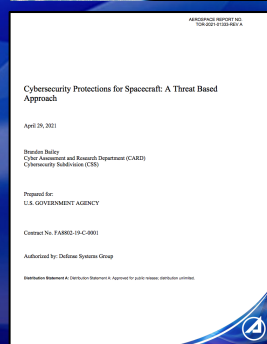




Value of Space Summit 2023 SPARTA 1 Year Update

Brandon Bailey, Brad Roeher, Randi Tinney
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](#)

brandon.bailey@aero.org
240.521.4326 (c)

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



Space Attack Research & Tactic Analysis (SPARTA) – Launched Oct 2022

Filling the TTP Gap for Space

- Cybersecurity matrices are industry-standard tools and approaches for commercial and government users to navigate rapidly evolving cyber threats and vulnerabilities and outpace cyber threats
 - They provide a critical knowledge base of adversary behaviors
 - Framework for adversarial actions across the attack lifecycle with applicable countermeasures
- Current cybersecurity matrices (including [MITRE ATT&CK](#)) are limited to ground systems which lead to a gap for space industry
- Aerospace’s SPARTA is the first-of-its-kind body of knowledge on cybersecurity protections for spacecraft and space systems, filling a critical vulnerability gap exists for the U.S. space enterprise



Space Attack Research & Tactic Analysis (SPARTA)

show sub-techniques hide sub-techniques

Reconnaissance 9 techniques	Resource Development 4 techniques	Initial Access 12 techniques	Execution 15 techniques	Persistence 4 techniques	Defense Evasion 6 techniques	Lateral Movement 4 techniques	Exfiltration 9 techniques	Impact 6 techniques
Gather Spacecraft Design Information (3)	Acquire Infrastructure (3)	Compromise Supply Chain (3)	Replay (2)	Memory Compromise (0)	Disable Fault Management (0)	Hosted Payload (0)	Replay (0)	Deception (or Misdirection) (0)
Gather Spacecraft Descriptors (3)	Compromise Infrastructure (3)	Compromise Software Defined Radio (0)	Position, Navigation, and Timing (PNT) Geofencing (0)	Backdoor (2)	Prevent Downlink (3)	Exploit Lack of Bus Segregation (0)	Side-Channel Attack (5)	Disruption (0)
Gather Spacecraft Communications Information (2)	Obtain Capabilities (2)	Crosslink via Compromised Neighbor (0)	Modify Authentication Process (0)	Ground System Presence (0)	Modify On-Board Values (12)	Constellation Hopping via Crosslink (0)	Eavesdropping (2)	Denial (0)
Gather Launch Information (1)	Stage Capabilities (2)	Secondary/Backup Communication Channel (2)	Compromise Boot Memory (0)	Replace Cryptographic Keys (0)	Masquerading (0)	Visiting Vehicle Interface(s) (0)	Out-of-Band Communications Link (0)	Degradation (0)
Eavesdropping (3)		Rendezvous & Proximity Operations (3)	Exploit Hardware/Firmware Corruption (2)		Exploit Reduced Protections During Safe Mode (0)			
		Compromise Hosted Payload (0)	Disable/Bypass Security (0)					

SPARTA provides unclassified information to space professionals about how spacecraft may be compromised/impacted via cyber or traditional counterspace mean



SPARTA Use Cases – Impact Across Community & Lifecycle

USG, Commercial Space, International, Collaborations, etc.

- Policy Makers – bridging the gap between policy and implementation guidance (e.g., SPD-5)
- Acquisition Professionals - tailor threat informed / risk-based requirements
- Standards development organizations (e.g., CCSDS, IEEE P3349)
- Space system developers (e.g., JAXA, NASA, etc.)
- Defensive Cyber Operations (e.g., USSF)
- Threat intelligence reporting / tracking of TTPs (e.g., Space ISAC Watch Center)
- Assessments / Table-Tops (e.g., MRAP-C, ATO)
- Education / Training - raises the bar on common space-cyber knowledge

SPARTA will crowdsource info from space enterprise researchers and threat intel via sparta@aero.org

SPARTA is a key tool to help Allies, Partners, USG and Commercial adopt a common and consistent cybersecurity posture

Deeper Dive on Use Cases at https://sparta.aerospace.org/resources/SPARTA_Overview_InDepth_Nov22.pdf

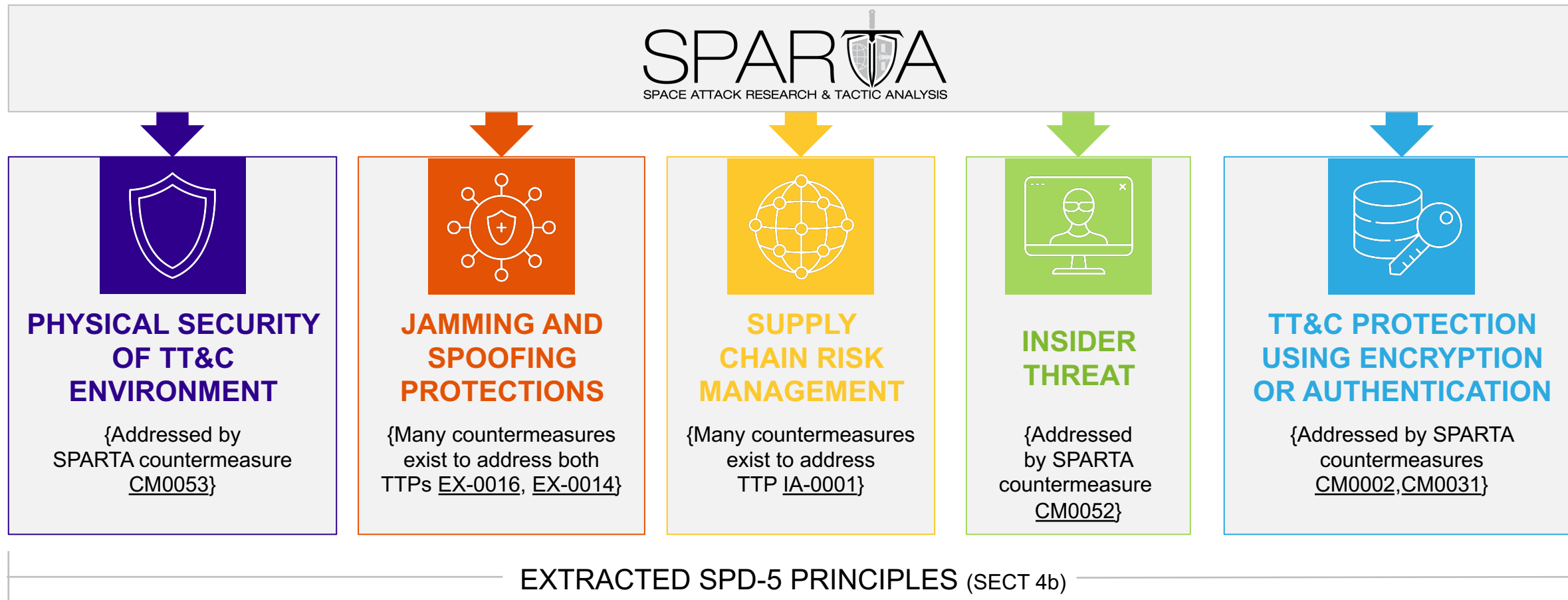


Example: SPD-5 and SPARTA Relationship

Bridging the Technical Gap Between Policy and Implementation

SPD-5 PROVIDES SOME GENERIC SECURITY GUIDANCE FOR SPACE SYSTEMS

Implementation details on these principles – SPARTA provides guidance on SPD-5 principles and beyond



Aerospace is working with Space ISAC to deliver space cyber best practice / implementation guidance using SPARTA



1 Year Highlights – Many Updates!!!



New Features Since Launch

- Keep an eye on <https://sparta.aerospace.org/resources/updates-current>
 - *All updates are posted and maintained*
- *~25% increase in the number of TTP {V1.0 TTPs=169 to V1.5 TTPs=213}*
- *~25% increase in the number of countermeasures {V1.0 CMs=69 to V1.5 CMs=87}*
- Blog Area Established - <https://medium.com/the-aerospace-corporation/space-cyber/home>
- Mapping to Standards
 - *ISO 27001 mapping* - <https://sparta.aerospace.org/countermeasures/iso>
 - *D3FEND Mapping* - <https://sparta.aerospace.org/countermeasures/d3fend/techniques>
 - *NIST 800-53 revision 5* - <https://sparta.aerospace.org/countermeasures/references>
- References Added to the TTPs based on CyberInFlight database
- Tools
 - *JSON Creator* - <https://sparta.aerospace.org/json-creator>
 - *Attack chain tools* – *manually click or use JSON creator*
 - Navigator - <https://sparta.aerospace.org/navigator>
 - Countermeasure Mapper - <https://sparta.aerospace.org/countermeasures/mapper>
 - *Control Mapper* - <https://sparta.aerospace.org/countermeasures/references/mapper>
 - *Notional Risk Scores* - <https://sparta.aerospace.org/notional-risk-scores>

Mapping to Standards



NIST References

The following references have been used in SPARTA Countermeasures and/or Defense-in-Depth Space Threats. While this is not a full list of the relevant NIST controls, these are the ones our subject matter experts found most relevant.

