
- Regardless of initial access vector, a vulnerability either exists or it doesn’t on the space vehicle
  - *Exploiting it could come from malicious commanding, malware, software / firmware poor coding, weak permissions, supply chain, insider, etc.*
- Initial Access should be accounted for when determining the risk of the vulnerability being exploiting resulting in impact
  - *Building the full attack chain can help with risk analysis*
    - Previous [SPARTA brief on attack chains](#)



Initial Access	
12 techniques	
	Software Dependencies & Development Tools
Compromise Supply Chain (3)	Software Supply Chain
	Hardware Supply Chain
Compromise Software Defined Radio (0)	
Crosslink via Compromised Neighbor (0)	
Secondary/Backup Communication Channel (2)	Ground Station
	Receiver
Rendezvous & Proximity Operations (3)	Compromise Emanations
	Docked Vehicle / OSAM
	Proximity Grappling
Compromise Hosted Payload (0)	
Compromise Ground System (2)	Compromise On-Orbit Update
	Malicious Commanding via Valid GS
	Rogue Ground Station
Rogue External Entity (3)	Rogue Spacecraft
	ASAT/Counterspace Weapon
	Mission Collaborator (academia, international, etc.)
Trusted Relationship (3)	Vendor
	User Segment
Exploit Reduced Protections During Safe-Mode (0)	
Auxiliary Device Compromise (0)	
Assembly, Test, and Launch Operation Compromise (0)	



# 1. Determining Techniques High Impact and/or High Likelihood

<https://sparta.aerospace.org/notional-risk-scores>

- **SPARTA Technique Likelihood:** The evaluation of technique likelihood includes three aspects: (i) adversary motivation, influenced by the system criticality with the assumption that adversaries are more motivated to attack high criticality rather than low criticality systems; (ii) exploitation difficulty, based on technique complexity; and, (iii) adversary capabilities, according to the following seven tiers, in increasing order: script kiddies, hackers for hire, small hacker teams, insider threats, large well organized teams, highly capable state actors, and most capable state actors. Subjective analysis on these three aspects provides the overall likelihood score which results in a range  $\{1, \dots, 5\}$ .
- **SPARTA Technique Impact:** The impact of a technique against a space system refers to the consequences, effects, or outcomes resulting from the successful execution of the technique. Subjective analysis considers wide ranging impact that may include mission disruption, data integrity, loss of control or availability, financial consequences, safety, or even national security implications. Also defined in a range  $\{1, \dots, 5\}$ .
- **Risk Matrix Representation (Risk Scores):** This is a 5x5 risk matrix representation of the notional risk scores of the SPARTA techniques evaluated. The matrix provides a risk score with respect to an assessed impact score from 1 to 5 (the x-axis) and a likelihood score from 1 to 5 (the y-axis); the risk scores are shown in the respective cells of the matrix and reflect the joint effect of impact and likelihood, risk scores range from 1 to 25

**Focus on scores for HIGH Criticality System within SPARTA's Notional Risk Scoring  
(critical infrastructure, military, intelligence, or similar)**

L i k e l i h o o d	5	7	16	20	23	25
	4	6	13	18	22	24
	3	4	10	15	19	21
	2	2	8	11	14	17
	1	1	3	5	9	12
		1	2	3	4	5

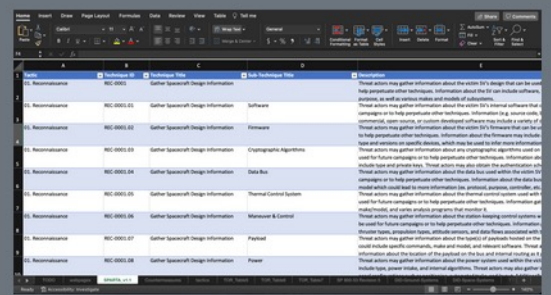
Impact



# 1. Determining Techniques High Impact and/or High Likelihood

## Notional Risk Scores (NRS) in SPARTA

- Performing own analysis is **preferred** but NRS can be used
- Can leverage the tool/page directly - <https://sparta.aerospace.org/notional-risk-scores>
- Or export data into Excel
  - <https://sparta.aerospace.org/resources/working-with>



### SPARTA in Excel

Excel spreadsheets representing the SPARTA dataset. These spreadsheets are dynamically built and provide a more human-accessible view into the knowledge base.

[Learn More](#)

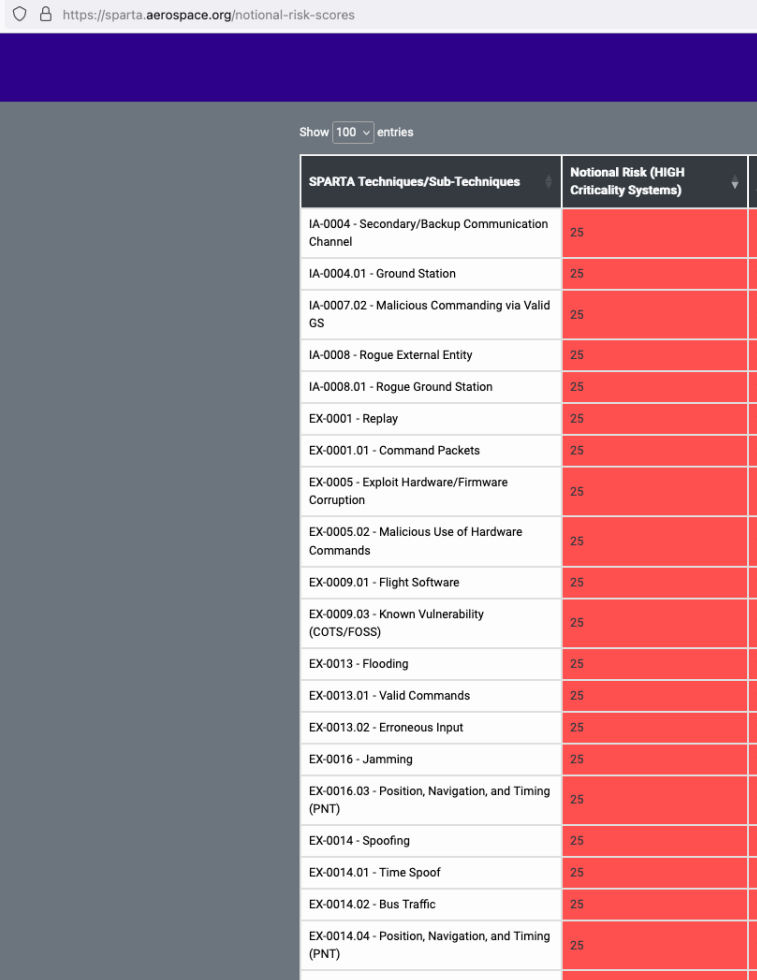
Download SPARTA Excel sheet with (select applicable box for export):

SPARTA Version **v1.5.1**

- SPARTA Tactic
- SPARTA Techniques
- SPARTA Countermeasures
- SPARTA NIST References
- Space Threats
- ISO 27001
- D3FEND Tactics, Techniques, and Artifacts

[Download](#)

The dynamically created Excel representation of the SPARTA dataset allows for users to select which datasets they wish to review and includes all information for the selected dataset. Each spreadsheet contains links to other datasets in order for users to quickly parse information and see how relationships are formed.



https://sparta.aerospace.org/notional-risk-scores

Show 100 entries

SPARTA Techniques/Sub-Techniques	Notional Risk (HIGH Criticality Systems)	N	C
IA-0004 - Secondary/Backup Communication Channel	25	2	2
IA-0004.01 - Ground Station	25	2	2
IA-0007.02 - Malicious Commanding via Valid GS	25	2	2
IA-0008 - Rogue External Entity	25	2	2
IA-0008.01 - Rogue Ground Station	25	2	2
EX-0001 - Replay	25	2	2
EX-0001.01 - Command Packets	25	2	2
EX-0005 - Exploit Hardware/Firmware Corruption	25	2	2
EX-0005.02 - Malicious Use of Hardware Commands	25	2	2
EX-0009.01 - Flight Software	25	2	2
EX-0009.03 - Known Vulnerability (COTS/FOSS)	25	2	2
EX-0013 - Flooding	25	2	2
EX-0013.01 - Valid Commands	25	2	2
EX-0013.02 - Erroneous Input	25	2	2
EX-0016 - Jamming	25	2	2
EX-0016.03 - Position, Navigation, and Timing (PNT)	25	2	2
EX-0014 - Spoofing	25	2	2
EX-0014.01 - Time Spoof	25	2	2
EX-0014.02 - Bus Traffic	25	2	2
EX-0014.04 - Position, Navigation, and Timing (PNT)	25	2	2
EX-0002 - Ground System Breach	25	2	2

– Note: data export currently not functioning on high-side replica. Likely need to move up export from low-side



# 1. Determining Techniques High Impact and/or High Likelihood

## Excel Voodoo

- Filtering out Initial Access, Resource Development, Impact, and Reconnaissance
- Text to columns the Risk Score column with | as the separator
- Sort descending order on the HIGH risk score will results in the highest risk techniques within the following tactics
  - [Execution](#)
  - [Persistence](#)
  - [Defense Evasion](#)
  - [Lateral Movement](#)
  - [Exfiltration](#)
- These techniques have high impact and likelihood from the SPARTA team's analysis
  - *To execute these techniques on a SV, must breakdown the SV/MISSION into capabilities, functions, etc.*

