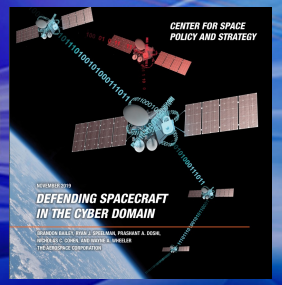
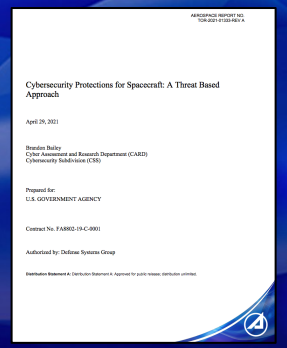
Value of Space Summit 2023
SPARTA 1 Year Update

Brandon Bailey, Brad Roeher, Randi Tinney
Cybersecurity and Advanced Platforms Subdivision (CAPS)
Cyber Assessment & Research Dept (CARD)
The Aerospace Corporation




Cybersecurity Protections for Spacecraft: A Threat Based Approach

April 29, 2021

Brandon Bailey
Cyber Assessment and Research Department (CARD)
Cybersecurity Subdivision (CSS)

Prepared for:
U.S. GOVERNMENT AGENCY

Contract No. FA8802-19-C-0001

Authorized by: Defense Systems Group

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)

Aerospace TechBlog | DIGITAL ENGINEERING | RESEARCH | SPACE CYBER | SPACE DEBRIS | TECH & POLICY | AEROSPACE.ORG

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

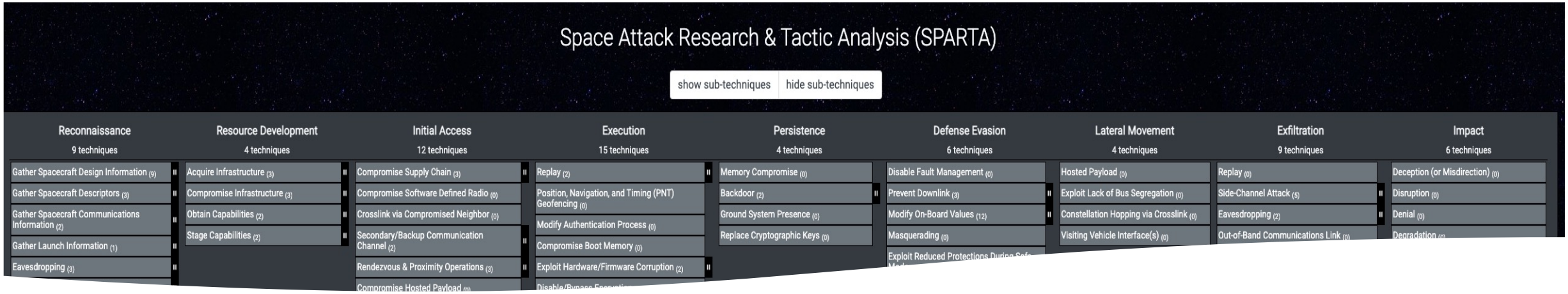
SPACE ATTACK RESEARCH & TACTIC ANALYSIS
https://sparta.aerospace.org/resources/

Approved for public release. OTR 2022-01250 & OTR-2023-00989

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**



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

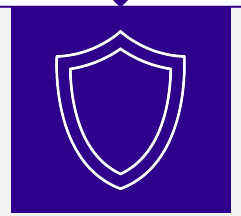
Example: SPD-5 and SPARTA Relationship

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

SPARTA
SPACE ATTACK RESEARCH & TACTIC ANALYSIS

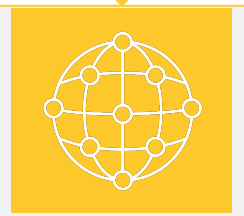


PHYSICAL SECURITY OF TT&C ENVIRONMENT

{Addressed by SPARTA countermeasure CM0053}

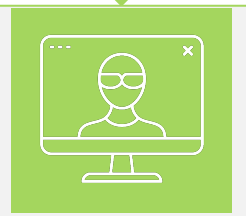
JAMMING AND SPOOFING PROTECTIONS

{Many countermeasures exist to address both TTPs EX-0016, EX-0014}



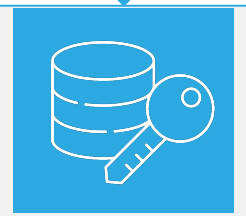
SUPPLY CHAIN RISK MANAGEMENT

{Many countermeasures exist to address TTP IA-0001}



INSIDER THREAT

{Addressed by SPARTA countermeasure CM0052}



TT&C PROTECTION USING ENCRYPTION OR AUTHENTICATION

{Addressed by SPARTA countermeasures CM0002,CM0031}

EXTRACTED SPD-5 PRINCIPLES (SECT 4b)

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

ID	Name	Description	NIST Rev5 Controls
CM0000	Countermeasure Not Identified	This technique is a result of utilizing TTPs to create an impact and the applicable countermeasures are associated with the TTPs leveraged to achieve the impact	None
CM0001	Protect Sensitive Information	Organizations should look to identify and properly classify mission sensitive design/operations information (e.g., fault management approach) and apply access control accordingly. Any location (ground system, contractor networks, etc.) storing design information needs to ensure design info is protected from exposure, exfiltration, etc. Space system sensitive information may be classified as Controlled	AC-3(11) | A 4(23) | AC-4 AC-4(6) | CA CM-12 | CM | PL-8 | PL-8 PM-11 | PM

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.

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 relevent NIST controls, these are the ones our subject matter experts found most relevent.

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	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 |

International Collaboration

CyberInflight

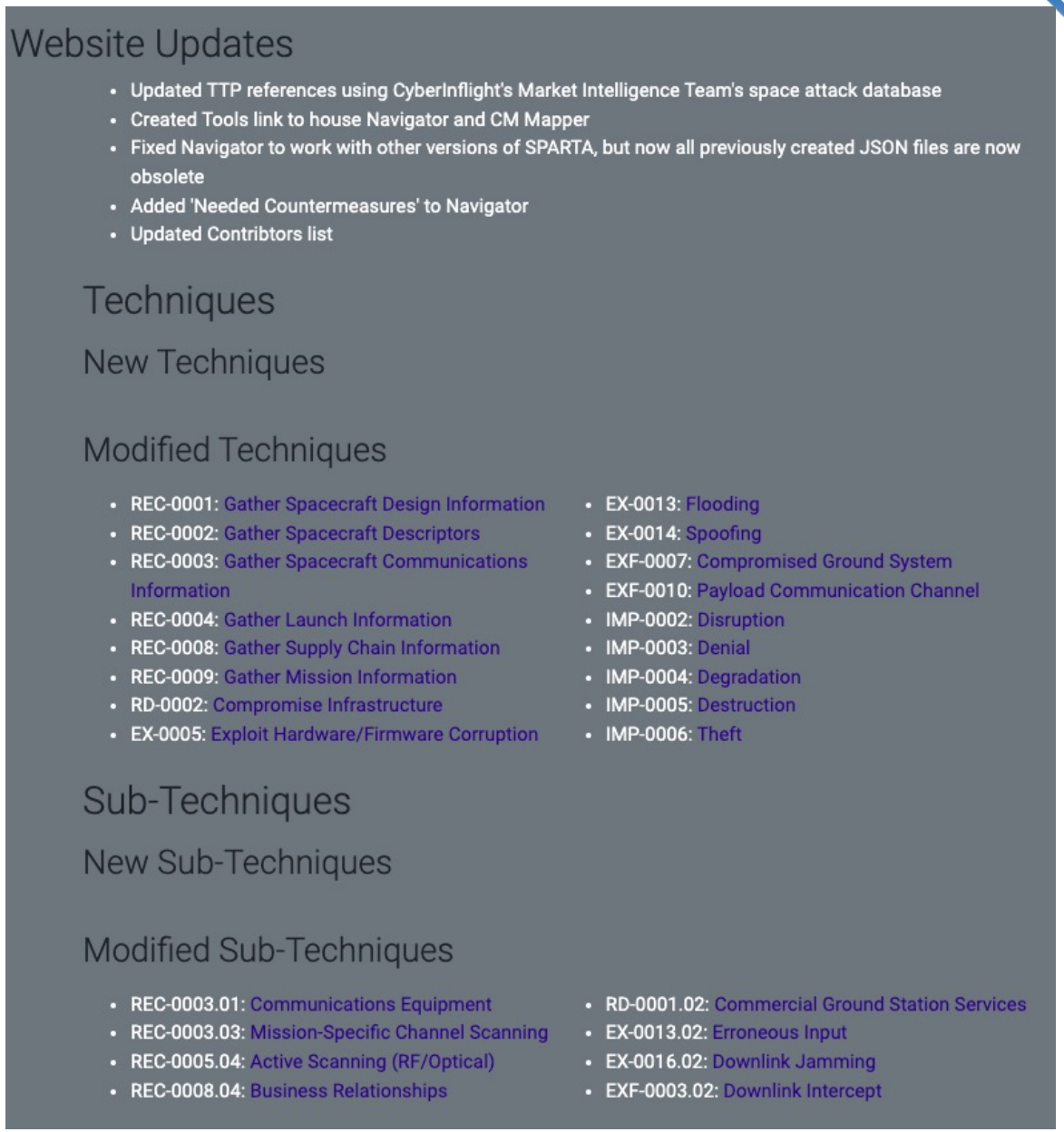
- Expanding the reference section with CyberInflight's space security attacks database
  - *Working with them to map TTPs to increase the real-world examples of the TTPs in use by threat actors*
- Inclusion of their database deployed in July 2023 – v1.3.2
  - https://sparta.aerospace.org/resources/updates/v1.3.2
- 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 Atlasis
- 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
- Héloise 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 Contribtors 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