ID	Name	Description	SPARTA Countermeasures	ISO 27001
AC-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] access control policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the access control policy and the associated access controls; b. Designate an [Assignment: organization-defined official] to manage compliance, regulatory, audit practices published by NIST and/or ISO.	CM0005	5.2 5.3 7.5.1 7.5.2 7.5.3 A.5.1 A.5.2 A.5.4 A.5.15

[View ISO 27001 Requirements](#) | [View ISO 27001 Controls](#)

ID	Name	SPARTA Countermeasures	NIST Rev 5
A.5	Organizational controls	None	None
A.5.1	Policies for information security	CM0005 CM0022 CM0024 CM0026 CM0027 CM0028 CM0004	AC-1 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IR-1 MA-1 MP-1 PE-1 PL-1 PM-1 PS-1 RA-1 SA-1 SC-1 SI-1 SR-1
A.5.2	Information security roles and responsibilities	CM0005 CM0020 CM0022 CM0041 CM0052 CM0054 CM0074 CM0075 CM0076 CM0079 CM0081 CM0087 CM0070 CM0006 CM0042 CM0044 CM0043 CM0045 CM0048 CM0001 CM0009 CM0024 CM0025 CM0026 CM0027 CM0028 CM0030 CM0031 CM0050 CM0004 CM0010 CM0011 CM0012 CM0013 CM0015 CM0017 CM0018 CM0019 CM0023 CM0039 CM0046 CM0047 CM0055 CM0035 CM0053 CM0056 CM0051 CM0037 CM0038 CM0057 CM0021	AC-1 AT-1 AU-1 CA-1 CM-1 CM-9 CP-1 CP-2 IA-1 IR-1 MA-1 MP-1 PE-1 PL-1 PM-1 PM-2 PM-10 PM-29 PS-1 PS-7 PS-9 RA-1 SA-1 SA-3 SA-9 SC-1 SI-1 SR-1
A.5.3	Segregation of duties	None	AC-5
A.5.4	Management responsibilities	CM0005 CM0024 CM0025 CM0026 CM0027 CM0028 CM0041 CM0004 CM0010 CM0012 CM0013 CM0015 CM0021 CM0048 CM0022	AC-1 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IR-1 MA-1 MP-1 PE-1 PL-1

D3FEND Techniques

MITRE published Detection, Denial, and Disruption Framework Empowering Network Defense (D3FEND) in 2021 and defines D3FEND as a "knowledge graph of cybersecurity countermeasure techniques." Like SPARTA, D3FEND discusses cyber countermeasures which are actions that need to be taken to increase cyber defense. D3FEND's goal is not to prescribe the exact implementation for a countermeasure, but rather, to provide a lexicon and framework for defensive techniques. Similar to other frameworks (i.e., ATT&CK, SPARTA, etc.), the D3FEND Matrix contains a definition of the countermeasure, how it works, considerations when using the countermeasure, and information about relevant types of digital artifacts.

D3FEND provides its own reference that depicts which countermeasures will help mitigate against various ATT&CK elements. Similarly, SPARTA wanted to provide a translation/mapping of D3FEND techniques and artifacts to the relevant SPARTA countermeasures. This should enable users of SPARTA to bridge the gap between countermeasures / courses of actions (COAs). Currently SPARTA's countermeasures provide varying levels of abstraction on details. Mapping SPARTA countermeasures to NIST 800-53, ISO 27001, and now D3FEND gives the SPARTA users additional context and data to improve cyber defenses on space systems.

ID	Name	Description
D3-AI	Asset Inventory	Asset inventorying identifies and records the organization's assets and enriches each inventory item with knowledge about their vulnerabilities.
D3-CI	Configuration Inventory	Configuration inventory identifies and records the configuration of software and hardware and their components throughout the organization.
D3-DI	Data Inventory	Data inventorying identifies and records the schemas, formats, volumes, and locations of data stored and used on the organization's architecture.
D3-SWI	Software Inventory	Software inventorying identifies and records the software items in the organization's architecture.
D3-AVE	Asset Vulnerability Enumeration	Asset vulnerability enumeration enriches inventory items with knowledge identifying their vulnerabilities.
D3-NNI	Network Node Inventory	Network node inventorying identifies and records all the network nodes (hosts, routers, switches, firewalls, etc.) in the organization's architecture.
D3-HCI	Hardware Component	Hardware component inventorying identifies and records the hardware items in the organization's architecture.



International Collaboration

CyberInflight

- Expanding the reference section with CyberInflight's space security attacks database
 - Working with them to map TTPs to increase the real-world examples of the TTPs in use by threat actors
- Inclusion of their database deployed in July 2023 – v1.3.2
 - <https://sparta.aerospace.org/resources/updates/v1.3.2>
- Since Oct 2022, received input from SPARTA from many government and commercial entities
 - Including inputs from several international partners

External Contributors

Special thanks to the following non-Aerospace Corporation individuals or organizations who have contributed to SPARTA content development and peer reviews:

- Gregory Falco
- Nick Tsamis
- Mario Zuniga
- Francesco Traini, Università Politecnica delle Marche
- Antonios Atalasi
- Ignacio Aguilar Sanchez
- Tim Dafoe
- Wayne Henry
- Andres Coronado
- Timothy O'Neill
- Florent Rizzo, CyberInflight's Market Intelligence Team
- Matthias Popoff, CyberInflight's Market Intelligence Team
- Héloïse Do Nascimento Cardoso, CyberInflight's Market Intelligence Team

<https://sparta.aerospace.org/contribute>

Website Updates

- Updated TTP references using CyberInflight's Market Intelligence Team's space attack database
- Created Tools link to house Navigator and CM Mapper
- Fixed Navigator to work with other versions of SPARTA, but now all previously created JSON files are now obsolete
- Added 'Needed Countermeasures' to Navigator
- Updated Contributors list

Techniques

New Techniques

Modified Techniques

- REC-0001: Gather Spacecraft Design Information
- REC-0002: Gather Spacecraft Descriptors
- REC-0003: Gather Spacecraft Communications Information
- REC-0004: Gather Launch Information
- REC-0008: Gather Supply Chain Information
- REC-0009: Gather Mission Information
- RD-0002: Compromise Infrastructure
- EX-0005: Exploit Hardware/Firmware Corruption
- EX-0013: Flooding
- EX-0014: Spoofing
- EXF-0007: Compromised Ground System
- EXF-0010: Payload Communication Channel
- IMP-0002: Disruption
- IMP-0003: Denial
- IMP-0004: Degradation
- IMP-0005: Destruction
- IMP-0006: Theft

Sub-Techniques

New Sub-Techniques

Modified Sub-Techniques

- REC-0003.01: Communications Equipment
- REC-0003.03: Mission-Specific Channel Scanning
- REC-0005.04: Active Scanning (RF/Optical)
- REC-0008.04: Business Relationships
- RD-0001.02: Commercial Ground Station Services
- EX-0013.02: Erroneous Input
- EX-0016.02: Downlink Jamming
- EXF-0003.02: Downlink Intercept



SPARTA JSON Creator

The SPARTA JSON Creator is a tool for creating JSON objects to be used in the various SPARTA mapping tools; Navigator, CM Mapper, and Control Mapper. The user can easily copy/paste SPARTA TTPs, SPARTA Countermeasures, NIST 800-53 Rev 5 IDs, or ISO 27001 IDs into the top text area and convert the data into a specific SPARTA tool format. This JSON can then be downloaded and imported into the tool for editing and creating visuals. The expected format of the controls **MUST** match the format within the Countermeasure section of SPARTA (**NIST, ISO**) . For example, NIST control must match control family-control number(enhancement number) with no leading zeros. This would look like AC-2(1) and not AC-02(1) or AC-02(01).

Navigator CM Mapper Control Mapper (NIST) Control Mapper (ISO 27001)

Building Spacecraft Attack Chains using Attack Chains / Attack Flow != Cyber Kill Chain



- Attack Chains help demonstrate exactly what an attacker is doing at every step of the way - in a simple and easy to understand visual story
 - This is not Cyber Kill Chain which are stages comprising a cyberattack, geared towards “breaking” any phase of the “kill chain” which stop an attacker



- Attack Chains using ATT&CK and or SPARTA are **more than a sequence** of attack tactics
 - Knowledge base that correlates environment-specific (IT, OT/ICS, Cloud, Space) cybersecurity information along a hierarchy of TTP, and other knowledge (detections, mitigations, countermeasures, etc.)
- Ex: building the attack chains in [Navigator](#) helps derive [countermeasures](#) | [mapper](#)

SPARTA Countermeasure Mapper
Instructions: Select a countermeasure below to see which techniques and subtechniques are covered