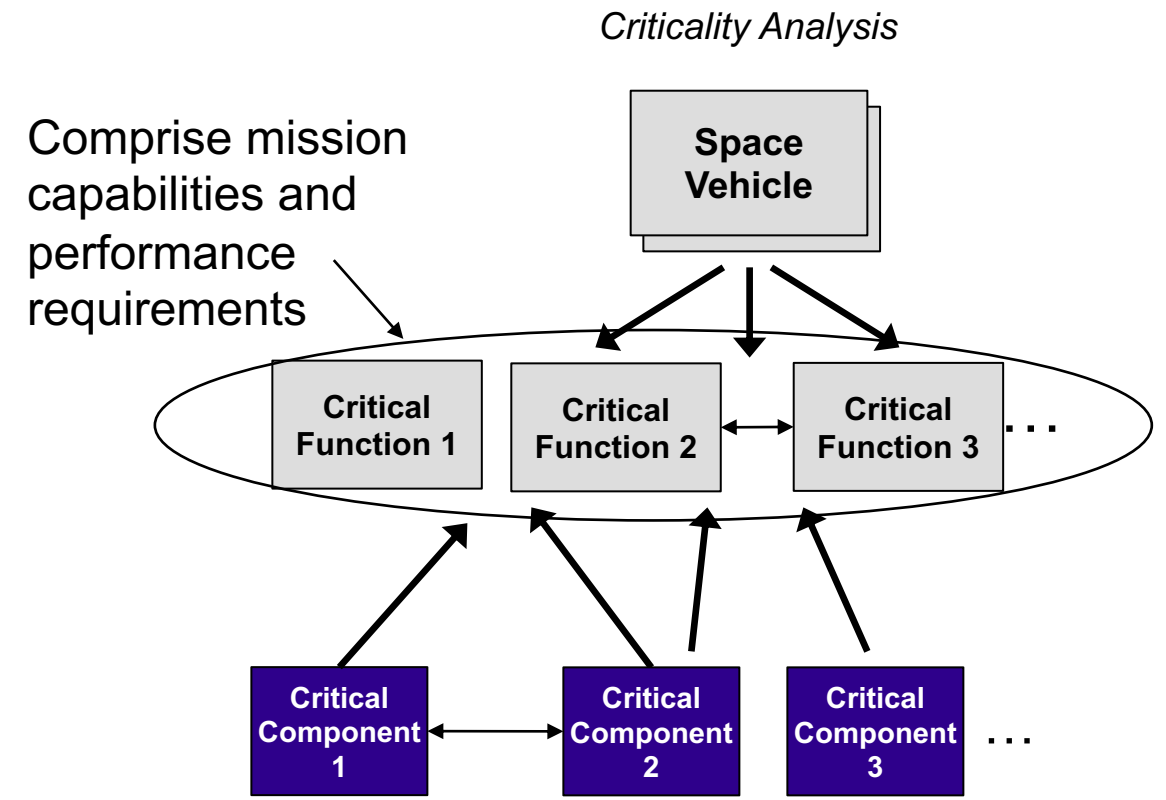
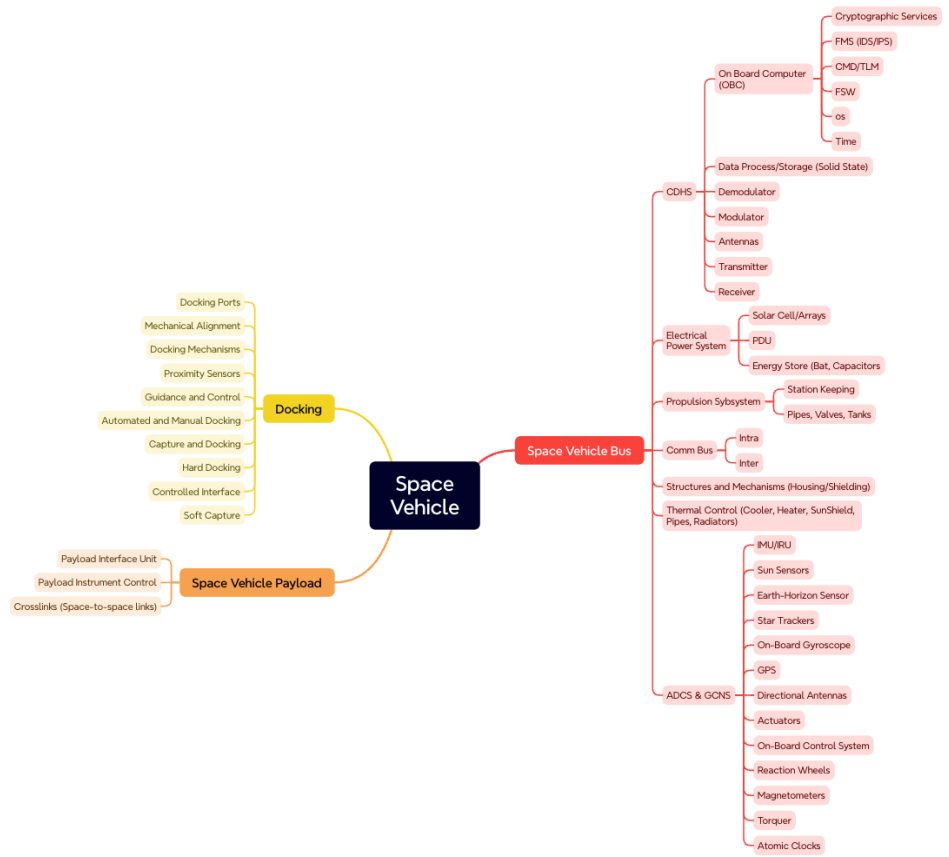
A	B	C	D
ID	Name	Description	Notional Risk Scores (HIGH)
EX-0001	Replay	Replay attacks involve threat act	25
EX-0001.01	Command Packets	Threat actors may interact with	25
EX-0005	Exploit Hardware/Firmware Corruption	Threat actors can target the und	25
EX-0005.02	Malicious Use of Hardware Commands	Threat actors may utilize variou	25
EX-0009.01	Flight Software	Threat actors may abuse known	25
EX-0009.03	Known Vulnerability (COTS/FOSS)	Threat actors may utilize knowle	25
EX-0013	Flooding	Threat actors use flooding attac	25
EX-0013.01	Valid Commands	Threat actors may utilize valid o	25
EX-0013.02	Erroneous Input	Threat actors inject noise/data/	25
EX-0016	Jamming	Threat actors may attempt to ja	25
EX-0016.03	Position, Navigation, and Timing (PNT)	Threat actors may attempt to ja	25
EX-0014	Spoofing	Threat actors may attempt to sp	25
EX-0014.01	Time Spoof	Threat actors may attempt to ta	25
EX-0014.02	Bus Traffic	Threat actors may attempt to ta	25
EX-0014.04	Position, Navigation, and Timing (PNT)	Threat actors may attempt to sp	25
PER-0003	Ground System Presence	Threat actors may compromise	25
DE-0002.02	Jam Link Signal	Threat actors may overwhelm/ja	25
EXF-0007	Compromised Ground System	Threat actors may compromise	25
EX-0001.02	Bus Traffic	Threat actors may abuse interna	24
EX-0005.01	Design Flaws	Threat actors may target design	24
EX-0006	Disable/Bypass Encryption	Threat actors may perform spec	24
EX-0009	Exploit Code Flaws	Threats actors may identify and	24
EX-0010.03	Rootkit	Rootkits are programs that hide	24
EX-0010.04	Bootkit	Adversaries may use bootkits to	24
EX-0011	Exploit Reduced Protections During Safe-Mode	Threat actors may take advanta	24
EX-0012.03	Memory Write/Loads	Threat actors may utilize the tar	24
EX-0012.06	Science/Payload Data	Threat actors may target the int	24
EX-0012.08	Attitude Determination & Control Subsystem	Threat actors may target the on	24
EX-0012.10	Command & Data Handling Subsystem	Threat actors may target the on	24
EX-0012.11	Watchdog Timer (WDT)	Threat actors may manipulate tl	24
EX-0016.01	Uplink Jamming	An uplink jammer is used to inte	24
PER-0002	Backdoor	Threat actors may find and targ	24
PER-0002.01	Hardware	Threat actors may find and targ	24





# Breaking Down the Mission and Scope

- Understanding the scope is important and the available resources. Let's focus on the space vehicle moving forward in the context of active assessment (pen-testing/red/purple)
- Decomposing the space vehicle into components/functions/etc. and how they support the execution of the mission helps inform the test team scope the TTPs







# Tracing Down into the Component Developing Test Objectives

- Identify the right components for each system, maintaining the appropriate level of abstraction
  - *Could be a part of key capabilities, functions, services, protocols, or essential hardware entities within each segment*
  - *Given the breadth and complexity of SVs, must strike a balance between detail and maintaining a manageable level of abstraction*
- Overall effect an attack may have on the SV's mission objective must be considered
  - *If using operational SV, care must be taking obviously*
- Physical nature of the space vehicle and operational environmental factors should be considered
  - *Communication, attitude control, and power are three likely target systems solely based on the effect it could have on the SV's mission*
    - Ex: If the ability to communicate is subverted then the asset's ability to support the mission is completely removed
      - *Should an adversary target the space vehicle's orbital dynamics by modifying the attitude control algorithm (attacking ADCS) or firing a thruster (attacking PS) to destabilize the space vehicle, the effects are equally devastating*
- The space vehicle must be able to communicate, maintain orbit, and deliver power to mission-significant components. With any capability degraded or removed, the mission objective could be compromised.
  - *The SV has many MISSION performance requirements which the attacks could prevent the system from achieving (e.g., causing processing delays on the onboard computer having downstream impact to the mission users)*
- Example of focusing the effort for testing / vulnerability assessment / testing
  - *SV > EPS > PDU {**objective:** disrupt power distribution}*
  - *SV > Payload > Payload Interface Unit {**objective:** disrupt payload communication}*
  - *SV > C&DH > Crypto {**objective:** disrupt communications}*
  - *SV > C&DH > FSW > Command Sequencing {**objective:** execute cmd on SV}*
  - *SV > ADCS > Attitude Sensor > Star Tracker {**objective:** affect attitude}*
  - *SV > ADCS > Actuator > Reaction Wheel {**objective:** affect attitude}*
  - *SV > C&DH > OBC/SBC > Timekeeping > Watch Dog Timer {**objective:** affect timing and task execution to disrupt operations}*

Critical to identify the testing objectives, components and the relationship to MISSION performance



# Examine the Attack Surface

*For the targeted component / function*

- Regardless of if the focus is a specific component like Reaction Wheel, a function like timekeeping, or the entire sub-system like EPS, enumerating the attack surface helps determine the types of SPARTA techniques you may want to execute
- Enumerating the attack surface for each component involves identifying and documenting all potential entry points or vulnerabilities that could be exploited by malicious actors.
  - *Define the behavior/function of the low-level component*
  - *Analyze how data, information, and control flow in and out of each component. Understand the inputs and outputs of each component, as well as the interactions between components*
  - *Determine interfaces, both internal and external, that connect to each component. These interfaces may include APIs, network connections, user interfaces, and communication channels*
  - *Identify any third-party or external dependencies that the component relies on, such as external services, libraries, or APIs. Assess the security of these dependencies and how they impact the attack surface*
- Then leverage the attack surface analysis in concert with the test objectives to identify the techniques to use for attacking the Ex: SV > C&DH > OBC/SBC > Timekeeping > Watch Dog Timer
  - **Objective:** *affect timing and task execution to disrupt operations*
    - According to ChatGPT, watch dog's routine leverages values in registers and periodically the software resets the watchdog timer to prevent it from timing out. This petting process involves writing a specific value or sequence to a register associated with the watchdog timer.
      - *A SPARTA technique would be [EX-0012.01: Modify On-Board Values: Registers](#) or [EX-0012.11: Modify On-Board Values: Watchdog Timer \(WDT\)](#)*