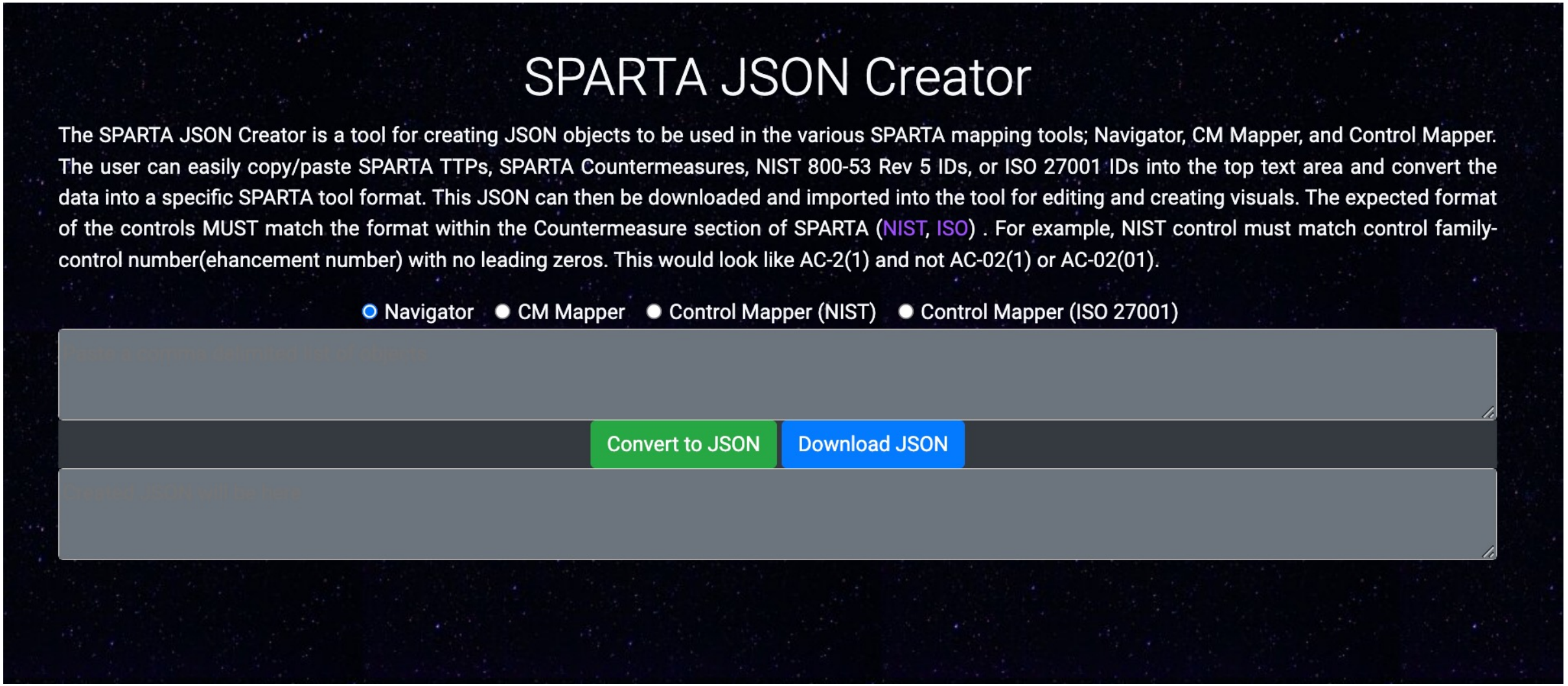
Sub-Techniques

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

JSON Creator



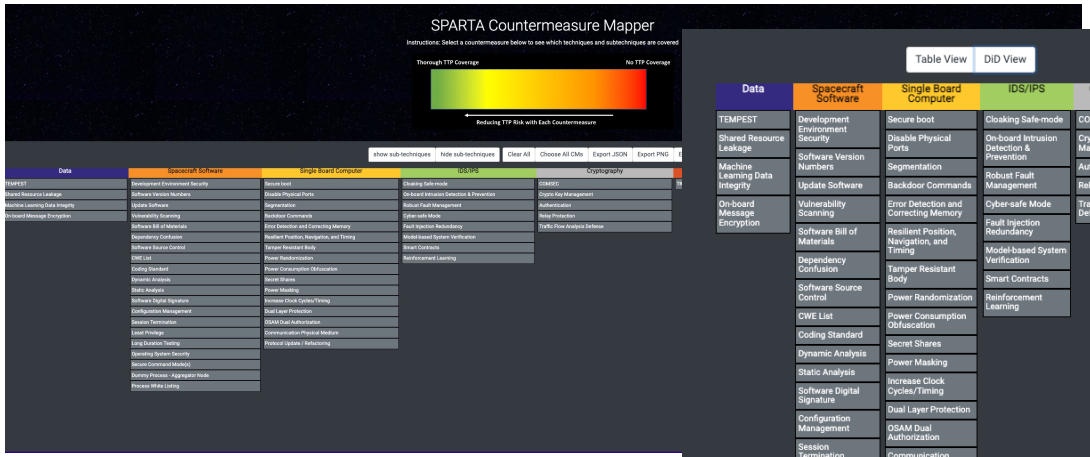
Building Spacecraft Attack Chains using

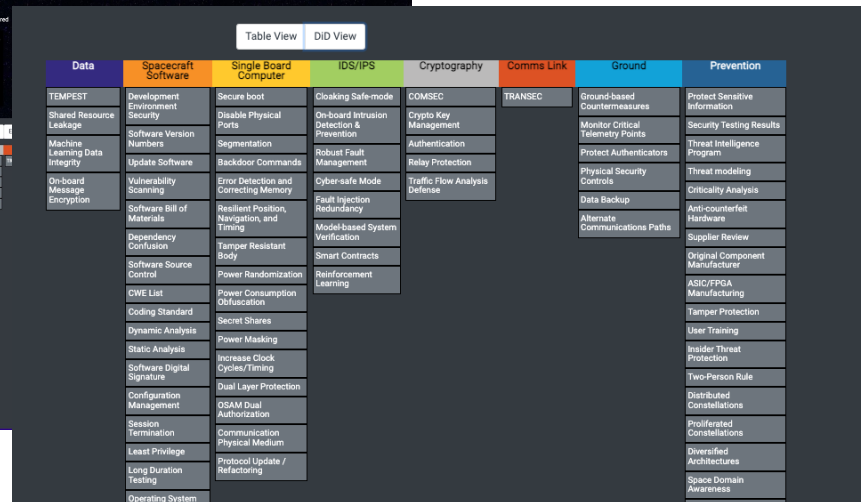
Attack Chains / Attack Flow != Cyber Kill Chain

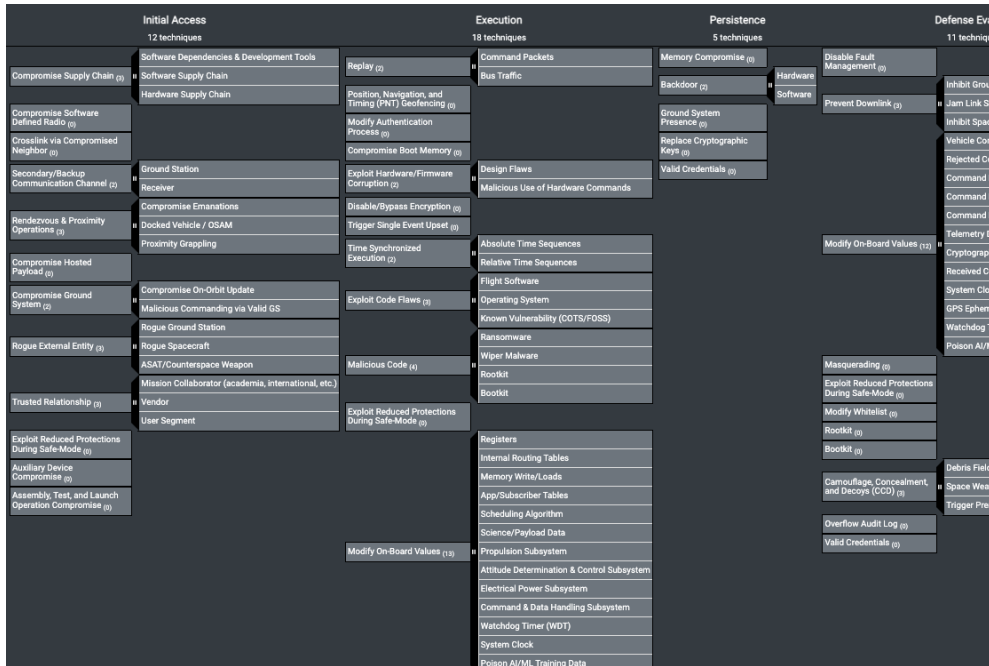
SPARTA
SPACE ATTACK RESEARCH & TACTIC ANALYSIS