Through TTP Coverage No TTP Coverage

Reducing TTP Risk with Each Countermeasure

Data	Spacecraft Software	Single Board Computer	IDS/IPS	Cryptography	Comms Link	Ground	Prevention
TEMPEST	Development Environment Security	Secure boot	Cloaking Safe-mode	COMSEC	TRANSEC	Ground-based Countermeasures	Protect Sensitive Information
Shared Resource Leakage	Software Version Numbers	Segmentation	On-board Intrusion Detection & Prevention	Crypto Key Management	Monitor Critical Telemetry Points	Security Testing Results	Security Testing Results
Machine Learning Data Integrity	Update Software	Backdoor Commands	Robust Fault Management	Relay Protection	Protect Authenticators	Threat Intelligence Program	Threat modeling
On-board Message Encryption	Vulnerability Scanning	Error Detection and Correcting Memory	Cyberbase Mode	Traffic Flow Analysis Defense	Physical Security Controls	Criticality Analysis	Anti-counterfeit Hardware
Dependency Confusion	Software Bill of Materials	Resilient Position, Navigation, and Timing	Fault Injection Redundancy	Model-based System Verification	Data Backup	Supplier Review	Original Component Manufacturer
Static Analysis	Dependency Confusion	Target Resistant Body	Smart Contracts	Reinforcement Learning	ASIC/FPGA Manufacturing	User Training	Insider Threat Protection
Dynamic Analysis	Software Source Control	Power Randomization	Power Masking	Secret Shares	ASIC/FPGA Manufacturing	Static Analysis	Two-Person Rule
Configuration Management	DWE List	Power Consumption Obfuscation	Increase Clock Cycles/Timing	Power Masking	ASIC/FPGA Manufacturing	Static Analysis	Distributed Constellations
Least Privilege	Configuration Management	OSAM Dual Authorization	OSAM Dual Authorization	Power Masking	ASIC/FPGA Manufacturing	Static Analysis	Prohibited Constellations
Long Duration Testing	Session Termination	Communication Physical Medium	Communication Physical Medium	Static Analysis	ASIC/FPGA Manufacturing	Static Analysis	Diversified Architectures
Identifying System Security	Least Privilege	Protocol Update / Refactoring	Protocol Update / Refactoring	Static Analysis	ASIC/FPGA Manufacturing	Static Analysis	Space Domain Awareness
Secure Control Models	Long Duration Testing	Operating System	Operating System	Static Analysis	ASIC/FPGA Manufacturing	Static Analysis	
Control Plane - Aggregate Nodes	Power Masking			Static Analysis	ASIC/FPGA Manufacturing	Static Analysis	
Process White Listing	Configuration Management			Static Analysis	ASIC/FPGA Manufacturing	Static Analysis	

Data	Spacecraft Software	Single Board Computer	IDS/IPS	Cryptography	Comms Link	Ground	Prevention
TEMPEST	Development Environment Security	Secure boot	Cloaking Safe-mode	COMSEC	TRANSEC	Ground-based Countermeasures	Protect Sensitive Information
Shared Resource Leakage	Software Version Numbers	Segmentation	On-board Intrusion Detection & Prevention	Crypto Key Management	Monitor Critical Telemetry Points	Security Testing Results	Security Testing Results
Machine Learning Data Integrity	Update Software	Backdoor Commands	Robust Fault Management	Relay Protection	Protect Authenticators	Threat Intelligence Program	Threat modeling
On-board Message Encryption	Vulnerability Scanning	Error Detection and Correcting Memory	Cyberbase Mode	Traffic Flow Analysis Defense	Physical Security Controls	Criticality Analysis	Anti-counterfeit Hardware
Dependency Confusion	Software Bill of Materials	Resilient Position, Navigation, and Timing	Fault Injection Redundancy	Model-based System Verification	Data Backup	Supplier Review	Original Component Manufacturer
Static Analysis	Dependency Confusion	Target Resistant Body	Smart Contracts	Reinforcement Learning	ASIC/FPGA Manufacturing	User Training	Insider Threat Protection
Dynamic Analysis	Software Source Control	Power Randomization	Power Masking	Secret Shares	ASIC/FPGA Manufacturing	Static Analysis	Two-Person Rule
Configuration Management	DWE List	Power Consumption Obfuscation	Increase Clock Cycles/Timing	Power Masking	ASIC/FPGA Manufacturing	Static Analysis	Distributed Constellations
Least Privilege	Configuration Management	OSAM Dual Authorization	OSAM Dual Authorization	Power Masking	ASIC/FPGA Manufacturing	Static Analysis	Prohibited Constellations
Long Duration Testing	Session Termination	Communication Physical Medium	Communication Physical Medium	Static Analysis	ASIC/FPGA Manufacturing	Static Analysis	Diversified Architectures
Identifying System Security	Least Privilege	Protocol Update / Refactoring	Protocol Update / Refactoring	Static Analysis	ASIC/FPGA Manufacturing	Static Analysis	Space Domain Awareness
Secure Control Models	Long Duration Testing	Operating System	Operating System	Static Analysis	ASIC/FPGA Manufacturing	Static Analysis	
Control Plane - Aggregate Nodes	Power Masking			Static Analysis	ASIC/FPGA Manufacturing	Static Analysis	
Process White Listing	Configuration Management			Static Analysis	ASIC/FPGA Manufacturing	Static Analysis	

Initial Access	Execution	Persistence	Defense Evade
12 techniques	18 techniques	5 techniques	11 techniques
Compromise Supply Chain (1)	Replay (2)	Command Packets (3)	Disable Fault Management (4)
Software Supply Chain	Position, Navigation, and Timing (PNT) Spoofing (5)	Bus Traffic	Hardware
Hardware Supply Chain	Modify Authentication Process (6)	Backdoor (7)	Software
Compromise Software Defined Radio (8)	Compromise Boot Memory (9)	Ground System Presence (10)	Prevent Downlink (11)
Crosslink via Compromised Neighbor (12)	Exploit Hardware/Firmware Corruption (13)	Replace Cryptographic Keys (14)	Inhibit Spacecraft
Secondary/Backup Communication Channel (1)	Design Flaws	Valid Credentials (15)	Vehicle Control
Receiver	Malicious Use of Hardware Commands		Rejected Commands
Compromise Emanations	Disable/Bypass Encryption (16)		Command
Docked Vehicle / OSAM	Trigger Single Event Upset (17)		Command
Proximity Grappling	Time Synchronized Execution (18)		Telemetry
Relative Time Sequences	Absolute Time Sequences		Modify On-Board Values (19)
Relative Time Sequences	Relative Time Sequences		Cryptographic
Flight Software	Operating System		Received Data
Known Vulnerability (COTS/FOSS)	Known Vulnerability (COTS/FOSS)		System Clock
Ransomware	Ransomware		GPS Ephemeris
Wiper Malware	Wiper Malware		Watchdog
Rootkit	Rootkit		Poison Audit
Bookkit	Bookkit		
Exploit Reduced Protections During Safe-Mode (20)	Registers		
Auxiliary Device Compromise (21)	Internal Routing Tables		
Scheduling Algorithm	Memory Write/Loads		
Science/Payload Data	App/Subscriber Tables		
Propulsion Subsystem	Scheduling Algorithm		
Attitude Determination & Control Subsystem	Science/Payload Data		
Electrical Power Subsystem	Propulsion Subsystem		
Command & Data Handling Subsystem	Attitude Determination & Control Subsystem		
Watchdog Timer (WDT)	Electrical Power Subsystem		
System Clock	Command & Data Handling Subsystem		
Poison A/M/L Training Data	Watchdog Timer (WDT)		
	System Clock		
	Poison A/M/L Training Data		



Building Spacecraft Attack Chains



Blast from the Past

- Replay Attack from DefCon 2020
- Memory Injection Attack DefCon 2022

New Attacks

- Supply Chain Attack – Time bomb that executes command sequence 30 secs after boot
- Reaction Wheel Attack – Sending commands from rogue ground station due to no auth/encryption

CySat 2023

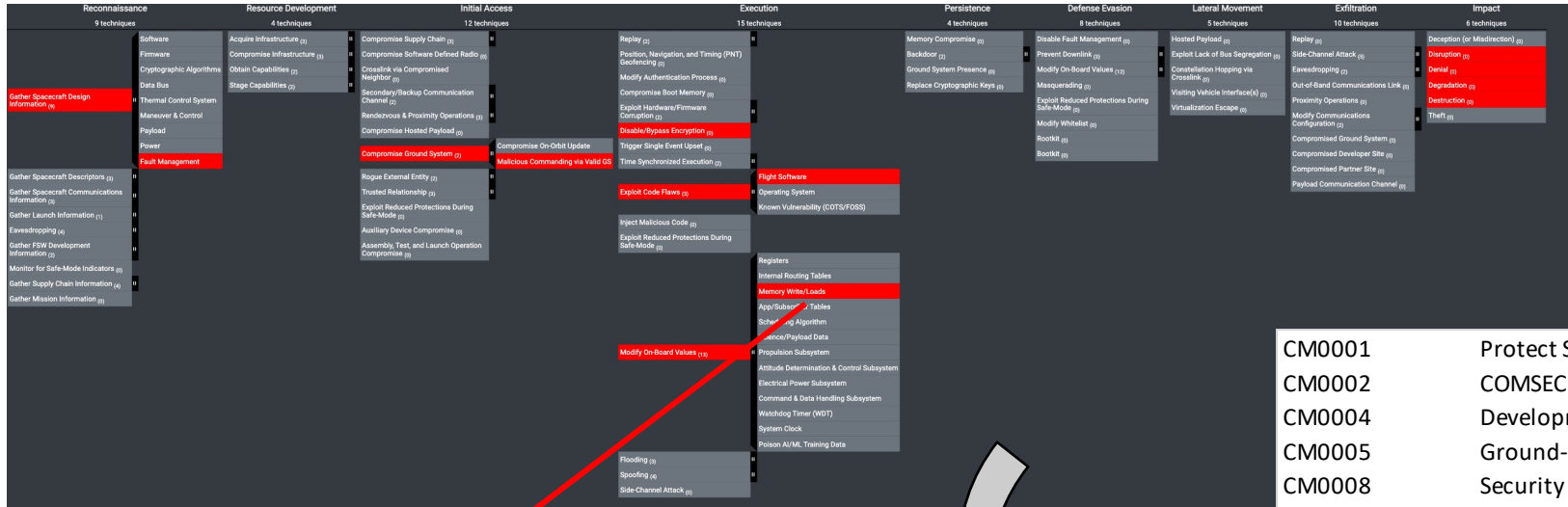
- ESA OPS-SAT Attack

Theoretical Attack Chain in Backup

- PCspooF

- [Hacking Spacecraft using Space Attack Research & Tactic Analysis | Video](#) (April 2023)
 - Updated version presented at [DEF CON 31](#)