# 1. Determining Techniques High Impact and/or High Likelihood

## Perform a Mapping Techniques to System Decomposition

- Leverage provided analysis to help identify techniques to sub-systems and their components
  - Below is an example of decomposing the SPARTA techniques to the applicable sub-systems

			ADCS	C&DH	Comm	Crypto	Docking	EPS	Payload	PS	S&M	TCS	Notional Risk Scores (HIGH Tier)
ID	Name	Description											
EX-0001	Replay	Replay attacks involve threat actors recording previously recorded data streams and then resending them at a later time. This attack can be used to fingerprint systems, gain elevated privileges, or even cause a denial of service.	YES	YES	YES	YES			YES				25
EX-0001.01	Command Packets	Threat actors may interact with the victim spacecraft by replaying captured commands to the spacecraft. While not necessarily malicious in nature, replayed commands can be used to overload the target spacecraft and cause it's onboard systems to crash, perform a DoS attack, or monitor various responses by the spacecraft. If critical commands are captured and replayed, thruster fires, then the impact could impact the spacecraft's attitude control/orbit.	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	25
EX-0005	Exploit Hardware/Firmware Corruption	Threat actors can target the underlying hardware and/or firmware using various TTPs that will be dependent on the specific hardware/firmware. Typically, software tools (e.g., antivirus, antimalware, intrusion detection) can protect a system from threat actors attempting to take advantage of those vulnerabilities to inject malicious code. However, there exist security gaps that cannot be closed by the above-mentioned software tools since they are not stationed on software applications, drivers or the operating system but rather on the hardware itself. Hardware components, like memory modules and caches, can be exploited under specific circumstances thus enabling backdoor access to potential threat actors. In addition to hardware, the firmware itself which often is thought to be software in its own right also provides an attack surface for threat actors. Firmware is programming that's written to a hardware device's non-volatile memory where the content is saved when a hardware device is turned off or loses its external power source. Firmware is written directly onto a piece of hardware during manufacturing and it is used to run on the device and can be thought of as the software that enables hardware to run. In the space vehicle context, firmware and field programmable gate array (FPGA)/application-specific integrated circuit (ASIC) logic/code is considered equivalent to firmware.	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	25
EX-0005.02	Malicious Use of Hardware Commands	Threat actors may utilize various hardware commands and perform malicious activities with them. Hardware commands typically differ from traditional command channels as they bypass many of the traditional protections and pathways and are more direct therefore they can be dangerous if not protected. Hardware commands are sometime a necessity to perform various actions such as configuring sensors, adjusting positions, and rotating internal motors. Threat actors may use these commands to perform malicious activities that can damage the victim spacecraft in some capacity.	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	25
EX-0009.01	Flight Software	Threat actors may abuse known or unknown flight software code flaws in order to further the attack campaign. Some FSW suites contain API functionality for operator interaction. Threat actors may seek to exploit these or abuse a vulnerability/misconfiguration to maliciously execute code or commands. In some cases, these code flaws can perpetuate throughout the victim spacecraft, allowing access to otherwise segmented subsystems.	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	25
EX-0009.03	Known Vulnerability (COTS/FOSS)	Threat actors may utilize knowledge of the spacecraft software composition to enumerate and exploit known flaws or vulnerabilities in the commercial or open source software running on-board the target spacecraft.	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	25
EX-0005.01	Design Flaws	Threat actors may exploit design flaws with the hardware design to their advantage to cause the desired impact. Threat actors may utilize the hardware design of the hardware (e.g. hardware timers, hardware interrupts, memory cells), which is intended to provide reliability, to their advantage to degrade other aspects like availability. Additionally, field programmable gate array (FPGA)/application-specific integrated circuit (ASIC) logic can be exploited just like software code can be exploited. There could be logic/design flaws embedded in the hardware (i.e., FPGA/ASIC) which may be exploitable by a threat actor.	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	24
EX-0006	Disable/Bypass Encryption	Threat actors may perform specific techniques in order to bypass or disable the encryption mechanism onboard the victim spacecraft. By bypassing or disabling this particular mechanism, further tactics can be performed, such as Exfiltration, that may have not been possible with the internal encryption process in place.				YES	YES		YES				24
EX-0009	Exploit Code Flaws	Threat actors may identify and exploit flaws or weaknesses within the software running on-board the target spacecraft. These attacks may be extremely targeted and tailored to specific coding errors introduced as a result of poor coding practices or they may target known issues in the commercial software components.	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	24
EX-0010.03	Rootkit	Rootkits are programs that hide the existence of malware by intercepting/hooks and modifying operating system API calls that supply system information. Rootkits or rootkit enabling functionality may reside at the flight software or kernel level in the operating system or lower, to include a hypervisor, Master Boot Record, or System Firmware.	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	24
EX-0010.04	Bootkit	Adversaries may use bootkits to persist on systems and evade detection. Bootkits reside at a layer below the operating system and may make it difficult to perform full remediation unless an organization suspects one was used and can act accordingly.	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	24
EX-0011	Exploit Reduced Protections During Safe-Mode	Threat actors may take advantage of the victim spacecraft being in safe mode and send malicious commands that may not otherwise be processed. Safe-mode is when all non-essential systems are shut down and only essential functions within the spacecraft are active. During this mode, several commands are available to be processed that are not normally processed. Further, many protections may be disabled at this time.	YES	YES	YES	YES			YES				24
EX-0012.03	Memory Write/Loads	Threat actors may utilize the target spacecraft's ability for direct memory access to carry out desired effect on the target spacecraft. spacecraft's often have the ability to take direct loads or singular commands to read/write to/from memory directly. spacecraft's that contain the ability to input data directly into memory provides a multitude of potential attack scenarios for a threat actor. Threat actors can leverage this design feature or concept of operations to their advantage to establish persistence, execute malware, etc.		YES					YES				24
EX-0012.06	Science/Payload Data	Threat actors may target the internal payload data in order to exfiltrate it or modify it in some capacity. Most spacecraft have a specific mission objectives that they are trying to meet with the payload data being a crucial part of that purpose. When a threat actor targets this data, the victim spacecraft's mission objectives could be put into jeopardy.				YES			YES				24
EX-0012.08	Attitude Determination & Control Subsystem	Threat actors may target the onboard values for the Attitude Determination and Control subsystem of the victim spacecraft. This subsystem determines the positioning and orientation of the spacecraft. Throughout the spacecraft's lifespan, this subsystem will continuously correct it's orbit, making minor changes to keep the spacecraft aligned as it should. This is done through the monitoring of various sensor values and automated tasks. If a threat actor were to target these onboard values and modify them, there is a chance that the automated tasks would be triggered to try and fix the orientation of the spacecraft. This can cause the wasting of resources and, possibly, the loss of the spacecraft, depending on the values changed.	YES	YES					YES				24

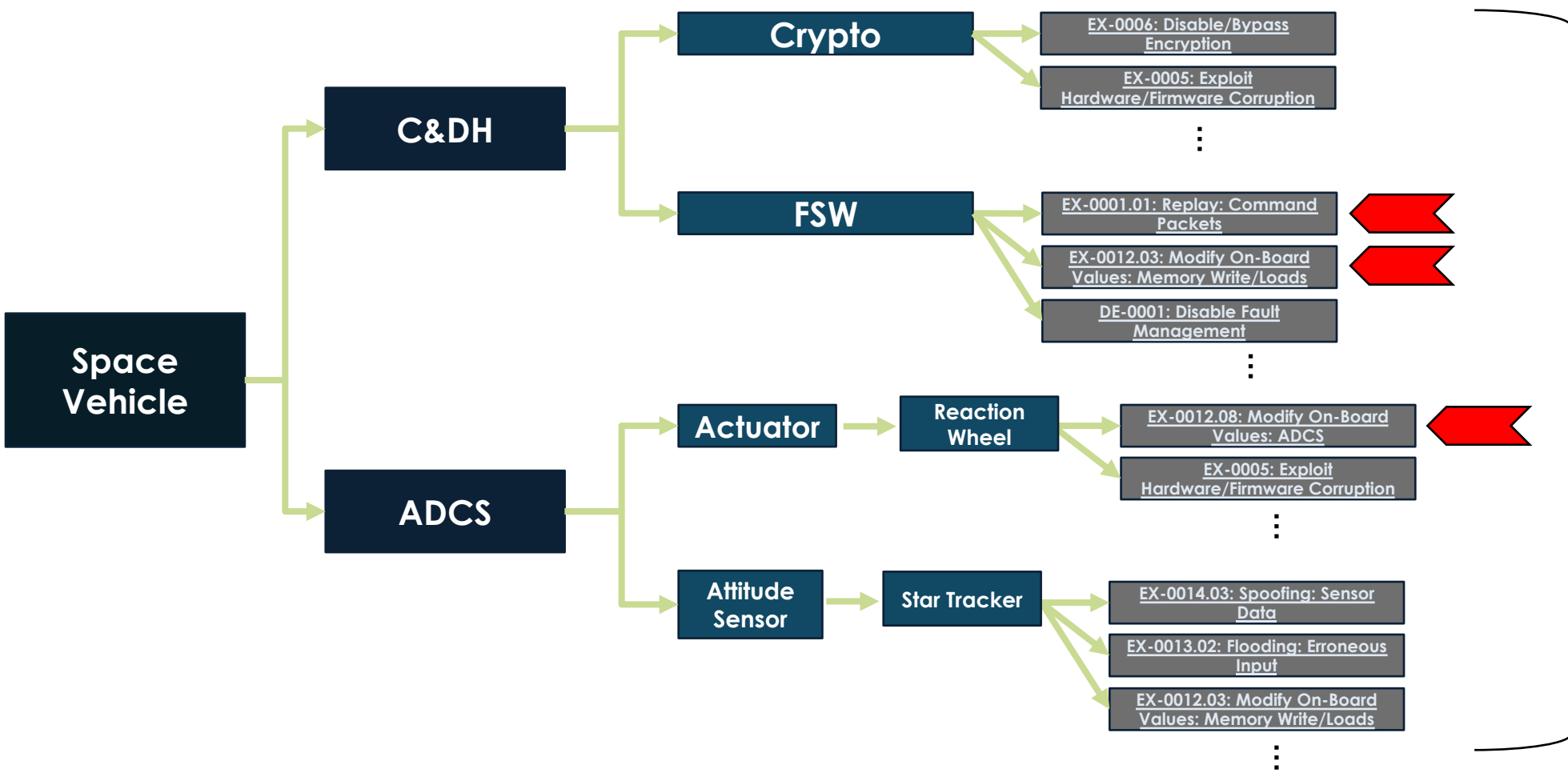


## Steps 2 and 3

### Three Exemplars

- The next three are examples where you take the SV's decomposition and attack surface to then execute the highlighted high-risk techniques, using default NRS, from SPARTA
  - Replay: Command Packets (NRS=25): Focused on the FSW and determining if the SV was vulnerable to replay attacks. Understanding the input and behavior of the C&DH / FSW – simply replaying command packets is a test that can be execute
    - Weakness exploited: no authentication, COP-1, vehicle command counter, etc.
  - Modify On-Board Values: Memory Write/Loads (NRS=24): Focused on the FSW having the ability to write data to critical memory regions that the OS would process as input
    - Weakness exploited: lack of memory protection on critical sectors, FSW running as “root”, PowerPC registers
  - Modify On-Board Values: Attitude Determination & Control Subsystem (NRS=24): Focused the FSW's capability within C&DH to command the reaction wheel to increase the torque of reaction wheel to affect the SV's attitude. Reaction wheels attack surface extends to the C&DH and FSW as it processes input from the FSW to perform physical actions
    - Weakness exploited: FSW / fault management not limit checking on reaction wheel torque values