- 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







Building Spacecraft Attack Chains

SPACE ATTACK RESEARCH & TACTIC ANALYSIS

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

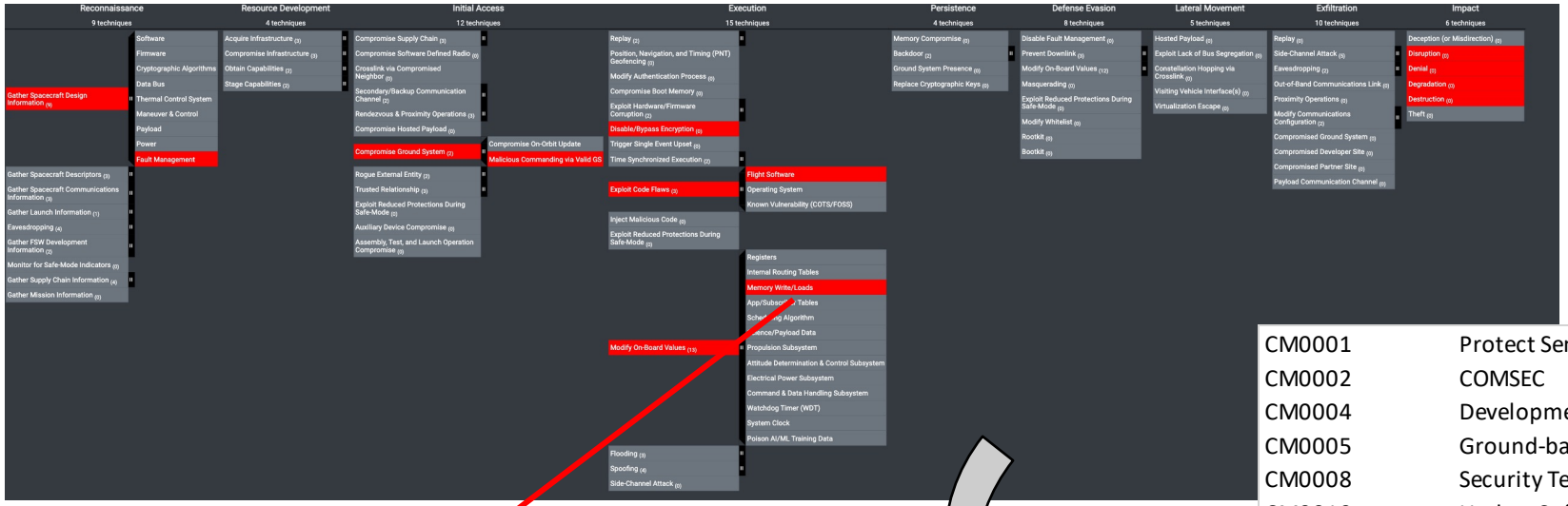
Blast from the Past
- Replay Attack from DefCon 2020
- Memory Injection Attack DefCon 2022

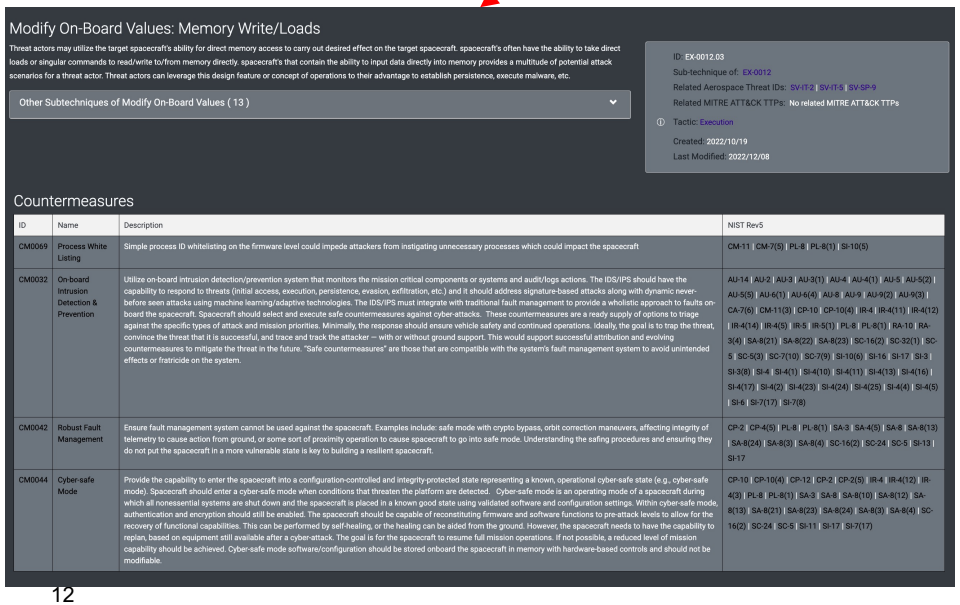
New Attacks
- Supply Chain Attack – Time bomb that executes command sequence 30 secs after boot
- Reaction Wheel Attack – Sending commands from rogue ground station due to no auth/encryption

CySat 2023
- ESA OPS-SAT Attack

Theoretical Attack Chain in Backup
- PCspooF

Mapping Attack Chain to Countermeasures





SPARTA has direct mapping from TTP to Countermeasures

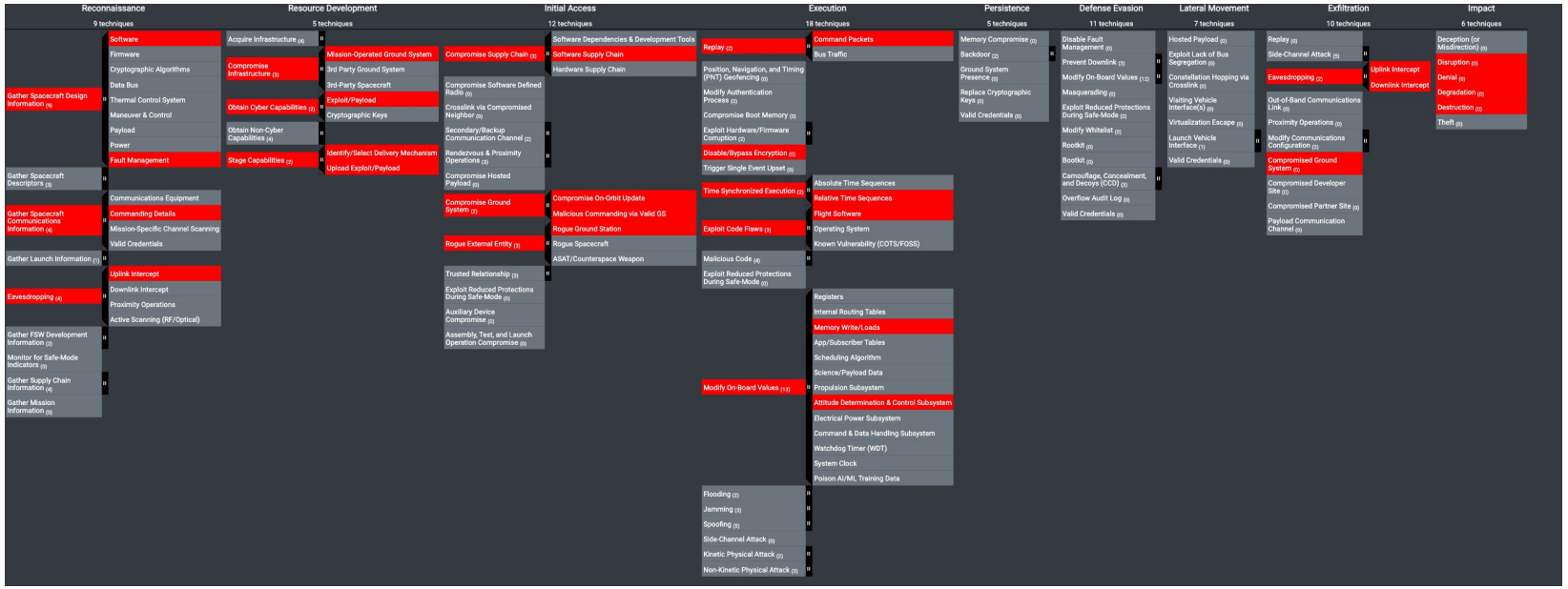
Many of these countermeasures likely not feasible for mission that are already launched

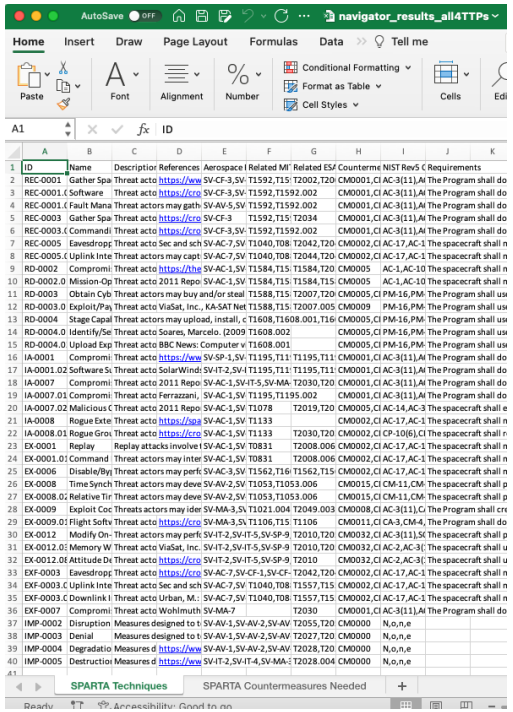
CM0001	Protect Sensitive Information	CM0029	TRANSEC
CM0002	COMSEC	CM0030	Crypto Key Management
CM0004	Development Environment Security	CM0031	Authentication
CM0005	Ground-based Countermeasures	CM0032	On-board Intrusion Detection & Prevention
CM0008	Security Testing Results	CM0033	Relay Protection
CM0010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