Mapping Attack Chain to Countermeasures



Many of these countermeasures likely not feasible for mission that are already launched

Modify On-Board Values: 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. Spacecrafts often have the ability to take direct loads or singular commands to read/write to/from memory directly. Spacecrafts 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.

Other Subtechniques of Modify On-Board Values (13)

ID: EK-0012.03
Sub-technique of: EK-0012
Related Aerospace Threat IDs: SVY12, SVY15, SV-SP-9
Related MITRE ATTACK TTPs: No related MITRE ATTACK TTPs
Tactic: Execution
Created: 2022/10/19
Last Modified: 2022/12/08

Countermeasures

ID	Name	Description	NIST Revs
CM0009	Process White Listing	Simple process ID whitelisting on the firmware level could impede attackers from instigating unnecessary processes which could impact the spacecraft.	CM-11, CM-7(5), PL-8, PL-1(1), IS-10(5)
CM0032	On-board Intrusion Detection & Prevention	Utilize on-board intrusion detection/prevention system that monitors the mission critical components or systems and audit/logs actions. The IDS/IPS should have the capability to respond to threats (initial access, execution, persistence, evasion, exfiltration, etc.) and it should address signature-based attacks along with dynamic never-before seen attacks using machine learning/adaptive technologies. The IDS/IPS must integrate with traditional fault management to provide a holistic approach to faults on-board the spacecraft. Spacecraft should select and execute safe countermeasures against cyber-attacks. These countermeasures are a ready supply of options to triage against the specific types of attack and mission priorities. Minimally, the response should ensure vehicle safety and continued operations. Ideally, the goal is to trap the threat, convince the threat that it is successful, and trace and track the attacker - with or without ground support. This would support successful attribution and evolving countermeasures to mitigate the threat in the future. "Safe countermeasures" are those that are compatible with the system's fault management system to avoid unintended effects or fratricide on the system.	AU-14, AU-2, AU-3, AU-9(1), AU-4, AU-4(1), AU-5, AU-5(2), AU-5(3), AU-4(1), AU-4(6), AU-8, AU-9, AU-9(2), AU-9(3), CA-7(6), CM-11(2), CP-10, CP-10(4), IR-4, IR-4(1), IR-4(2), IR-4(14), IR-4(5), IR-8, IR-8(1), PL-8, PL-8(1), RA-10, RA-3(4), SA-8(21), SA-8(22), SA-8(23), SC-14(2), SC-32(1), SC-3, SC-5(3), SC-7(10), SC-7(9), SI-10(6), SI-16, SI-17, SI-8, SI-8(8), SI-4, SI-4(1), SI-4(10), SI-4(11), SI-4(13), SI-4(16), SI-4(17), SI-4(2), SI-4(23), SI-4(24), SI-4(25), SI-4(4), SI-4(5), SI-4, SI-7(17), SI-7(6)
CM0042	Robust Fault Management	Ensure fault management system cannot be used against the spacecraft. Examples include: safe mode with crypto bypass, orbit correction maneuvers, affecting integrity of telemetry to cause action from ground, or some sort of proximity operation to cause spacecraft to go into safe mode. Understanding the sailing procedures and ensuring they do not put the spacecraft in a more vulnerable state is key to building a resilient spacecraft.	CP-2, CP-4(5), PL-8, PL-8(1), SA-3, SA-4(8), SA-8, SA-8(13), SA-8(24), SA-8(3), SA-8(4), SC-16(2), SC-24, SC-5, SC-13, SI-17
CM0044	Cybersafe Mode	Provide the capability to enter the spacecraft into a configuration-controlled and integrity-protected state representing a known, operational cyber-safe state (e.g., cyber-safe mode). Spacecraft should enter a cyber-safe mode when conditions that threaten the platform are detected. Cyber-safe mode is an operating mode of a spacecraft during which all nonessential systems are shut down and the spacecraft is placed in a known good state using validated software and configuration settings. Within cyber-safe mode, authentication and encryption should still be enabled. The spacecraft should be capable of reconstructing firmware and software functions to pre-attack levels to allow for the recovery of functional capabilities. This can be performed by self-healing, or the healing can be aided from the ground. However, the spacecraft needs to have the capability to repair, based on equipment still available after a cyber-attack. The goal is for the spacecraft to resume full mission operations. If not possible, a reduced level of mission capability should be achieved. Cyber-safe mode software/configuration should be stored onboard the spacecraft in memory with hardware-based controls and should not be modifiable.	CP-10, CP-10(4), CP-12, CP-2, CP-2(5), IR-4, IR-4(12), IR-4(3), PL-8, PL-8(1), SA-3, SA-8, SA-8(10), SA-8(12), SA-8(13), SA-8(21), SA-8(23), SA-8(24), SA-8(3), SA-8(4), SC-16(2), SC-24, SC-5, SI-11, SI-17, SI-7(17)

SPARTA has direct mapping from TTP to Countermeasures

- CM0001 Protect Sensitive Information
- CM0002 COMSEC
- CM0004 Development Environment Security
- CM0005 Ground-based Countermeasures
- CM0008 Security Testing Results
- CM0010 Update Software
- CM0011 Vulnerability Scanning
- CM0012 Software Bill of Materials
- CM0013 Dependency Confusion
- CM0014 Secure boot
- CM0015 Software Source Control
- CM0016 CWE List
- CM0017 Coding Standard
- CM0018 Dynamic Analysis
- CM0019 Static Analysis
- CM0020 Threat modeling
- CM0021 Software Digital Signature
- CM0023 Configuration Management
- CM0025 Supplier Review
- CM0026 Original Component Manufacturer
- CM0029 TRANSEC
- CM0030 Crypto Key Management
- CM0031 Authentication
- CM0032 On-board Intrusion Detection & Prevention
- CM0033 Relay Protection
- CM0034 Monitor Critical Telemetry Points
- CM0035 Protect Authenticators
- CM0039 Least Privilege
- CM0040 Shared Resource Leakage
- CM0042 Robust Fault Management
- CM0043 Backdoor Commands
- CM0044 Cyber-safe Mode
- CM0047 Operating System Security
- CM0052 Insider Threat Protection
- CM0053 Physical Security Controls
- CM0054 Two-Person Rule
- CM0055 Secure Command Mode(s)
- CM0069 Process White Listing
- CM0070 Alternate Communications Paths



SPARTA Countermeasure Mapper / Defensive Gap Analyzer

<https://sparta.aerospace.org/countermeasures/mapper>

- Attack chains built in SPARTA's navigator can help identify countermeasures against the TTPs used in the attack
 - Many users do not know TTPs, they only know the countermeasures they have implemented (or plan to)...
- The SPARTA capability enables a graphical mechanism to select and deselect countermeasures from SPARTA's defense-in-depth view, as the starting point, to drive TTP mitigation & security planning
 - It can export the data into Excel which provides tabs for coverage and gaps from a TTP perspective, including NIST controls
- Below depicts the TTPs that have some mitigation when only applying COMSEC/TRANSEC/TEMPEST
 - **Green/Yellow/Orange** indicates some level of coverage where **Red** indicates no coverage of the TTP