# Visual Example Decomposition to Technique







# 2. Build Procedures to Implement the Techniques to Execute on the SV

## Replay Attack on FSW within C&DH

- Example: Replay: Command Packets

<https://sparta.aerospace.org/technique/EX-0001/01/>

- C&DH > FSW processes the **input** of command packets
- Technique is to simply record and playback command packets

ID: EX-0001.01  
 Sub-technique of: EX-0001  
 Notional Risk (H | M | L): 25 | 24 | 21  
 Related Aerospace Threat IDs: SV-AC-1 | SV-AC-2  
 Related MITRE ATT&CK TTPs: T0831  
 Related ESA SPACE-SHIELD TTPs: T2008.006 | T2019.005  
 ① Tactic: Execution  
 Created: 2022/10/19  
 Last Modified: 2022/12/08

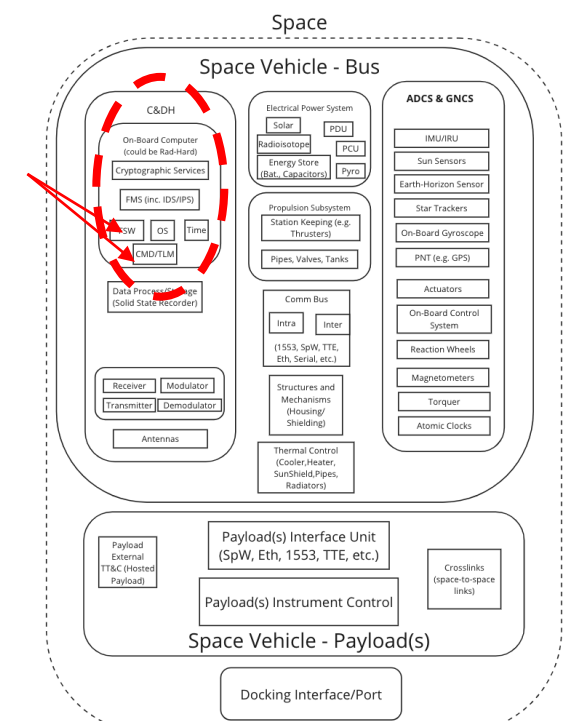
### SPARTA **Replay Attack**

SPACE ATTACK RESEARCH & TACTIC ANALYSIS

#### DefCon 2020 – Exploiting Spacecraft Example (<https://www.youtube.com/watch?v=b8QWNiqTx1c>)

Attacker performs a man-in-the-middle attack at the ground station where they record command packets in the UDP traffic [REC-0005, RD-0005.01] for replaying to the spacecraft [EX-0001.01]. In this example UDP mimics the radio frequency link. This same attack could be applied through RF signal sniffing [REC-0005.01, IA-0008.01] vice UDP captures. From the spacecraft perspective, the flight software processes the traffic whether or not the traffic is coded to radio frequency signals and then decoded on the spacecraft. Upon receiving commands, the spacecraft flight software responds by downlinking command counter data to the ground indicating that commands were received [EXF-0003.02]. In this scenario, the attacker collected the commands at the ground station [EXF-0003.01, EXF-0007] and then promptly replay the traffic to the spacecraft [EX-0001.01] thereby causing the flight software to reprocess the commands again [EX-0001]. This would be visible in the downlinked command counters [REC-0005.02, EXF-0003.02] and unless the ground operators are monitoring specific telemetry points, this attack would likely go unnoticed. If the replayed commands were considered critical commands like firing thrusters, then more critical impact on the spacecraft could be encountered [IMP-0002, IMP-0004, IMP-0005].

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Defense Evasion	Lateral Movement	Exfiltration	Impact
9 techniques	5 techniques	12 techniques	18 techniques	5 techniques	11 techniques	7 techniques	10 techniques	6 techniques
Gather Spacecraft Design Information (2) Gather Spacecraft Descriptors (2) Gather Spacecraft Communications Information (2) Gather Launch Information (2)	Acquire Infrastructure (2) Compromise Infrastructure (2) Third Party Ground System Third Party Spacecraft	Mission-Operated Ground System Compromise Supply Chain (2) Compromise Software Defined Radio (2) Ground System Penetration (2) Replace Cryptographic Keys (2) Valid Credentials (2)	Replay (2) Position, Navigation, and Timing (PNT) Spoofing (2) Modify Authentication Process (2) Compromise Boot Memory (2) Exploit Hardware/Firmware Corruption (2) Disable/Bypass Encryption (2) Trigger Single Event Upset (2) Time Synchronized Execution (2) Exploit Code Flaws (2) Malicious Code (2) ASAT/Counterspace Weapon	Memory Compromise (2) Backdoor (2) Ground System Penetration (2) Replace Cryptographic Keys (2) Valid Credentials (2)	Disable Fault Management (2) Prevent Downlink (2) Modify On-Board Values (2) Masquerading (2) Exploit Reduced Protections During Safe-Mode (2) Modify Whistlebl (2) Routlet (2) Boottel (2) Camouflage, Concealment, and Deceits (CCD) (2) Overflow Audit Log (2) Valid Credentials (2)	Hosted Payload (2) Exploit Lack of Bus Segregation (2) Consultation Hopping via Crosslink (2) Visiting Vehicle Interface(s) (2) Virtualization Escape (2) Launch Vehicle Interface (2) Valid Credentials (2)	Replay (2) Side Channel Attack (2) Eavesdropping (2) Out-of-Band Communications Link (2) Proximity Operations (2) Modify Communications Configuration (2) Compromised Ground System (2) Compromised Partner Site (2) Compromised Partner Site (2) Payload Communication Channel (2)	Disruption (or Misdirection) (2) Denial (2) Degradation (2) Destruction (2) Theft (2)







# 2. Build Procedures to Implement the Techniques to Execute on the SV

## Memory Attack on OBC, FSW, and OS within C&DH

- Example: Memory Write - <https://sparta.aerospace.org/technique/EX-0012/03/>
  - FSW can **write data** that OS **processes** within critical memory regions
    - Technique is to simply leverage FSW to write data to corrupt OS

ID: EX-0012.03  
 Sub-technique of: EX-0012  
 Notional Risk (H | M | L): 24 | 21 | 17  
 Related Aerospace Threat IDs: SV-IT-2 | SV-IT-5 | SV-SP-9  
 Related MITRE ATT&CK TTPs: No related MITRE ATT&CK TTPs  
 Related ESA SPACE-SHIELD TTPs: T2010 | T2054 | T2054.003  
 Tactic: Execution  
 Created: 2022/10/19  
 Last Modified: 2023/05/08

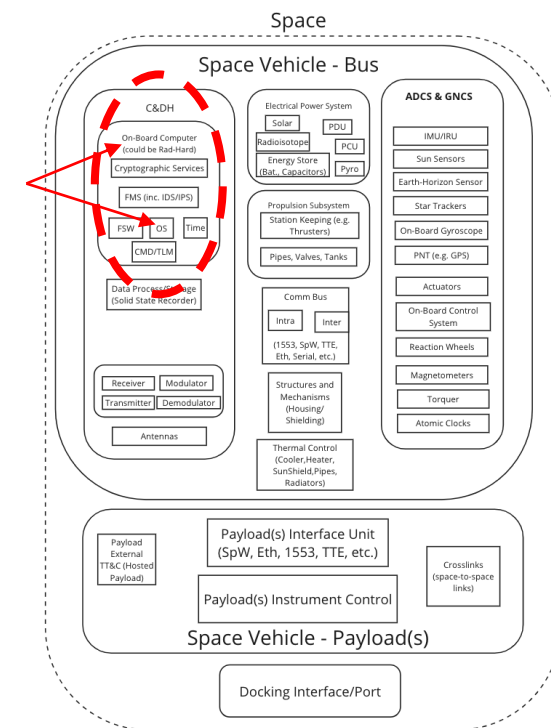
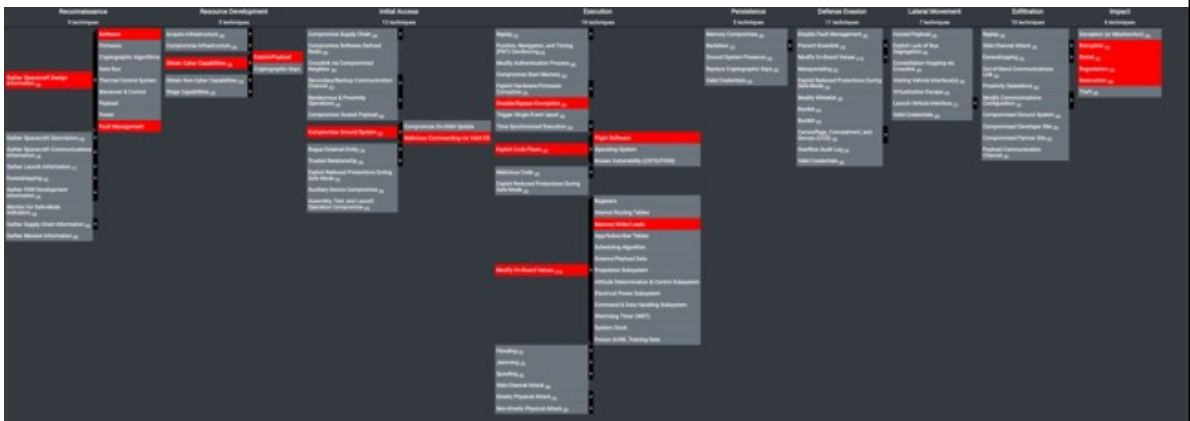
### SPARTA **Memory Write/Loads**

SPACE ATTACK RESEARCH & TACTIC ANALYSIS

DefCon 2022 - Memory Manipulation Attack ([https://www.youtube.com/watch?v=t\\_efCpd2PbM](https://www.youtube.com/watch?v=t_efCpd2PbM))

This example requires significant effort in the reconnaissance phase [REC-0001, REC-0003] to understand the specific attack vectors. However, after understanding the memory maps/locations and how the VxWorks and PowerPC interrelates, the attack can be performed to disrupt [IMP-0002] and deny [IMP-0003] the spacecraft's ability to process information. Upon performing all the necessary research, a single command packet is all that is required to affect the spacecraft. Understanding the precise memory location and overwriting it with desired values, exploits the inherit trust between the ground and the spacecraft [IA-0009].