Combining the 4 Attack Chains

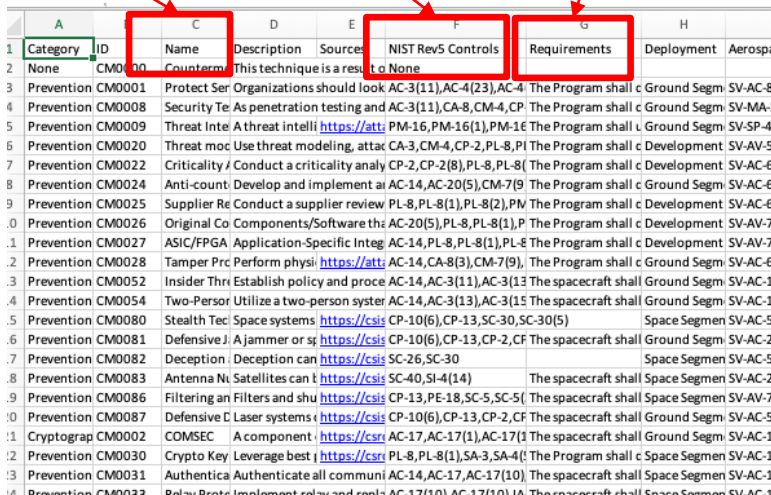
SPARTA Navigator – Extracting Countermeasures / NIST Controls

https://sparta.aerospace.org/navigator





Countermeasure **NIST 800-53** **Sample "Shalls"**

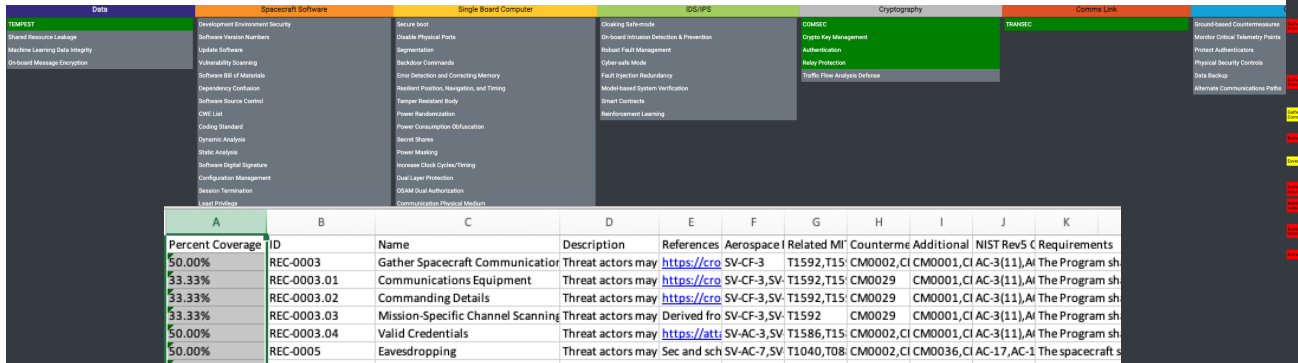


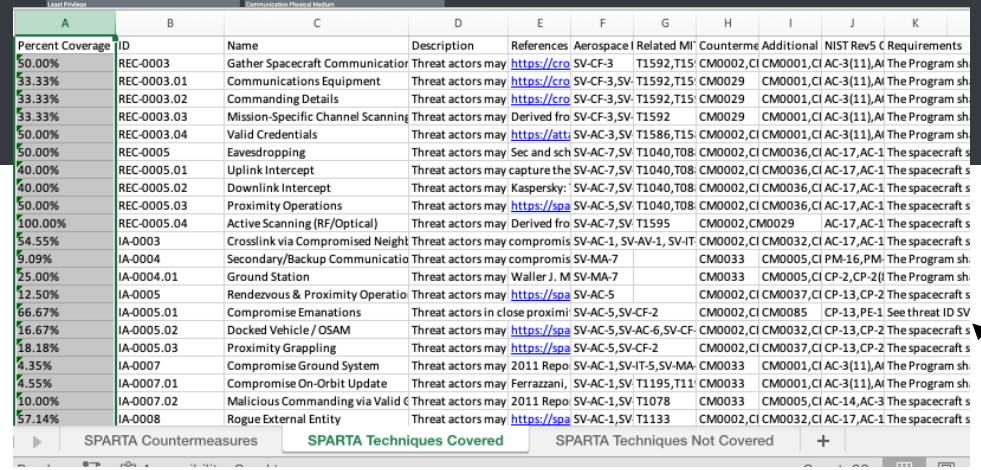
	A	B	C	D	E	F	G	H
1	Category	ID	Name	Description	Sources	NIST Rev5 Controls	Requirements	Deployment
2	None	CM0000	Countermeasure	This technique is a result o		None		
3	Prevention	CM0001	Protect Ser	Organizations should look		AC-3(11),AC-4(23),AC-4	The Program shall c	Ground Segm
4	Prevention	CM0008	Security Te	As penetration testing and		AC-3(11),CA-8,CM-4,CP	The Program shall c	Ground Segm
5	Prevention	CM0009	Threat Inte	A threat intelli	https://att	PM-16,PM-16(1),PM-16	The Program shall c	Ground Segm
6	Prevention	CM0020	Threat mod	Use threat modeling, attac		CA-3,CM-4,CP-2,PL-8,PI	The Program shall c	Development
7	Prevention	CM0022	Criticality A	Conduct a criticality analy		CP-2,CP-2(8),PL-8,PL-8(	The Program shall c	Development
8	Prevention	CM0024	Anti-count	Develop and implement a		AC-14,AC-20(5),CM-7(9	The Program shall c	Ground Segm
9	Prevention	CM0025	Supplier Re	Conduct a supplier review		PL-8,PL-8(1),PL-8(2),PM	The Program shall c	Development
10	Prevention	CM0026	Original Co	Components/Software tha		AC-20(5),PL-8,PL-8(1),P	The Program shall c	Development
11	Prevention	CM0027	ASIC/FPGA	Application-Specific Integ		AC-14,PL-8,PL-8(1),PL-8	The Program shall c	Development
12	Prevention	CM0028	Tamper Pro	Perform physi	https://att	AC-14,CA-8(3),CM-7(9),	The Program shall c	Ground Segm
13	Prevention	CM0052	Insider Thr	Establish policy and proce		AC-14,AC-3(11),AC-3(13	The spacecraft shall	Ground Segm
14	Prevention	CM0054	Two-Persor	Utilize a two-person syster		AC-14,AC-3(13),AC-3(15	The spacecraft shall	Ground Segm
15	Prevention	CM0080	Stealth Tec	Space systems	https://csis	CP-10(6),CP-13,SC-30,SC-30(5)		Space Segmen
16	Prevention	CM0081	Defensive J	A jammer or sp	https://csis	CP-10(6),CP-13,CP-2,CF	The spacecraft shall	Ground Segm
17	Prevention	CM0082	Deception	Deception can	https://csis	SC-26,SC-30		Space Segmen
18	Prevention	CM0083	Antenna Nu	Satellites can t	https://csis	SC-40,SI-4(14)	The spacecraft shall	Space Segmen
19	Prevention	CM0086	Filtering an	Filters and shu	https://csis	CP-13,PE-18,SC-5,SC-5(	The spacecraft shall	Space Segmen
20	Prevention	CM0087	Defensive D	Laser systems	https://csis	CP-10(6),CP-13,CP-2,CF	The spacecraft shall	Ground Segm
21	Cryptograp	CM0002	COMSEC	A component	https://csrc	AC-17,AC-17(1),AC-17(1	The spacecraft shall	Ground Segm
22	Prevention	CM0030	Crypto Key	Leverage best	https://csrc	PL-8,PL-8(1),SA-3,SA-4(1	The Program shall c	Space Segmen
23	Prevention	CM0031	Authentica	Authenticate all communi		AC-14,AC-17,AC-17(10),	The spacecraft shall	Space Segmen

