SPACE ISAC

VALUE OF SPACE SUMMIT 2023

Co-hosted by AEROSPACE

SPACE ISAC

VALUE OF SPACE SUMMIT 2023

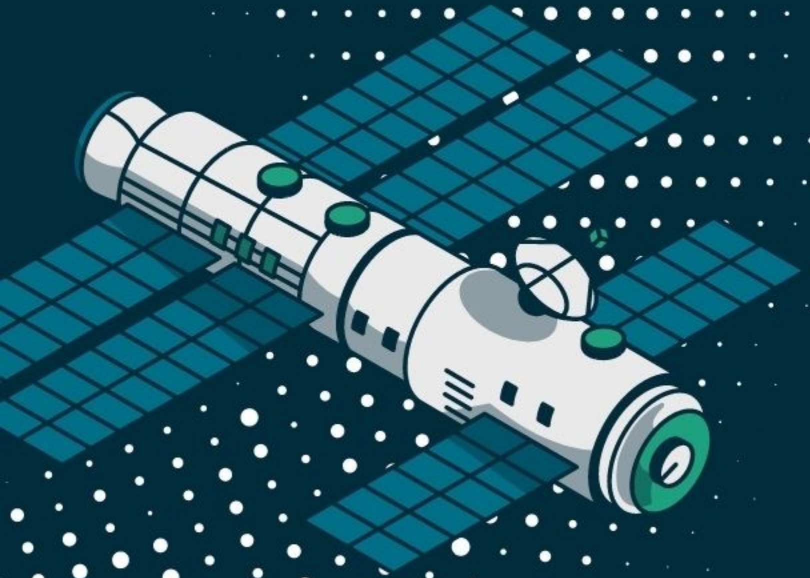
Co-hosted by AEROSPACE

Alasyn Zimmerman

Investigative Reporter, KOAA5

Alasyn Zimmerman is an Investigative Reporter with KOAA News5. She's covered state government and politics throughout the past six years in southern Colorado, with an emphasis on elections and election law. Over the past couple of years, she's covered the national decision on the permanent home of U.S. Space Command. She's led her station's coverage of state, local, and national elections since 2020. Zimmerman has received three awards through the Colorado Broadcasters Association for her political coverage, including “Best Public Affairs Program” in 2022 for an election special she produced, reported, and anchored. Zimmerman is a University of Colorado-Boulder alum with a B.S. in Journalism.

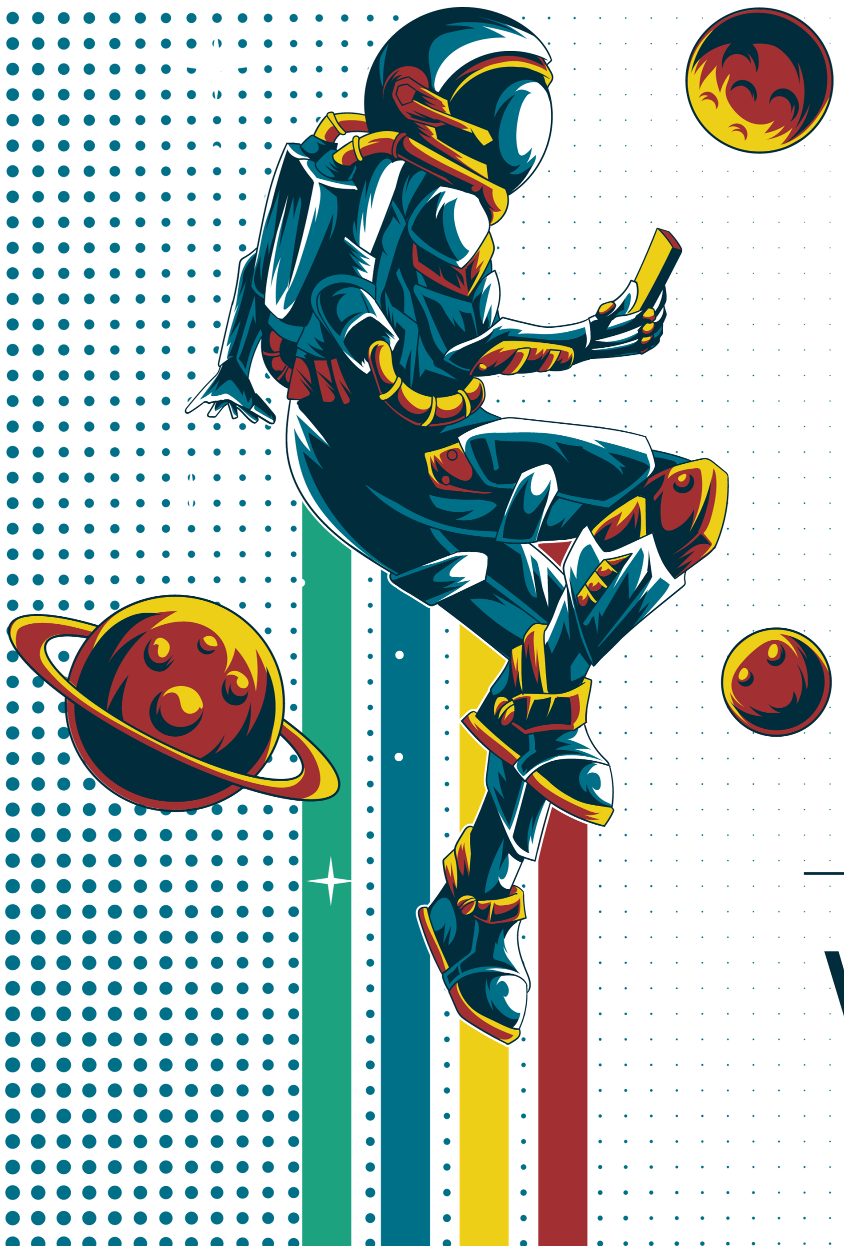
October 17 - 19, 2023
Colorado Springs, CO USA



"The Next Giant Leap: Building Cyber Resilience for the Global Space Industry"

This theme will explore the critical importance of cybersecurity in the rapidly advancing commercial space sector. Drawing parallels between the monumental technological advances that propelled humanity to the moon in the late 1960s and the current state of the space industry, this conference aims to shed light on the profound changes we are experiencing and the urgent need for cyber resilience in the space domain.

Venue Hosts: UCCS University of Colorado Colorado Springs | KRATOS® READY FOR WHAT'S NEXT™ | Booz | Allen | Hamilton®



WELCOME

SPACE ISAC

Co-hosted by

AEROSPACE

VALUE OF SPACE SUMMIT 2023

VALUE OF SPACE SUMMIT 2023

Sponsors

CYWARE™

KRATOS®
READY FOR WHAT'S NEXT™

Constellation

Deloitte.

RADICL
Nation State Threat Defense

ExoAnalytic
SOLUTIONS

RAPIDASCENT

thinklogical®
A BELDEN BRAND

Dr. Jennifer Sobanet,
Interim Chancellor
University of Colorado
Colorado Springs (UCCS)

elara NOVA
THE SPACE CONSULTANCY

Maj. Gen. (Ret) Kim Crider
Founding Partner
Elara Nova: The Space Consultancy

SPACE ISAC

KRATOS

READY FOR WHAT'S NEXT™

Frank Backes, Senior Vice President, Kratos Space Federal

Board Chair, Space ISAC

Anjana Rajan, Assistant National Cyber Director, The White House Office of the National Cyber Director (ONCD)

Kassandra Vogel

Principal Space Systems Security Architect

Blue Origin

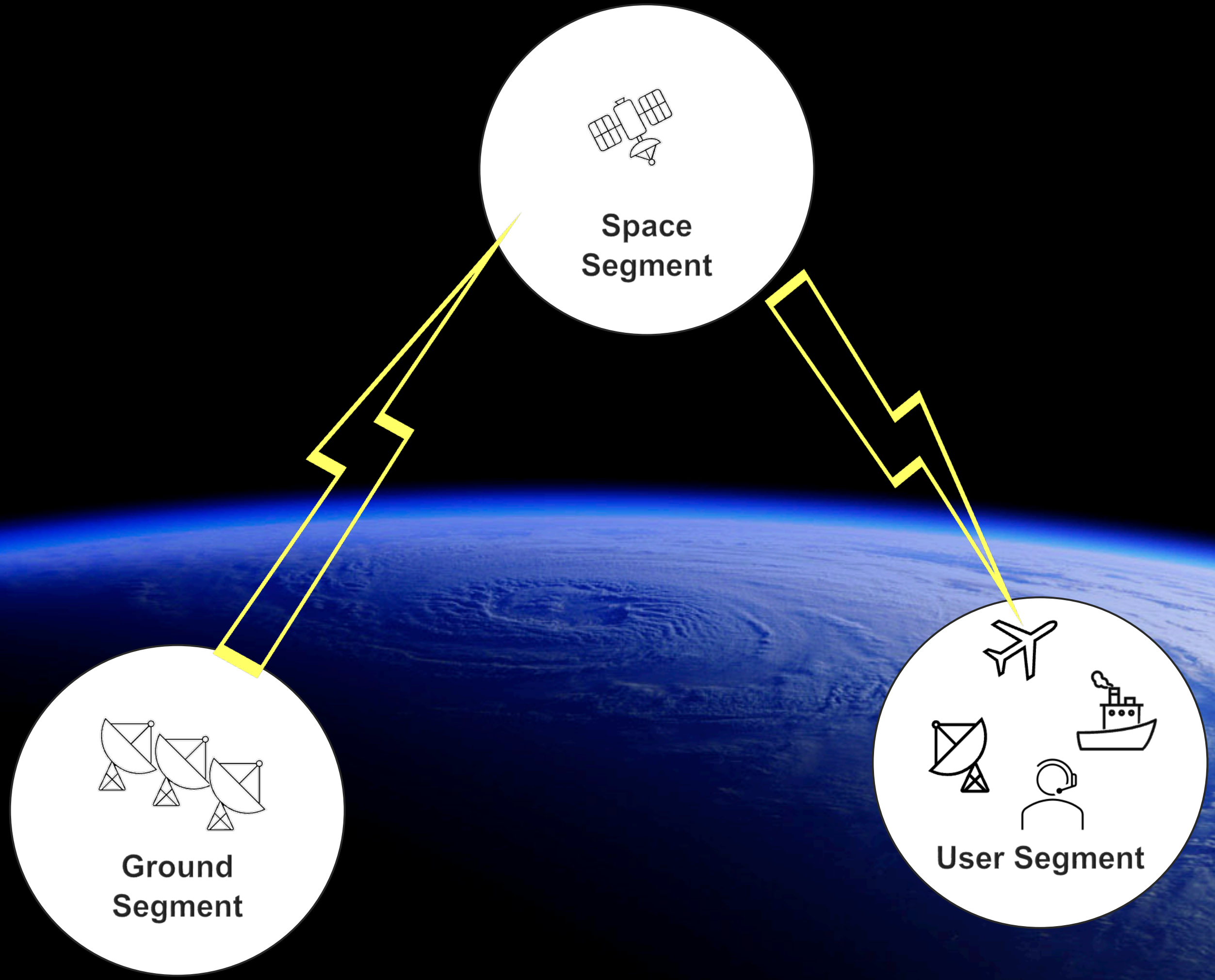
THE NEXT GIANT LEAP:

Building Cyber Resilience for the Global Space Industry

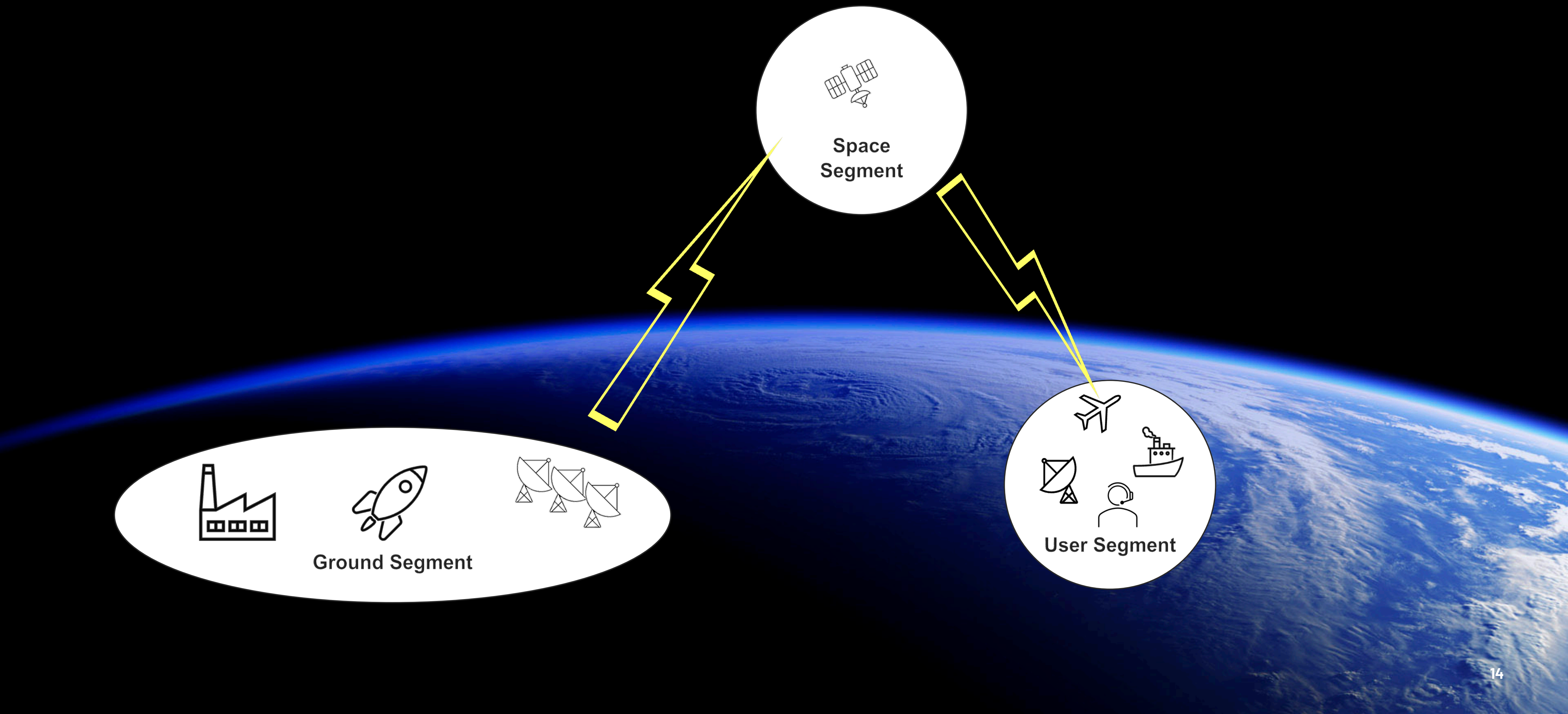
THE GLOBAL SPACE ECOSYSTEM

Beginning with the End in Mind

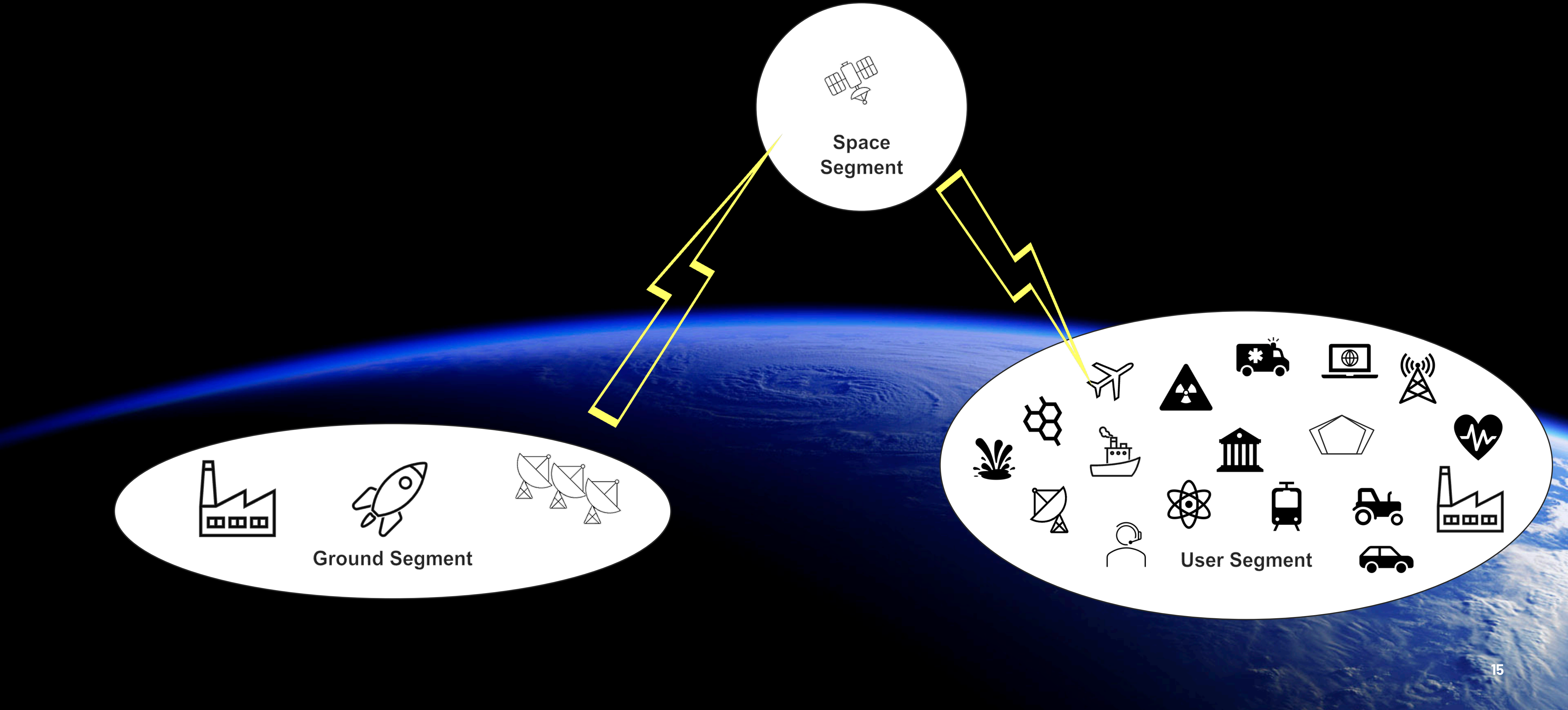
From Here……



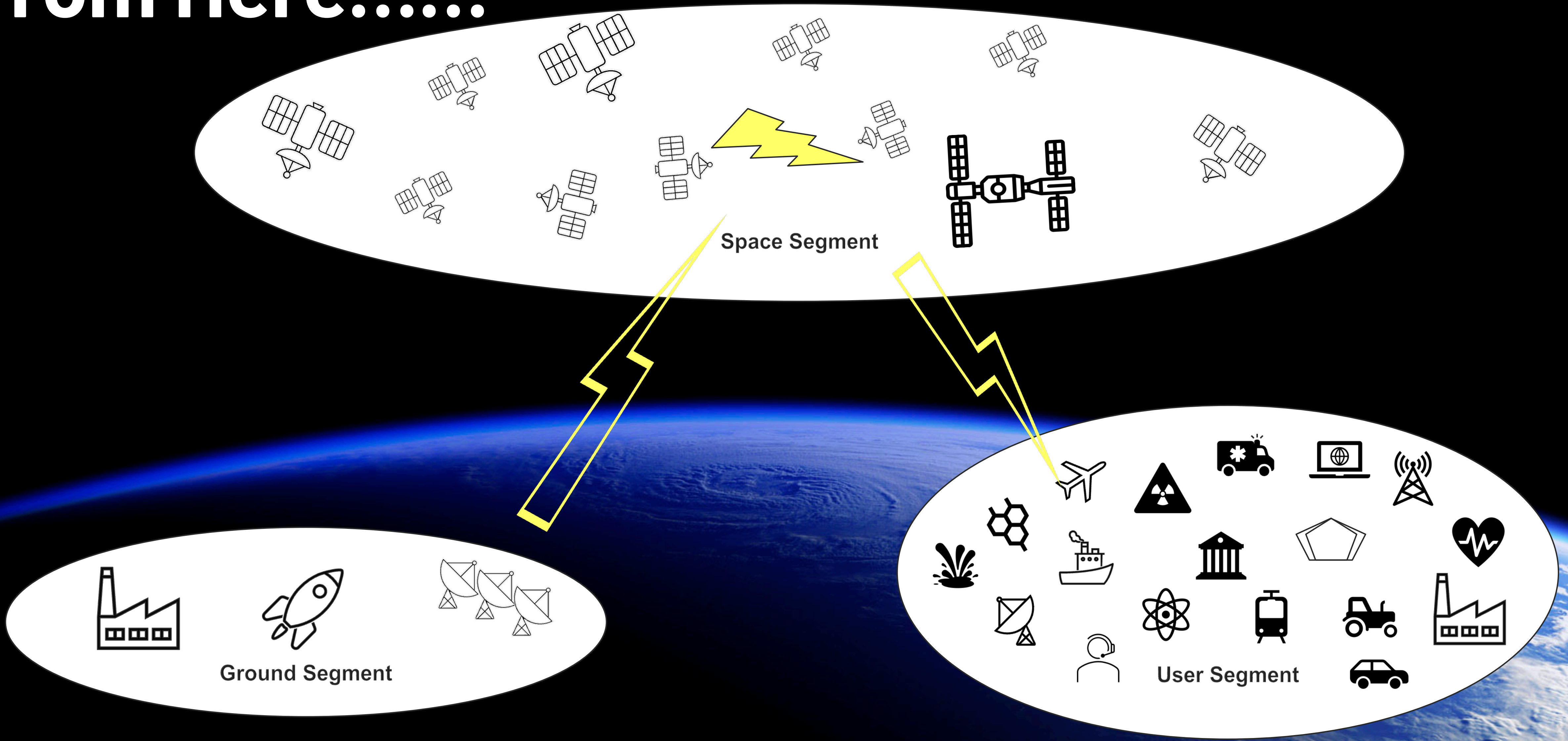
From Here……



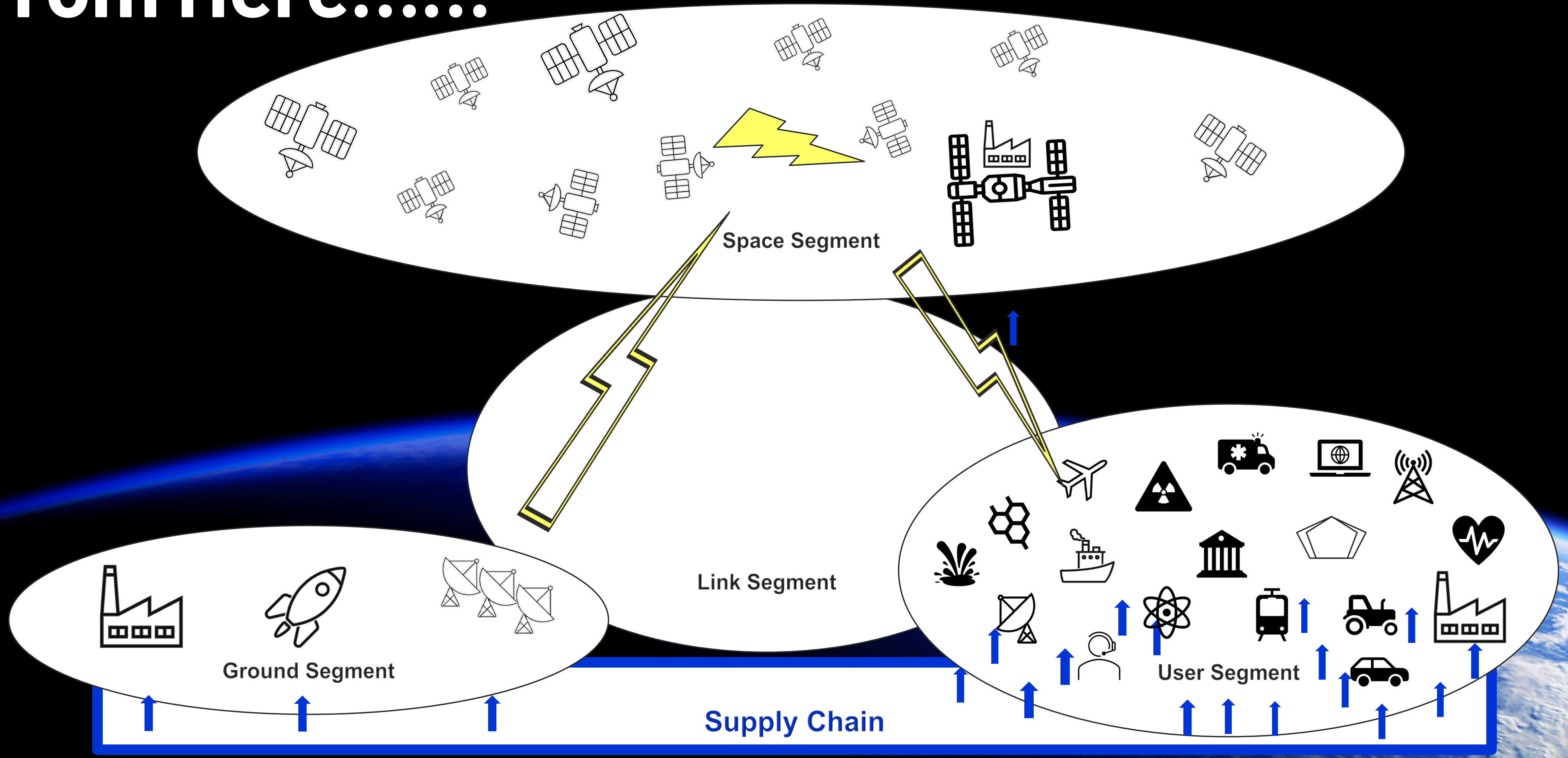
From Here......