Percent Coverage	ID	Name	Description	References	Aerospace	Related MI	Countermeasures	Additional	NIST Rev 5	C	Requirements
50.00%	REC-0003	Gather Spacecraft Communication	Threat actors may	https://cro	SV-CF-3	T1592, T15	CM0002, CI	CM0001, CI	AC-3(11), AI	The Program sh	
33.33%	REC-0003.01	Communications Equipment	Threat actors may	https://cro	SV-CF-3, SV	T1592, T15	CM0029	CM0001, CI	AC-3(11), AI	The Program sh	
33.33%	REC-0003.02	Commanding Details	Threat actors may	https://cro	SV-CF-3, SV	T1592, T15	CM0029	CM0001, CI	AC-3(11), AI	The Program sh	
33.33%	REC-0003.03	Mission-Specific Channel Scanning	Threat actors may	Derived fro	SV-CF-3, SV	T1592	CM0029	CM0001, CI	AC-3(11), AI	The Program sh	
50.00%	REC-0003.04	Valid Credentials	Threat actors may	https://att	SV-AC-3, SV	T1586, T15	CM0002, CI	CM0001, CI	AC-3(11), AI	The Program sh	
50.00%	REC-0005	Eavesdropping	Threat actors may	Sec and sch	SV-AC-7, SV	T1040, T08	CM0002, CI	CM0036, CI	AC-17, AC-1	The spacecraft s	
100.00%	REC-0005.01	Uplink Intercept	Threat actors may	capture the	SV-AC-7, SV	T1040, T08	CM0002, CI	CM0036, CI	AC-17, AC-1	The spacecraft s	
100.00%	REC-0005.02	Downlink Intercept	Threat actors may	Kaspersky's	SV-AC-7, SV	T1040, T08	CM0002, CI	CM0036, CI	AC-17, AC-1	The spacecraft s	
50.00%	REC-0005.03	Proximity Operations	Threat actors may	https://spa	SV-AC-5, SV	T1040, T08	CM0002, CI	CM0036, CI	AC-17, AC-1	The spacecraft s	
100.00%	REC-0005.04	Active Scanning (RF/Optical)	Threat actors may	Derived fro	SV-AC-7, SV	T1595	CM0002, CM0029		AC-17, AC-1	The spacecraft s	
54.55%	IA-0003	Crosslink via Compromised Neigh	Threat actors may	compromis	SV-AC-1, SV	AV-1, SV-IT	CM0002, CI	CM0032, CI	AC-17, AC-1	The spacecraft s	
9.09%	IA-0004	Secondary/Backup Communicatio	Threat actors may	compromis	SV-MA-7		CM0033	CM0005, CI	PM-16, PM	The Program sh	
25.00%	IA-0004.01	Ground Station	Threat actors may	Waller J. M	SV-MA-7		CM0033	CM0005, CI	CP-2, CP-2	(The Program sh	
12.50%	IA-0005	Rendezvous & Proximity Operatio	Threat actors may	https://spa	SV-AC-5		CM0002, CI	CM0037, CI	CP-13, CP-2	The spacecraft s	
66.67%	IA-0005.01	Compromise Emanations	Threat actors in close proxim	SV-AC-5, SV	CF-2		CM0002, CI	CM0085	CP-13, PE-1	See threat ID SV	
16.67%	IA-0005.02	Docked Vehicle / OSAM	Threat actors may	https://spa	SV-AC-5, SV	AC-6, SV-CF	CM0002, CI	CM0032, CI	CP-13, CP-2	The spacecraft s	
18.18%	IA-0005.03	Proximity Grappling	Threat actors may	https://spa	SV-AC-5, SV	CF-2	CM0002, CI	CM0037, CI	CP-13, CP-2	The spacecraft s	
4.35%	IA-0007	Compromise Ground System	Threat actors may	2011 Repo	SV-AC-1, SV	IT-5, SV-MA	CM0033	CM0001, CI	AC-3(11), AI	The Program sh	
4.55%	IA-0007.01	Compromise On-Orbit Update	Threat actors may	Ferrazzani,	SV-AC-1, SV	T1195, T11	CM0033	CM0001, CI	AC-3(11), AI	The Program sh	
10.00%	IA-0007.02	Malicious Commanding via Valid C	Threat actors may	2011 Repo	SV-AC-1, SV	T1078	CM0033	CM0005, CI	AC-14, AC-3	The spacecraft s	
57.14%	IA-0008	Rogue External Entity	Threat actors may	https://spa	SV-AC-1, SV	T1133	CM0002, CI	CM0032, CI	AC-17, AC-1	The spacecraft s	

Excel Output

Thorough TTP Coverage (Green) to No TTP Coverage (Red)

Reducing TTP Risk Each with Each Countermeasure



SPARTA Control Mapper

The SPARTA control mapper enables the user to select individual NIST controls and enhancements or ISO 27001 requirements/controls using graphical user interface. This feature is particularly useful when chaining together many controls to build a security architecture for the spacecraft. Before selecting any control, all the techniques/sub-techniques will appear in red but as the user selects control(s), the techniques/sub-techniques turn green indicating some level of coverage and risk reduction. It is important to understand that a single control has little impact on a TTP within SPARTA. Because these controls are more granular than SPARTA countermeasures in general, it will take a multitude of controls to fully mitigate a TTP. The functionality of the control mapper leverages the relationship between SPARTA countermeasures and controls that have been published under the countermeasure section of SPARTA. When done selecting the controls, the user can export the TTP graphic but more importantly the user can export the data to Excel. The Excel workbook will report the selected controls, the TTPs covered as well as the gaps in TTP coverage in respective tabs of the workbook. From a security engineering perspective, this will ensure system designers can better understand where their gaps and potential risk resides. In contrast to the SPARTA countermeasures, there are many more controls from a NIST or ISO perspective. Therefore, users can leverage the [JSON creator tool](#) to create their own custom overlays of controls vice manually selecting from the graphical interface.