SPARTA Countermeasure Mapper / Defensive Gap Analyzer

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

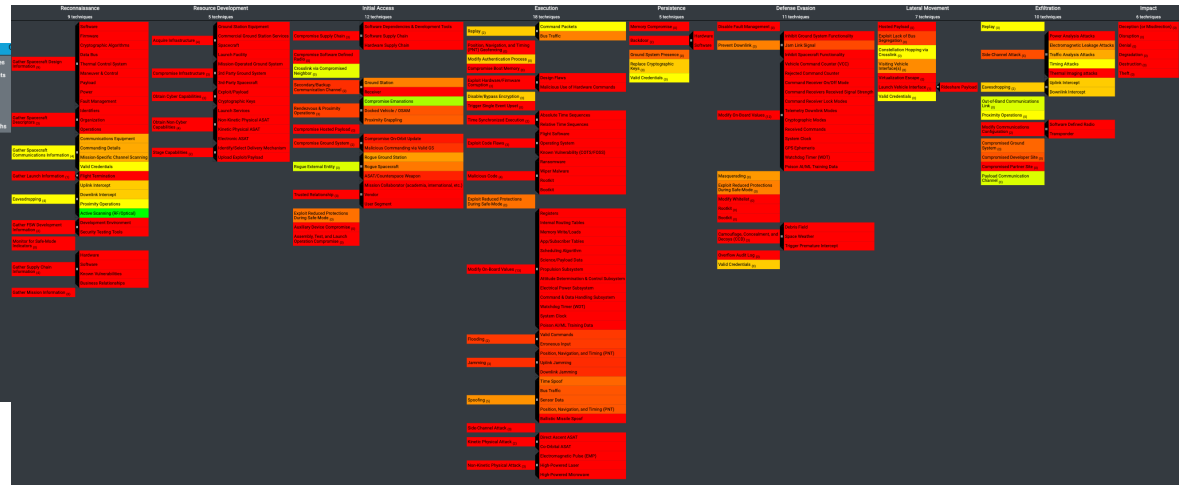
- Attack chains built in SPARTA's navigator can help identify countermeasures against the TTPs used in the attack
  - *Many users do not know TTPs, they only know the countermeasures they have implemented (or plan to)…*
- The SPARTA capability enables a graphical mechanism to select and deselect countermeasures 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*



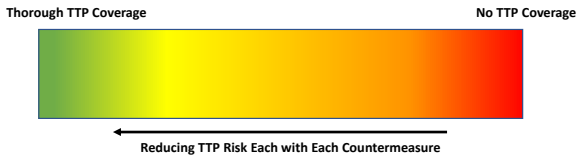


Percent Coverage	ID	Name	Description	References	Aerospace I	Related MI	Counterme	Additional	NIST Rev5 (	Requirements
50.00%	REC-0003	Gather Spacecraft Communicatior	Threat actors may	https://cro	SV-CF-3	T1592,T15	CM0002,CI	CM0001,CI	AC-3(11),AI	The Program sh
33.33%	REC-0003.01	Communications Equipment	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
40.00%	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
40.00%	REC-0005.02	Downlink Intercept	Threat actors may	Kaspersky:	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,CM	0029	AC-17,AC-1	The spacecraft s
54.55%	IA-0003	Crosslink via Compromised Neight	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(I	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 proximi		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

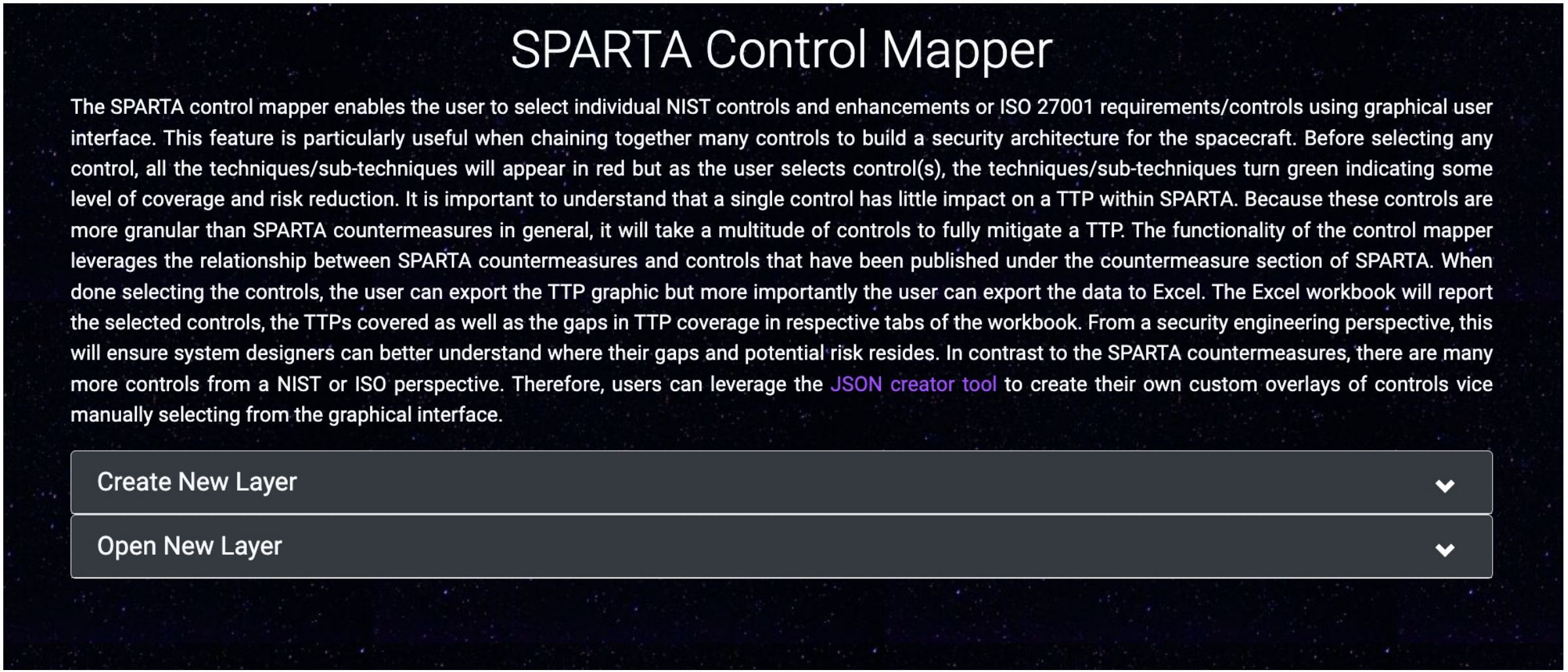
SPARTA Countermeasures | SPARTA Techniques Covered | SPARTA Techniques Not Covered