In this exploit example, the attacker leverages the authenticated/encrypted command pathway to send two commands to the spacecraft [IA-0007.02, EX-0006]. A simple NO-OP for demonstration purposes followed by a "magic packet" or "kill-pill" that corrupts the running state of the PowerPC processor thereby disabling the spacecraft's ability to process information. The below figure shows redacted information to remove the actual corrupting content, but the "vxworks!" is essentially the kernel throwing a panic and crashing. This is where having direct memory access [EX-0012.03] via the spacecraft flight software can be dangerous and must be protected [EX-0009.01]. There are many instances where the ground can issue legitimate commands to degrade/deny/destroy [IMP-0004, IMP-0003, IMP-0005] the spacecraft which puts pressure on fault management to account for this truth [REC-0001.09].









## 2. Build Procedures to Implement the Techniques to Execute on the SV

### Malicious Command via C&DH on Reaction Wheel within ADCS / GNCS

- Example: Modify Reaction Wheel Data via Malicious Command from Ground

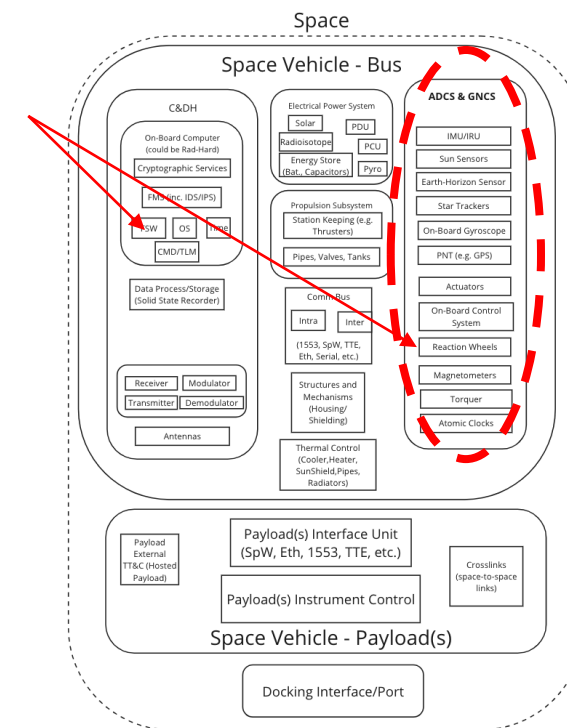
<https://sparta.aerospace.org/technique/EX-0012/08/>

- Exploit the FSW's capability {EX-0009.01} within C&DH to command the reaction wheel to increase the torque of reaction wheel to affect the SV's attitude {EX-0012.08}

– *Reaction wheels attack surface extends to the C&DH and FSW as it processes input from the FSW to perform physical actions*

- The attacker leverages the fact the FSW does not properly control the limits of torque values which causes the SV to spin uncontrollably

ID: EX-0012.08  
Sub-technique of: EX-0012  
Notional Risk (H | M | L): 24 | 21 | 17  
Related Aerospace Threat IDs: SV-IT-2 | SV-IT-5 | SV-SP-9 | SV-MA-3  
Related MITRE ATT&CK TTPs: No related MITRE ATT&CK TTPs  
Related ESA SPACE-SHIELD TTPs: T2010  
① Tactic: Execution  
Created: 2022/10/19  
Last Modified: 2023/05/08



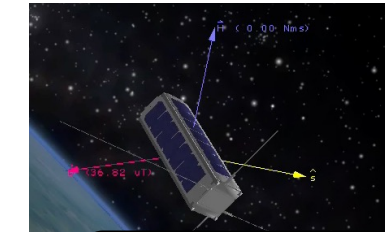




# 3. Determine Actual Impact in Context of the Mission

## Spinning a CubeSat Uncontrollably

- Many CubeSats do not implement strong, sometimes any, authentication / encryption – therefore, can be vulnerable to command link intrusion from Rogue Ground Station
- This attack creates a CCSDS frame to send to spacecraft from a rogue ground station



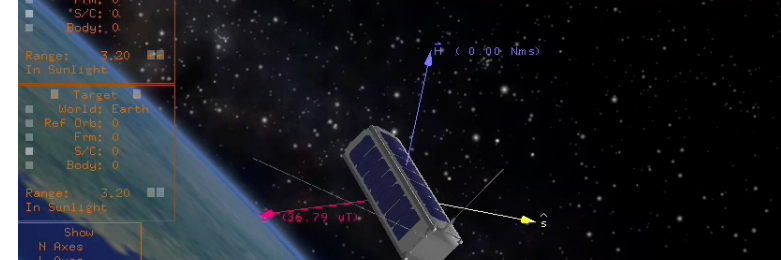
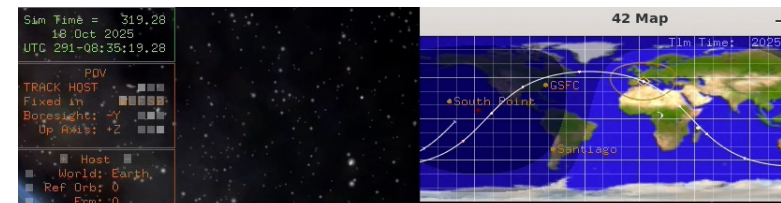
Modify On-Board Values: Attitude Determination & Control  
<https://sparta.aerospace.org/technique/EX-0012/08/>

1992c00000303001400

Rogue Ground System SW

Command Link Intrusion from Rogue Ground  
<https://sparta.aerospace.org/technique/IA-0008/01/>

```
00000000 0d0a 0a0d 0060 0000 3c4d 1a2b 0001 0000
00000010 ffff ffff ffff ffff 0004 003a 6445 7469
00000020 6163 2070 5728 7269 7365 6168 6b72 2029
00000030 2e33 2e32 2033 4728 7469 7620 2e33 2e32
00000040 2033 6170 6b63 6761 6465 6120 2073 2e33
00000050 2e32 2d33 2931 0000 0000 0000 0060 0000
00000060 0001 0000 0014 0000 0001 0000 0000 0004
00000070 0014 0000 0006 0000 0054 0000 0000 0000
00000080 f7a5 0005 23d7 faa0 0032 0000 0032 0000
00000090 0000 0000 0000 0000 0000 0000 0008 0045
000000a0 2400 58a6 0040 1140 6e96 007f 0100 007f
000000b0 0100 acbc 9413 1000 23fe 9219 00c0 0300
000000c0 0003 0014 0054 0000
000000c8 -
```



Disrupt/Denial/Degrade  
<https://sparta.aerospace.org/technique/IMP-0002/>  
<https://sparta.aerospace.org/technique/IMP-0003/>  
<https://sparta.aerospace.org/technique/IMP-0004/>

Impact is instability in the SV's ability to maintain attitude / orbit

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Defense Evasion	Lateral Movement	Elevation	Impact
<ul style="list-style-type: none"> <li>Active Reconnaissance</li> <li>Passive Reconnaissance</li> <li>Signal Intelligence</li> <li>Human Intelligence</li> <li>Open Source Intelligence</li> <li>Geospatial Intelligence</li> <li>Signals Intelligence</li> <li>Human Intelligence</li> <li>Open Source Intelligence</li> <li>Geospatial Intelligence</li> <li>Signals Intelligence</li> </ul>	<ul style="list-style-type: none"> <li>Open Source Intelligence</li> <li>Human Intelligence</li> <li>Open Source Intelligence</li> <li>Human Intelligence</li> <li>Open Source Intelligence</li> <li>Human Intelligence</li> <li>Open Source Intelligence</li> <li>Human Intelligence</li> </ul>	<ul style="list-style-type: none"> <li>Initial Access</li> <li>Initial Access</li> <li>Initial Access</li> <li>Initial Access</li> <li>Initial Access</li> <li>Initial Access</li> <li>Initial Access</li> <li>Initial Access</li> </ul>	<ul style="list-style-type: none"> <li>Execution</li> <li>Execution</li> <li>Execution</li> <li>Execution</li> <li>Execution</li> <li>Execution</li> <li>Execution</li> <li>Execution</li> </ul>	<ul style="list-style-type: none"> <li>Persistence</li> <li>Persistence</li> <li>Persistence</li> <li>Persistence</li> <li>Persistence</li> <li>Persistence</li> <li>Persistence</li> <li>Persistence</li> </ul>	<ul style="list-style-type: none"> <li>Defense Evasion</li> <li>Defense Evasion</li> <li>Defense Evasion</li> <li>Defense Evasion</li> <li>Defense Evasion</li> <li>Defense Evasion</li> <li>Defense Evasion</li> <li>Defense Evasion</li> </ul>	<ul style="list-style-type: none"> <li>Lateral Movement</li> <li>Lateral Movement</li> <li>Lateral Movement</li> <li>Lateral Movement</li> <li>Lateral Movement</li> <li>Lateral Movement</li> <li>Lateral Movement</li> <li>Lateral Movement</li> </ul>	<ul style="list-style-type: none"> <li>Elevation</li> <li>Elevation</li> <li>Elevation</li> <li>Elevation</li> <li>Elevation</li> <li>Elevation</li> <li>Elevation</li> <li>Elevation</li> </ul>	<ul style="list-style-type: none"> <li>Impact</li> <li>Impact</li> <li>Impact</li> <li>Impact</li> <li>Impact</li> <li>Impact</li> <li>Impact</li> <li>Impact</li> </ul>