From Here......



From Here……



Space Segment
Link Segment
Ground Segment
User Segment
Supply Chain

......To There

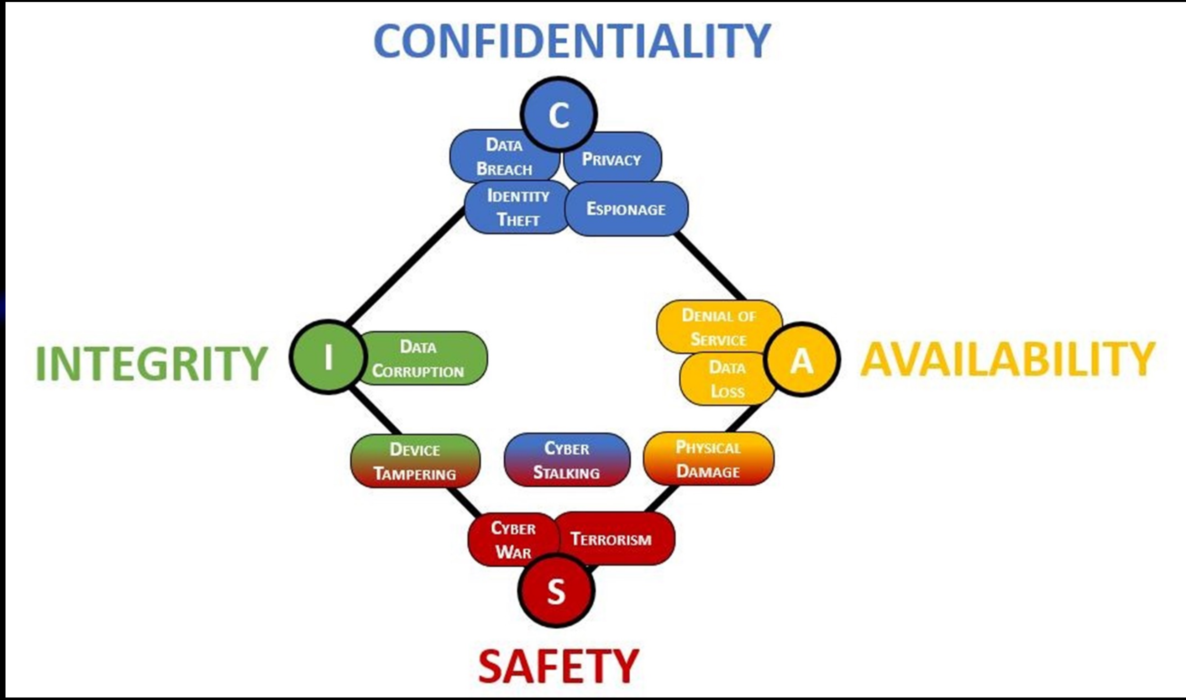
BUILDING CYBER RESILIENCE

Beginning with the End in Mind

Cyber Resilience: Key Concepts

Cybersecurity is a triad!

- Sensitive data protection is not the only driving consideration
- Critical elements require integrity and availability protections by definition
- Loss of integrity and/or availability may impact safety



Resilience engineering is concerned with critical systems

Cyber Resilience is an ability to:

- **Anticipate –** maintain a state of informed preparedness
- **Withstand –** continue essential functions despite
- **Recover** – continue essential functions during and after
- **Adapt** – modify functions and/or capabilities in response to predicted changes

…to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

Cyber Resilience for and In Space

Anticipate – maintain a state of informed preparedness

- While the majority of this threat intelligence will be collected on the ground, space-based sensors and even contextual telemetry are needed

Withstand - continue essential functions <u>despite</u>

- We need incident response exercises and simulations that inform playbooks to enable speedy *appropriate* responses
- Everything incident response related must include elements we've likely not included before – supply chain, maintenance/factories, launch segment, hosted payloads

Recover - continue essential functions <u>during and after</u>

- Requires *extremely granular and current* inventory and configuration data for all critical components *and dependencies*

Adapt - modify functions and/or capabilities in response to predicted changes

- Must be <u>built</u> to be adaptable

Building Cyber Resilience

Have a blueprint before building…anything

- A core set of cybersecurity functions must be baselined for critical IT and OT
- Build with the end in mind - resilience

Apply zero trust principles to all critical elements

- Everywhere, always, and that includes the components we launch and the actors in each environment (even Dr. Hedrick and her lunar rover)

Leverage technology

- Digital twins are superior for modeling and simulating resilience in unfavorable conditions
- Apply AI/ML for threat hunting and incident response planning, to characterize and predict behavior, and identify and optimize responses

Let us not reinvent the wheel in space

- (That TT&C subsystem sure looks like a wireless access point)


INTERPLANETARY
ROAD
TO
SPACE
MILE
0
LC-36

BLUE ORIGIN

FOR THE BENEFIT OF **EARTH**

KASSANDRA VOGEL

PRINCIPAL SPACE SYSTEMS SECURITY ARCHITECT

Space Systems Designation as Critical Infrastructure Sector

Samuel S. Visner, Fellow, The Aerospace Corporation

Commercial Protection Before, During and After a Cyber Incident

Erin Miller, Executive Director, Space ISAC

Marina Hague, Commercial Space Issues Manager, Office of the Director of National Intelligence (ODNI)

Lauryn Williams, Senior Advisor for Strategy, The White House Office of the National Cyber Director (ONCD)

Aerospace SPARTA Updates

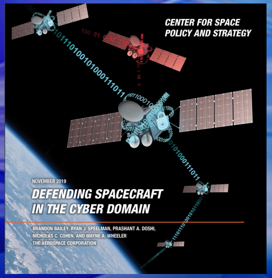
Brandon Bailey, Senior Project Leader, Cyber Assessments and Research Department, The Aerospace Corporation

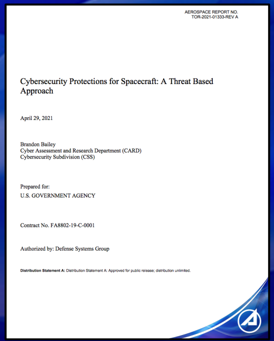
SPARTA

SPACE ATTACK RESEARCH & TACTIC ANALYSIS

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





AEROSPACE REPORT NO.
TOR-2021-01333-REV A

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

Distribution Statement A: Distribution Statement A: Approved for public release; distribution unlimited.

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

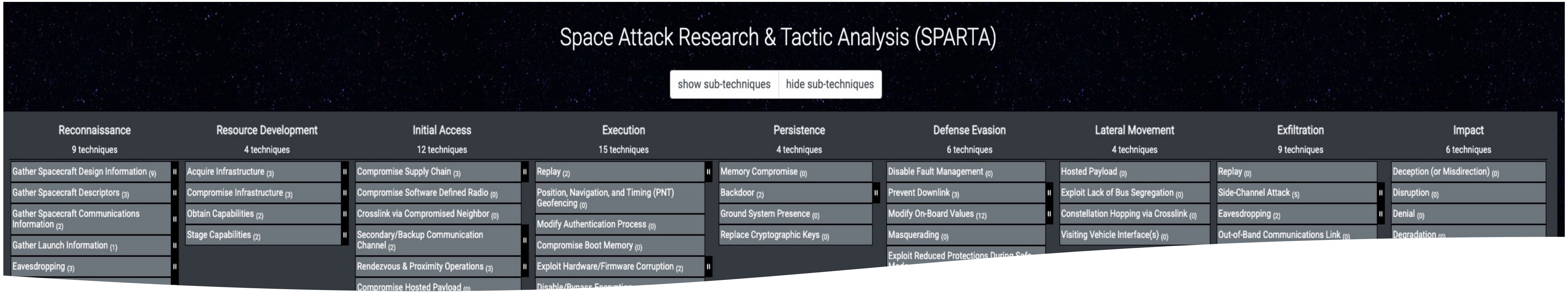
Space Cyber
https://medium.com/the-aerospace-corporation/space-cyber/home

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

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 <u>first-of-its-kind body of knowledge</u> 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, IEEEE 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 V1.4 TTPs=213}
- ~25% increase in the number of countermeasures {V1.0 CMs=69 to V1.4 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

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 |

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 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

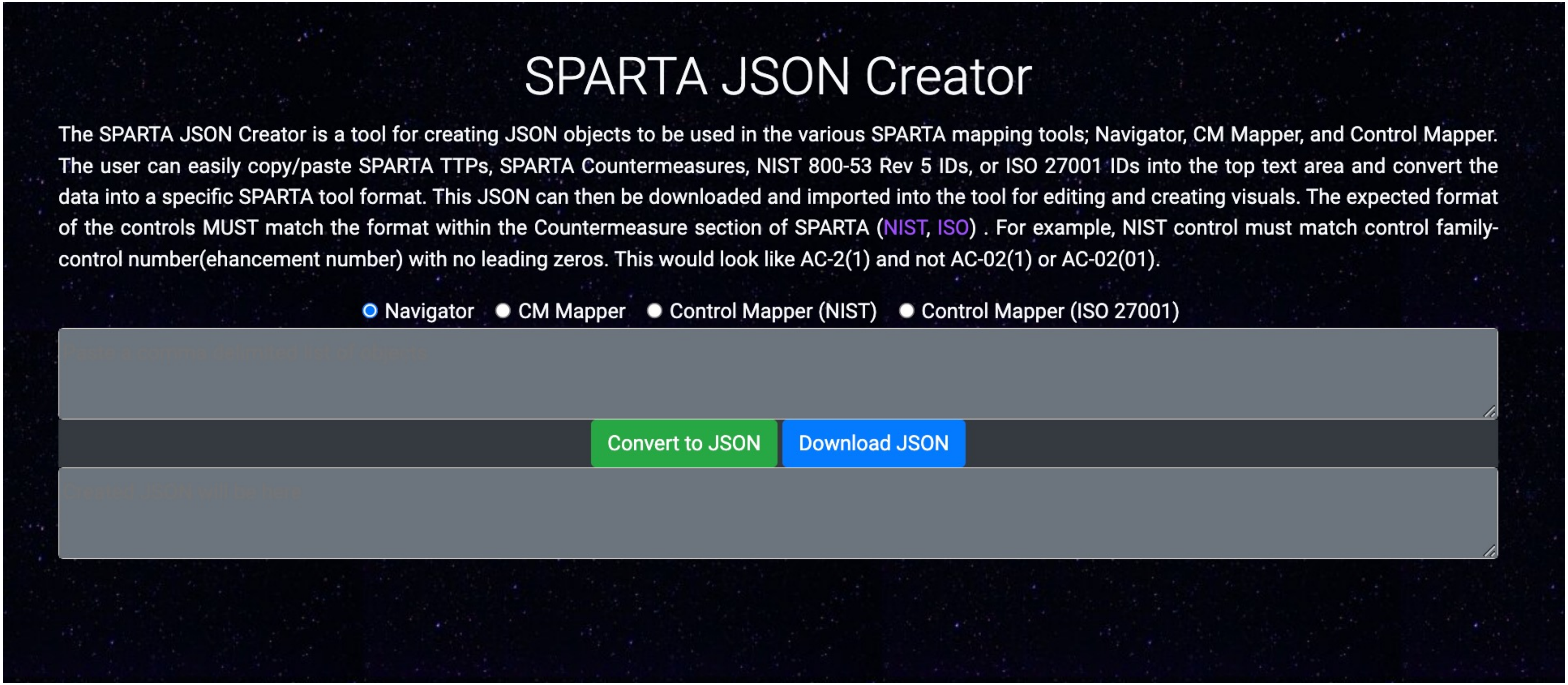
Sub-Techniques

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



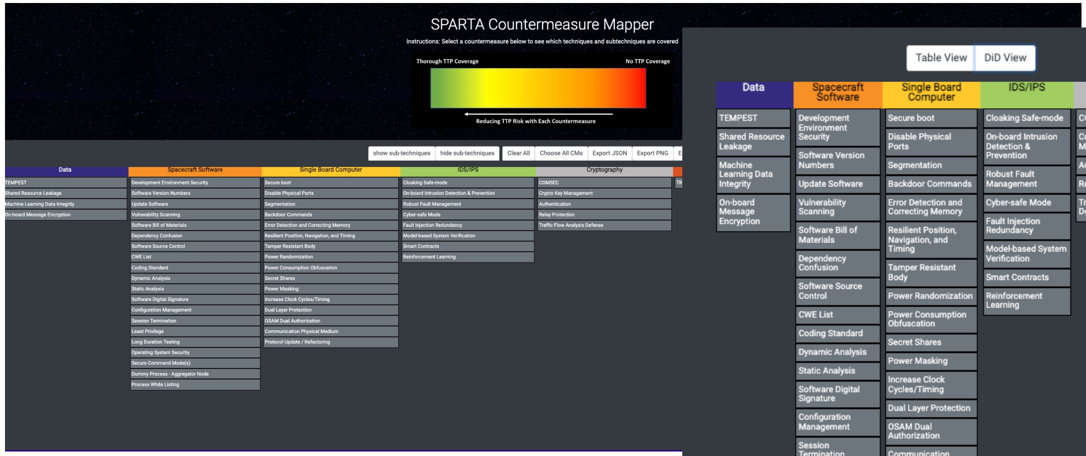
Building Spacecraft Attack Chains using SPARTA

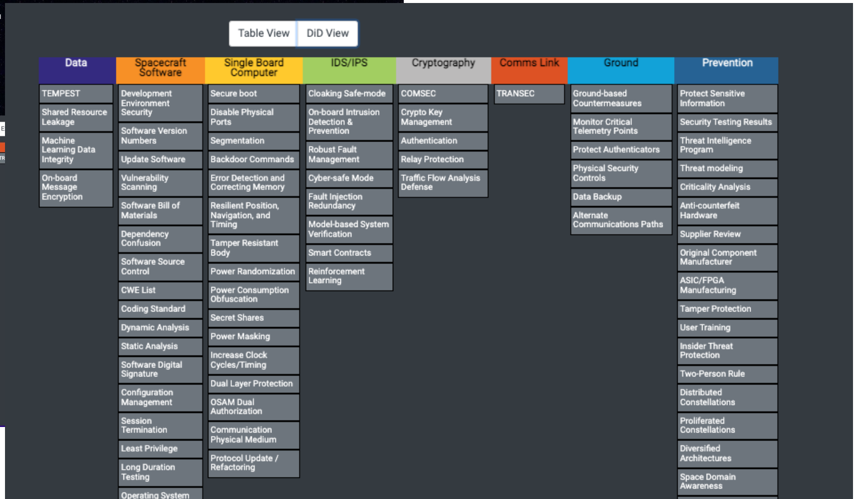
SPACE ATTACK RESEARCH & TACTIC ANALYSIS

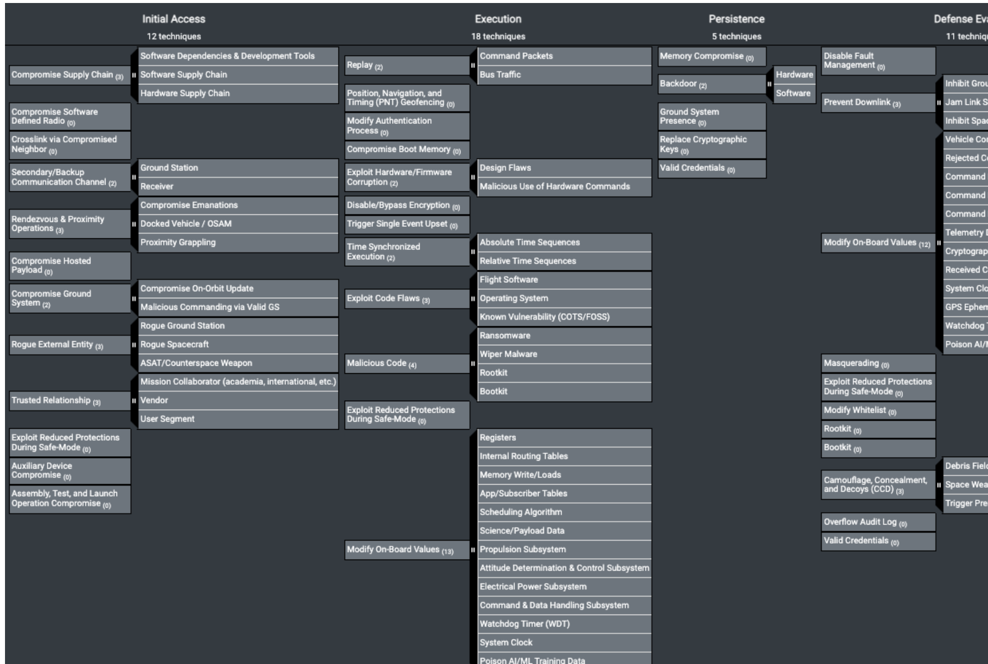
*Attack Chains / Attack Flow != Cyb*er Kill Chain

- 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 Cyb*er 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

SPARTA
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

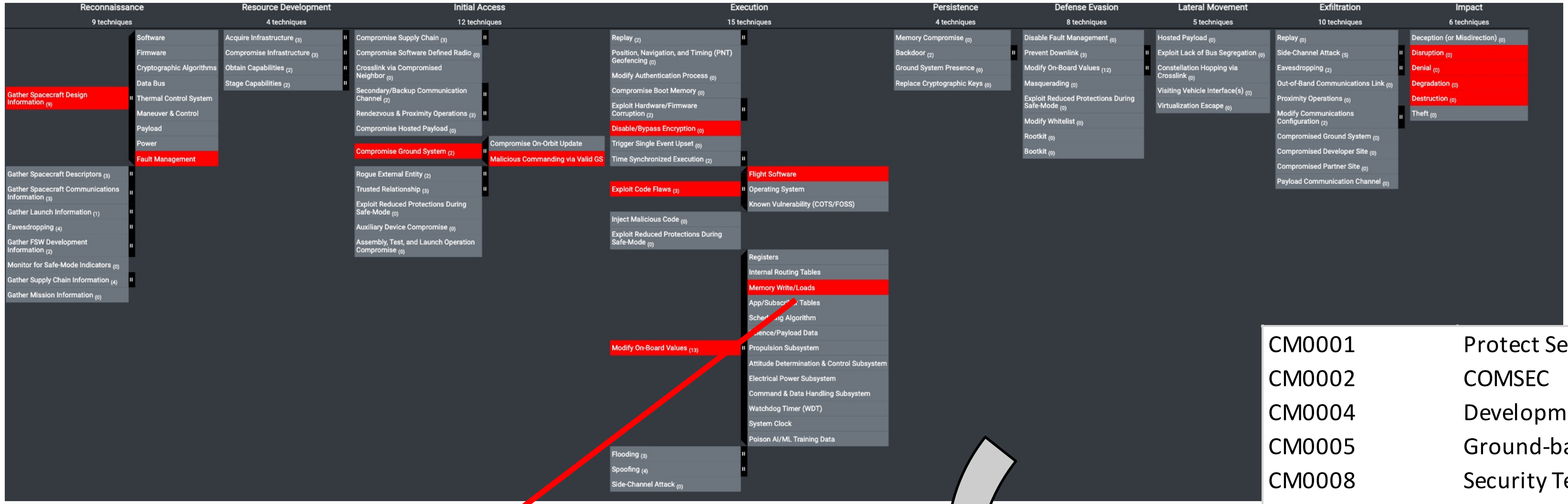
CySat 2023

- ESA OPS-SAT Attack

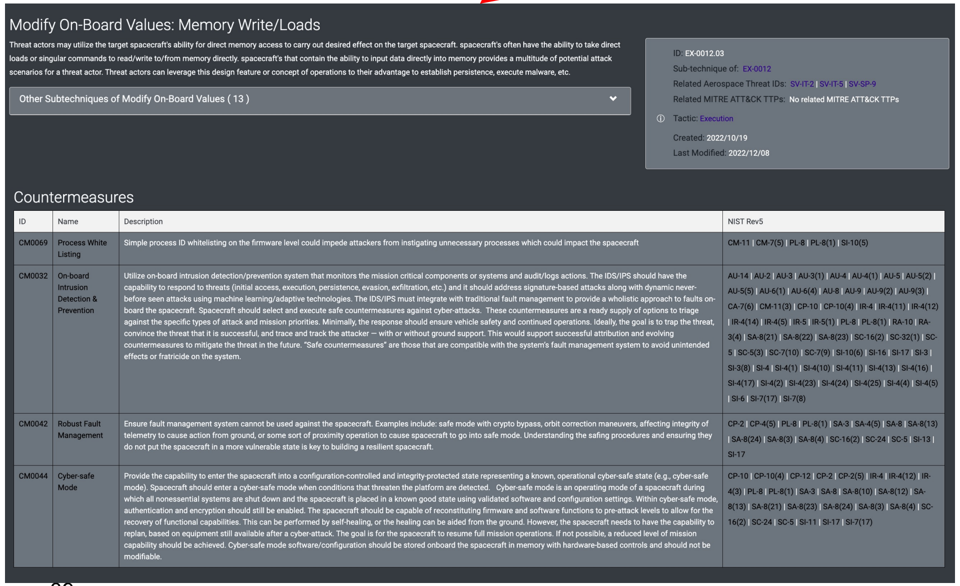
Theoretical Attack Chain in Backup

- PCspooF

Mapping Attack Chain to Countermeasures



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



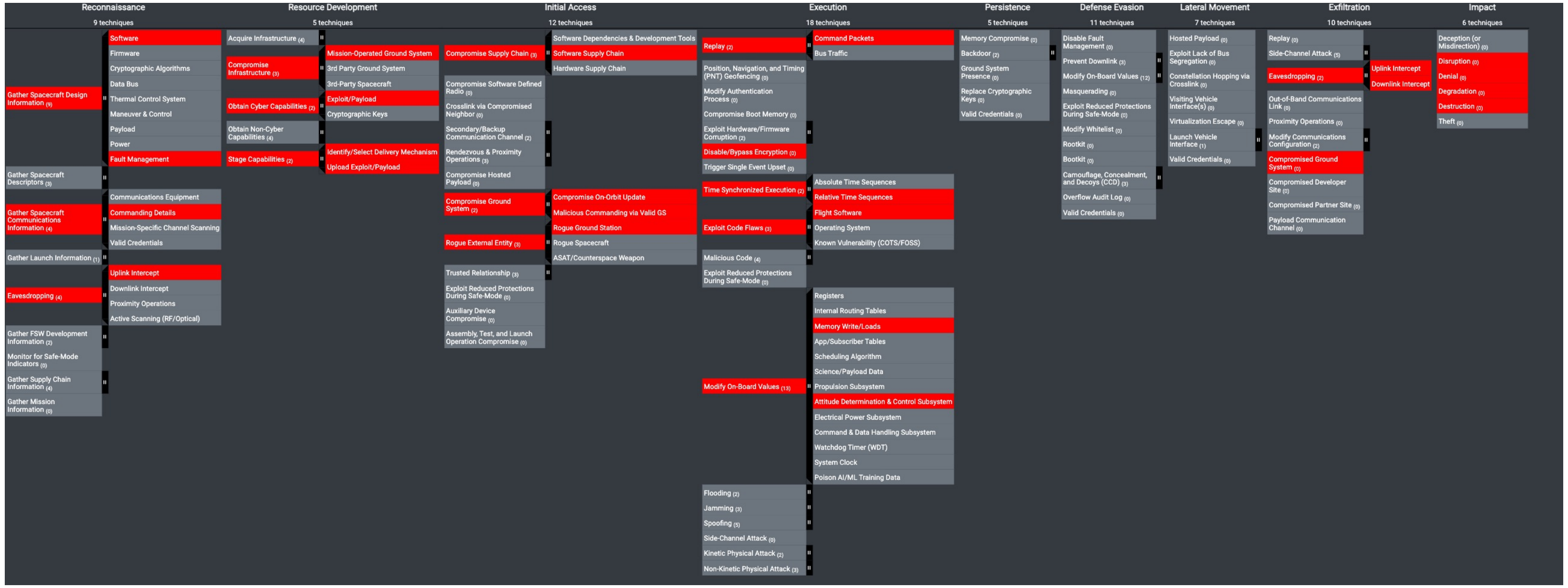
SPARTA has direct mapping from TTP to Countermeasures