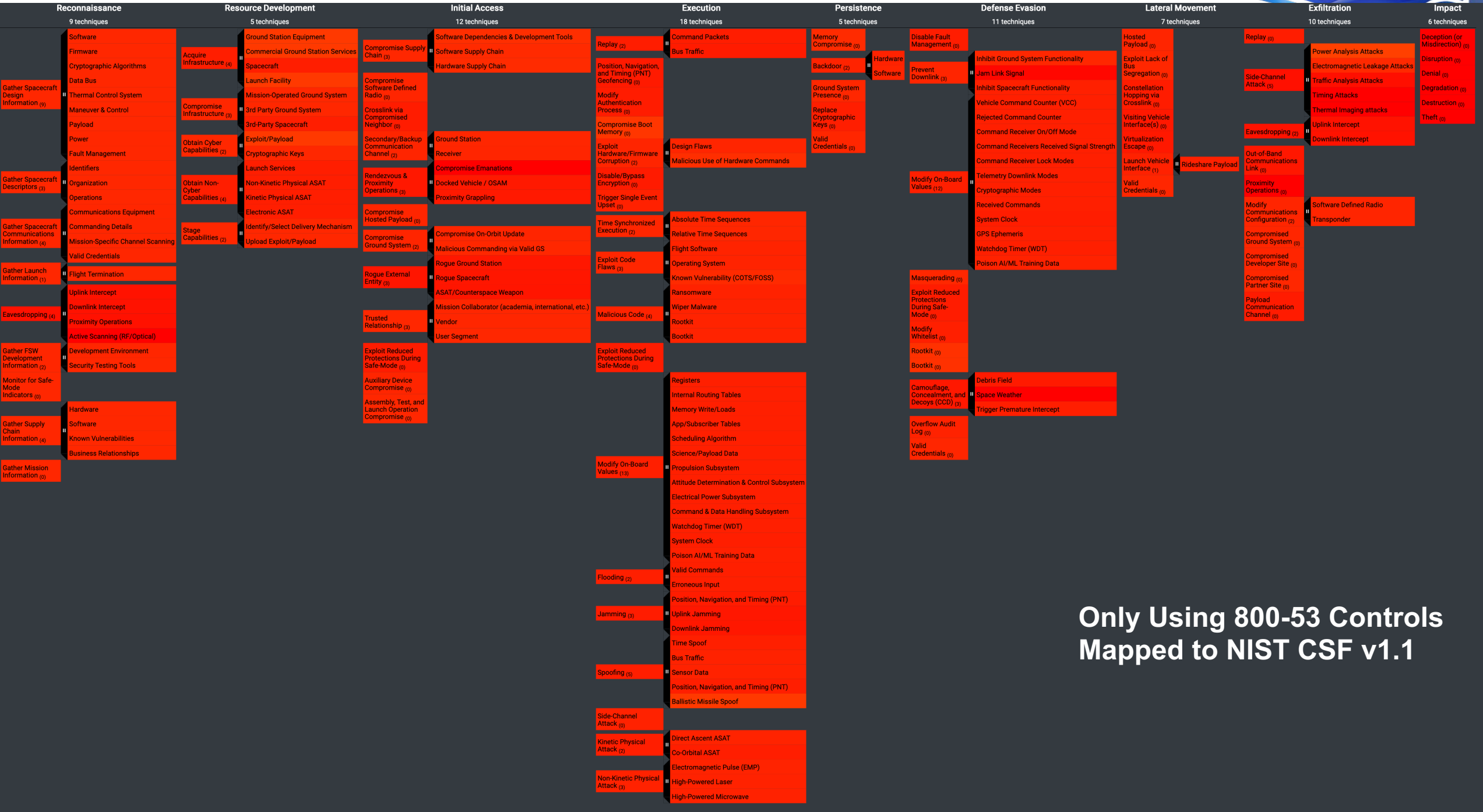
Excel Output



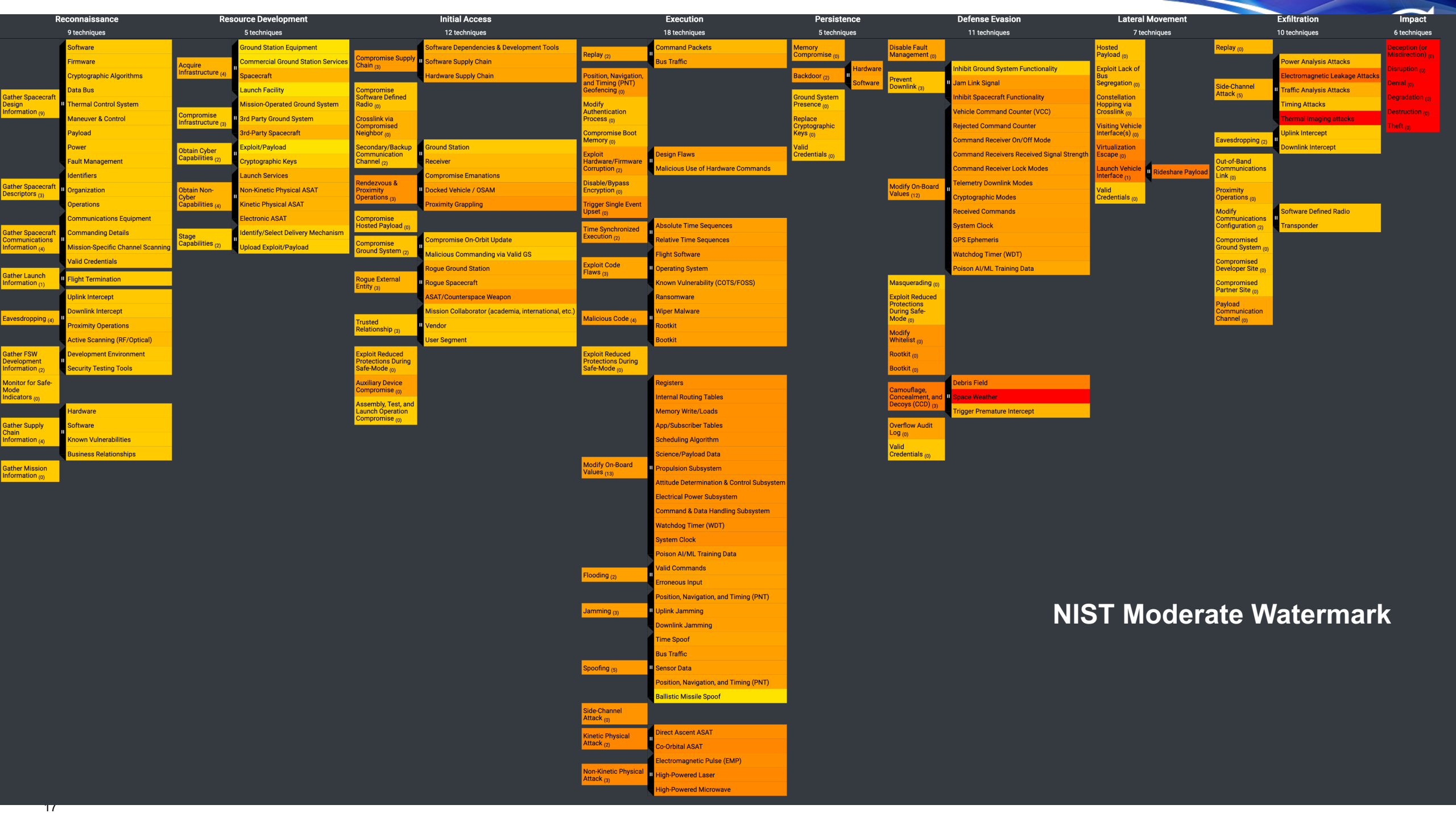
Control Mapper

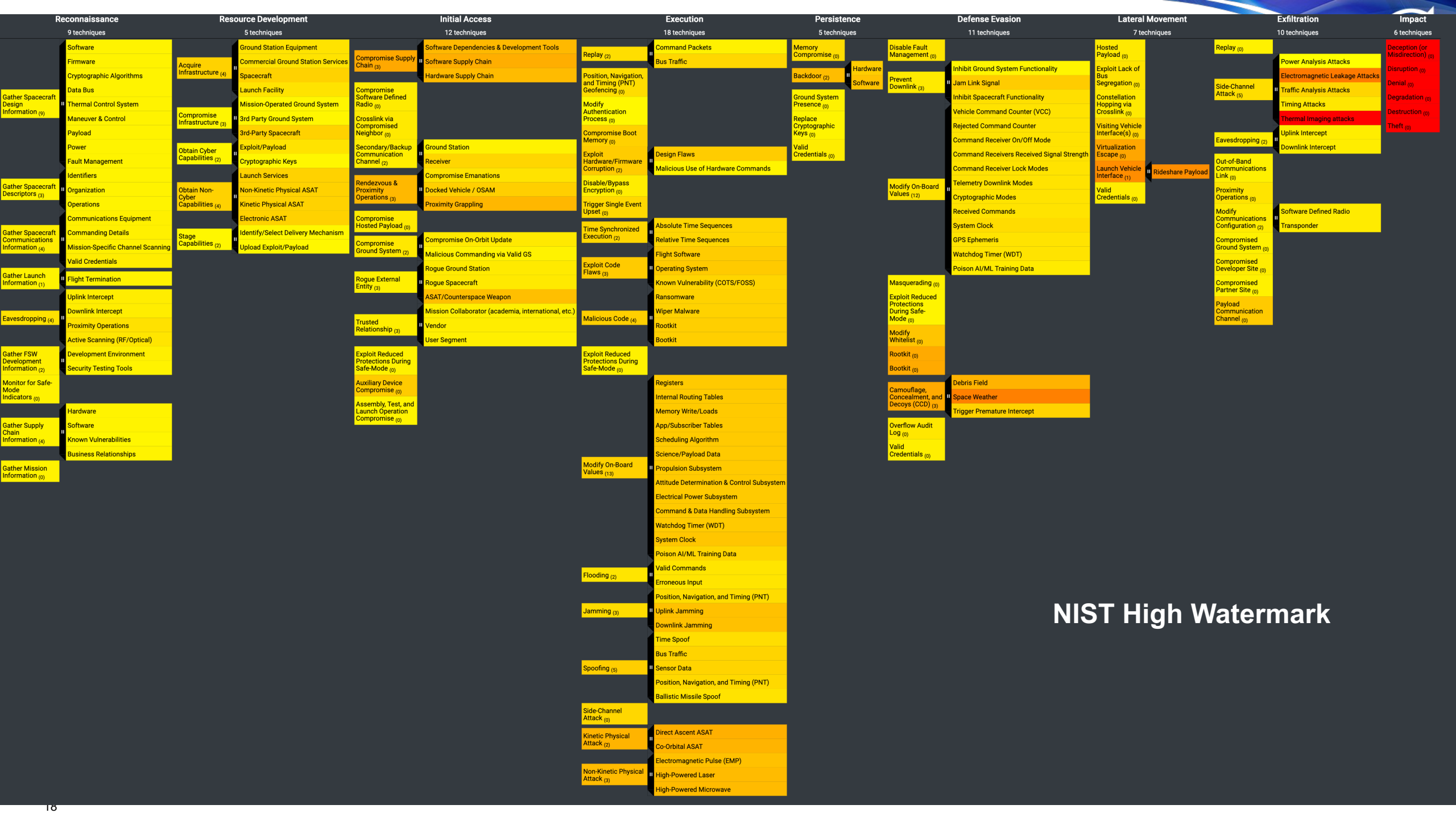


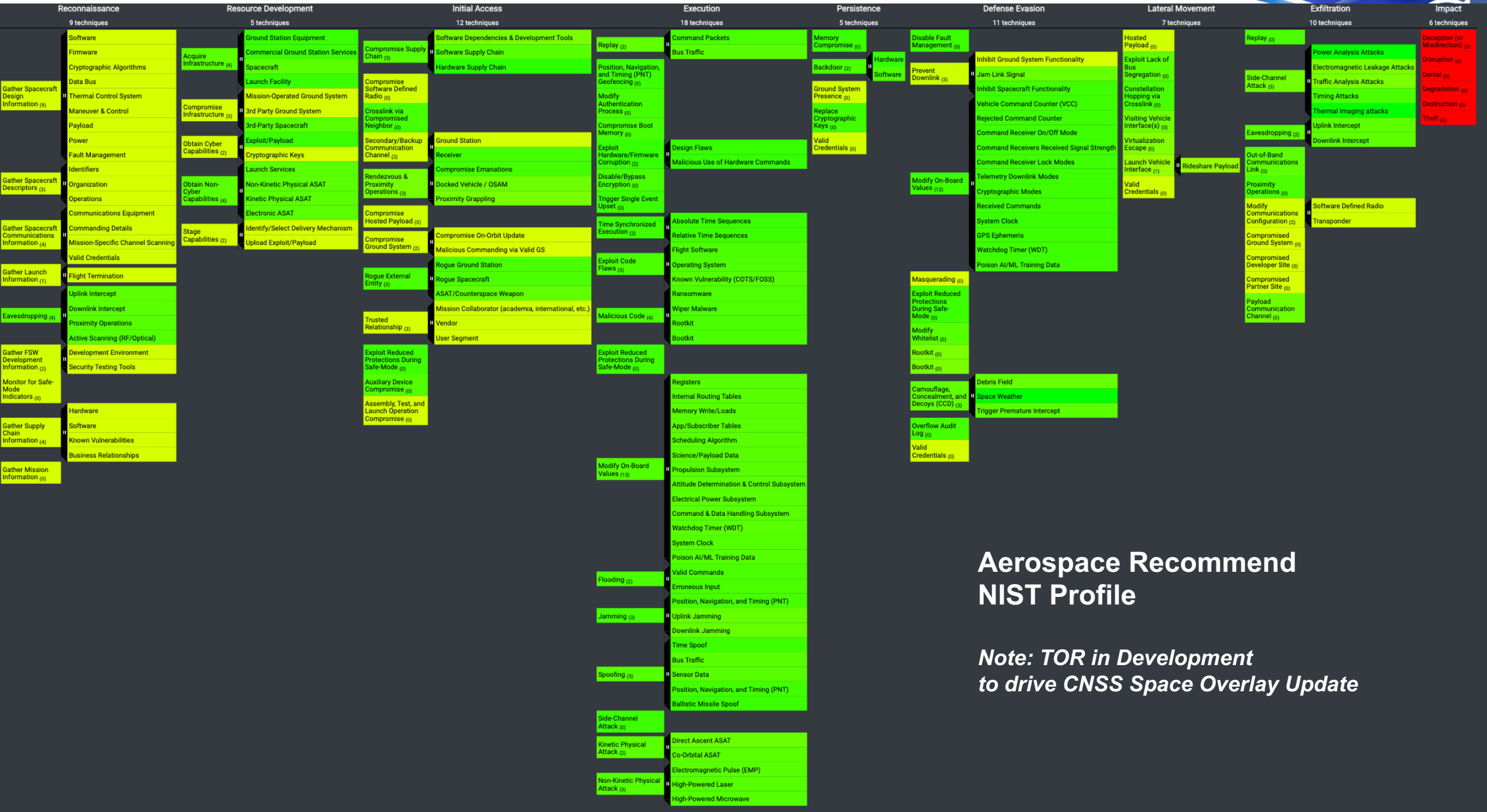
Control Mapper is Good for Comparing NIST 800-53 Control Baselines and their TTP Mitigation



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


Reconnaissance
9 techniques
Gather Spacecraft Design Information (9)
Software
Firmware
Cryptographic Algorithms
Data Bus
Thermal Control System
Maneuver & Control
Payload
Power
Fault Management
Gather Spacecraft Descriptors (3)
Identifiers
Organization
Operations
Gather Spacecraft Communications Information (4)
Communications Equipment
Commanding Details
Mission-Specific Channel Scanning
Valid Credentials
Gather Launch Information (1)
Flight Termination
Eavesdropping (4)
Uplink Intercept
Downlink Intercept
Proximity Operations
Active Scanning (RF/Optical)
Gather FSW Development Information (2)
Development Environment
Security Testing Tools
Monitor for Safe-Mode Indicators (0)
Gather Supply Chain Information (4)
Hardware
Software
Known Vulnerabilities
Business Relationships
Gather Mission Information (0)
Resource Development
5 techniques
Acquire Infrastructure (4)
Ground Station Equipment
Commercial Ground Station Services
Spacecraft
Launch Facility
Compromise Infrastructure (3)
Mission-Operated Ground System
3rd Party Ground System
3rd-Party Spacecraft
Obtain Cyber Capabilities (2)
Exploit/Payload
Cryptographic Keys
Obtain Non-Cyber Capabilities (4)
Launch Services
Non-Kinetic Physical ASAT
Kinetic Physical ASAT
Electronic ASAT
Stage Capabilities (2)
Identify/Select Delivery Mechanism
Upload Exploit/Payload
Initial Access
12 techniques
Compromise Supply Chain (3)
Software Dependencies & Development Tools
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 External Entity (3)
Rogue Ground Station
Rogue Spacecraft
ASAT/Counterspace Weapon
Trusted Relationship (3)
Mission Collaborator (academia, international, etc.)
Vendor
User Segment
Exploit Reduced Protections During Safe-Mode (0)
Auxiliary Device Compromise (0)
Assembly, Test, and Launch Operation Compromise (0)
Execution
18 techniques
Replay (2)
Command Packets
Bus Traffic
Position, Navigation, and Timing (PNT) Geofencing (0)
Modify Authentication Process (0)
Compromise Boot Memory (0)
Exploit Hardware/Firmware Corruption (2)
Design Flaws
Malicious Use of Hardware Commands
Disable/Bypass Encryption (0)
Trigger Single Event Upset (0)
Time Synchronized Execution (2)
Absolute Time Sequences
Relative Time Sequences
Exploit Code Flaws (3)
Flight Software
Operating System
Known Vulnerability (COTS/FOSS)
Malicious Code (4)