astro Labels  
 x Truth Vectors  
 x FSU Vectors  
 x Milky Way  
 x Fermi 5Kg

<https://github.com/nasa/nos3>

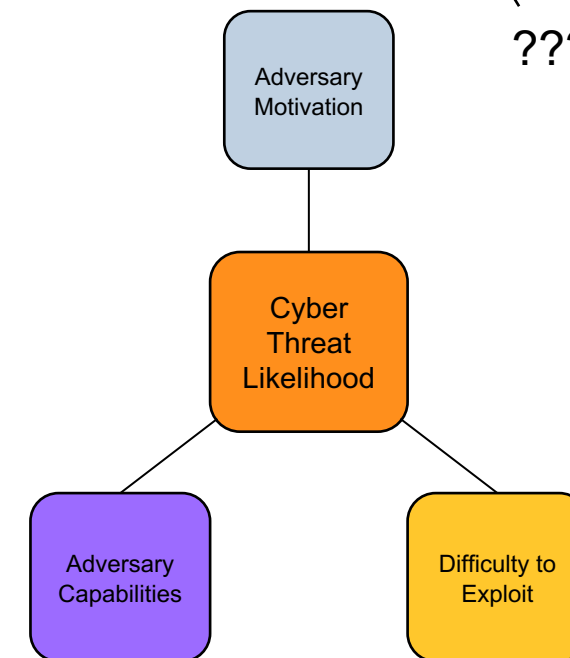
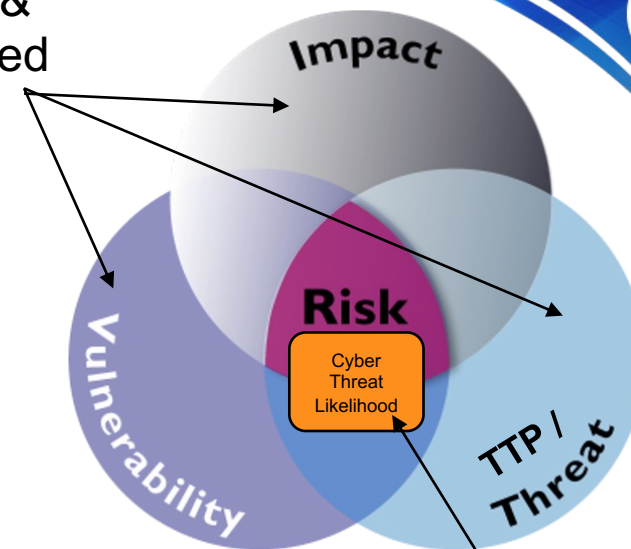
MOMENTUM=0.000000

# Attempting to Understand Risk to SV

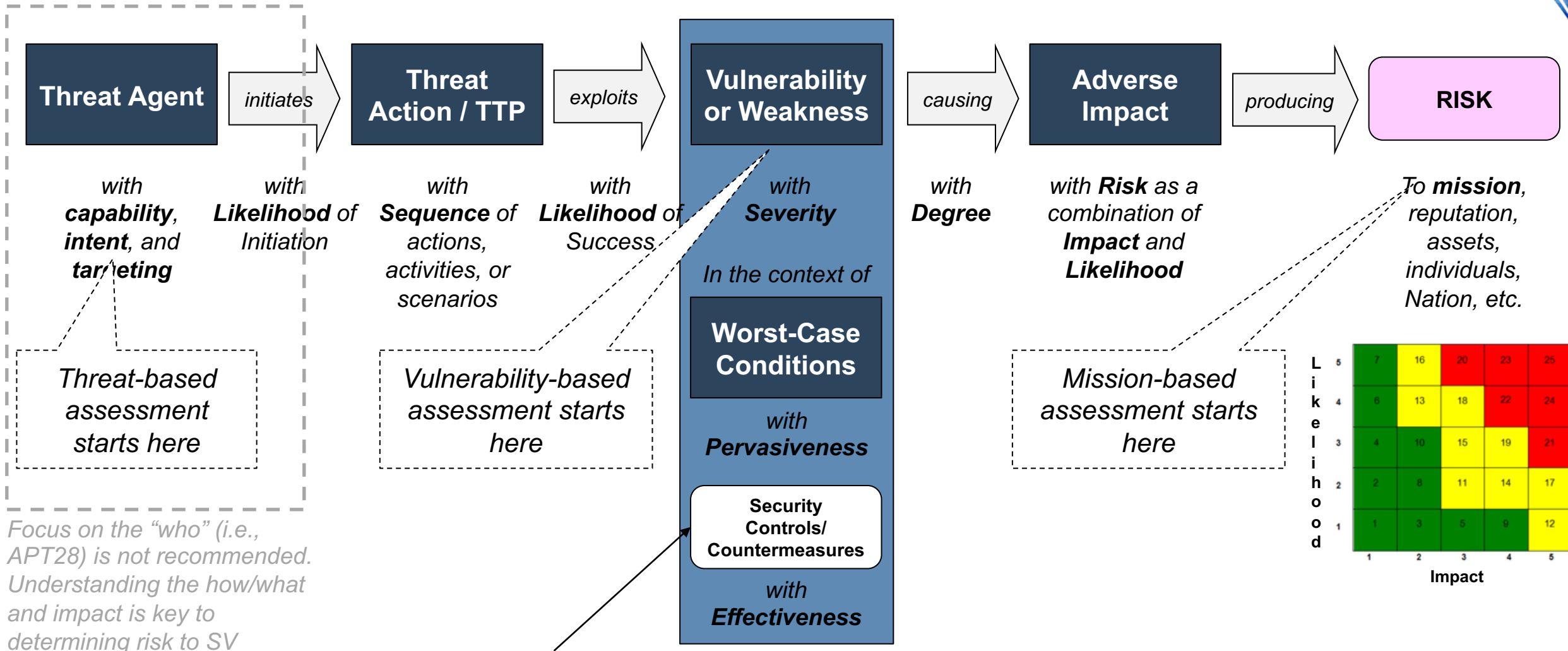
Not always required but it is recommended

- The execution of the TTP demonstrates impact to the SV under test and confirms vulnerability/weakness
- The variable is how “likely” the threat actor can exploit the weakness/vulnerability
- Likelihood – a three-legged stool
  - *How difficult would it be to exploit accounting for mission design, operational environment, etc.*
    - This is where full attack chain analysis and accounting for initial access can reduce likelihood
  - *What actions are required? What are the capabilities of the threat actor?*
    - Real threat intel (if available) with known adversary capabilities and motivation. Can they defeat current security (e.g., crypto)?
    - Can leverage tiered generic threat model when real intel not available (e.g., script kiddie to nation state)
    - What is skill level of the test team?
  - *Why would threat agent act? What is their motivation?*
    - Assumed to be high for critical infrastructure/military

Known & confirmed via test



# Generic Cyber Risk Model



Focus on the "who" (i.e., APT28) is not recommended. Understanding the how/what and impact is key to determining risk to SV

This is where Initial Access and System Design should be factored in

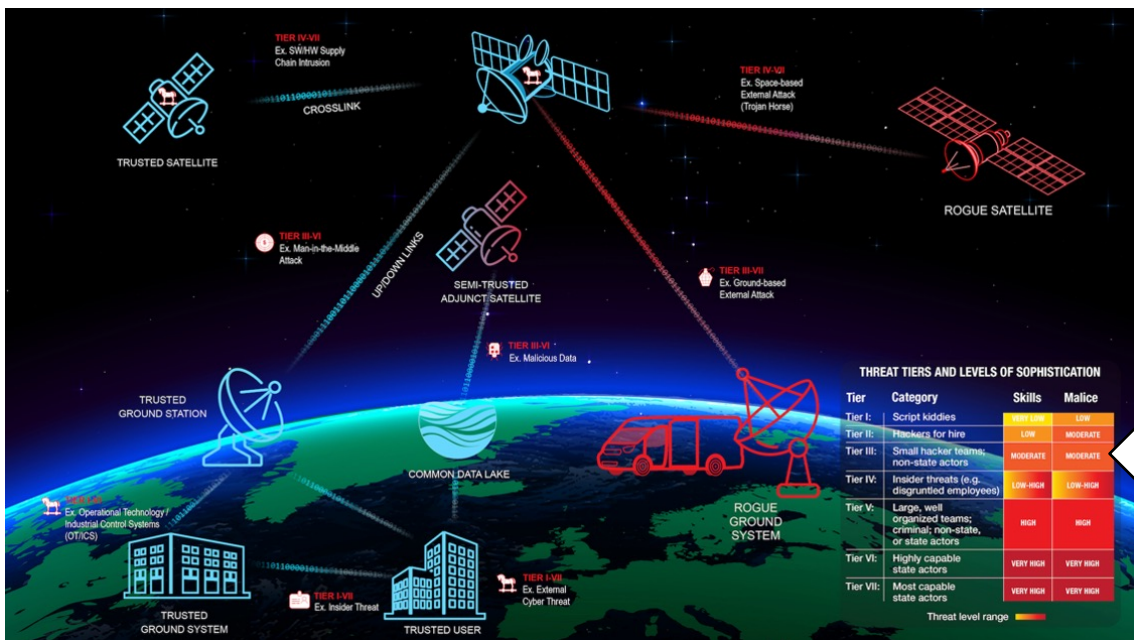




# Example: Aerospace's Space-Cyber Risk Assessment

<https://sparta.aerospace.org/related-work/threat-levels>

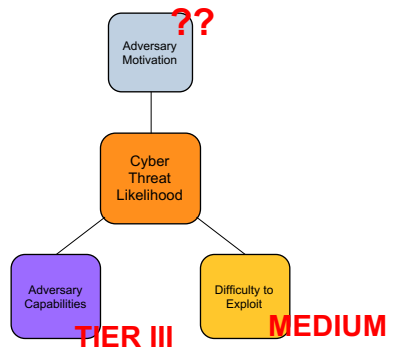
Example: Given the basic failures such as no encryption or authentication on the TT&C link, Mission X currently could be impacted by TIER III threat