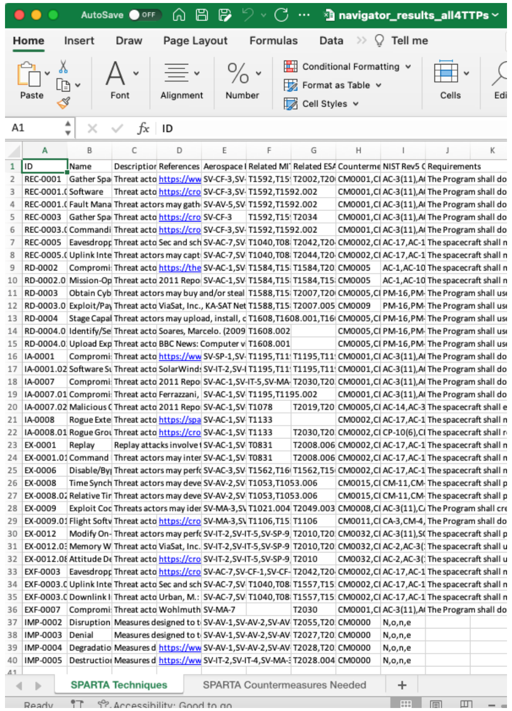
CM0001	Protect Sensitive Information	CM0029	TRANSEC
CM0002	COMSEC	CM0030	Crypto Key Management
CM0004	Development Environment Security	CM0031	Authentication
CM0005	Ground-based Countermeasures	CM0032	On-board Intrusion Detection & Prevention
CM0008	Security Testing Results	CM0033	Relay Protection
CM0010	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

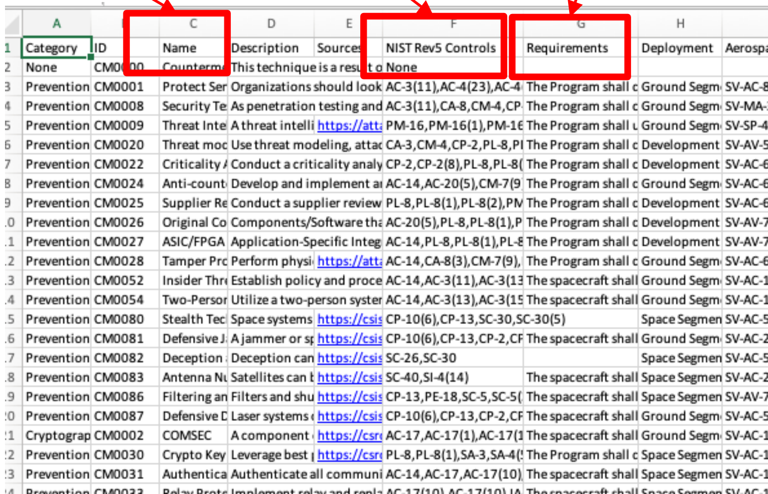
SPARTA Navigator – Extracting Countermeasures / NIST Controls

https://sparta.aerospace.org/navigator





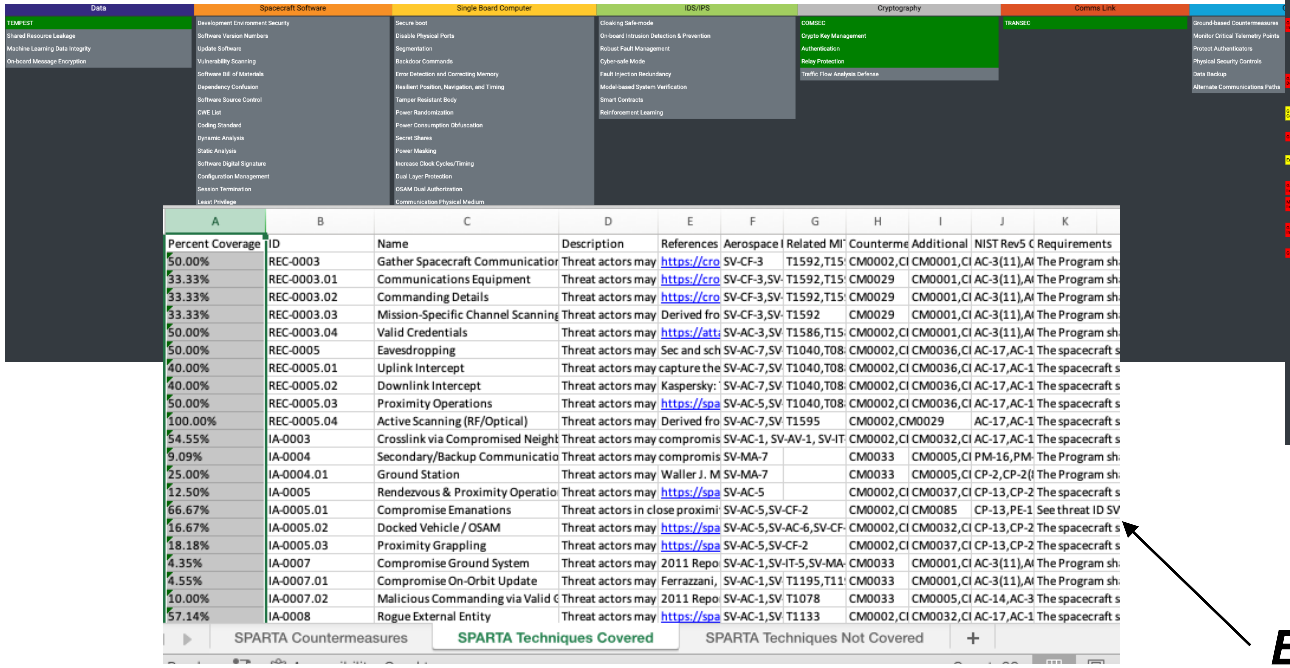
Countermeasure　NIST 800-53　Sample “Shalls”



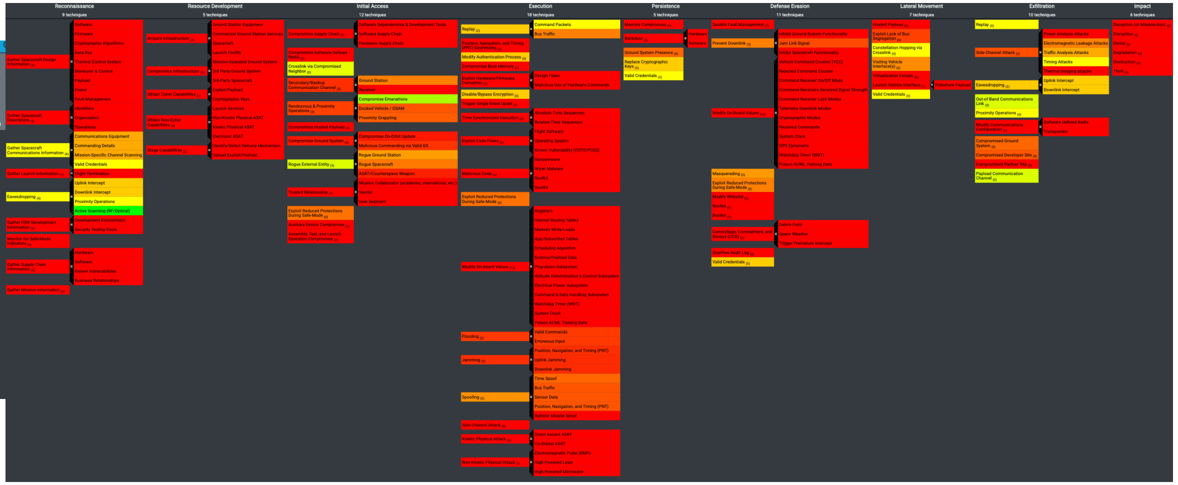
SPARTA Countermeasure Mapper / Defensive Gap Analyzer

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

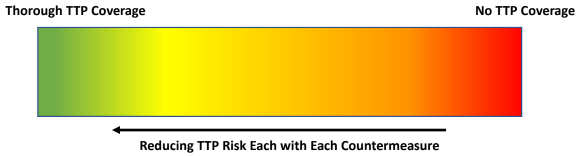
- Attack chains built in SPARTA's navigator can help identify countermeasures against the TTPs used in the attack
  - *Many users do not know TTPs, they only know the countermeasures they have implemented (or plan to)…*
- The SPARTA capability enables a graphical mechanism to select and deselect countermeasures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



A	B	C	D	E	F	G	H	I	J	K
Percent Coverage	ID	Name	Description	References	Aerospace I	Related MI	Counterme	Additional	NIST Rev5 C	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),A	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),A	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),A	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),A	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),A	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,CM0029		AC-17,AC-1	The spacecraft s
54.55%	IA-0003	Crosslink via Compromised Neighb	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 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),A	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),A	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



Control Mapper

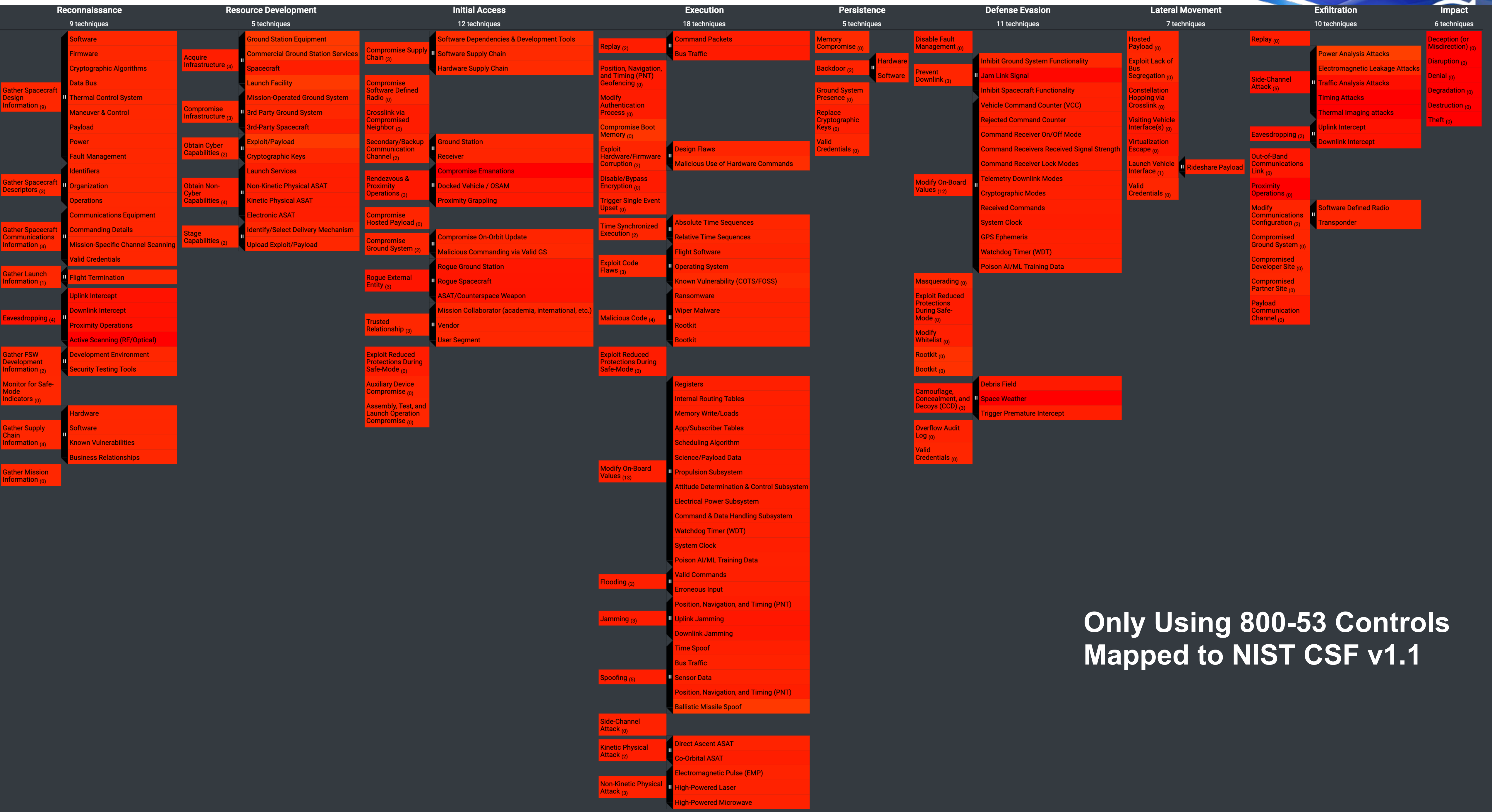
SPARTA Control Mapper

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.

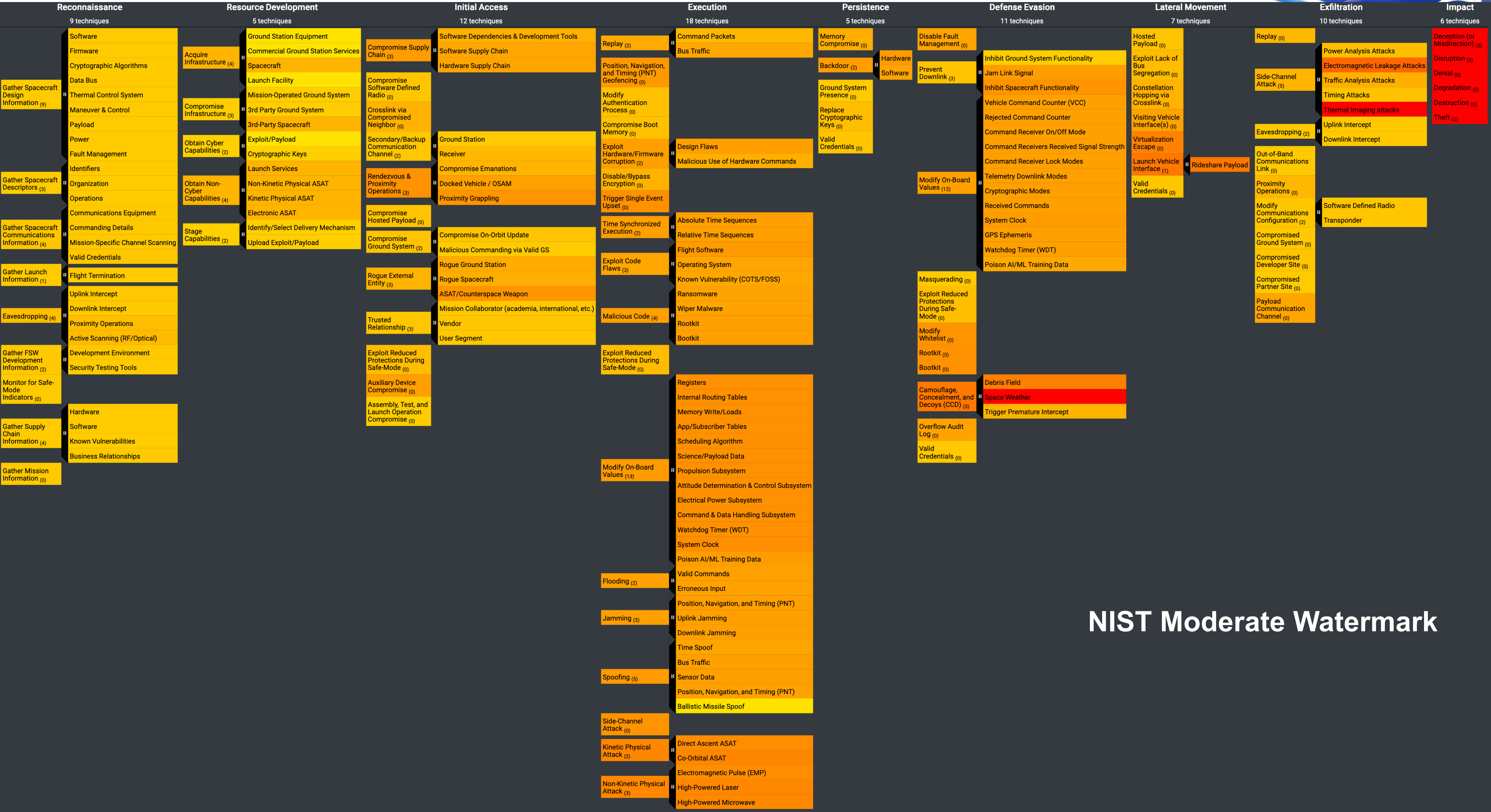
Create New Layer

Open New Layer

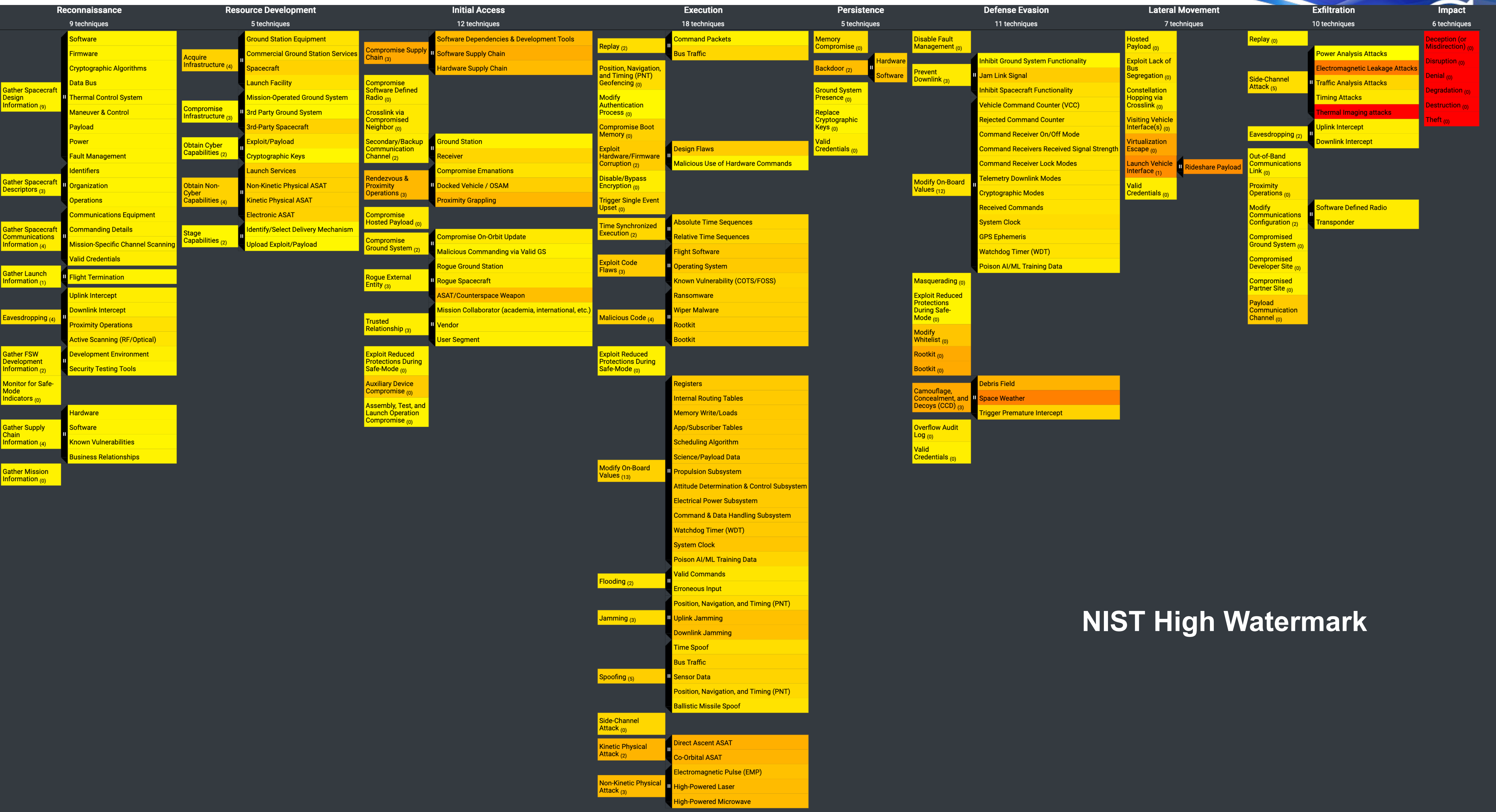
Control Mapper is Good for Comparing NIST 800-53 Control Baselines and their TTP Mitigation



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



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
Modify On-Board Values (12)
Vehicle Command Counter (VCC)
Rejected Command Counter
Command Receiver On/Off Mode
Command Receivers Received Signal Strength
Command Receiver Lock Modes
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)
Side-Channel Attack (5)
Power Analysis Attacks
Electromagnetic Leakage Attacks
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
Modify On-Board Values (12)
Vehicle Command Counter (VCC)
Rejected Command Counter
Command Receiver On/Off Mode
Command Receivers Received Signal Strength
Command Receiver Lock Modes
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)
Side-Channel Attack (5)
Power Analysis Attacks
Electromagnetic Leakage Attacks
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

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
- Modify On-Board Values (12)
  - Vehicle Command Counter (VCC)
  - Rejected Command Counter
  - Command Receiver On/Off Mode
  - Command Receivers Received Signal Strength
  - Command Receiver Lock Modes
  - 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

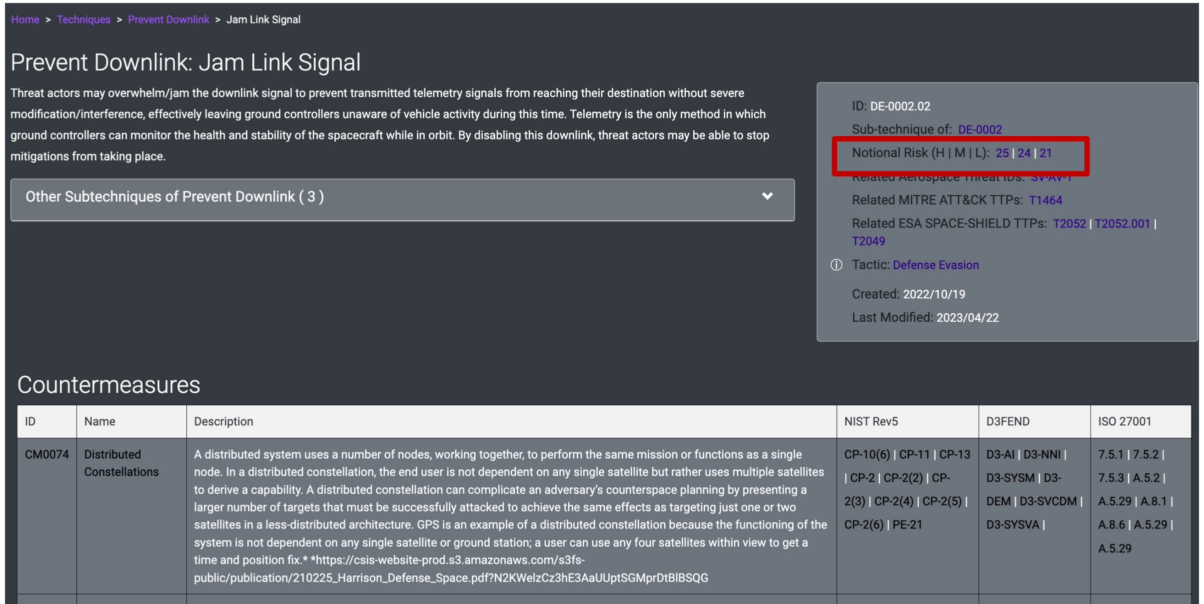
- Replay (0)
- Side-Channel Attack (5)
  - Power Analysis Attacks
  - Electromagnetic Leakage Attacks
  - Traffic Analysis Attacks
  - Timing Attacks
  - Thermal Imaging attacks
- Eavesdropping (2)
  - Uplink Intercept
  - Downlink Intercept
- Out-of-Band Communications Link (0)
- Proximity Operations (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)

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#*



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 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

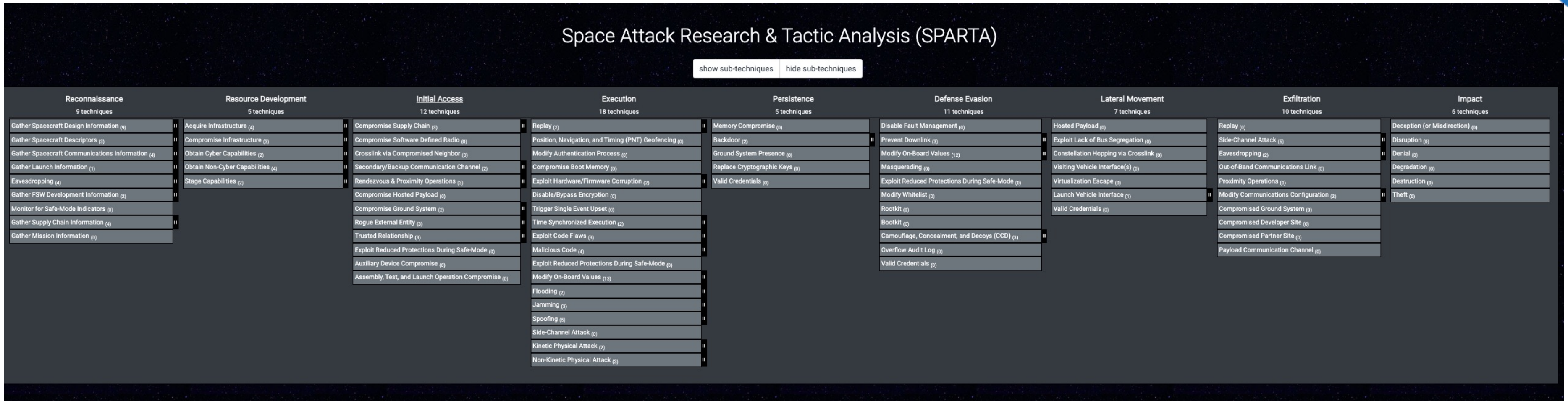
<table>
<tr><th>ID</th><th>Name</th><th>Description</th><th>NIST Rev5</th><th>D3FEND</th><th>ISO 27001</th></tr>
<tr><td>CM0074</td><td>Distributed Constellations</td><td>A distributed system uses a number of nodes, working together, to perform the same mission or functions as a single node. In a distributed 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?N2KWelzCz3hE3AaUUptSGMprDtBIBSQG</td><td>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</td><td>D3-AI | D3-NNI | D3-SYSM | D3-DEM | D3-SVCDM | D3-SYSVA |</td><td>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</td></tr>
</table>