Ransomware
Wiper Malware
Rootkit
Bootkit
Exploit Reduced Protections During Safe-Mode (0)
Registers
Internal Routing Tables
Memory Write/Loads
App/Subscriber Tables
Modify On-Board Values (13)
Scheduling Algorithm
Science/Payload Data
Propulsion Subsystem
Attitude Determination & Control Subsystem
Electrical Power Subsystem
Command & Data Handling Subsystem
Watchdog Timer (WDT)
System Clock
Poison AI/ML Training Data
Flooding (2)
Valid Commands
Erroneous Input
Jamming (3)
Position, Navigation, and Timing (PNT)
Uplink Jamming
Downlink Jamming
Time Spoof
Spoofing (5)
Bus Traffic
Sensor Data
Position, Navigation, and Timing (PNT)
Ballistic Missile Spoof
Side-Channel Attack (0)
Kinetic Physical Attack (2)
Direct Ascent ASAT
Co-Orbital ASAT
Non-Kinetic Physical Attack (3)
Electromagnetic Pulse (EMP)
High-Powered Laser
High-Powered Microwave
Persistence
5 techniques
Memory Compromise (0)
Backdoor (2)
Hardware
Software
Ground System Presence (0)
Replace Cryptographic Keys (0)
Valid Credentials (0)
Defense Evasion
11 techniques
Disable Fault Management (0)
Prevent Downlink (3)
Inhibit Ground System Functionality
Jam Link Signal
Inhibit Spacecraft Functionality
Vehicle Command Counter (VCC)
Rejected Command Counter
Command Receiver On/Off Mode
Command Receivers Received Signal Strength
Command Receiver Lock Modes
Modify On-Board Values (12)
Telemetry Downlink Modes
Cryptographic Modes
Received Commands
System Clock
GPS Ephemeris
Watchdog Timer (WDT)
Poison AI/ML Training Data
Masquerading (0)
Exploit Reduced Protections During Safe-Mode (0)
Modify Whitelist (0)
Rootkit (0)
Bootkit (0)
Camouflage, Concealment, and Decoys (CCD) (3)
Debris Field
Space Weather
Trigger Premature Intercept
Overflow Audit Log (0)
Valid Credentials (0)
Lateral Movement
7 techniques
Hosted Payload (0)
Exploit Lack of Bus Segregation (0)
Constellation Hopping via Crosslink (0)
Visiting Vehicle Interface(s) (0)
Virtualization Escape (0)
Launch Vehicle Interface (1)
Rideshare Payload
Valid Credentials (0)
Exfiltration
10 techniques
Replay (0)
Power Analysis Attacks
Electromagnetic Leakage Attacks
Side-Channel Attack (5)
Traffic Analysis Attacks
Timing Attacks
Thermal Imaging attacks
Eavesdropping (2)
Uplink Intercept
Downlink Intercept
Out-of-Band Communications Link (0)
Proximity Operations (0)
Modify Communications Configuration (2)
Software Defined Radio
Transponder
Compromised Ground System (0)
Compromised Developer Site (0)
Compromised Partner Site (0)
Payload Communication Channel (0)
Impact
6 techniques
Deception (or Misdirection) (0)
Disruption (0)
Denial (0)
Degradation (0)
Destruction (0)
Theft (0)
NIST Moderate Watermark