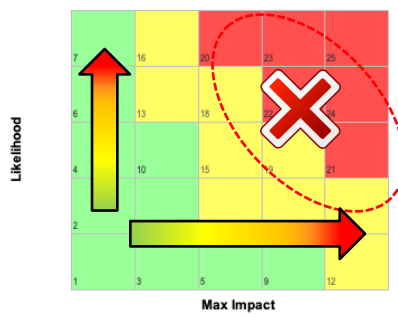
	Tier II Hackers for Hire	Tier III: Small Hacker Teams, Non-State Actors OR Disorganized/Non-Advanced State Actors
<b>Ability to Access Networks</b>	<ul style="list-style-type: none"> <li>Can inject traffic into a short-range RF-based internal access link lacking access controls.</li> <li>Can flood or intercept wired internet access links lacking access controls.</li> <li>Can jam, flood, or intercept access-controlled short-range RF access links to unclassified networks.</li> <li>Can jam wired, access-controlled links to unclassified networks.</li> </ul>	<ul style="list-style-type: none"> <li>Can inject traffic into a wired internet access link lacking access controls.</li> <li>Can jam, flood, or intercept land-based or long-distance RF-based internet access links lacking access controls.</li> <li>Can inject traffic into an access-controlled short-range RF-based access link to an unclassified network.</li> <li>Can flood, intercept, or inject traffic into an access-controlled, wired access link to an unclassified network.</li> <li>Can jam a short-range RF access link a tactical network.</li> </ul>
<b>Ability to Discover &amp; Exploit Vulnerabilities</b>	<ul style="list-style-type: none"> <li>Exploits known vulnerabilities in OS, firmware, application SW, or hypervisor of embedded systems.</li> <li>Can discover zero days in OS, firmware, or application SW of computers, smart phones, network appliances, and embedded systems.</li> </ul>	<ul style="list-style-type: none"> <li>Exploits known vulnerabilities in OS, firmware, application SW, or hypervisor of high assurance systems.</li> <li>Can discover zero days in hypervisor of computers, smart phones, network appliances, and embedded systems.</li> <li>Can develop highly-stealthy implants for OS or application SW of computer or smart phone.</li> </ul>
<b>Ability to Defeat Crypto &amp; Authentication</b>	<ul style="list-style-type: none"> <li>Defeats strong passwords not protected by strong hashing.</li> <li>Defeats strong passwords protected by strong hashing by exploiting implementation vulnerabilities.</li> </ul>	<ul style="list-style-type: none"> <li>Can use brute force searches to defeat strong passwords protected by strong hashing.</li> <li>Defeats strong commercial crypto by exploiting implementation vulnerabilities.</li> <li>Defeats commercial crypto (weak or strong) by obtaining key material.</li> </ul>
<b>Command &amp; Control Sophistication</b>	<ul style="list-style-type: none"> <li>Can execute centralized C2 of millions of nodes, partially-distributed C2 of tens of thousands of nodes, and highly-distributed C2 of hundreds of nodes, with minimal stealth.</li> <li>Can execute centralized C2 of tens of thousands of nodes and partially-distributed C2 of hundreds of nodes, while evading detection by COTS tools.</li> </ul>	<ul style="list-style-type: none"> <li>Can execute partially distributed or highly-distributed C2 of millions of nodes, with minimal stealth.</li> <li>Can execute centralized or partially-distributed C2 of millions of nodes, or highly distributed C2 of tens of thousands of nodes, while evading detection by COTS tools.</li> <li>Can execute centralized C2 of millions of nodes, or partially-distributed C2 of tens of thousands of nodes, while evading detection by GOTS tools.</li> </ul>
<b>Ability to Affect Cyber/Physical Systems</b>	No distinction from lower tiers in this category.	<ul style="list-style-type: none"> <li>Can create coordinated effects on co-located devices in systems well-documented in open literature.</li> </ul>
<b>Ability to Gain Physical Access</b>	<ul style="list-style-type: none"> <li>Can obtain physical access to unclassified systems (poorly-protected or access-controlled) in a way that will not be evident to casual observers, and is unlikely to be detected by users or guards within 1 week.</li> <li>Uses moderately sophisticated social engineering techniques.</li> <li>Uses moderately sophisticated HUMINT techniques in social settings.</li> </ul>	<ul style="list-style-type: none"> <li>Can obtain physical access to classified systems with light physical protection in a way that will not be evident to casual observers, but will be evident to guards and users.</li> <li>Uses highly-sophisticated social engineering techniques.</li> <li>Uses highly-sophisticated HUMINT techniques in social settings.</li> </ul>
<b>Sophistication of Human Influence</b>		

- TIER III sophistication likely required to pair basic TT&C vulnerabilities to mission impact; however, a TIER I adversary could operate with reckless abandon and cause significant headache or reputational risk for mission if they gain foothold on the ground

**Initial Access is crucial to protect!!**  
**Either rogue ground or attacking from authorized ground**



Likelihood is difficult to determine due to motivation, but medium tier capabilities/difficulty pushes it up/high, and impact is right/high given success during testing





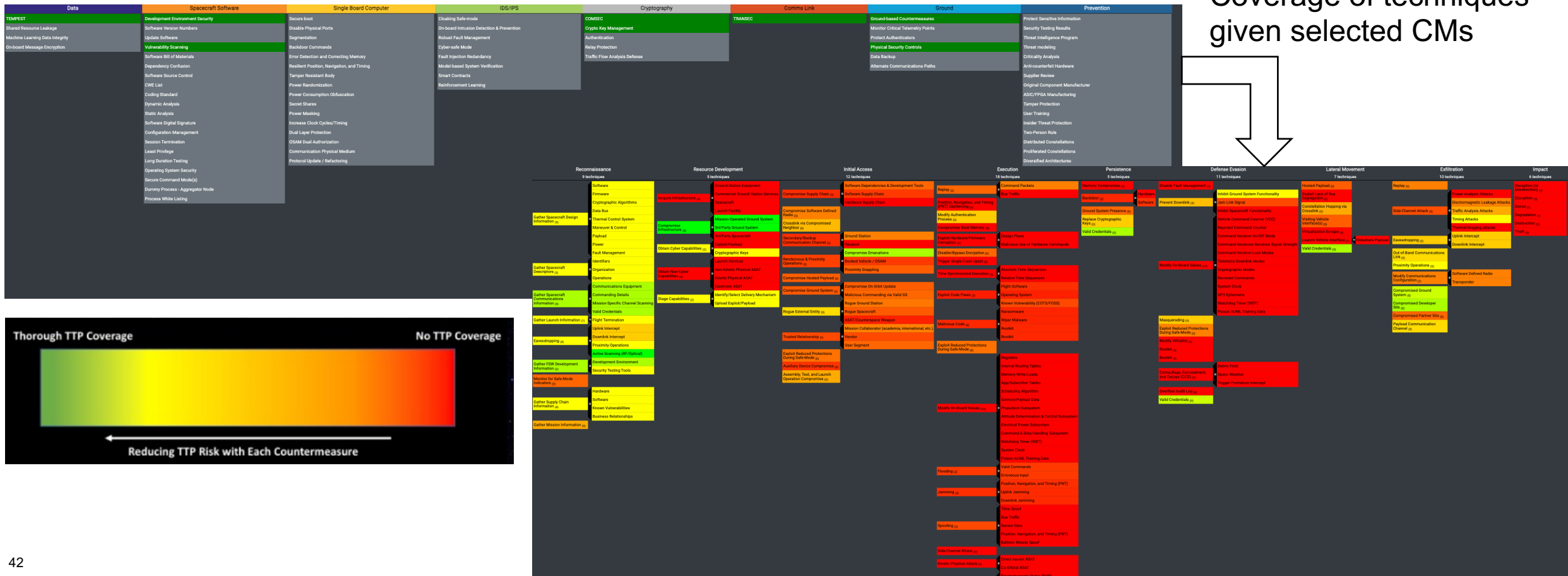




# Alternative Approach to Assessment

- Caveat to this approach is you are “assuming” the implemented controls / countermeasures are **effectively** implemented – this is not recommended but can be beneficial if confident in implementation
- Can use Countermeasure Mapper or Control Mapper to see residual risk / applicable techniques to attempt
  - <https://sparta.aerospace.org/countermeasures/mapper>
  - <https://sparta.aerospace.org/countermeasures/references/mapper>

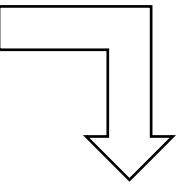
Coverage of techniques given selected CMs



# Using SPARTA's Control Mapper



Access Control	Assessment and Testing	Audit and Accountability	Assessment, Authorization, and Monitoring	Configuration Management	Contingency Planning	Identification and Authentication	Incident Response	Maintenance	Media Protection	Physical and Environmental Protection	Planning	Program Management	Personnel Security	Policy, Procedures, and Compliance	Risk Assessment	System and Services Acquisition	System and Information Integrity	Supply Chain Risk Management
AC-1 Policy and Procedures	AT-1 Policy and Procedures	AC-2 Policy and Procedures	AM-1 Policy and Procedures	CM-1 Policy and Procedures	CP-1 Policy and Procedures	IA-1 Policy and Procedures	IR-1 Policy and Procedures	MA-1 Policy and Procedures	MP-1 Policy and Procedures	PE-1 Policy and Procedures	PL-1 Policy and Procedures	PM-1 Policy and Procedures	PS-1 Policy and Procedures	PP-1 Policy and Procedures	RA-1 Policy and Procedures	SA-1 Policy and Procedures	SI-1 Policy and Procedures	SC-1 Policy and Procedures