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

SPD-5 Presentation

Brandon Bailey, Senior Project Leader, Cyber Assessments and Research Department, The Aerospace Corporation

Kassandra Vogel, Principal Space Systems Security Architect, Blue Origin

SPACE ISAC

Space Information Sharing and Analysis Center

Space Policy Directive 5 ISAC Task Force

Paper and Path Ahead

SPACE ISAC

SPD-5 High Level

Space Policy Directive 5 (SPD-5) states, "*the United States considers unfettered freedom to operate in space vital to advancing the security, economic prosperity, and scientific knowledge of the Nation…Therefore, it is essential to protect space systems from cyber incidents in order to prevent disruptions to their ability to provide reliable and efficient contributions to the operations of the Nation's critical infrastructure.*"

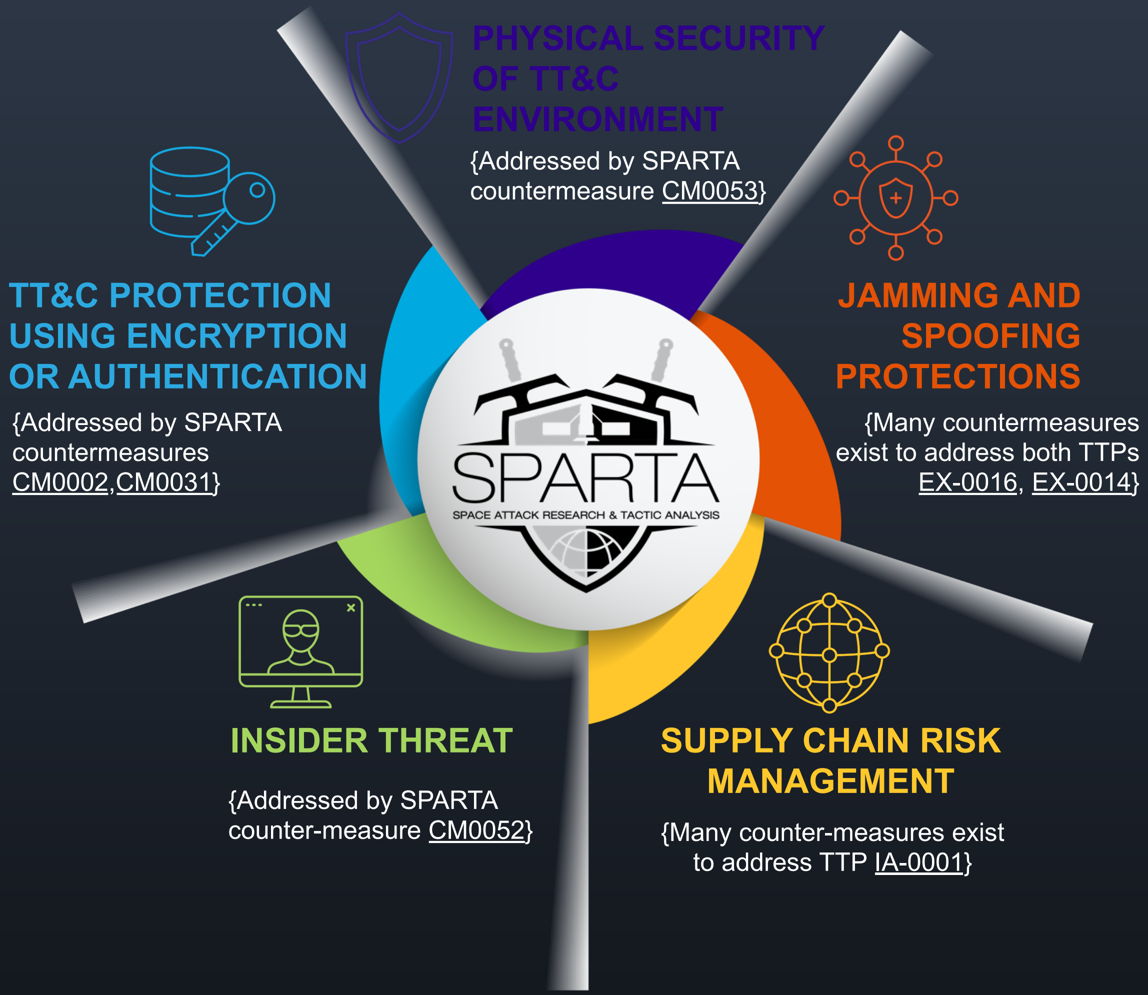
SPD-5 also defines "Space System" as "a combination of systems, to include ground systems, sensor networks, and one or more space vehicles, that provides a space-based service."

It also describes how "*space system owners and operators should collaborate to promote the development of best practices, to the extent permitted by applicable law. They should also share threat, warning, and incident information within the space industry, using venues such as ISAC to the greatest extent possible, consistent with applicable law.*"

SPD 5: Cybersecurity Principles for Space Systems

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

- Space systems should be developed to continuously monitor, anticipate, and adapt to mitigate evolving malicious cyber activities that could manipulate, deny, degrade, disrupt, destroy, surveil, or eavesdrop on space system operations.
- Space system configurations should be resourced and actively managed to achieve and maintain an effective and resilient cyber survivability posture throughout the space
- Space system owners and operators should develop and implement cybersecurity plans for their space systems that incorporate capabilities to ensure operators or automated control center systems can retain or recover positive control of space vehicles



SPD-5 Work at ISAC

Space ISAC Members have led several initiatives to review, implement, and provide suggestions for SPD-5

- Performed a survey across membership base on standards being used
- The Aerospace Corporation published a quick look at SPD-5 in October 2020 and later, in 2021, Members of the Space ISAC also published implementation suggestions for SPD- 5 in a published white paper.
- Originally, Space ISAC put together a working group to discuss and develop implementation guidance for SPD-5.
    - While there was no formal deliverable produced by that working group, the need for best practice publication persists and the responsibility falls within the newly formed SPD-5 Task Force
- First draft of initial deliverable from SPD-5 Task Force has been published and sent to White House Office of the National Cyber Director (ONCD) – discussed on subsequent slides

SPD-5 Gaps…Does Not

- Address key elements of the space ecosystem such as launch, manufacturing, and crewed vehicles
- Account for the full cyber threat landscape as it relates to the space threat environment across legacy and new developments
- Account for emerging space capabilities such as lunar permanence or cislunar-and-beyond missions
- Acknowledge the gap in space-specific best practices that enable space protection concepts and does not offer a perspective regarding the lack of space-qualified cybersecurity and security- enabled technologies
  - Simply following industry best practices, as the policy states, implies there are well established cyber best practices for the space industry
- Have any enforcement elements
- Acknowledge lack of space-qualified cybersecurity technologies {low TRL}
- Address intersection of safety and security needs which would provide valuable context to the protection principles, which could be accomplished by a companion set of threat informed cybersecurity best practices to aid practitioners with the implementation of The Directive.

Threat Informed Covering All Segments/Phases

- Recommended that Space ISAC constructs best practices using the following organization. Supply chain considerations span all elements of the lifecycle and segments of a space system.

	Space System Lifecycle	Space System Segment			
		Ground	Link	Space	User
Supply Chain	Acquisition	x	x	x	x
	Design	x	x	x	x
	Prelaunch/Manufacturing/ Development	x	x	x	x
	Launch	x	x	x	x
	Orbit/Operations/On Orbit Servicing Assembly Manufacturing (OSAM) (Includes updates/dev/on-orbit servicing)	x	x	x	x
	Decommission	x		x	x

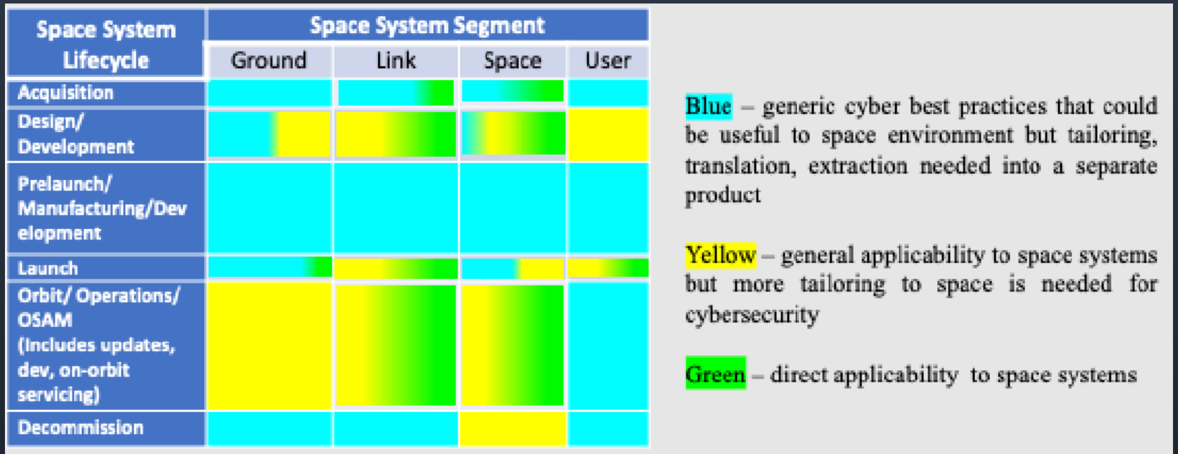
- This concept translates to providing best practices on design and development of the ground, space, link, and user segments

- Using threat and tactics, techniques, and procedures (TTPs) to drive best practice development should ensure the best practices are motivated by necessity and not compliance with a regulation or standard that typically trails the threat landscape. { ATT&CK and SPARTA can help here }

- Must address verification and validation of security implementations. Not a checklist exercise!! Must have demonstratable evidence

Threat Informed Covering All Segments/Phases

- A summary graphic was created to articulate the current state of cybersecurity best practices and standards across the lifecycle

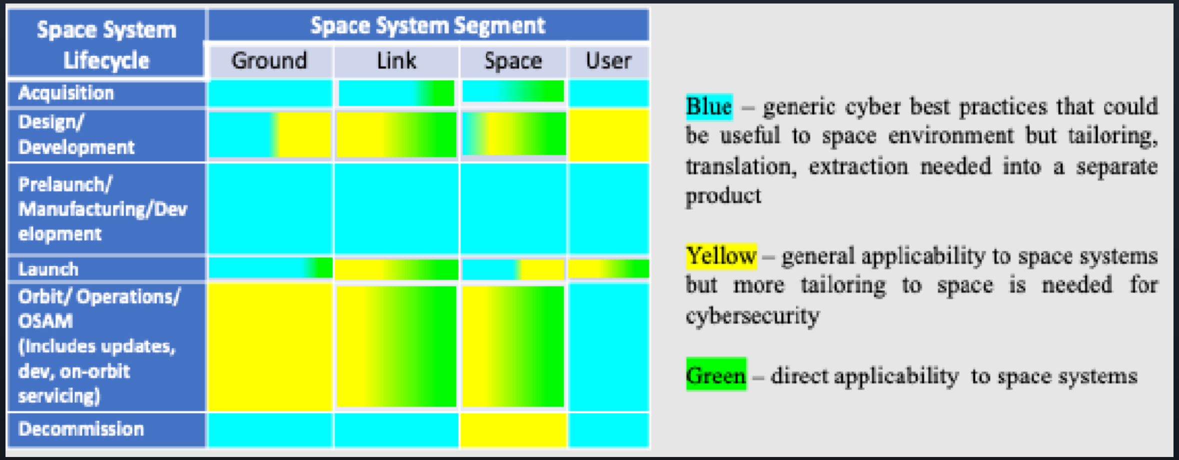


- Space ISAC community to define the top 5-10 threats with a focus on mitigation techniques as the first step for the SPD-5 Task Force
  - Translating the thousands of pages of existing guidance using threats and TTPs as the catalyst into manageable guidance, which will greatly benefit the space industry

- Breaking the problem down into increments across the lifecycle and segment ensures the problem is more manageable vice treating as a monolithic cyber black box.
  - Leverage community to ensure best practices are realistic

Future Work

- Update initial ONCD deliverable based on feedback
- Increase participation in SPD-5 Task Force – Come Join Us!!!
- Establish top 5-10 threats/TTPs to drive countermeasures / best practices development
  - Must consider legacy vs new development, enforcement, cost, etc.
  - Iterate, rinse, repeat – will need to continue until all phases, segments are covered adequately
- Want to turn this graphic to be greener over time!
  - Generic guidance must be tailored with space considerations
    - Threats/TTP and risk driven



Discussion

Comments

Questions

SPACE ISAC

VALUE OF SPACE SUMMIT 2023

Co-hosted by AEROSPACE

KRATOS®
READY FOR WHAT'S NEXT™

Networking Reception and Star Party

Where: 3650 N Nevada Ave.

When: 7:00PM MT

William Murtagh, Program Coordinator, National Oceanic and Atmospheric Administration (NOAA) Space Weather Prediction Center (SWPC)

Bob Rutledge, Principal Director, Space Science Applications Laboratory, The Aerospace Corporation

Dr. Delores Knipp, Research Professor, Smead Aerospace Engineering Sciences Dept, University of Colorado Boulder

Dr. John Noto, Chief Scientist, Orion Space Solutions

Space Environment and Space Weather

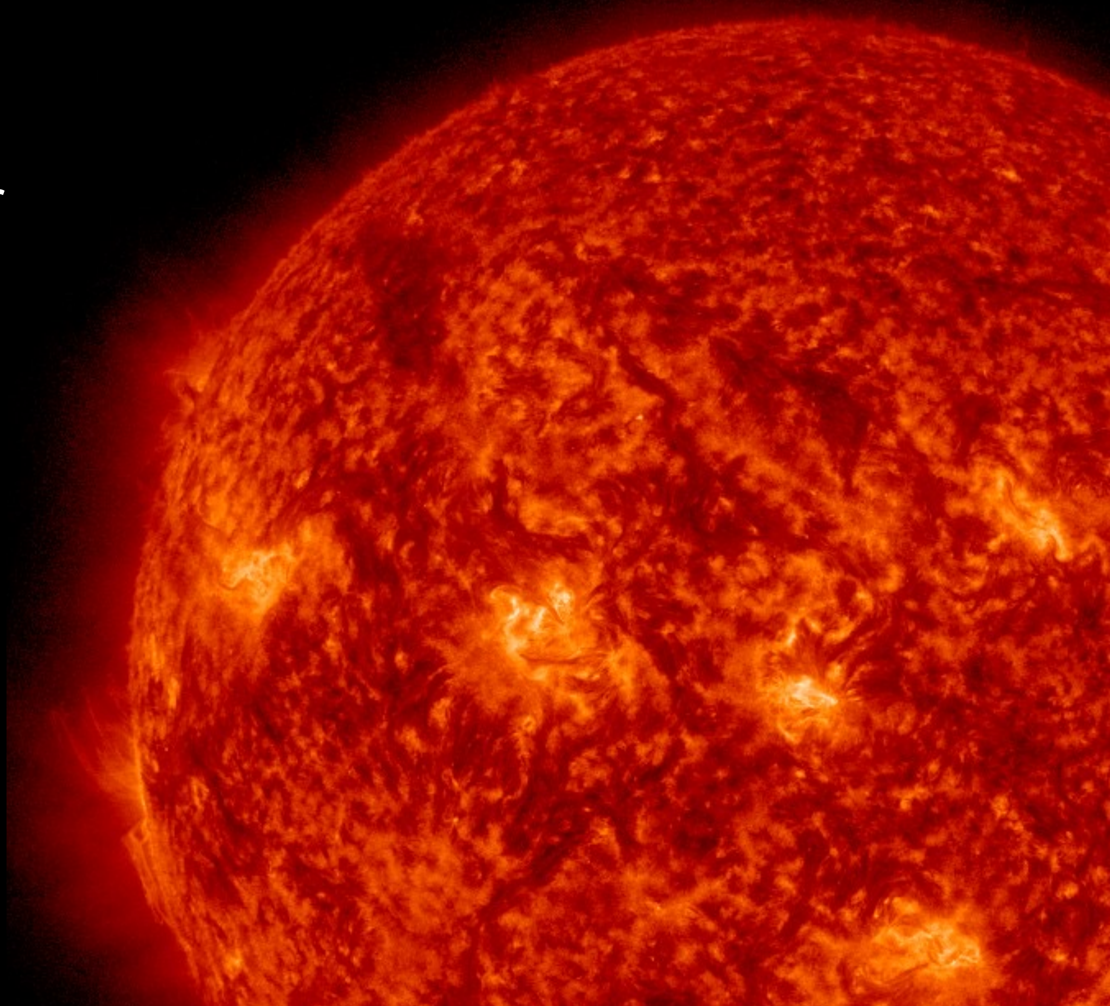
Space Weather and the Space Environment

Bill Murtagh, NOAA Space Weather Prediction Center

Bob Rutledge, Director, Space Science Department,
Aerospace Corporation

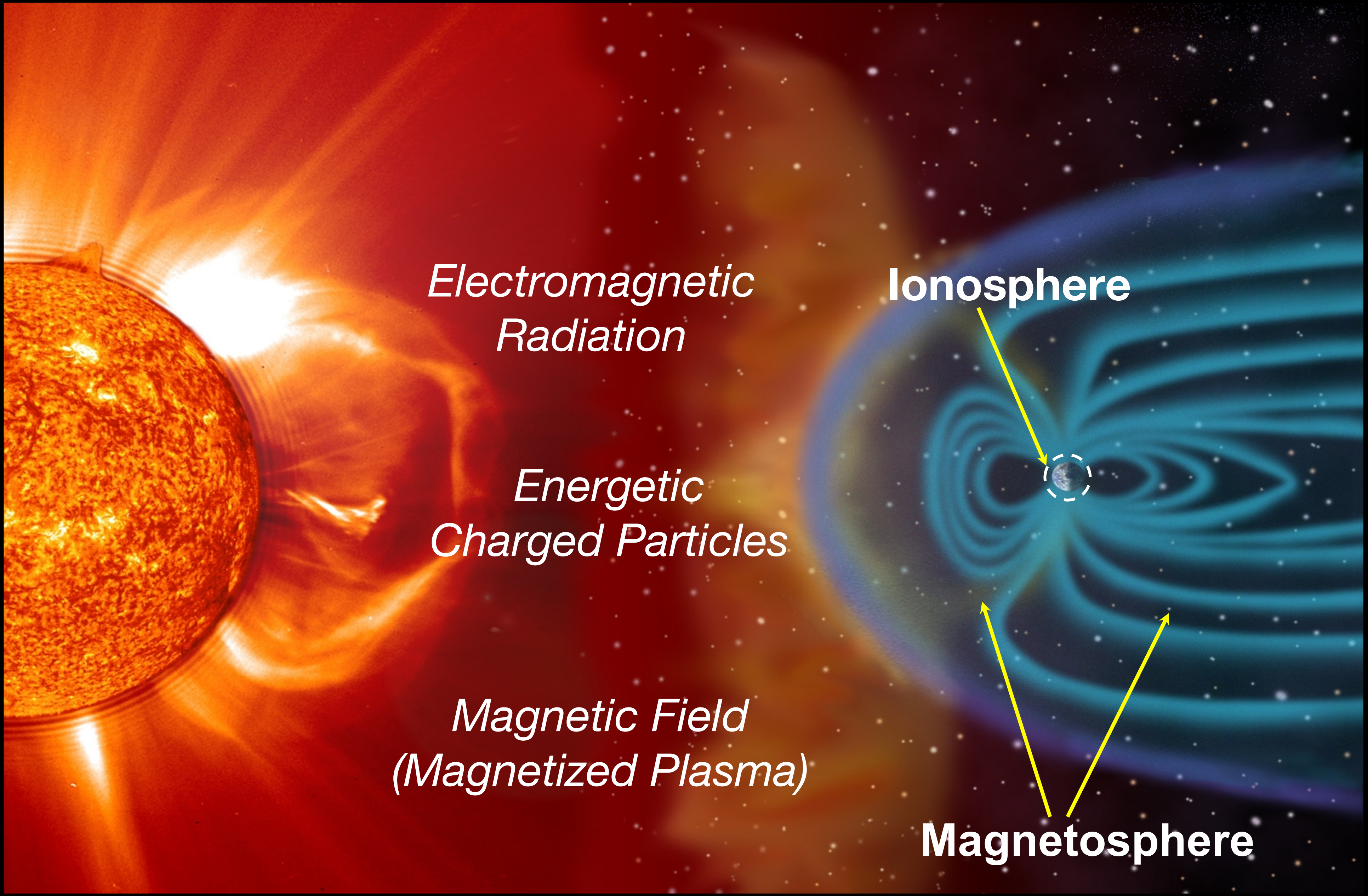
Dr. Delores Knipp, Research Professor, Smead
Aerospace Engineering Sciences Dept, CU

Dr. John Noto, Chief Scientist, Orion Space Solutions



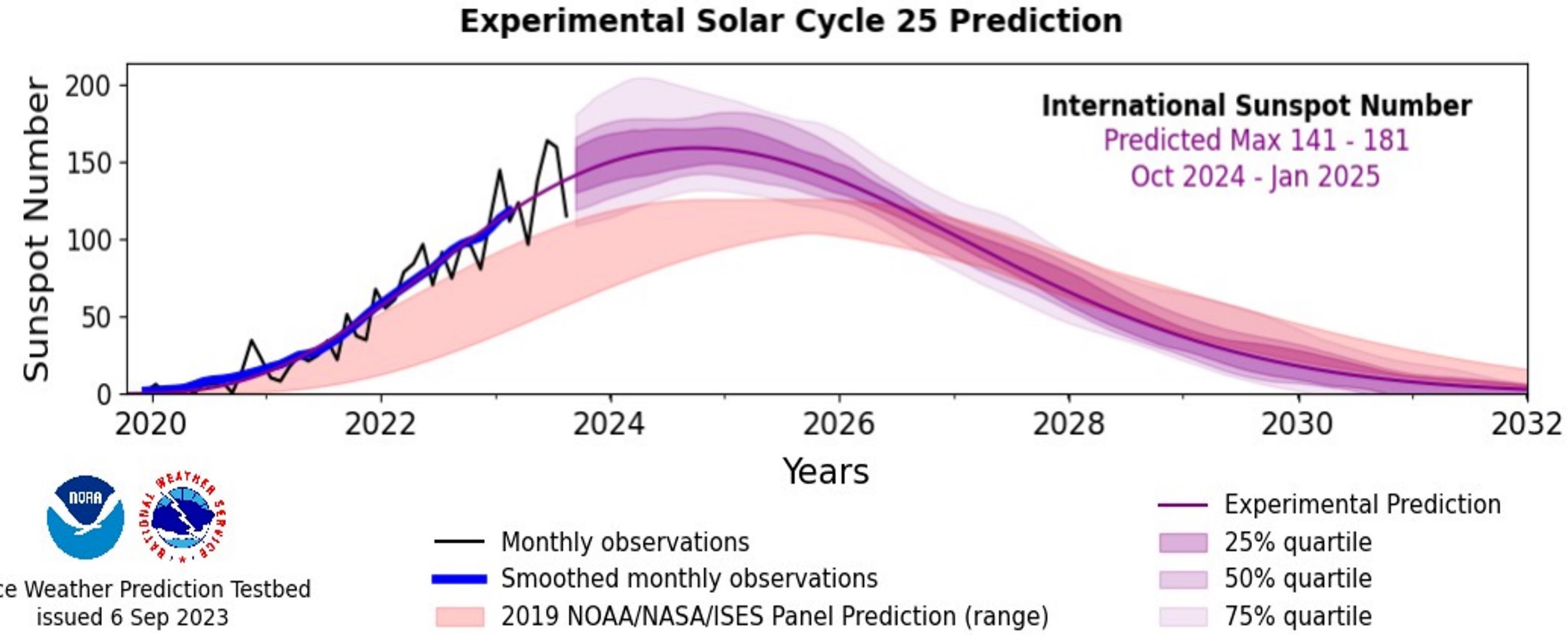
Space ISAC Value of Space Summit
17 Oct 2023