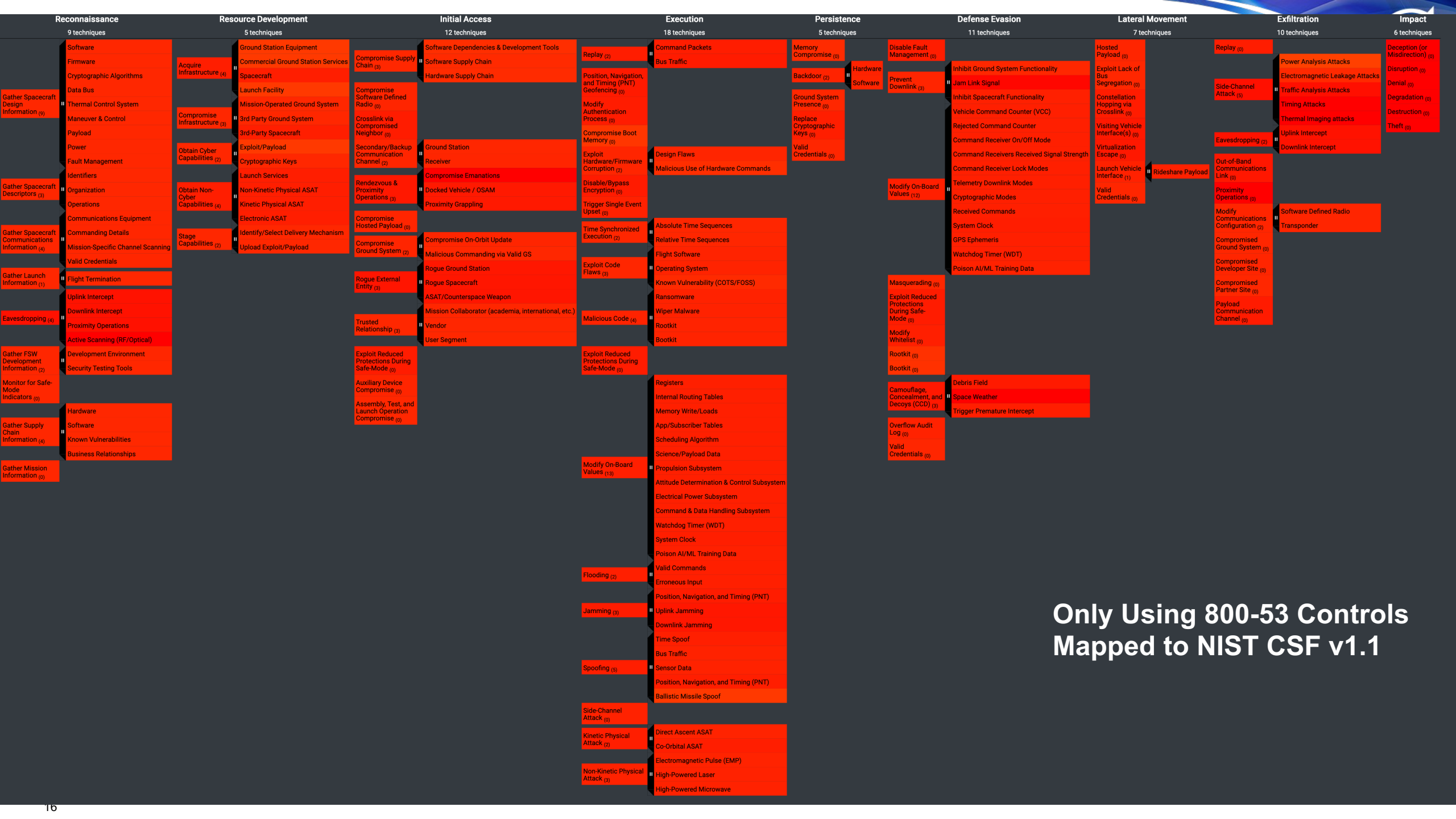
Create New Layer



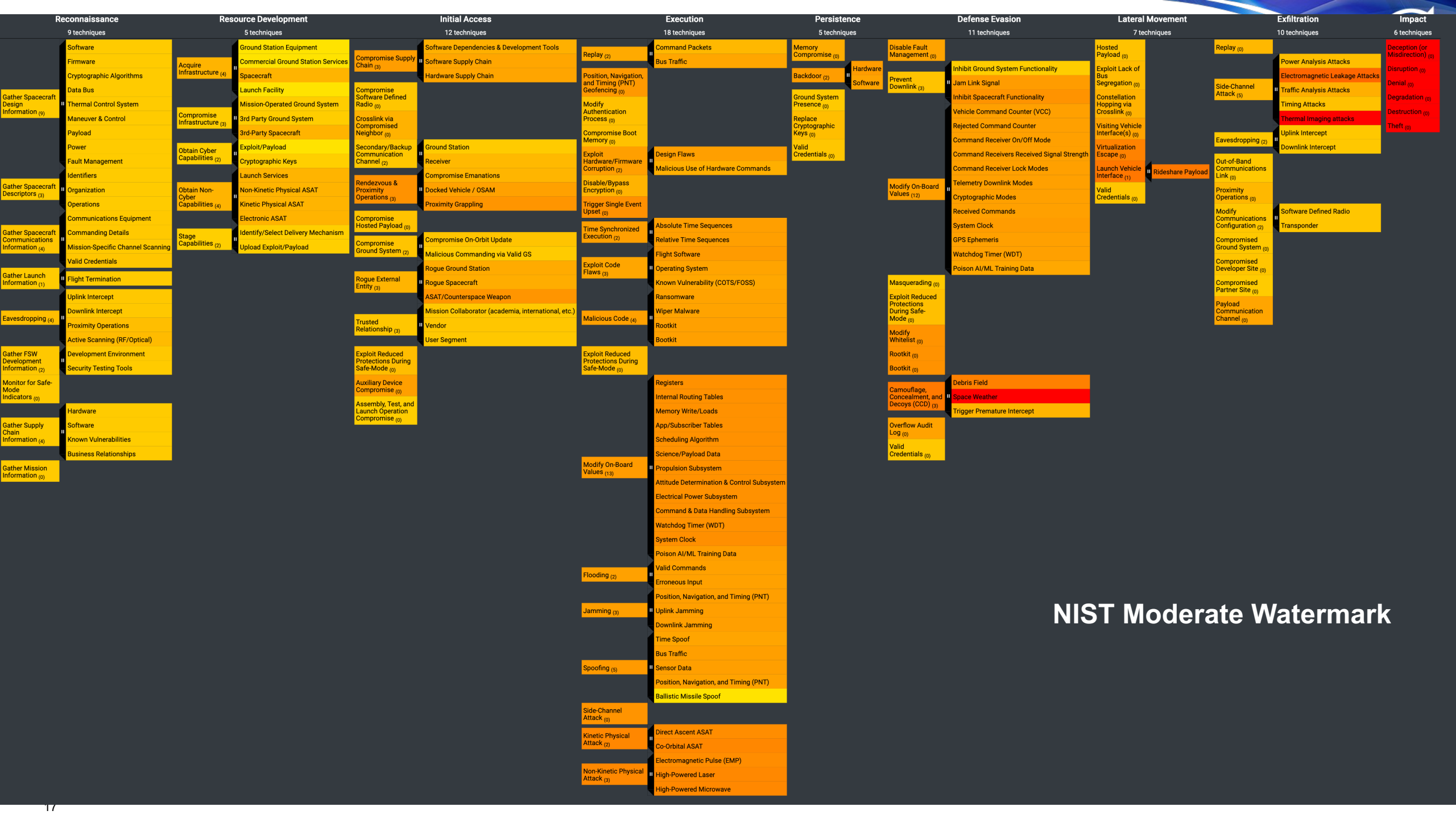
Open New Layer



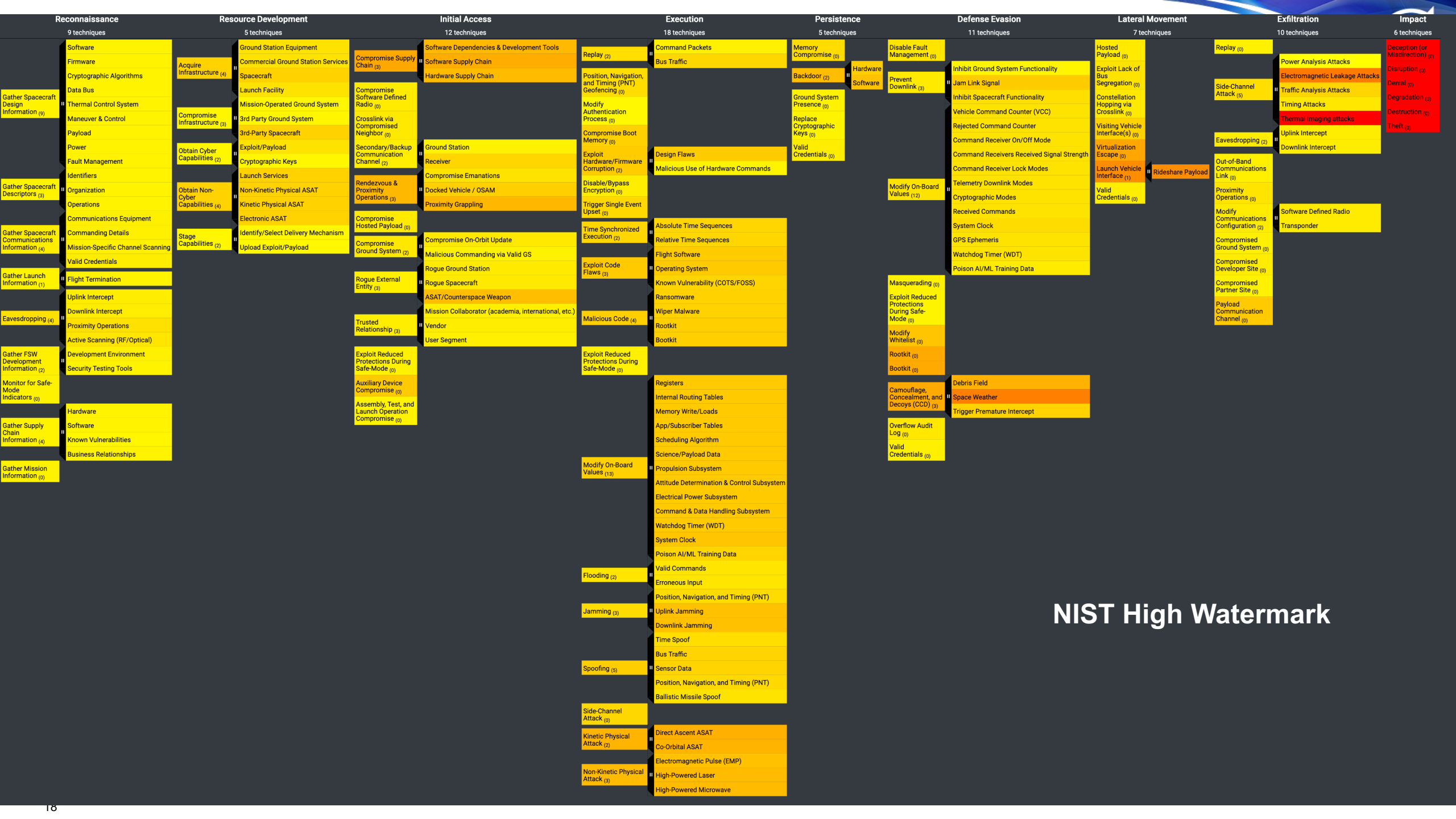
Control Mapper is Good for Comparing NIST 800-53 Control Baselines and their TTP Mitigation