Coverage of techniques given selected NIST 800-53 controls

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Defense Evasion	Lateral Movement	Exfiltration	Impact
<b>9 techniques</b> Software Firmware Cryptographic Algorithms Thermal Control System Manoeuvre & Control Payload Power Fault Management Identifiers Communications Equipment Commanding Details Mission-Specific Channel Scanning Valid Credentials Flight Termination Uplink Intercept Downlink Intercept Proximity Operations Active Scanning (RF/Optical) Development Environment Security Testing Tools Monitor for Safe-Mode Indicators Hardware Gather Supply Chain Information Software Known Vulnerabilities Business Relationships Gather Mission Information	<b>9 techniques</b> Ground Station Equipment Commercial Ground Station Services Launch Facility Mission-Operated Ground System 3rd Party Ground System 3rd Party Spacecraft Exploit Payload Cryptographic Keys Launch Services Organization Non-Kinetic Physical ASAT Kinetic Physical ASAT Electronic ASAT Identify/Select Delivery Mechanism Stage Capabilities Upload Exploit/Payload	<b>12 techniques</b> Software Dependencies & Development Tools Software Supply Chain Hardware Supply Chain Compromise Supply Chain Compromise Software Defined Radio Secondary Backup Communication Channel Ground Station Receiver Compromise Emanations Rendezvous & Proximity Operations Docked Vehicle / OSAM Proximity Grappling Compromise Hosted Payload Compromise Ground System Malicious Commanding via Valid GS Rogue Ground Station Rogue Spacecraft ASAT/Counterspace Weapon Mission Collaborator (academia, international, etc.) User Segment Trusted Relationship Exploit Reduced Protections During Safe-Mode Auxiliary Device Compromise Assembly, Test, and Launch Operation Compromise	<b>18 techniques</b> Replay Position, Navigation, and Timing (PNT) Spoofing Modify Authentication Process Compromise Boot Memory Design Flaws Malicious Use of Hardware Commands Time Synchronized Execution Flight Software Operating System Known Vulnerability (COTS/FOSS) Wiper Malware Rootkit Bootkit Registers Internal Routing Tables Memory Write/Loads App/Subscriber Tables Scheduling Algorithm Science/Payload Data Population Subsystem Attitude Determination & Control Subsystem Electrical Power Subsystem Command & Data Handling Subsystem Watchdog Timer (WDT) System Clock Poison AI/ML Training Data Valid Commands Erroneous Input Position, Navigation, and Timing (PNT) Uplink Jamming Downlink Jamming Time Spoof Bus Traffic Spoofing Sensor Data Position, Navigation, and Timing (PNT) Ballistic Missile Spoof Flooding Jamming Spoofing Side-Channel Attack Kinetic Physical Attack Non-Kinetic Physical Attack High-Powered Laser High-Powered Microwave	<b>5 techniques</b> Memory Compromise Backdoor Ground System Presence Valid Cryptographic Keys Credentials Modify On-Board Values Received Modes System Clock GPS Ephemeris Watchdog Timer (WDT) Poison AI/ML Training Data Masquerading Exploit Reduced Protections During Safe-Mode Modify Whitelist Rootkit Bootkit Camouflage, Concealment, and Disguise (CCD) Overflow Audit Log Valid Credentials	<b>11 techniques</b> Disable Fault Management Prevent Downlink Jam Link Signal Inhibit Spacecraft Functionality Vehicle Command Counter (VCC) Rejected Receiver Received Signal Strength Command Receiver Lock Modes Telemetry Downlink Modes Cryptographic Modes System Clock GPS Ephemeris Watchdog Timer (WDT) Poison AI/ML Training Data Masquerading Exploit Reduced Protections During Safe-Mode Modify Whitelist Rootkit Bootkit Camouflage, Concealment, and Disguise (CCD) Overflow Audit Log Valid Credentials Debris Field Space Weather Trigger Premature Intercept	<b>7 techniques</b> Hosted Payload Exploit Lack of Bus Segregation Constellation Hopping via Drosslink Visualizing Escapes Launch Vehicle Inter-Seat Side-Share Payload Out-of-Band Communications Link Modify Communications Configuration Transponder Compromised Ground System Compromised Partner Site Payload Communication Channel	<b>10 techniques</b> Replay Power Analysis Attacks Traffic Analysis Attacks Timing Attacks Signal Interception Eavesdropping Downlink Intercept Out-of-Band Communications Link Modify Communications Configuration Transponder Compromised Ground System Compromised Partner Site Payload Communication Channel	<b>5 techniques</b> Disruption of Mission Denial Degradation Theft

## NIST Moderate Watermark



# Summary

- SPARTA's tools can be leveraged to help focus techniques for execution when conducting a penetration test/red team/purple team
  - *Also, beneficial when doing vulnerability assessments only (i.e., table-tops analysis)*
    - Hard to confirm / demonstrate impact from vulnerability assessments only
- SPARTA updates in the near future will contain SV functional breakdown and correlation of techniques to SV functional breakdown
  - *DRAFT document and sheet embedded in this presentation*
- Notional Risk Score can help target specific techniques
  - *Library of techniques can create to help test or baseline SVs, but the procedures are where the differences come into play*
    - How to inject into memory for Mission X is different from Mission Y
    - Exploiting weak permissions in the Operating System and FSW will likely be different across missions
    - Etc.
  - *NRS can help quantify risk calculations using the default impact x likelihood scores*
- Technique to countermeasure correlation can help with recommendations



Space Attack Research & Tactic Analysis (SPARTA)

show sub-techniques | hide sub-techniques

Reconnaissance 9 techniques	Resource Development 5 techniques	Initial Access 12 techniques	Execution 18 techniques	Persistence 5 techniques	Defense Evasion 11 techniques	Lateral Movement 7 techniques	Exfiltration 10 techniques	Impact 6 techniques
Gather Spacecraft Design Information (1)	Acquire Infrastructure (4)	Compromise Supply Chain (1)	Replay (1)	Memory Compromise (1)	Disable Fault Management (1)	Hosted Payload (1)	Replay (1)	Deception (or Misdirection) (1)
Gather Spacecraft Descriptors (1)	Compromise Infrastructure (1)	Compromise Software Defined Radio (1)	Position, Navigation, and Timing (PNT) Geofencing (1)	Backdoor (1)	Prevent Download (1)	Exploit Lack of Bus Segregation (1)	Side-Channel Attack (1)	Disruption (1)
Gather Spacecraft Communications Information (1)	Obtain Cyber Capabilities (1)	Crosslink via Compromised Neighbor (1)	Modify Authentication Process (1)	Ground System Presence (1)	Modify On-Board Values (1)	Constellation Hopping via Crosslink (1)	Eavesdropping (1)	Denial (1)
Gather Launch Information (1)	Obtain Non-Cyber Capabilities (1)	Secondary/Backup Communication Channel (1)	Compromise Boot Memory (1)	Replace Cryptographic Keys (1)	Masquerading (1)	Visiting Vehicle Interface(s) (1)	Out-of-Band Communications Link (1)	Degradation (1)
Eavesdropping (1)	Stage Capabilities (1)	Rendezvous & Proximity Operations (1)	Exploit Hardware/Firmware Corruption (1)	Valid Credentials (1)	Exploit Reduced Protections During Safe-Mode (1)	Virtualization Escape (1)	Proximity Operations (1)	Destruction (1)
Gather FBW Development Information (1)		Compromise Hosted Payload (1)	Disable/Bypass Encryption (1)		Modify Whitehat (1)	Launch Vehicle Interface (1)	Modify Communications Configuration (1)	Theft (1)
Monitor for Safe-Mode Indicators (1)		Compromise Ground System (1)	Trigger Single Event Upset (1)		Rocket (1)	Valid Credentials (1)	Compromised Ground System (1)	
Gather Supply Chain Information (1)		Rogue External Entity (1)	Time Synchronized Execution (1)		BooKIt (1)		Compromised Developer Site (1)	
Gather Mission Information (1)		Trusted Relationship (1)	Exploit Code Flaws (1)		Camouflage, Concealment, and Deceits (CCCD) (1)		Compromised Partner Site (1)	
		Exploit Reduced Protections During Safe-Mode (1)	Malicious Code (1)		Overflow Audit Log (1)		Payload Communication Channel (1)	
		Auxiliary Device Compromise (1)	Exploit Reduced Protections During Safe-Mode (1)		Valid Credentials (1)			
		Assembly, Test, and Launch Operation Compromise (1)	Modify On-Board Values (1)					
			Flooding (1)					
			Jamming (1)					
			Spoofing (1)					
			Side-Channel Attack (1)					
			Kinetic Physical Attack (1)					
			Non-Kinetic Physical Attack (1)					

## Sample Media Links:

- <https://cyberscoop.com/space-satellite-cybersecurity-sparta/>
- <https://www.darkreading.com/ics-ot/space-race-defenses-satellite-cyberattacks>
- <https://thecyberwire.com/podcasts/daily-podcast/1715/notes> & <https://thecyberwire.com/newsletters/signals-and-space/6/21>

## Overview Briefings:

- [DEF CON 31: Building Space Attack Chains using SPARTA](#) (August 2023)
- [Hacking Spacecraft using Space Attack Research & Tactic Analysis | Video](#) (April 2023)
- [In-depth Overview - Space Attack Research & Tactic Analysis](#) (November 2022)

## Key SPARTA Links:

- Getting Started with SPARTA: <https://sparta.aerospace.org/resources/getting-started> | <https://sparta.aerospace.org/resources/>
- Understanding Space-Cyber TTPs with the SPARTA Matrix: <https://aerospace.org/article/understanding-space-cyber-threats-sparta-matrix>
- Leveraging the SPARTA Matrix: <https://aerospace.org/article/leveraging-sparta-matrix>
- Use Case w/ PCspooF:
  - <https://aerospacecorp.medium.com/sparta-cyber-security-for-space-missions-4876f789e41c>
  - <https://medium.com/the-aerospace-corporation/a-look-into-sparta-countermeasures-358e2fcd43ed>
- FAQ: <https://sparta.aerospace.org/resources/faq>
- Matrix: <https://sparta.aerospace.org>
- Navigator: <https://sparta.aerospace.org/navigator> | Countermeasure Mapper: <https://sparta.aerospace.org/countermeasures/mapper>
- Notional Risk Scores on 5x5: <https://sparta.aerospace.org/notional-risk-scores>
- Related Work: <https://sparta.aerospace.org/related-work/did-space> with ties into [TOR 2021-01333 REV A](#)



# Other Aerospace Papers and Resources

*Many Were Input into SPARTA*

- DEF CON Presentations:
  - [DEF CON 2020: Exploiting Spacecraft](#)
  - [DEF CON 2021: Unboxing the Spacecraft Software BlackBox Hunting for Vulnerabilities](#)
  - [DEF CON 2022: Hunting for Spacecraft Zero Days using Digital Twins](#)
  - [DEF CON 2023: Building Space Attack Chains using SPARTA](#)
- Papers/Articles:
  - 2019: [Defending Spacecraft in the Cyber Domain](#)
  - 2020: [Establishing Space Cybersecurity Policy, Standards, & Risk Management Practices](#)
  - 2021: [Cybersecurity Protections for Spacecraft: A Threat Based Approach](#)
  - 2021: [The Value of Space](#)
  - 2021: [Translating Space Cybersecurity Policy into Actionable Guidance for Space Vehicles](#)
  - 2022: [Protecting Space Systems from Cyber Attack](#)
- July 2022 Congressional Testimony:
  - Video: <https://science.house.gov/hearings?ID=996438A6-A93E-4469-8618-C1B59BC5A964>
  - Written Testimony: <https://republicans-science.house.gov/cache/files/2/9/29fff6d3-0176-48bd-9c04-00390b826aed/A8F54300A11D55BEA5AF2CE305C015BA.2022-07-28-bailey-testimony.pdf>