Key drivers of space weather

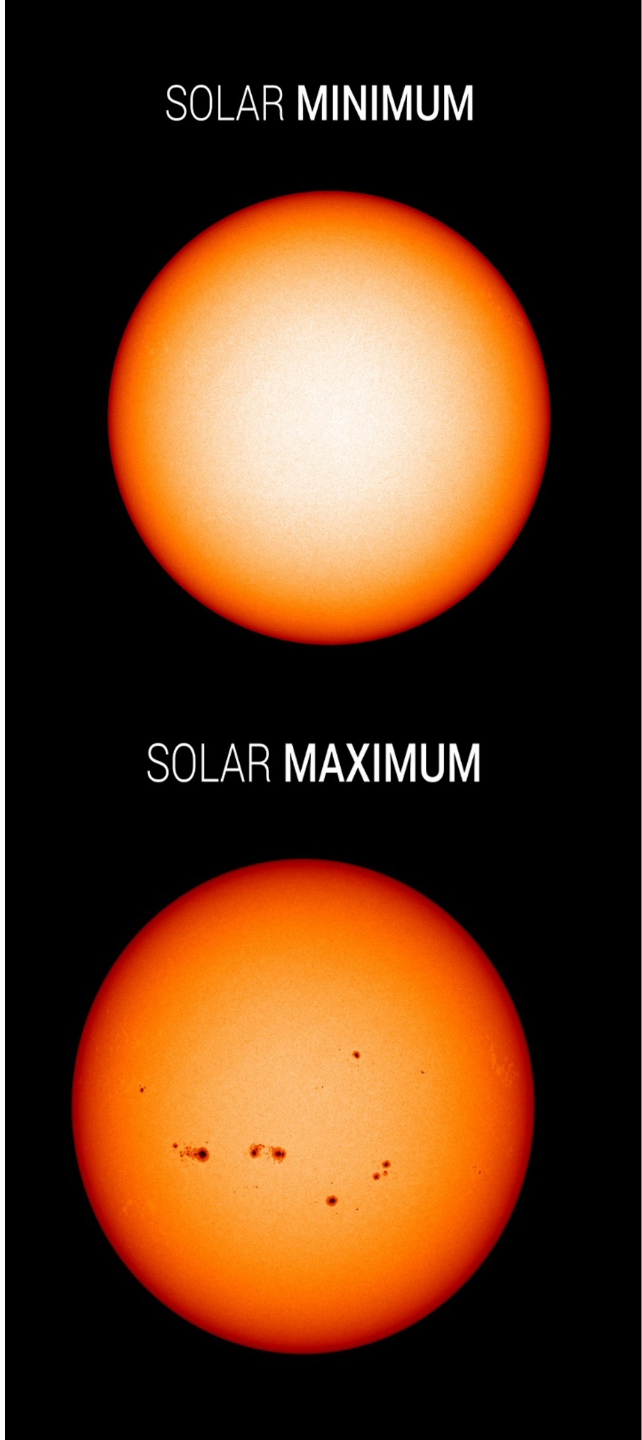


Solar Cycle

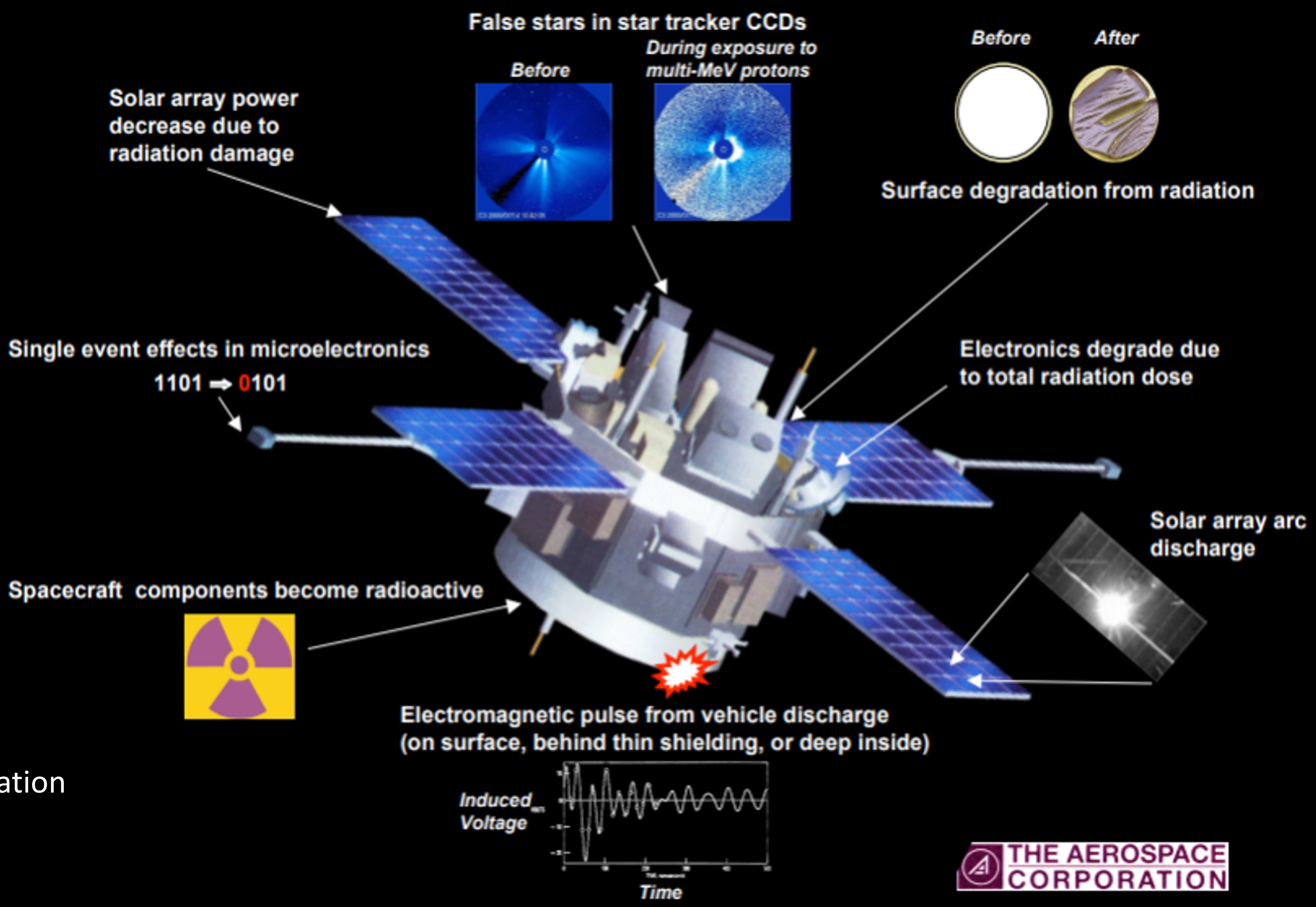
Approaching Solar Maximum



Space Weather Prediction Testbed
issued 6 Sep 2023



Space weather impacts on Satellites



Signal degradation

Satellite drag

The Sun: Jammer, Spoofer, Data Denier

Graphic created for August 1972 event
Courtesy Australian Broadcasting Corp, Used with Permission

Delores Knipp

Smead Aerospace Engineering Science

Space Weather Technology Research & Education Center

University of Colorado Boulder

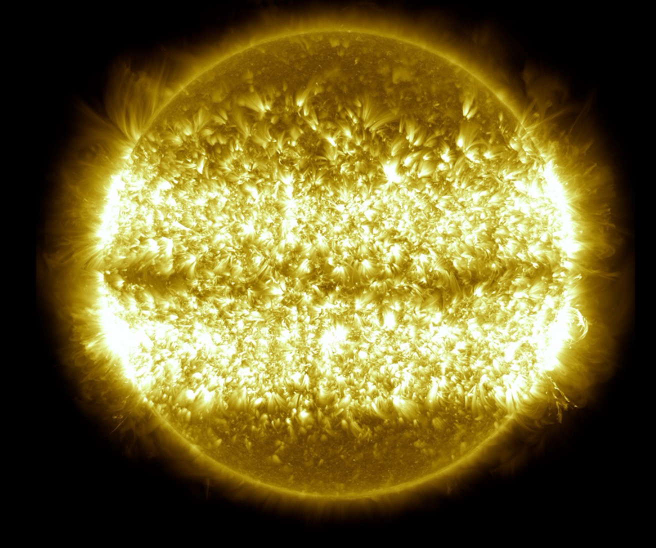
Space ISAC
17 October 2023

SWx TREC

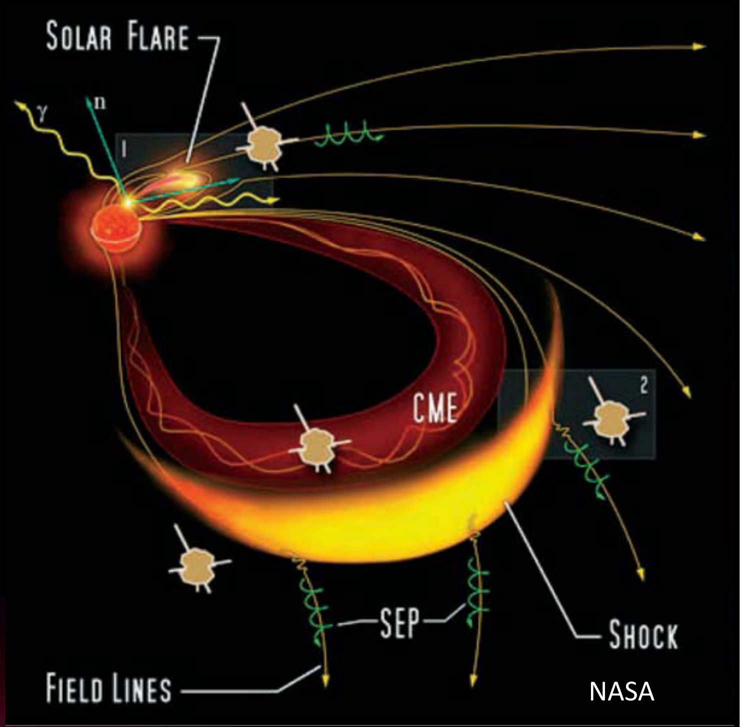
Supported by AFOSR, NASA & NSF

The Sun: Magnetically Active Star

10 Years of Solar Active Regions from SDO



Credit NASA SDO



NASA

Credit NASA ISS

- **Mostly well-behaved local star**

- **Periodically bristles with:**
  - Sunspots/Magnetic Active Regions
    - Flares
    - Solar Energetic Particles
    - Coronal Mass Ejecta

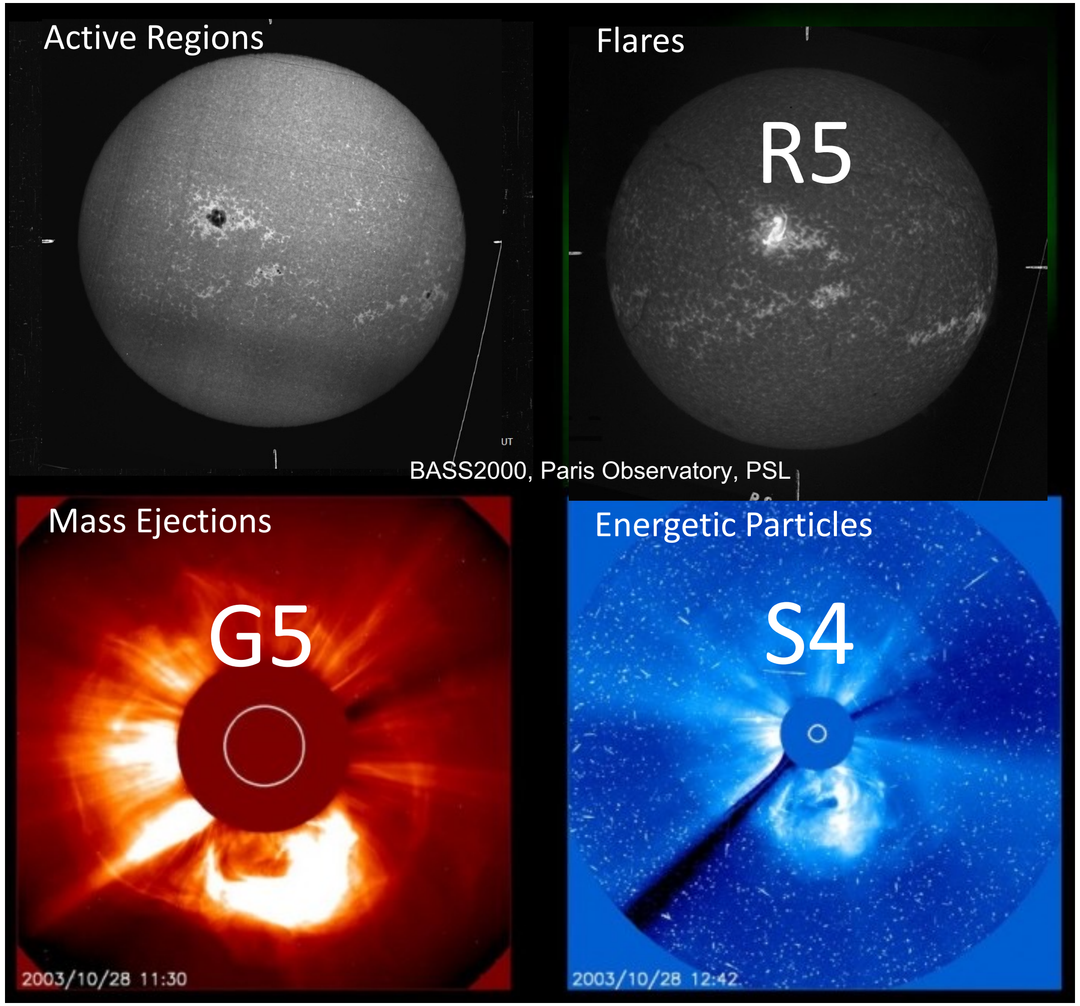
- **The results: Space Weather**
  - **R**adio/Comms/GNSS Challenges
  - Radiations **S**torms
  - **G**eomagnetic Storms

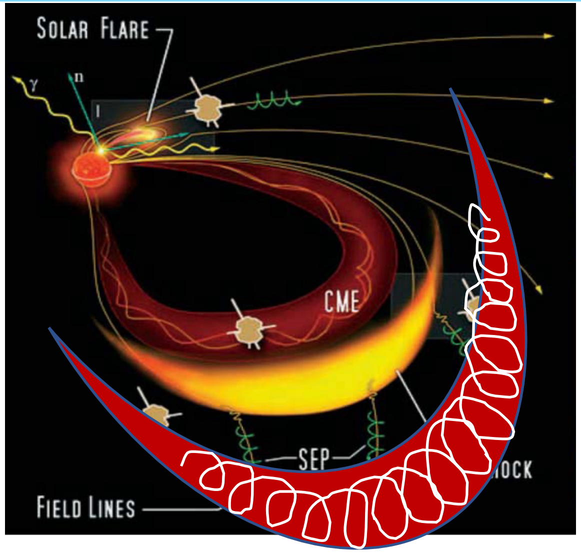
  - Beautiful Aurora

  - R/S/G scales 1-5

Sun: Jammer, Spoofer, Data Denier

August 4 1972



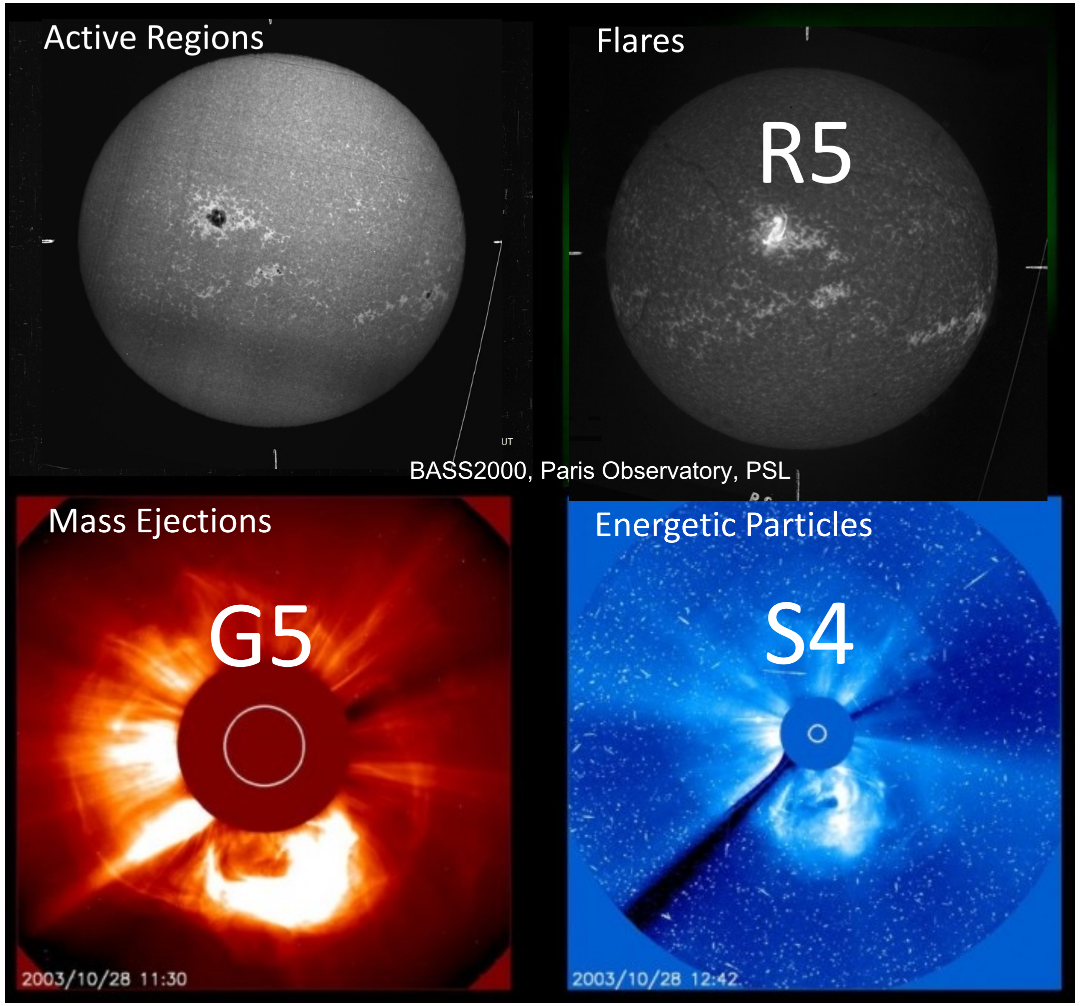


- Multiple flares and ejecta from “delta’ sunspot
  - Flare saturated new Navy solar detectors
  - Radio burst 100 x background @1 GHz
  - HF frequency communications not possible
  - VLF frequency comms greatly disturbed

- Fast Interacting Ejecta
- Extreme Solar Energetic Particle (SEP) event
  - Particles trapped between converging shocks
  - Space based detectors & solar panels swamped

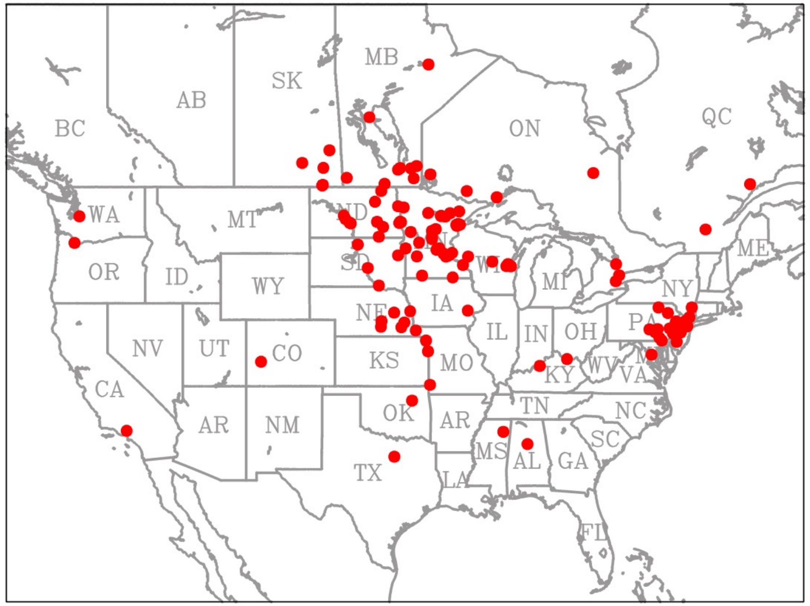
Sun: Jammer, Spoofer, Data Denier

August 4 1972



- **Early ejecta cleared path for following ejecta**
  - **Subsequent interacting ejecta**
  - **~2300 km/s speeds (fastest recorded)**
  - **~ Mach 10**
- **Extraordinary compression of geomagnetic field**
  - **Excited Currents Particles, E&M Waves**

(b) August 1972 power–grid anomalies

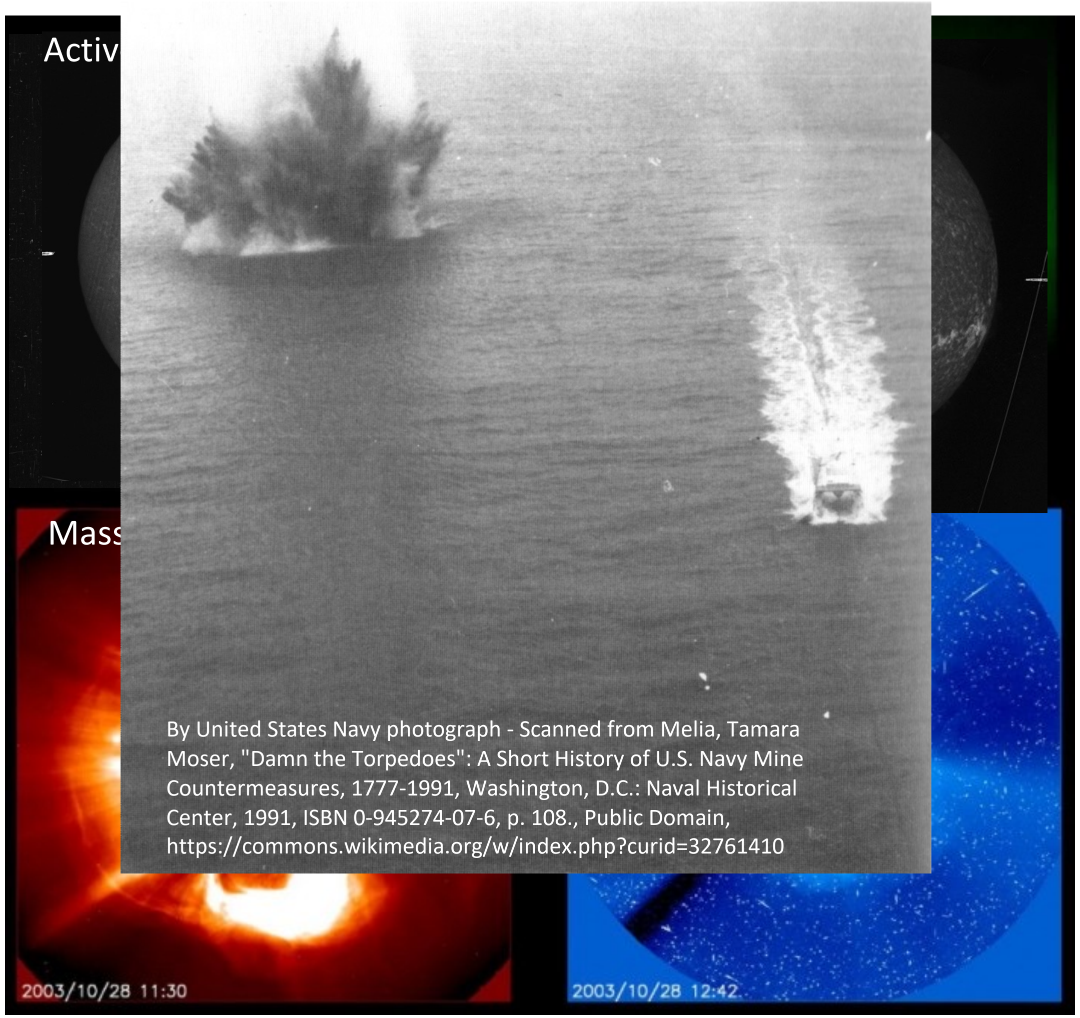


Long distance comm lines failed

Love (2022)

Sun: Jammer, Spoofer, Data Denier

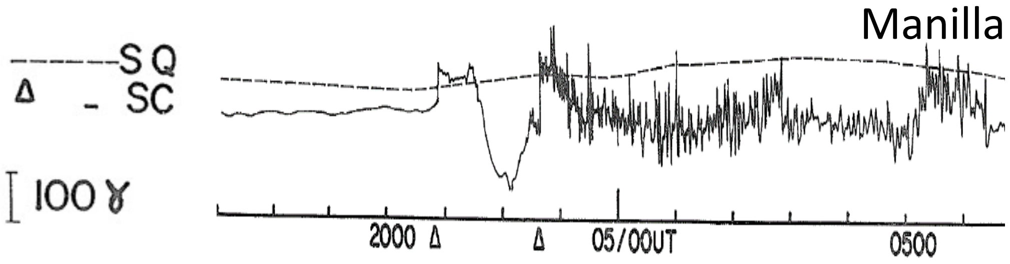
August 4 1972



By United States Navy photograph - Scanned from Melia, Tamara Moser, "Damn the Torpedoes": A Short History of U.S. Navy Mine Countermeasures, 1777-1991, Washington, D.C.: Naval Historical Center, 1991, ISBN 0-945274-07-6, p. 108., Public Domain, https://commons.wikimedia.org/w/index.php?curid=32761410

- **Extraordinary compression of geomagnetic field**
  - **Excited Currents Particles, E&M Waves**

"… the Haiphong Destructor (mine) Field was actually swept by a solar magnetic storm in August of 1972." Hartmann & Truver (1991)

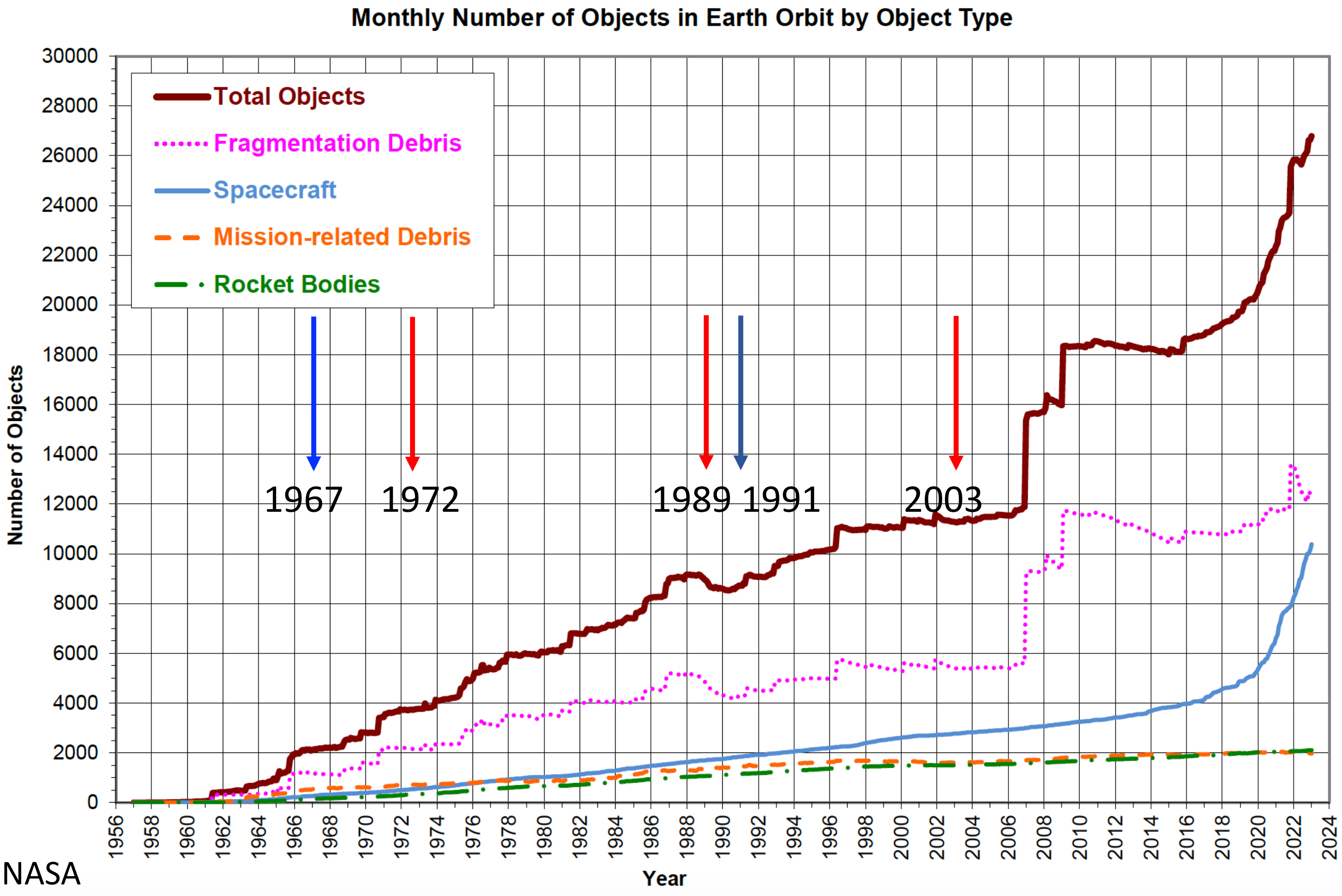


"..a series of extremely strong solar flares caused a fluctuation of the magnetic fields, in and around, Southeast Asia. The resulting chain of events caused the premature detonation of over 4,000 magnetically sensitive DSTs (Destructor mines)" Gonzales, https://www.angelo.edu/content/files/21974-a

•Knipp, D. J., et al. (2018), Space Weather, 16. https://doi.org/10.1029/2018SW002024

Today if the Sun Goes REALLY Rogue: What Gives Me Pause?