Only Using 800-53 Controls Mapped to NIST CSF v1.1



NIST Moderate Watermark



NIST High Watermark

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 (9)	Software	Acquire Infrastructure (4)	Ground Station Equipment	Compromise Supply Chain (3)	Software Dependencies & Development Tools	Replay (2)	Command Packets	Memory Compromise (0)	Hardware	Disable Fault Management (0)	Inhibit Ground System Functionality	Hosted Payload (0)	Replay (0)	Power Analysis Attacks	Deception (or Misdirection) (0)		
	Firmware		Commercial Ground Station Services		Software Supply Chain	Bus Traffic	Backdoor (2)			Software						Prevent Downlink (3)	Exploit Lack of Bus Segregation (0)
	Cryptographic Algorithms		Spacecraft		Hardware Supply Chain	Position, Navigation, and Timing (PNT) Geofencing (0)	Ground System Presence (0)	Modify On-Board Values (12)	Jam Link Signal			Constellation Hopping via Crosslink (0)	Traffic Analysis Attacks				
	Data Bus		Launch Facility	Compromise Software Defined Radio (0)	Modify Authentication Process (0)	Replace Cryptographic Keys (0)	Valid Credentials (0)	Inhibit Spacecraft Functionality	Visiting Vehicle Interface(s) (0)	Timing Attacks							
	Thermal Control System		Mission-Operated Ground System	Crosslink via Compromised Neighbor (0)	Compromise Boot Memory (0)	Design Flaws		Masquerading (0)	Vehicle Command Counter (VCC)			Virtualization Escape (0)	Thermal Imaging attacks				
	Maneuver & Control	3rd Party Ground System	Secondary/Backup Communication Channel (2)	Exploit Hardware/Firmware Corruption (2)	Malicious Use of Hardware Commands	Exploit Reduced Protections During Safe-Mode (0)	Rejected Command Counter		Launch Vehicle Interface (1)	Uplink Intercept							
	Payload	3rd-Party Spacecraft	Rendezvous & Proximity Operations (3)	Disable/Bypass Encryption (0)	Time Synchronized Execution (2)		Exploit Reduced Protections During Safe-Mode (0)	Command Receiver On/Off Mode	Valid Credentials (0)			Downlink Intercept					
	Power	Obtain Cyber Capabilities (2)	Launch Services	Trigger Single Event Upset (0)	Absolute Time Sequences	Masquerading (0)		Command Receivers Received Signal Strength	Rideshare Payload	Out-of-Band Communications Link (0)							
	Fault Management	Exploit/Payload	Non-Kinetic Physical ASAT	Time Synchronized Execution (2)	Relative Time Sequences		Exploit Reduced Protections During Safe-Mode (0)	Command Receiver Lock Modes	Modify On-Board Values (12)			Proximity Operations (0)					
	Identifiers	Cryptographic Keys	Kinetic Physical ASAT	Exploit Code Flaws (3)	Flight Software	Exploit Reduced Protections During Safe-Mode (0)		Telemetry Downlink Modes	Valid Credentials (0)	Software Defined Radio							
Gather Spacecraft Descriptors (3)	Organization	Obtain Non-Cyber Capabilities (4)	Electronic ASAT	Operating System	Exploit Reduced Protections During Safe-Mode (0)		Cryptographic Modes	Valid Credentials (0)	Software Defined Radio								
	Operations	Stage Capabilities (2)	Identify/Select Delivery Mechanism	Known Vulnerability (COTS/FOSS)		Exploit Reduced Protections During Safe-Mode (0)	Received Commands			Valid Credentials (0)	Transponder						
	Communications Equipment	Valid Credentials	Upload Exploit/Payload	Malicious Commanding via Valid GS	Ransomware		Exploit Reduced Protections During Safe-Mode (0)	System Clock	Valid Credentials (0)			Compromised Ground System (0)					
Gather Spacecraft Communications Information (4)	Commanding Details	Rogue External Entity (3)	Rogue Ground Station	Exploit Code Flaws (3)	Wiper Malware	GPS Ephemeris		Valid Credentials (0)		Compromised Developer Site (0)							
	Mission-Specific Channel Scanning		Malicious Commanding via Valid GS	Rogue Spacecraft	Malicious Code (4)	Rootkit	Watchdog Timer (WDT)		Valid Credentials (0)		Compromised Partner Site (0)						
Gather Launch Information (1)	Flight Termination	Trusted Relationship (3)	ASAT/Counterspace Weapon	Exploit Reduced Protections During Safe-Mode (0)	Rootkit	Poison AI/ML Training Data	Valid Credentials (0)	Payload Communication Channel (0)									
	Uplink Intercept	Vendor	Mission Collaborator (academia, international, etc.)	Registers	Exploit Reduced Protections During Safe-Mode (0)	Poison AI/ML Training Data			Valid Credentials (0)	Payload Communication Channel (0)							
Eavesdropping (4)	Downlink Intercept	Assembly, Test, and Launch Operation Compromise (0)	Mission Collaborator (academia, international, etc.)	Internal Routing Tables		Exploit Reduced Protections During Safe-Mode (0)	Debris Field	Valid Credentials (0)			Payload Communication Channel (0)						
	Proximity Operations	User Segment	Mission Collaborator (academia, international, etc.)	Memory Write/Loads	Exploit Reduced Protections During Safe-Mode (0)		Space Weather		Valid Credentials (0)	Payload Communication Channel (0)							
Gather FSW Development Information (2)	Active Scanning (RF/Optical)	Auxiliary Device Compromise (0)	Mission Collaborator (academia, international, etc.)	App/Subscriber Tables		Exploit Reduced Protections During Safe-Mode (0)	Trigger Premature Intercept	Valid Credentials (0)			Payload Communication Channel (0)						
	Development Environment	Assembly, Test, and Launch Operation Compromise (0)	Mission Collaborator (academia, international, etc.)	Scheduling Algorithm	Exploit Reduced Protections During Safe-Mode (0)		Trigger Premature Intercept		Valid Credentials (0)	Payload Communication Channel (0)							
Monitor for Safe-Mode Indicators (0)	Security Testing Tools	Assembly, Test, and Launch Operation Compromise (0)	Mission Collaborator (academia, international, etc.)	Science/Payload Data		Exploit Reduced Protections During Safe-Mode (0)	Trigger Premature Intercept	Valid Credentials (0)			Payload Communication Channel (0)						
	Hardware	Assembly, Test, and Launch Operation Compromise (0)	Mission Collaborator (academia, international, etc.)	Propulsion Subsystem	Exploit Reduced Protections During Safe-Mode (0)		Trigger Premature Intercept		Valid Credentials (0)	Payload Communication Channel (0)							
Gather Supply Chain Information (4)	Software	Assembly, Test, and Launch Operation Compromise (0)	Mission Collaborator (academia, international, etc.)	Attitude Determination & Control Subsystem		Exploit Reduced Protections During Safe-Mode (0)	Trigger Premature Intercept	Valid Credentials (0)			Payload Communication Channel (0)						
	Known Vulnerabilities	Assembly, Test, and Launch Operation Compromise (0)	Mission Collaborator (academia, international, etc.)	Electrical Power Subsystem	Exploit Reduced Protections During Safe-Mode (0)		Trigger Premature Intercept		Valid Credentials (0)	Payload Communication Channel (0)							
Gather Mission Information (0)	Business Relationships	Assembly, Test, and Launch Operation Compromise (0)	Mission Collaborator (academia, international, etc.)	Command & Data Handling Subsystem		Exploit Reduced Protections During Safe-Mode (0)	Trigger Premature Intercept	Valid Credentials (0)			Payload Communication Channel (0)						
		Business Relationships	Assembly, Test, and Launch Operation Compromise (0)	Mission Collaborator (academia, international, etc.)	Watchdog Timer (WDT)		Exploit Reduced Protections During Safe-Mode (0)		Trigger Premature Intercept	Valid Credentials (0)		Payload Communication Channel (0)					
	Business Relationships	Assembly, Test, and Launch Operation Compromise (0)	Mission Collaborator (academia, international, etc.)	System Clock	Exploit Reduced Protections During Safe-Mode (0)	Trigger Premature Intercept		Valid Credentials (0)	Payload Communication Channel (0)								
	Business Relationships	Assembly, Test, and Launch Operation Compromise (0)	Mission Collaborator (academia, international, etc.)	Poison AI/ML Training Data		Exploit Reduced Protections During Safe-Mode (0)	Trigger Premature Intercept			Valid Credentials (0)	Payload Communication Channel (0)						
	Business Relationships	Assembly, Test, and Launch Operation Compromise (0)	Mission Collaborator (academia, international, etc.)	Valid Commands	Exploit Reduced Protections During Safe-Mode (0)		Trigger Premature Intercept	Valid Credentials (0)	Payload Communication Channel (0)								
	Business Relationships	Assembly, Test, and Launch Operation Compromise (0)	Mission Collaborator (academia, international, etc.)	Erroneous Input		Exploit Reduced Protections During Safe-Mode (0)	Trigger Premature Intercept			Valid Credentials (0)	Payload Communication Channel (0)						
	Business Relationships	Assembly, Test, and Launch Operation Compromise (0)	Mission Collaborator (academia, international, etc.)	Position, Navigation, and Timing (PNT)	Exploit Reduced Protections During Safe-Mode (0)		Trigger Premature Intercept	Valid Credentials (0)	Payload Communication Channel (0)								
	Business Relationships	Assembly, Test, and Launch Operation Compromise (0)	Mission Collaborator (academia, international, etc.)	Uplink Jamming		Exploit Reduced Protections During Safe-Mode (0)	Trigger Premature Intercept			Valid Credentials (0)	Payload Communication Channel (0)						
	Business Relationships	Assembly, Test, and Launch Operation Compromise (0)	Mission Collaborator (academia, international, etc.)	Downlink Jamming	Exploit Reduced Protections During Safe-Mode (0)		Trigger Premature Intercept	Valid Credentials (0)	Payload Communication Channel (0)								
	Business Relationships	Assembly, Test, and Launch Operation Compromise (0)	Mission Collaborator (academia, international, etc.)	Time Spoof		Exploit Reduced Protections During Safe-Mode (0)	Trigger Premature Intercept			Valid Credentials (0)	Payload Communication Channel (0)						
	Business Relationships	Assembly, Test, and Launch Operation Compromise (0)	Mission Collaborator (academia, international, etc.)	Bus Traffic	Exploit Reduced Protections During Safe-Mode (0)		Trigger Premature Intercept	Valid Credentials (0)	Payload Communication Channel (0)								
	Business Relationships	Assembly, Test, and Launch Operation Compromise (0)	Mission Collaborator (academia, international, etc.)	Sensor Data		Exploit Reduced Protections During Safe-Mode (0)	Trigger Premature Intercept			Valid Credentials (0)	Payload Communication Channel (0)						
	Business Relationships	Assembly, Test, and Launch Operation Compromise (0)	Mission Collaborator (academia, international, etc.)	Position, Navigation, and Timing (PNT)	Exploit Reduced Protections During Safe-Mode (0)		Trigger Premature Intercept	Valid Credentials (0)	Payload Communication Channel (0)								
	Business Relationships	Assembly, Test, and Launch Operation Compromise (0)	Mission Collaborator (academia, international, etc.)	Ballistic Missile Spoof		Exploit Reduced Protections During Safe-Mode (0)	Trigger Premature Intercept			Valid Credentials (0)	Payload Communication Channel (0)						
	Business Relationships	Assembly, Test, and Launch Operation Compromise (0)	Mission Collaborator (academia, international, etc.)	Side-Channel Attack (0)	Exploit Reduced Protections During Safe-Mode (0)		Trigger Premature Intercept	Valid Credentials (0)	Payload Communication Channel (0)								
	Business Relationships	Assembly, Test, and Launch Operation Compromise (0)	Mission Collaborator (academia, international, etc.)	Kinetic Physical Attack (2)		Exploit Reduced Protections During Safe-Mode (0)	Trigger Premature Intercept			Valid Credentials (0)	Payload Communication Channel (0)						
	Business Relationships	Assembly, Test, and Launch Operation Compromise (0)	Mission Collaborator (academia, international, etc.)	Non-Kinetic Physical Attack (1)	Exploit Reduced Protections During Safe-Mode (0)		Trigger Premature Intercept	Valid Credentials (0)	Payload Communication Channel (0)								
	Business Relationships	Assembly, Test, and Launch Operation Compromise (0)	Mission Collaborator (academia, international, etc.)	High-Powered Laser		Exploit Reduced Protections During Safe-Mode (0)	Trigger Premature Intercept			Valid Credentials (0)	Payload Communication Channel (0)						
	Business Relationships	Assembly, Test, and Launch Operation Compromise (0)	Mission Collaborator (academia, international, etc.)	High-Powered Microwave	Exploit Reduced Protections During Safe-Mode (0)		Trigger Premature Intercept	Valid Credentials (0)	Payload Communication Channel (0)								