Reconnaissance
9 techniques
Gather Spacecraft Design Information (9)
Software
Firmware
Cryptographic Algorithms
Data Bus
Thermal Control System
Maneuver & Control
Payload
Power
Fault Management
Gather Spacecraft Descriptors (3)
Identifiers
Organization
Operations
Gather Spacecraft Communications Information (4)
Communications Equipment
Commanding Details
Mission-Specific Channel Scanning
Valid Credentials
Gather Launch Information (1)
Flight Termination
Eavesdropping (4)
Uplink Intercept
Downlink Intercept
Proximity Operations
Active Scanning (RF/Optical)
Gather FSW Development Information (2)
Development Environment
Security Testing Tools
Monitor for Safe-Mode Indicators (0)
Gather Supply Chain Information (4)
Hardware
Software
Known Vulnerabilities
Business Relationships
Gather Mission Information (0)
Resource Development
5 techniques
Acquire Infrastructure (4)
Ground Station Equipment
Commercial Ground Station Services
Spacecraft
Launch Facility
Compromise Infrastructure (3)
Mission-Operated Ground System
3rd Party Ground System
3rd-Party Spacecraft
Obtain Cyber Capabilities (2)
Exploit/Payload
Cryptographic Keys
Obtain Non-Cyber Capabilities (4)
Launch Services
Non-Kinetic Physical ASAT
Kinetic Physical ASAT
Electronic ASAT
Stage Capabilities (2)
Identify/Select Delivery Mechanism
Upload Exploit/Payload
Initial Access
12 techniques
Compromise Supply Chain (3)
Software Dependencies & Development Tools
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 External Entity (3)
Rogue Ground Station
Rogue Spacecraft
ASAT/Counterspace Weapon
Trusted Relationship (3)
Mission Collaborator (academia, international, etc.)
Vendor
User Segment
Exploit Reduced Protections During Safe-Mode (0)
Auxiliary Device Compromise (0)
Assembly, Test, and Launch Operation Compromise (0)
Execution
18 techniques
Replay (2)
Command Packets
Bus Traffic
Position, Navigation, and Timing (PNT) Geofencing (0)
Modify Authentication Process (0)
Compromise Boot Memory (0)
Exploit Hardware/Firmware Corruption (2)
Design Flaws
Malicious Use of Hardware Commands
Disable/Bypass Encryption (0)
Trigger Single Event Upset (0)
Time Synchronized Execution (2)
Absolute Time Sequences
Relative Time Sequences
Exploit Code Flaws (3)
Flight Software
Operating System
Known Vulnerability (COTS/FOSS)
Malicious Code (4)
Ransomware
Wiper Malware
Rootkit
Bootkit
Exploit Reduced Protections During Safe-Mode (0)
Modify On-Board Values (13)
Registers
Internal Routing Tables
Memory Write/Loads
App/Subscriber Tables
Scheduling Algorithm
Science/Payload Data
Propulsion Subsystem
Attitude Determination & Control Subsystem
Electrical Power Subsystem
Command & Data Handling Subsystem
Watchdog Timer (WDT)
System Clock
Poison AI/ML Training Data
Flooding (2)
Valid Commands
Erroneous Input
Jamming (3)
Position, Navigation, and Timing (PNT)
Uplink Jamming
Downlink Jamming
Spoofing (5)
Time Spoof
Bus Traffic
Sensor Data
Position, Navigation, and Timing (PNT)
Ballistic Missile Spoof
Side-Channel Attack (0)
Kinetic Physical Attack (2)
Direct Ascent ASAT
Co-Orbital ASAT
Non-Kinetic Physical Attack (3)
Electromagnetic Pulse (EMP)
High-Powered Laser
High-Powered Microwave
Persistence
5 techniques
Memory Compromise (0)
Backdoor (2)
Hardware
Software
Ground System Presence (0)
Replace Cryptographic Keys (0)
Valid Credentials (0)
Defense Evasion
11 techniques
Disable Fault Management (0)
Prevent Downlink (3)
Inhibit Ground System Functionality
Jam Link Signal
Inhibit Spacecraft Functionality
Vehicle Command Counter (VCC)
Rejected Command Counter
Command Receiver On/Off Mode
Command Receivers Received Signal Strength
Command Receiver Lock Modes
Modify On-Board Values (12)
Telemetry Downlink Modes
Cryptographic Modes
Received Commands
System Clock
GPS Ephemeris
Watchdog Timer (WDT)
Poison AI/ML Training Data
Masquerading (0)
Exploit Reduced Protections During Safe-Mode (0)
Modify Whitelist (0)
Rootkit (0)
Bootkit (0)
Camouflage, Concealment, and Decoys (CCD) (3)
Debris Field
Space Weather
Trigger Premature Intercept
Overflow Audit Log (0)
Valid Credentials (0)
Lateral Movement
7 techniques
Hosted Payload (0)
Exploit Lack of Bus Segregation (0)
Constellation Hopping via Crosslink (0)
Visiting Vehicle Interface(s) (0)
Virtualization Escape (0)
Launch Vehicle Interface (1)
Rideshare Payload
Valid Credentials (0)
Exfiltration
10 techniques
Replay (0)
Power Analysis Attacks
Electromagnetic Leakage Attacks
Side-Channel Attack (5)
Traffic Analysis Attacks
Timing Attacks
Thermal Imaging attacks
Eavesdropping (2)
Uplink Intercept
Downlink Intercept
Out-of-Band Communications Link (0)
Proximity Operations (0)
Modify Communications Configuration (2)
Software Defined Radio
Transponder
Compromised Ground System (0)
Compromised Developer Site (0)
Compromised Partner Site (0)
Payload Communication Channel (0)
Impact
6 techniques
Deception (or Misdirection) (0)
Disruption (0)
Denial (0)
Degradation (0)
Destruction (0)
Theft (0)
NIST High Watermark

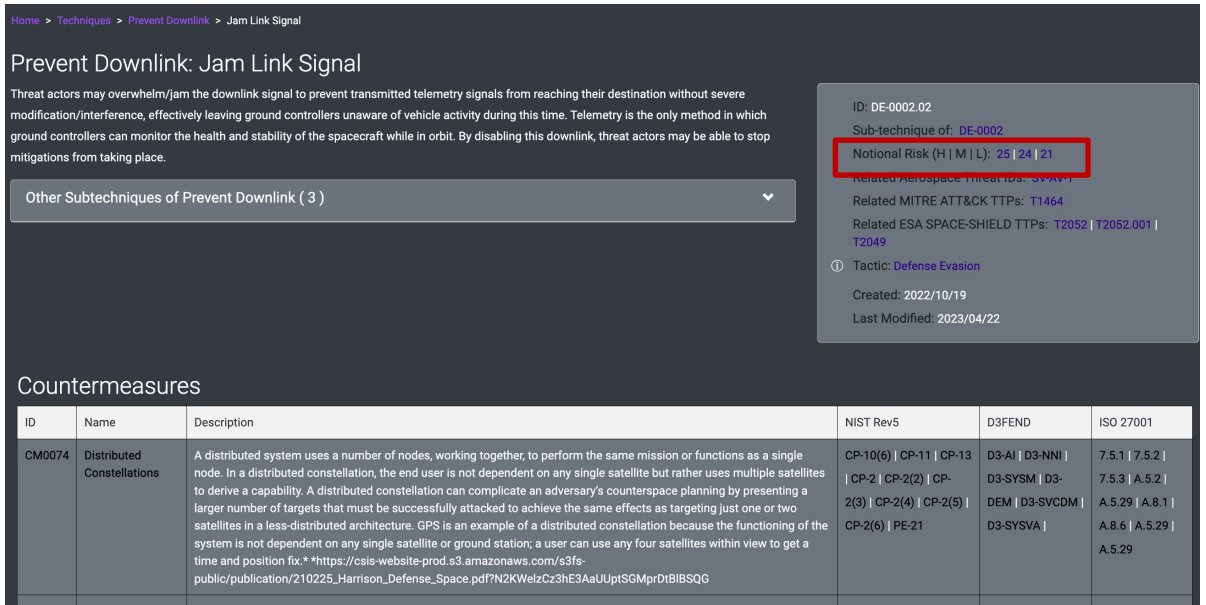


Aerospace Recommend NIST Profile

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#*

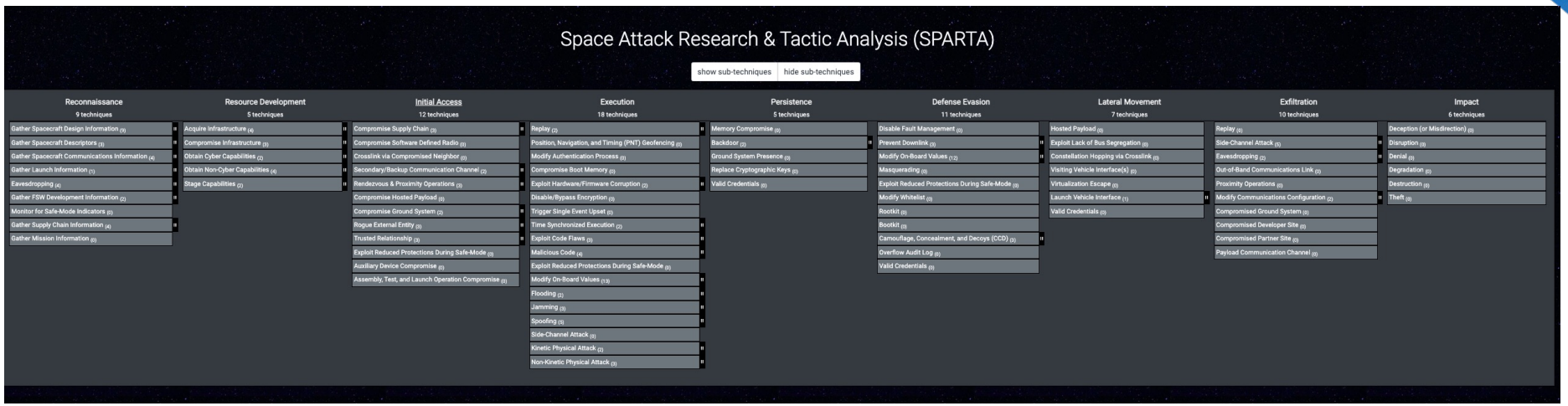


Show 100 entries Search: 25

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

https://sparta.aerospace.org

SPARTA
SPACE ATTACK RESEARCH & TACTIC ANALYSIS



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