Objects Including Debris

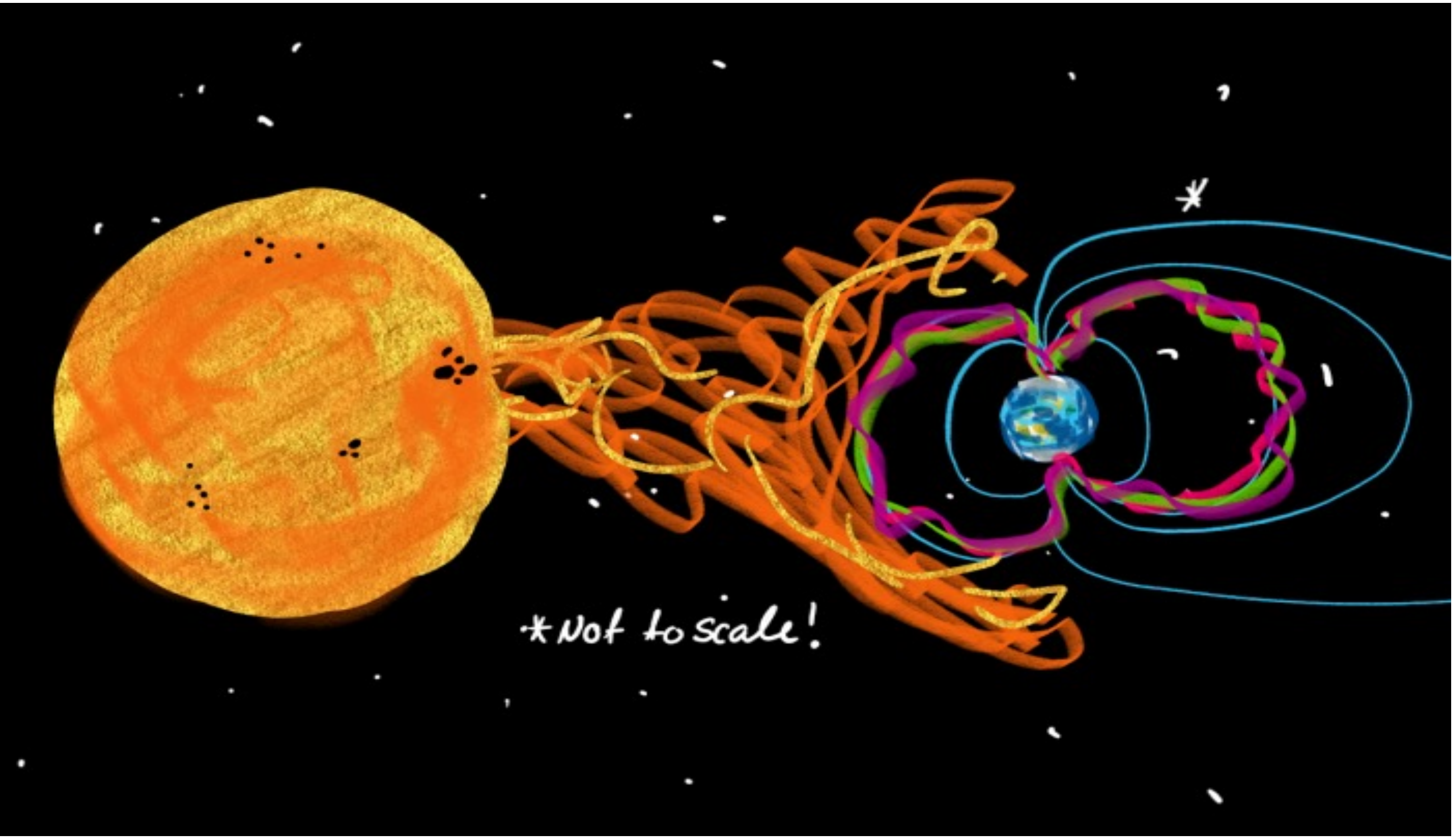


NASA

Spacecraft Orbiting Earth

- Vast majority in Low Earth Orbit (LEO)
- Arrows
  - Publicly known events where catalog had to be 'reassembled' due to Space Weather event
- Monitored by USAF/USSF as Catalog of Resident Space Objects
  - Position & Track
- Growing debris field
- Spacecraft # increase in late 2000's due to satellite constellations
- 20 years since last widely acknowledged catalog event

The Sun: Jammer, Spoofer, Data Denier



Graphic created for August 1972 event
Courtesy Australian Broadcasting Corp, Used with Permission

What is the Sun capable of in today's electronically reliant world?

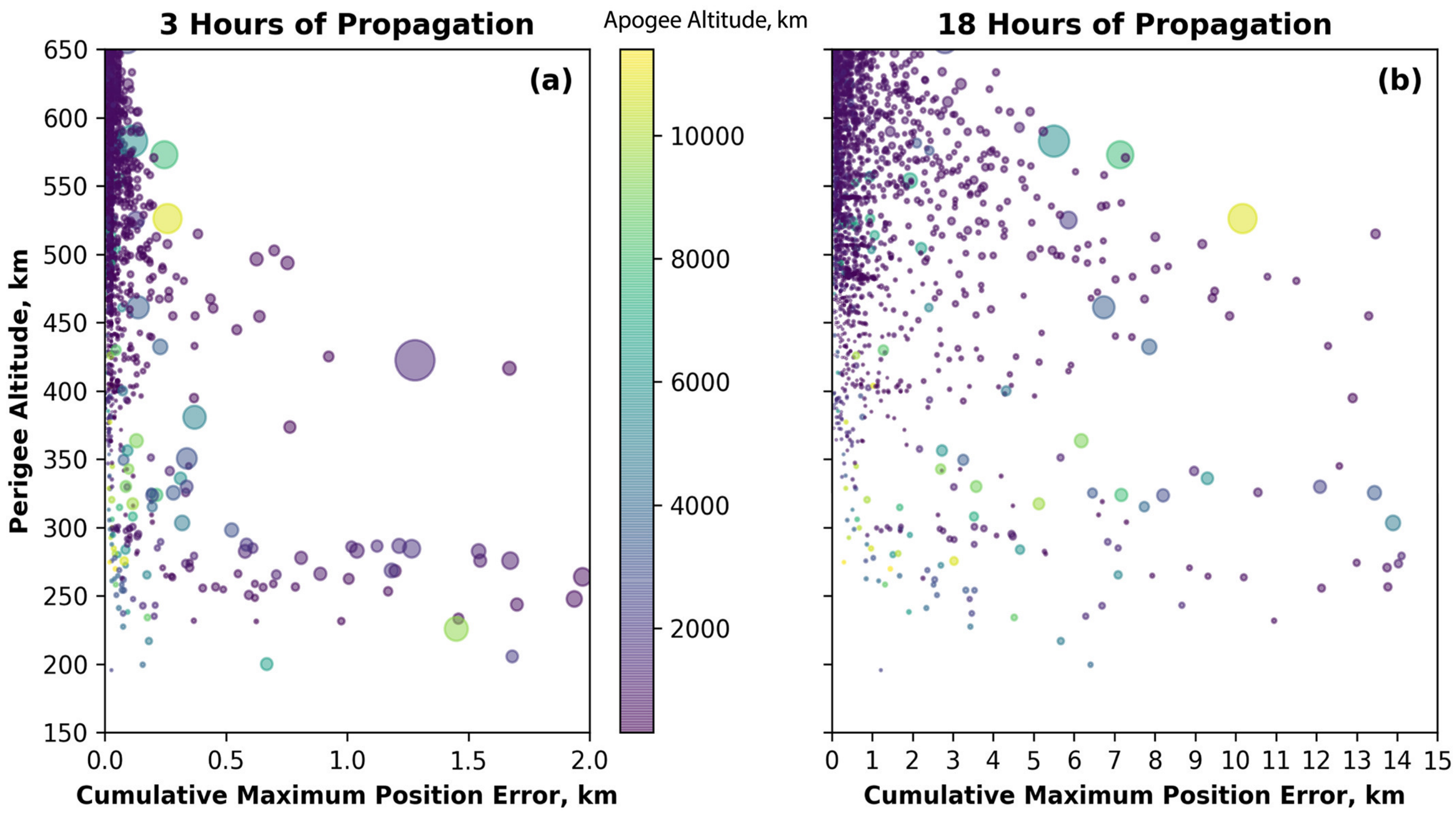
How much notice?

Could adversaries take advantage of data denial, jamming, satellite tracking issues?

SWx TREC

Backup

Congested LEO/Space Catalog Transition



Berger et al. (2020) SWE Journal

,

Satellites big and small

Position errors in the 10’s km range for **moderate** space weather

Limited operator experience with big solar events

Anything Reliant on Global Navigation Spacecraft System:

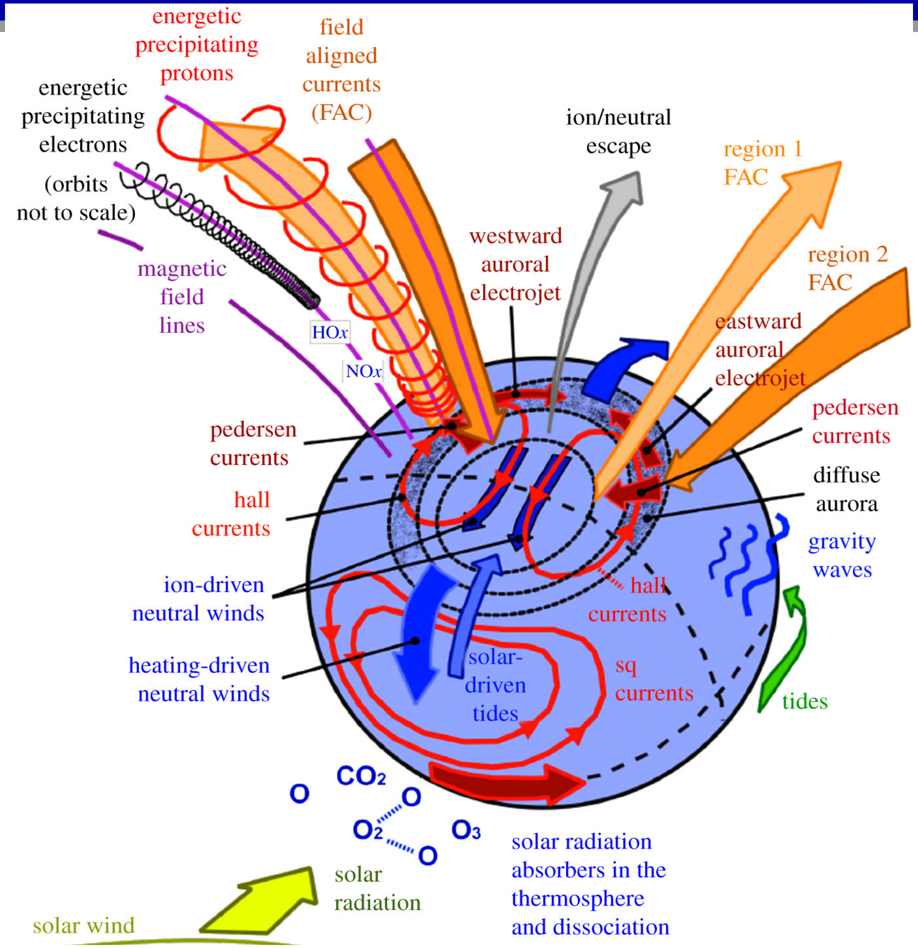
Trains, Planes, Automobiles, Ships, Drones Can ‘Lose Lock’

Why we need to improve Space Weather Forecasting

ORION SPACE SOLUTIONS

Space ISAC
John Noto
10/17/23

Why do we care?



Interaction of the magnetosphere with the Ionosphere and Thermosphere, and the solar wind. From [Sarris, 2019]

Ionospheric effects

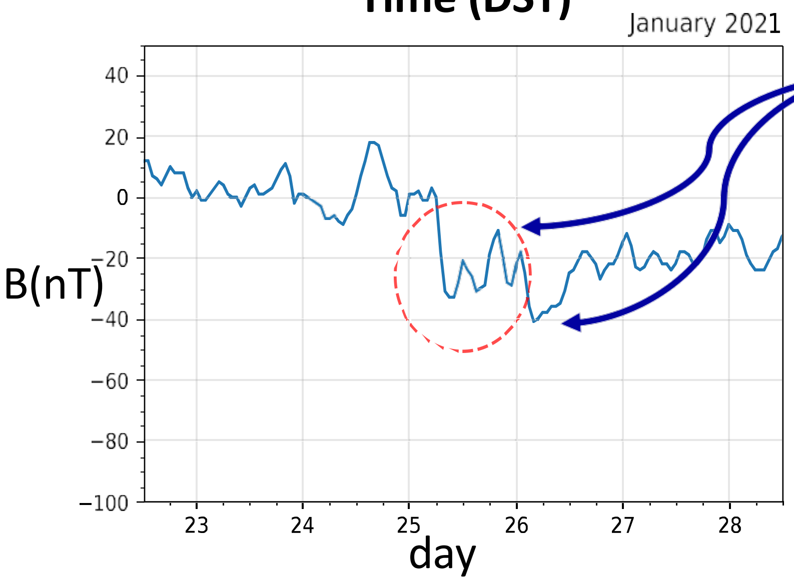
- Communicate
  - HF propagation issues
  - Sat-Comm VHF-S band
- Navigate
  - L-band GPS and PNT disruption (scintillation)
- Surveillance
  - OTH Radar

Neutral Atmosphere effects

- Space Traffic Management
  - Orbital Maneuvers
  - Collision avoidance
  - Catalog Maintenance

Small Storm, Big Effects

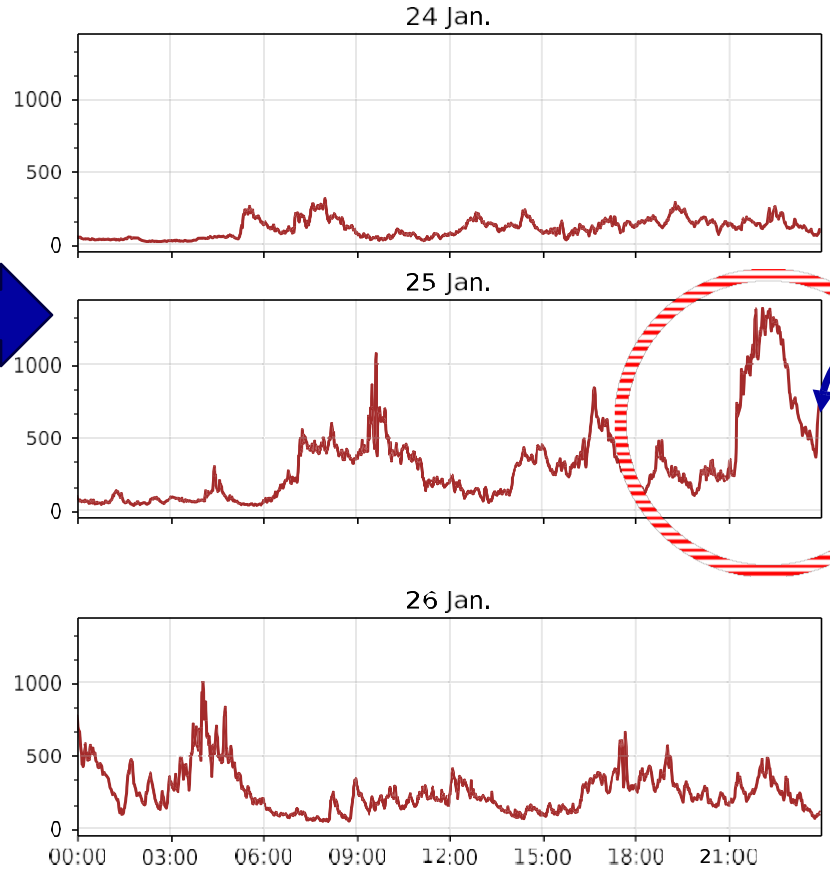
Disturbance -Storm Time (DST)



Solar wind energy transferred to the magnetosphere

AE represents enhanced B from ionospheric current in and below the auroral zone

Auroral Electrojet (AE) Index

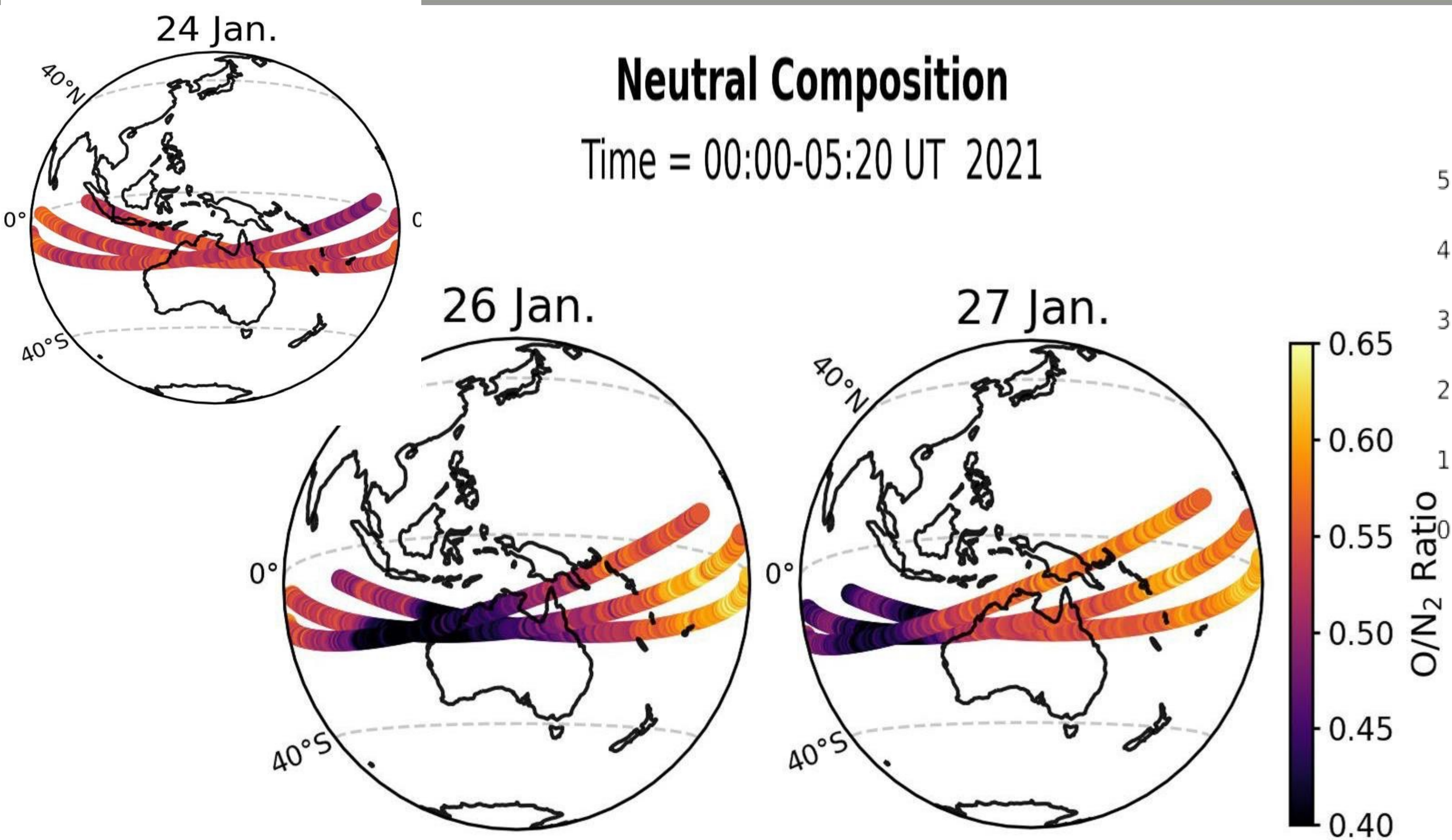


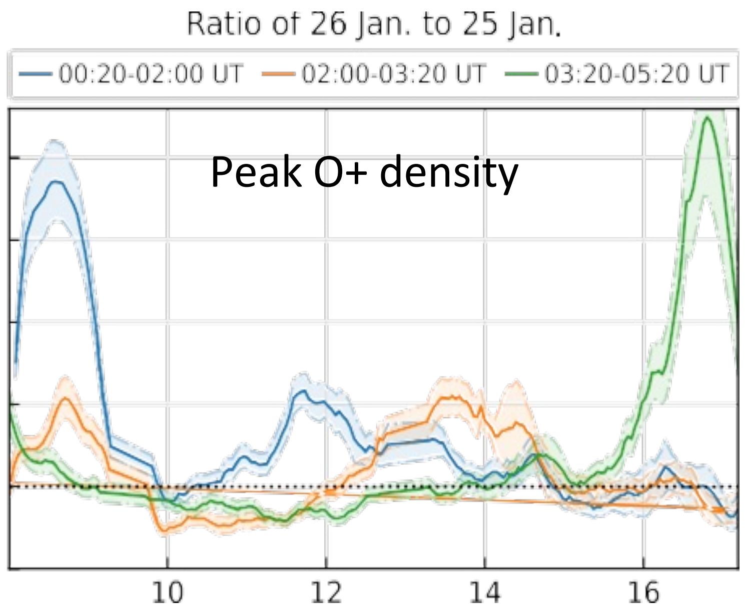
heating

moderate (−50 nT > minimum of Dst > −100 nT), intense (−100 nT > minimum Dst > −250 nT) or super-storm (minimum of Dst < −250 nT).

McGinness, et al.,The effects of a small geomagnetic storm on Earth's thermosphere and ionosphere: ICON observations of the 25 January 2021 disturbance. *Journal of Geophysical Research: Space Physics*, *128*, e2022JA031207.