Aerospace Recommend NIST Profile

Note: TOR in Development to drive CNSS Space Overlay Update



Notional Risk Scores

- Builds on previous work published in Aerospace Report [TOR-2021-01333-REV A](#) which details a generic threat model and risk assessment approach that considers a high-level view of adversary capabilities and ranks them into tiers.
- TTPs potential impact, resulting in a [NOTIONAL risk determination](#) which can be represented in a standard [5x5 risk matrix](#).
- Three notional risk values are now provided for TTPs, sorted by system/mission criticality as follows:
 - *HIGH Criticality System (critical infrastructure, military, intelligence, or similar)*
 - *MEDIUM Criticality System (civil, science/weather, commercial, or similar)*
 - *LOW Criticality System (academic, research, or similar)*
- Ranging from 1-25, each of these three distinct values can be placed on the [risk matrix 5x5](#), and will be presented on TTP pages
 - *Notional Risk (H | M | L): HighRisk# | MediumRisk# | LowRisk#*

Show 100 entries Search: 25

SPARTA TTP	Notional Risk (HIGH Criticality Systems)	Notional Risk (MEDIUM Criticality Systems)	Notional Risk (LOW Criticality Systems)
DE-0002.02 - Jam Link Signal	25	24	21
EX-0001 - Replay	25	24	21
EX-0001.01 - Command Packets	25	24	21
EX-0005 - Exploit Hardware/Firmware Corruption	25	24	21
EX-0005.02 - Malicious Use of Hardware Commands	25	24	21
EX-0009.01 - Flight Software	25	24	21
EX-0009.03 - Known Vulnerability (COTS/FOSS)	25	24	21
EX-0013 - Flooding	25	24	21
EX-0013.01 - Valid Commands	25	24	21
EX-0013.02 - Erroneous Input	25	24	21
EX-0014 - Spoofing	25	24	21
EX-0014.01 - Time Spoof	25	24	21
EX-0014.02 - Bus Traffic	25	24	21
EX-0014.04 - Position, Navigation, and Timing (PNT)	25	24	21

Home > Techniques > Prevent Downlink > Jam Link Signal

Prevent Downlink: Jam Link Signal

Threat actors may overwhelm/jam the downlink signal to prevent transmitted telemetry signals from reaching their destination without severe modification/interference, effectively leaving ground controllers unaware of vehicle activity during this time. Telemetry is the only method in which ground controllers can monitor the health and stability of the spacecraft while in orbit. By disabling this downlink, threat actors may be able to stop mitigations from taking place.

Other Subtechniques of Prevent Downlink (3)

ID: DE-0002.02
 Sub-technique of: DE-0002
Notional Risk (H | M | L): 25 | 24 | 21
 Related Aerospace Threat IDs: SVXV-1
 Related MITRE ATT&CK TTPs: T1464
 Related ESA SPACE-SHIELD TTPs: T2052 | T2052.001 | T2049
 Tactic: Defense Evasion
 Created: 2022/10/19
 Last Modified: 2023/04/22

Countermeasures

ID	Name	Description	NIST Rev5	D3FEND	ISO 27001
CM0074	Distributed Constellations	A distributed system uses a number of nodes, working together, to perform the same mission or functions as a single node. In a distributed constellation, the end user is not dependent on any single satellite but rather uses multiple satellites to derive a capability. A distributed constellation can complicate an adversary's counterspace planning by presenting a larger number of targets that must be successfully attacked to achieve the same effects as targeting just one or two satellites in a less-distributed architecture. GPS is an example of a distributed constellation because the functioning of the system is not dependent on any single satellite or ground station; a user can use any four satellites within view to get a time and position fix.* *https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210225_Harrison_Defense_Space.pdf?N2KWelzCz3hE3AaUUpSGMprDtBIBSQG	CP-10(6) CP-11 CP-13 CP-2 CP-2(2) CP-2(3) CP-2(4) CP-2(5) CP-2(6) PE-21	D3-AI D3-NNI D3-SYSTEM D3-DEM D3-SVCDM D3-SYSVA	7.5.1 7.5.2 7.5.3 A.5.2 A.5.29 A.8.1 A.8.6 A.5.29 A.5.29



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 (2)	Replay (2)	Memory Compromise (2)	Disable Fault Management (1)	Hosted Payload (2)	Replay (1)	Deception (or Misdirection) (2)
Gather Spacecraft Descriptors (1)	Compromise Infrastructure (1)	Compromise Software Defined Radio (1)	Position, Navigation, and Timing (PNT) Geofencing (2)	Backdoor (2)	Prevent Downlink (1)	Exploit Lack of Bus Segregation (2)	Side-Channel Attack (2)	Disruption (2)
Gather Spacecraft Communications Information (4)	Obtain Cyber Capabilities (2)	Crosslink via Compromised Neighbor (1)	Modify Authentication Process (1)	Ground System Presence (2)	Modify On-Board Values (12)	Constellation Hopping via Crosslink (2)	Eavesdropping (2)	Denial (2)
Gather Launch Information (1)	Obtain Non-Cyber Capabilities (4)	Secondary/Backup Communication Channel (2)	Compromise Boot Memory (1)	Replace Cryptographic Keys (2)	Masking (2)	Visiting Vehicle Interface(s) (1)	Out-of-Band Communications Link (2)	Degradation (2)
Eavesdropping (2)	Stage Capabilities (2)	Rendezvous & Proximity Operations (2)	Exploit Hardware/Firmware Corruption (2)	Valid Credentials (2)	Exploit Reduced Protections During Safe-Mode (2)	Virtualization Escape (2)	Proximity Operations (2)	Destruction (2)
Gather FSW Development Information (2)		Compromise Hosted Payload (1)	Disable/Bypass Encryption (2)		Modify Whitelist (2)	Launch Vehicle Interface (1)	Modify Communications Configuration (2)	Theft (2)
Monitor for Safe-Mode Indicators (2)		Compromise Ground System (2)	Trigger Single Event Upset (2)		Rootkit (2)	Valid Credentials (2)	Compromised Ground System (2)	
Gather Supply Chain Information (4)		Rogue External Entity (2)	Time Synchronized Execution (2)		Rootkit (2)		Compromised Developer Site (2)	
Gather Mission Information (2)		Trusted Relationship (2)	Exploit Code Flaws (2)		Camouflage, Concealment, and Deceits (CCD) (2)		Compromised Partner Site (2)	
		Exploit Reduced Protections During Safe-Mode (2)	Malicious Code (2)		Overflow Audit Log (2)		Payload Communication Channel (2)	
		Auxiliary Device Compromise (2)	Exploit Reduced Protections During Safe-Mode (2)		Valid Credentials (2)			
		Assembly, Test, and Launch Operation Compromise (2)	Modify On-Board Values (12)					
			Flooding (2)					
			Jamming (2)					
			Spoofing (2)					
			Side-Channel Attack (1)					
			Kinetic Physical Attack (2)					
			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:

- [Hacking Spacecraft using Space Attack Research & Tactic Analysis \(April 2023\)](#)
- [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>
- 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

- Indiana University Space Cybersecurity Digital Badge - <https://kelley.iu.edu/programs/executive-education/programs-for-individuals/digital-badges/cybersecurity-foundations.html>
- DefCON 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](#)
- 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](#)
 - 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>