Observed changes in density





The NmF2 ratio of 26 January to 25 January at 223 km as a function of solar local time for ICON's first three daytime passes.

McGinness, et al.,The effects of a small geomagnetic storm on Earth's thermosphere and ionosphere: ICON observations of the 25 January 2021 disturbance. *Journal of Geophysical Research: Space Physics*, *128*, e2022JA031207.

The problem!

ORION SPACE SOLUTIONS

Management

- Space traffic growing exponentially, with no sign of slowing down
- Space Force tracks over 29,000 objects in Low Earth Orbit, in an increasingly crowded environment
- Satellite orbits are affected by space weather via changes in atmospheric drag

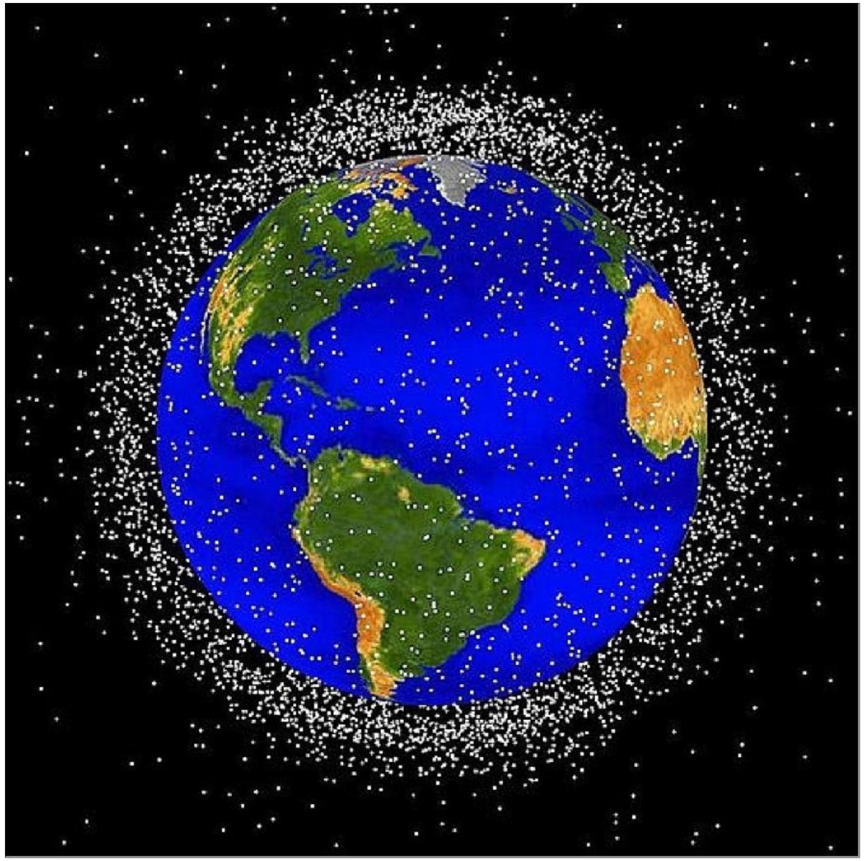
Interruption/failure

Proper Attribution

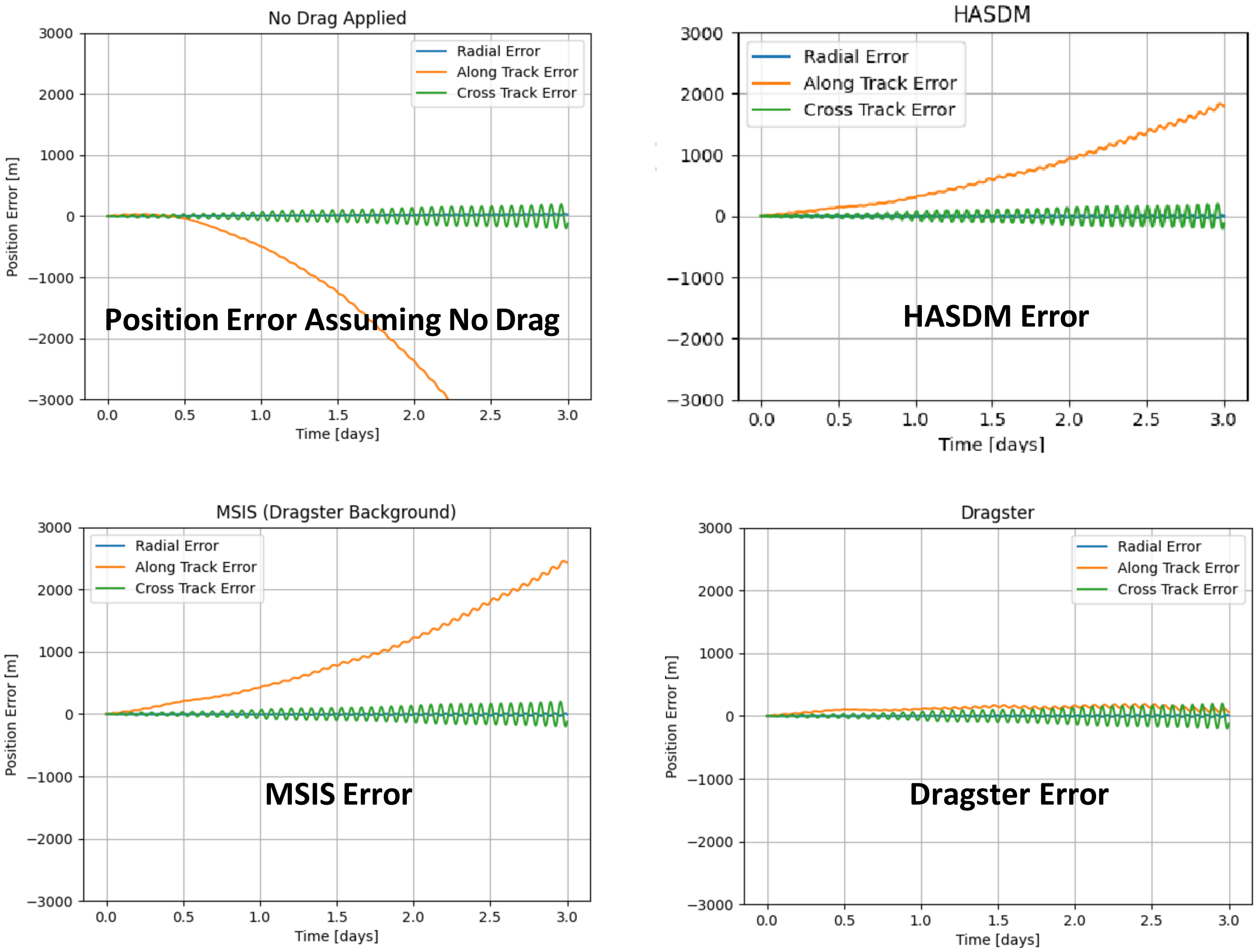
- Equipment
- Environment
- Enemy/Adversary

Using physics based and assimilative models we can provide better forecasting for both the neutral and ionized parts of the atmosphere!

But we need more data!



Improvements in satellite drag prediction



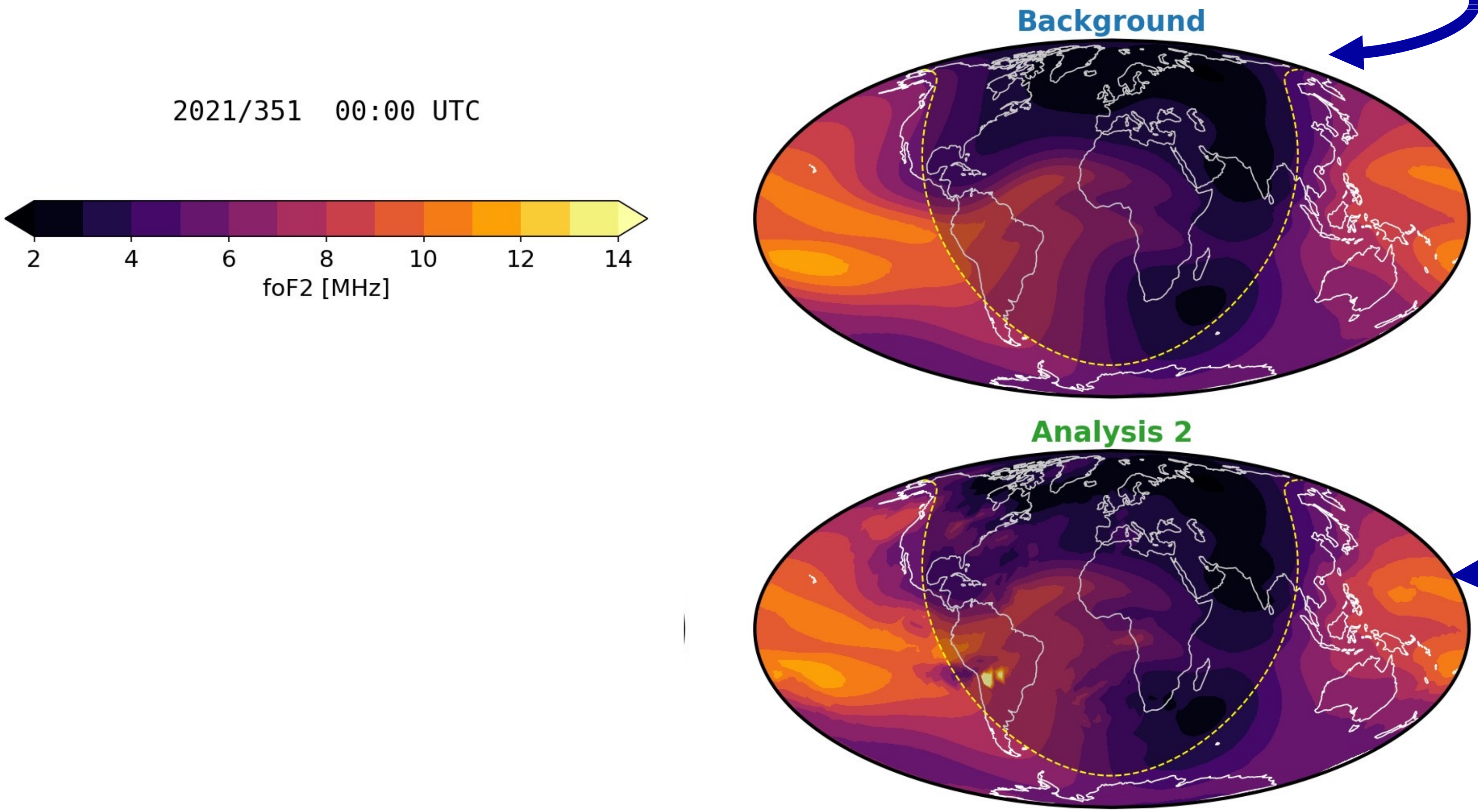
Validation Satellite: Swarm-A (450 km)

Ensemble Kalman filter provides more precise predictions of orbital dynamics than other models.

The smaller error would reduce collision uncertainties and the number of false alarms.

Improvements in Ionosphere prediction

baseline



Baseline
+
Ground
based TEC
+
Ionosonde
+
Cosmic 2
+
PlanetIQ

A better result validated by ground based ionosondes

Evolvable Cislunar Space Ecosystem: Sharing Data Across Systems of Systems

Ronald Birk, Principal Director, The Aerospace Corporation

Dr. Aaron Enes, Principal Engineer, Blue Origin

Dr. Michael Klipstein, CISM, CISSP, Senior Public Policy Advisor, Baker Donelson

Debi Tomek, Senior Advisor, National Aeronautics and Space Administration (NASA)

Ben Reed, Chief Technology Officer (CTO), Quantum Space

Cislunar Ecosystem

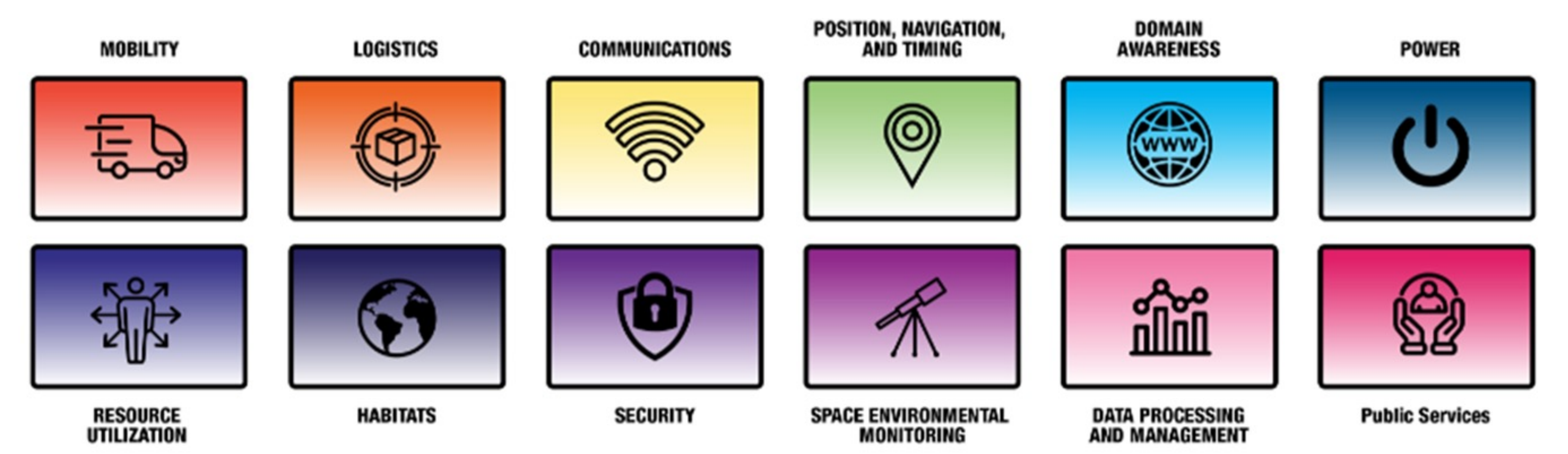
Ron Birk
Space Enterprise Evolution
Civil Systems Group

October 10, 2023

ESTABLISHING A SUSTAINABLE CISLUNAR ECOSYSTEM

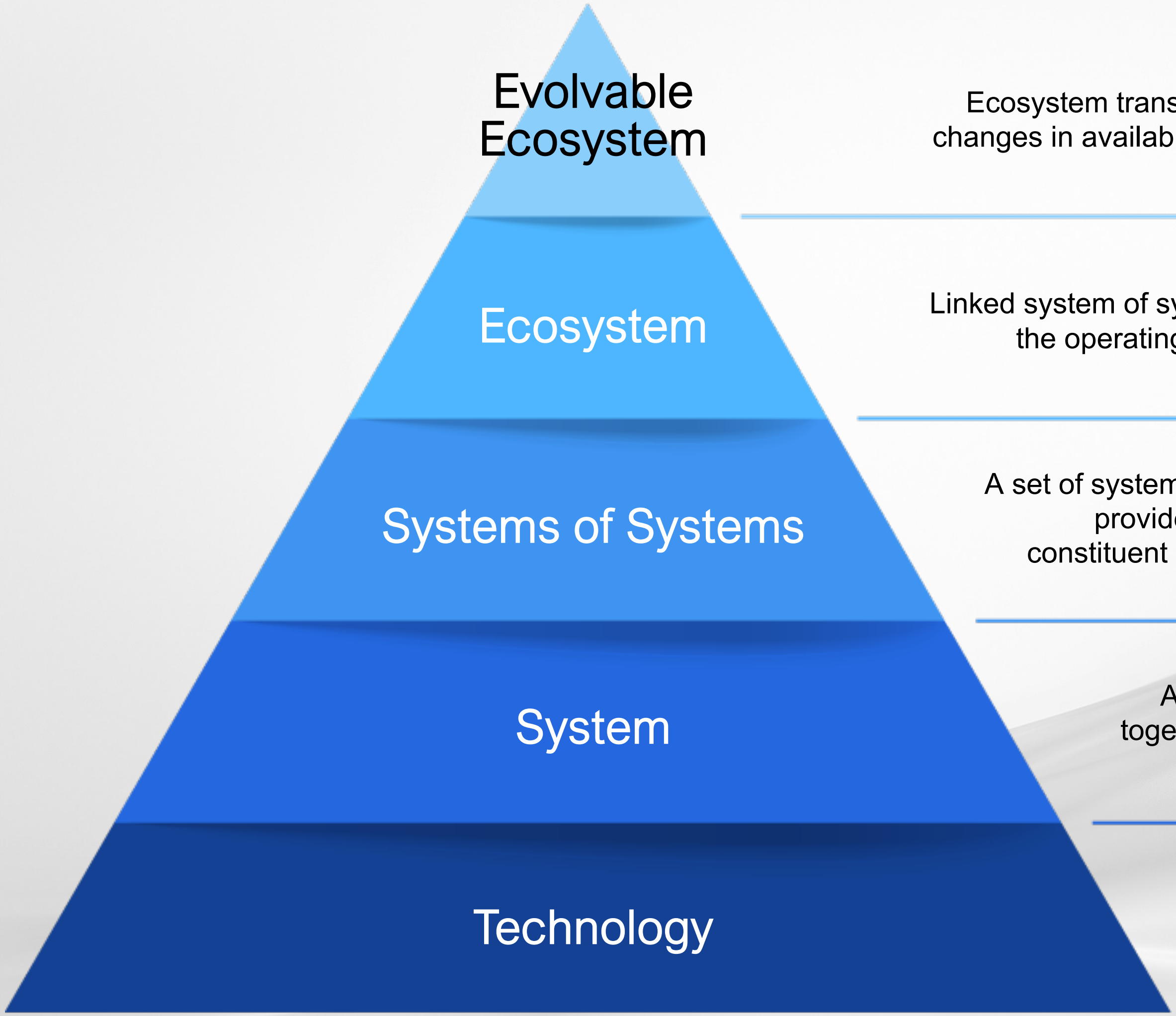
Enterprise integration across 12 layers of infrastructure

- *Extend human economic activity into deep space by establishing a permanent human presence on the Moon, and, in cooperation with private industry and international partners, develop infrastructure and services that will enable science-driven exploration, space resource utilization, and human missions to Mars. -* National-Space-Policy.pdf



ENABLING SPACE ENTERPRISE EVOLUTION

Fit together >> Interoperate together >> Evolve together



Ecosystem transformations over time as a function of changes in available operating systems and functions. [2]

Linked system of systems, symbiotic functionalities, and the operating environments where they interact. [2]

A set of systems or system elements that interact to provide a unique capability that none of the constituent systems can accomplish on its own.[1]

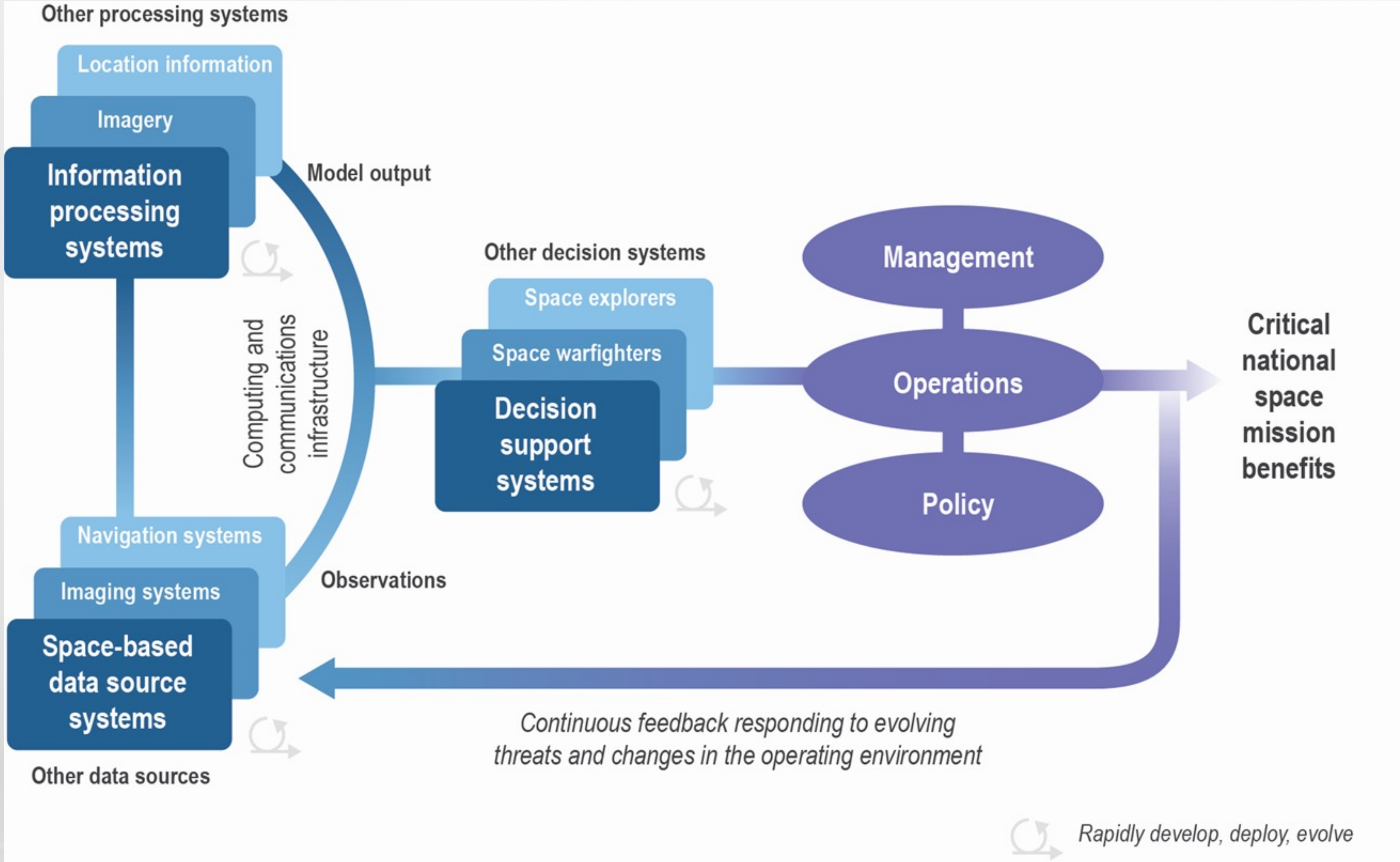
Arrangement of parts or elements that together exhibit behavior or meaning that the individual constituents do not. [1]

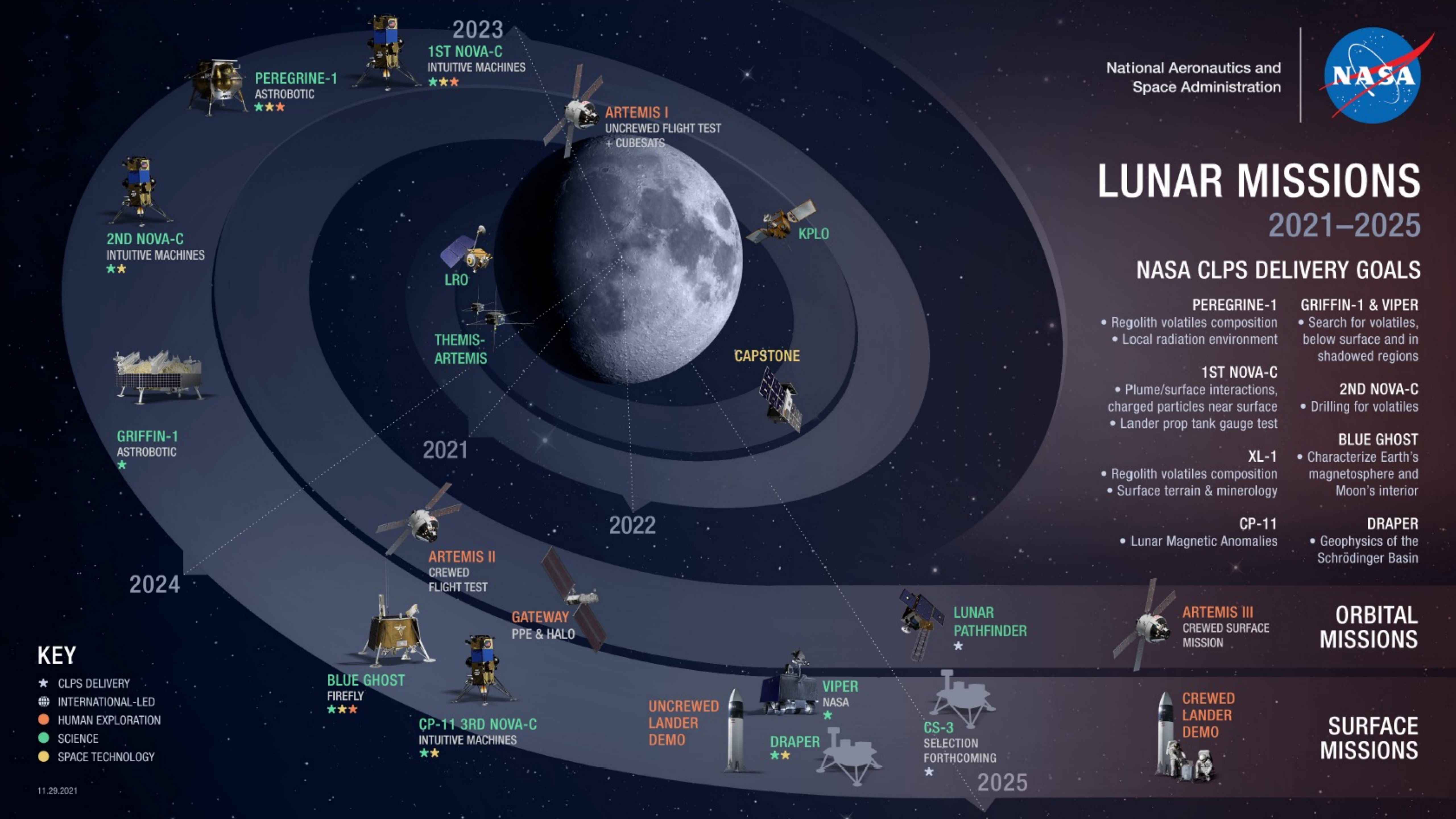
Application of scientific knowledge to a practical means.

1. INCOSE: https://sebokwiki.org/wiki/Systems_of_Systems_(SoS)
2. Birk/Guidi definition

ACHIEVING SPACE ENTERPRISE INTEGRATION

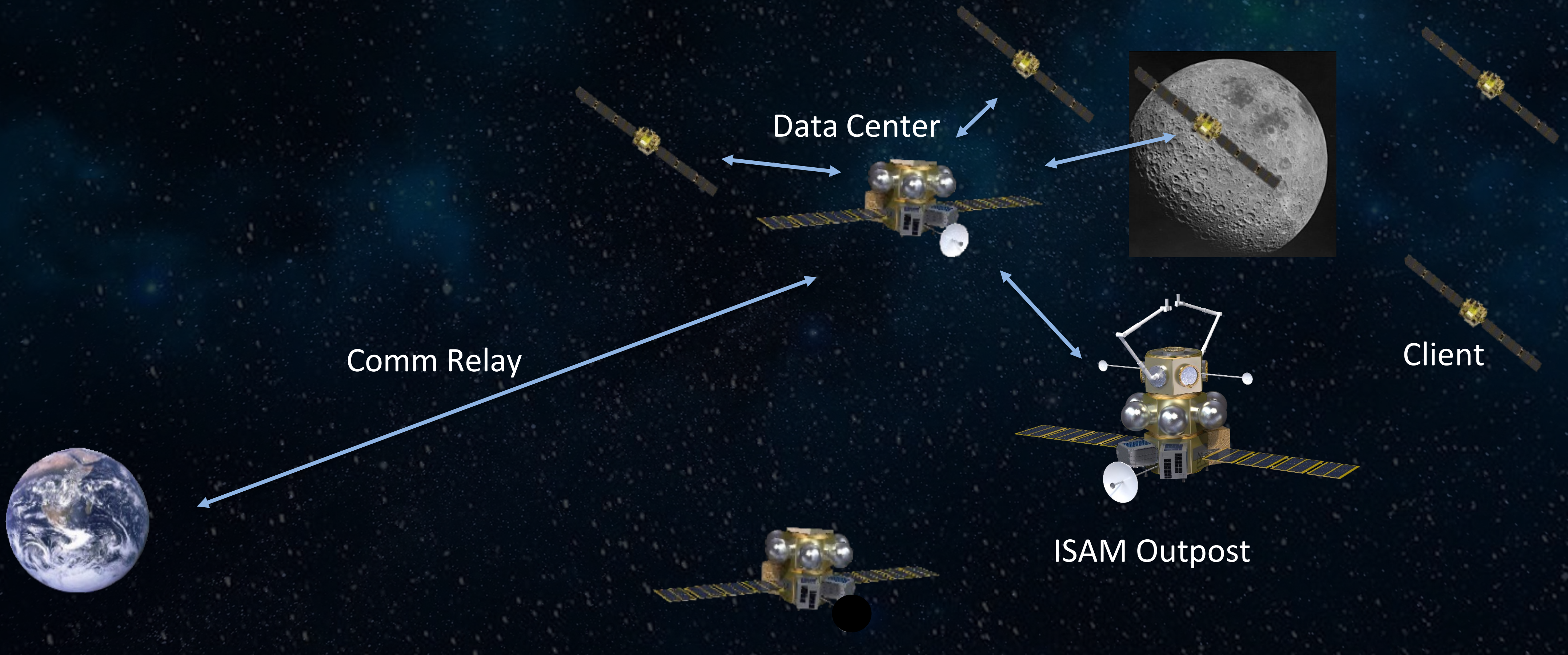
Across Owners/Operations of Space, Ground, and Decision Support Systems





National Aeronautics and Space Administration
NASA
LUNAR MISSIONS
2021–2025
NASA CLPS DELIVERY GOALS
PEREGRINE-1
• Regolith volatiles composition
• Local radiation environment
1ST NOVA-C
• Plume/surface interactions, charged particles near surface
• Lander prop tank gauge test
XL-1
• Regolith volatiles composition
• Surface terrain & minerology
CP-11
• Lunar Magnetic Anomalies
GRIFFIN-1 & VIPER
• Search for volatiles, below surface and in shadowed regions
2ND NOVA-C
• Drilling for volatiles
BLUE GHOST
• Characterize Earth's magnetosphere and Moon's interior
DRAPER
• Geophysics of the Schrödinger Basin
2021
2022
2023
2024
2025
PEREGRINE-1
ASTROBOTIC
1ST NOVA-C
INTUITIVE MACHINES
ARTEMIS I
UNCREWED FLIGHT TEST
+ CUBESATS
2ND NOVA-C
INTUITIVE MACHINES
KPLO
LRO
THEMIS-
ARTEMIS
CAPSTONE
GRIFFIN-1
ASTROBOTIC
ARTEMIS II
CREWED
FLIGHT TEST
GATEWAY
PPE & HALO
BLUE GHOST
FIREFLY
CP-11 3RD NOVA-C
INTUITIVE MACHINES
UNCREWED
LANDER
DEMO
VIPER
NASA
DRAPER
LUNAR
PATHFINDER
CS-3
SELECTION
FORTHCOMING
ARTEMIS III
CREWED SURFACE
MISSION
CREWED
LANDER
DEMO
ORBITAL
MISSIONS
SURFACE
MISSIONS
KEY
CLPS DELIVERY
INTERNATIONAL-LED
HUMAN EXPLORATION
SCIENCE
SPACE TECHNOLOGY
11.29.2021

QuantumNet provides data and mobility infrastructure



Consortium for Space Mobility and ISAM Capabilities (COSMIC)

Ronald Birk, Principal Director,
The Aerospace Corporation

COSMIC

THE POWER OF COLLABORATION

CONSORTIUM FOR SPACE MOBILITY AND ISAM CAPABILITIES

Overview Briefing

Ron Birk
The Aerospace Corporation

October 2023

- The **Consortium for Space Mobility and ISAM Capabilities (COSMIC)** is a nationwide coalition that will invigorate a domestic in-space servicing, assembly, and manufacturing (ISAM) capability.
- COSMIC will:
  - **Mobilize, advance, and leverage** community expertise spanning **users and providers** across federal agencies, industry, and academia.
  - Accelerate **wide-spread adoption** of ISAM capabilities as an integrated segment of the space enterprise architecture.
  - Steer the future of ISAM as a coordinated and collaborated effort for space mission lifecycles to **enhance mission capability, reduce costs, and increase operational efficiency** due to **enhanced longevity, utility, and resilience.**

What is ISAM?

COSMIC
CONSORTIUM FOR SPACE MOBILITY AND ISAM CAPABILITIES

In-Space Servicing, Assembly, and Manufacturing

SERVICING

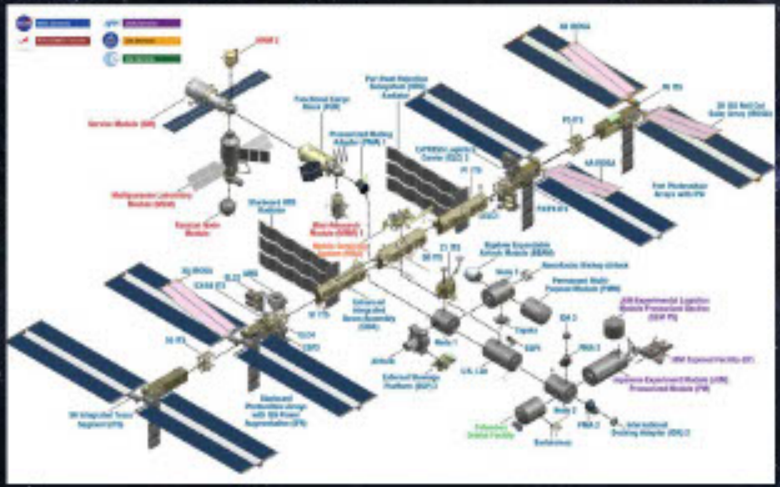
- Design of modular, serviceable, upgradeable, and evolvable systems

ASSEMBLY

- Assembly of simple to complex space systems

MANUFACTURING

- Manufacturing in space using Earth- and locally-sourced materials



ISAM National Strategy and Implementation Plan

FOSTER AN ECOSYSTEM TO LEVERAGE ISAM CAPABILITIES

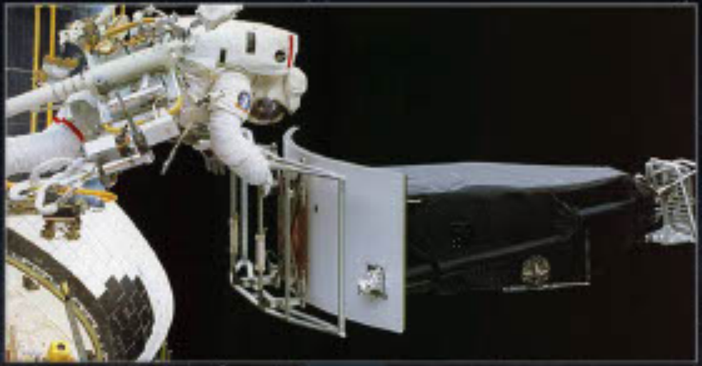
- Support and stimulate USG, academic, and commercial ISAM capability development
- Consistent with US Space Priorities Framework (Dec 2021)

BENEFITS

- Promote a sustainable space environment
- Improve scientific output of spacecraft and payloads
- Create robust, sustainable, and enduring in-space infrastructure
- Expand performance, availability, resilience, and lifetime of space systems

STRATEGIC GOALS

1. Advance ISAM research & development
2. Prioritize expanding scalable ISAM infrastructure
3. Accelerate the emerging ISAM commercial industry
4. Promote international collaboration and cooperation
5. Prioritize environmental sustainability
6. Inspire a diverse future space workforce



COSMIC: A Nationwide Alliance for ISAM

VISION

Create a nationwide alliance that enables the U.S. space community to provide global leadership in ISAM.

MISSION STATEMENT

Making ISAM a routine part of space architectures and mission lifecycles.

CAPABILITY DEVELOPMENT

Develop, mature, and demonstrate ISAM technologies that enable and enhance mission utility.

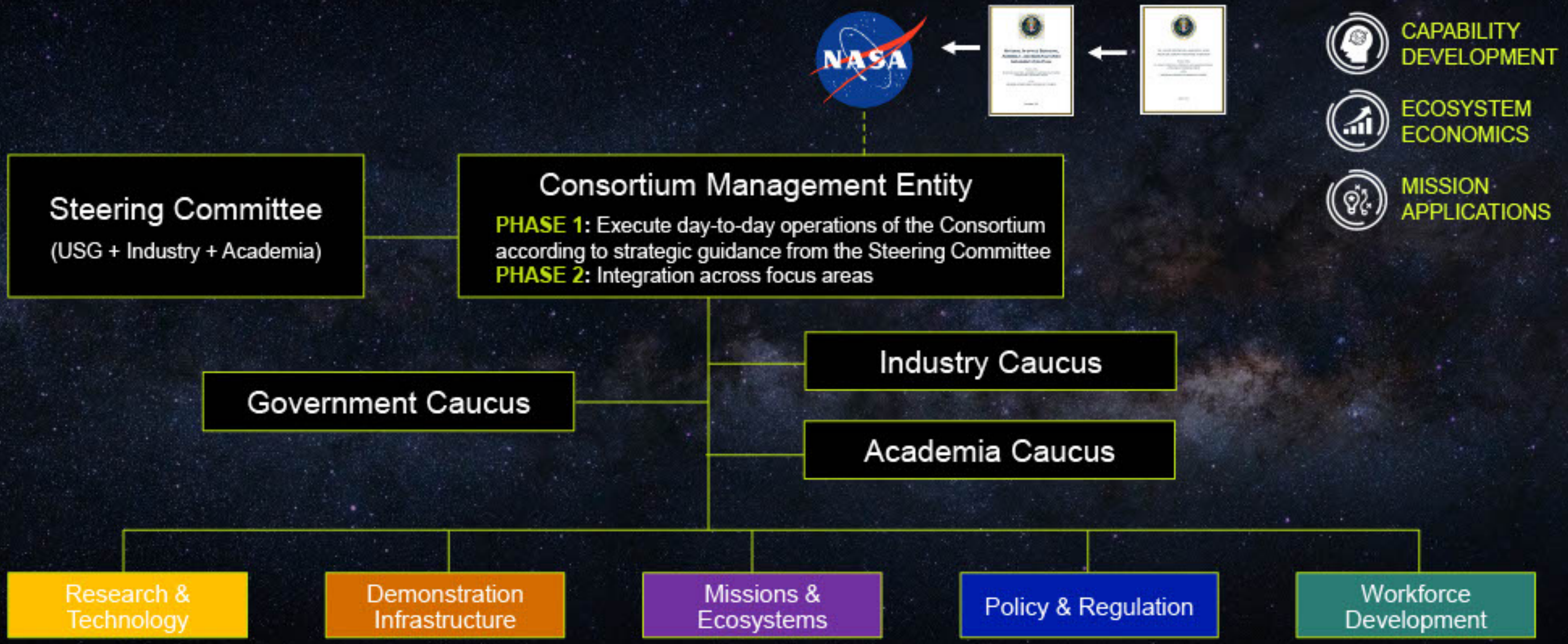
ECOSYSTEM ECONOMICS

Promote U.S. leadership in ISAM technologies and capabilities that change the business model away from single-use space assets.

MISSION APPLICATIONS

Encourage and guide missions to use ISAM capabilities as part of commercial and government program lifecycles.

COSMIC Organization



Steering Committee – Inaugural Membership

Koki Ho

Brad Kinsey

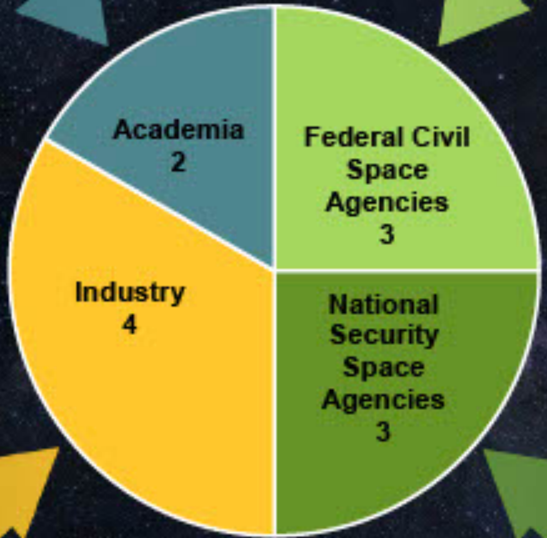
Ben Reed

Joe Anderson

Lee Rosen

Joe Chan

STEERING COMMITTEE COMPOSITION



Bo Naasz - CHAIR

Carolyn Mercer

Stephen Duall

Bernie Kelm

Col Joyce Bulson

Col Eddie Ferguson

COSMIC information approved for unlimited public release

Consortium Definition

COSMIC IS	COSMIC IS <u>NOT</u>
- A forum for collaboration and knowledge sharing	- A funding body
- A consortium designed to produce useful products	- A solicitation vehicle
	- A standards body
	- A lobbying organization
- A U.S. consortium	- An international consortium
- Sponsored by NASA	- Led by NASA

COSMIC Coordination

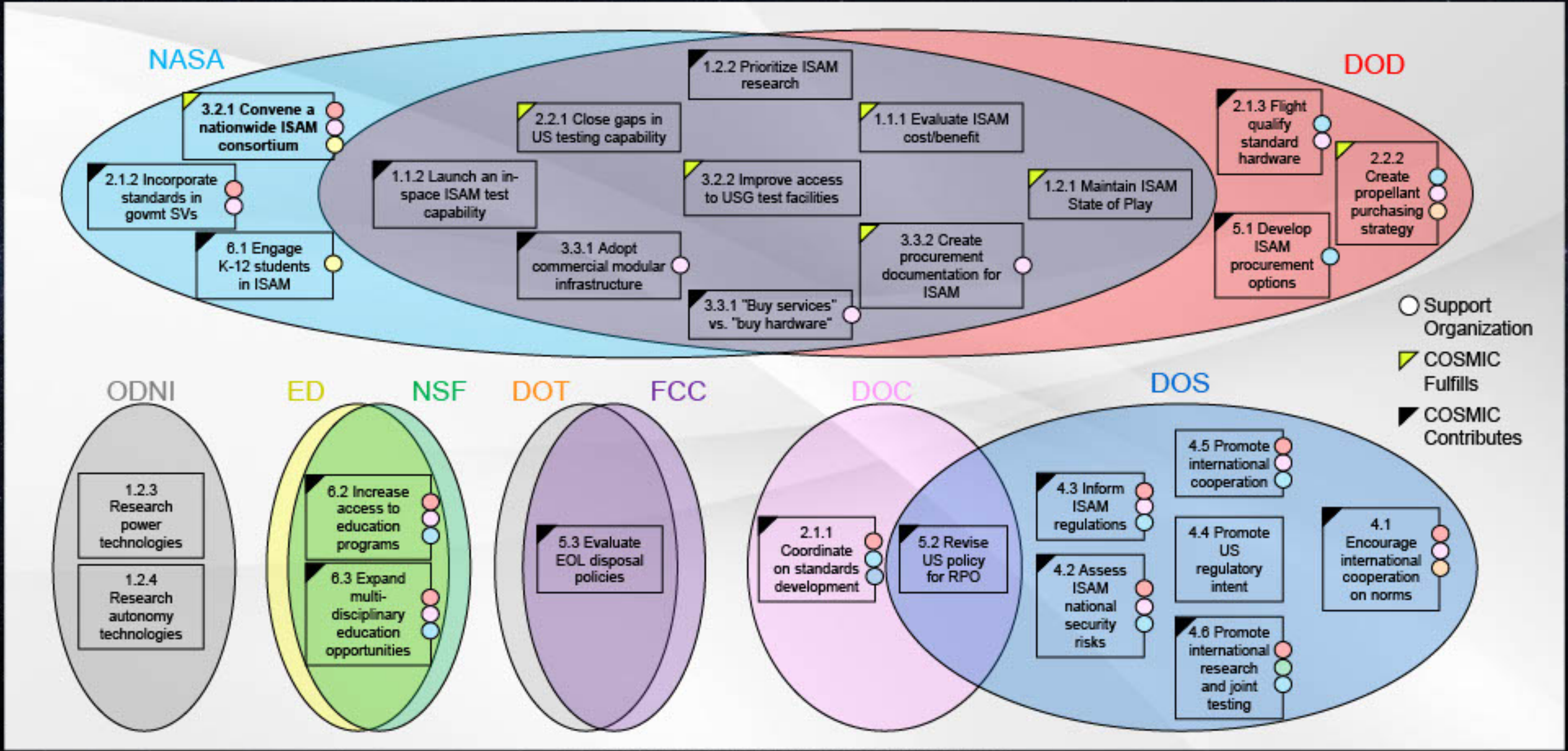
COSMIC
Consortium for Space Mobility and ISAM Capabilities

	3Q FY22	4Q FY22	1Q FY23	2Q FY23	3Q FY23	4Q FY23
NATIONAL	OMB; ISAM National Strategy	OSTP ISAM IWG		ISAM National Implementation Plan		OMB; National Space Council
PUBLIC *US ONLY	Space Technology Industry-Government-University Roundtable (STIGUR)	AIAA ASCEND				COSMIC Engagement Session
DOD	USSF/SSC; USSF SPoC; SPACECOM	AFRL; USSF/SSC	SAF/ SQ	DIU; NRL	SSIB Workshop; Space Safety Institute	USSF; SPACECOM
CIVIL		JPL	NASA ISAM Workshop; LaRC; GSFC; MSFC; JSC	NASA Center Tri-Annual, ARC; ESDMD, SOMD, SMD, OTPS	NASA HQ	NASA HQ; FCC
INDUSTRY	CONFERS Leadership	SpaceLogistics; Redwire; CONFERS GSSF	Astroscale; Lockheed Martin; Orbitfab; Starfish Space	Axiom Space; Nanoracks; Sierra Space; Maxar		CONFERS; SIA; Intelsat; ULA; CESMII; CONFERS
ACADEMIA					Space Grant	

COSMIC information approved for unlimited public release

COSMIC's Proposed Role
in the National ISAM Implementation Plan

CONSORTIUM FOR SPACE MOBILITY AND ISAM CAPABILITIES



COSMIC information approved for unlimited public release

COSMIC

CONSORTIUM FOR SPACE MOBILITY AND ISAM CAPABILITIES

KICKOFF MEETING

ANNOUNCING OUR DISTINGUISHED KEYNOTE SPEAKERS

COL. PAM MELROY, (USAF RET.)
DEPUTY ADMINISTRATOR
NASA

DR. EZINNE UZO-OKORO
ASSISTANT DIRECTOR FOR SPACE POLICY
WHITE HOUSE OFFICE OF
SCIENCE & TECHNOLOGY POLICY

MAJ. GEN. JOHN M. OLSON
CHIEF OF SPACE OPERATIONS
MOBILIZATION ASSISTANT
U.S. SPACE FORCE

November 7-8, 2023

University of Maryland
College Park, MD

COSMICspace.org


COSMIC
THE POWER OF COLLABORATION
CONSORTIUM FOR SPACE MOBILITY
AND ISAM CAPABILITIES
cosmicspace.org

COSMIC Responds to the National Need

COSMIC
CONSORTIUM FOR SPACE MOBILITY AND ISAM CAPABILITIES

Tasking	Plan
This OSAM consortium should focus on developing technologies needed by the commercial space industry (as a potential user, not just as a provider).	✓ Commercial mission models and business infusion are represented in the "Missions and Ecosystems" focus area. ✓ Industry members are a critical part of the Steering Committee.
To this end, the OSAM consortium should consider co-funding partners from the commercial space industry.	✓ Government, industry, and academic members fund their own participation.
In establishing this consortium, STMD should convene a nationwide alliance of government departments and agencies, universities, nonprofit research institutions, NASA centers and mission directorates, and commercial companies, to include space start-up community and under-represented companies (i.e. small and minority-owned businesses).	✓ COSMIC is built as a nationwide alliance that includes a broad cross-section of the U.S. space community. ✓ Enhances the role of universities and innovative startups in early stage R&D for ISAM applications.
STMD should ensure these partners have a vested interest in the nation's leadership in OSAM as an enabling technology and as a vehicle for workforce development.	✓ Participation in COSMIC opens up opportunities for industry and government collaboration, partnerships, and tech transfer. ✓ University participation enables and enhances the ISAM-savvy workforce of the future.
This OSAM consortium should collaborate where there may be possible synergies and to avoid unnecessarily overlapping or duplicative federal efforts.	✓ Identified potential USG partners based on existing interests, expressed via membership in the OSAM National Initiative, ISAM Interagency Working Group, and other community forums.

COSMIC and CONFERS: Invigorating the Community

COSMIC — CONSORTIUM FOR SPACE MOBILITY AND ISAM CAPABILITIES

CONFERS — FOSTERING THE SATELLITE SERVICING INDUSTRY

PURPOSE

COSMIC: "Making ISAM a routine part of space mission lifecycles"

- Facilitate collaborative relationships between U.S. government departments and agencies, universities, commercial companies, and nonprofit research institutions
- Create products that address National ISAM Implementation Plan actions, such as
  - A repository of available ISAM capabilities and facilities
  - Assessment of missions enabled or enhanced by ISAM R&D

CONFERS: "Servicing empowering a robust space economy"

- Developing industry-led standards that contribute to a sustainable, safe, and diverse space economy
- Engaging with global governmental legislative and regulatory bodies on policies and oversight of satellite servicing activities

MEMBERSHIP

COSMIC: US-ONLY MEMBERSHIP

- Nationwide consortium to advance U.S. leadership in ISAM
- Members must have a vested interest in the nation's leadership in ISAM

CONFERS: INTERNATIONAL MEMBERSHIP

- Industry-led initiative where industry members vote
- Government members (including USG and international) are observers only

FUNDING

COSMIC: NO MEMBERSHIP DUES

- Management entity funded by NASA to support whole-of-nation needs
- Members fund their own participation

CONFERS: 100% FUNDED BY MEMBER DUES

- Management entity funded by membership dues
- Initial seed funding from DARPA starting in 2017
- Now a stand-alone not-for-profit trade group
- Members fund their own participation

SPACE ISAC

VALUE OF SPACE SUMMIT 2023

Co-hosted by AEROSPACE

Charting the Path to Prosperity: Navigating the Future of the Space Economy

Lesley Conn, Senior Director, Space Foundation

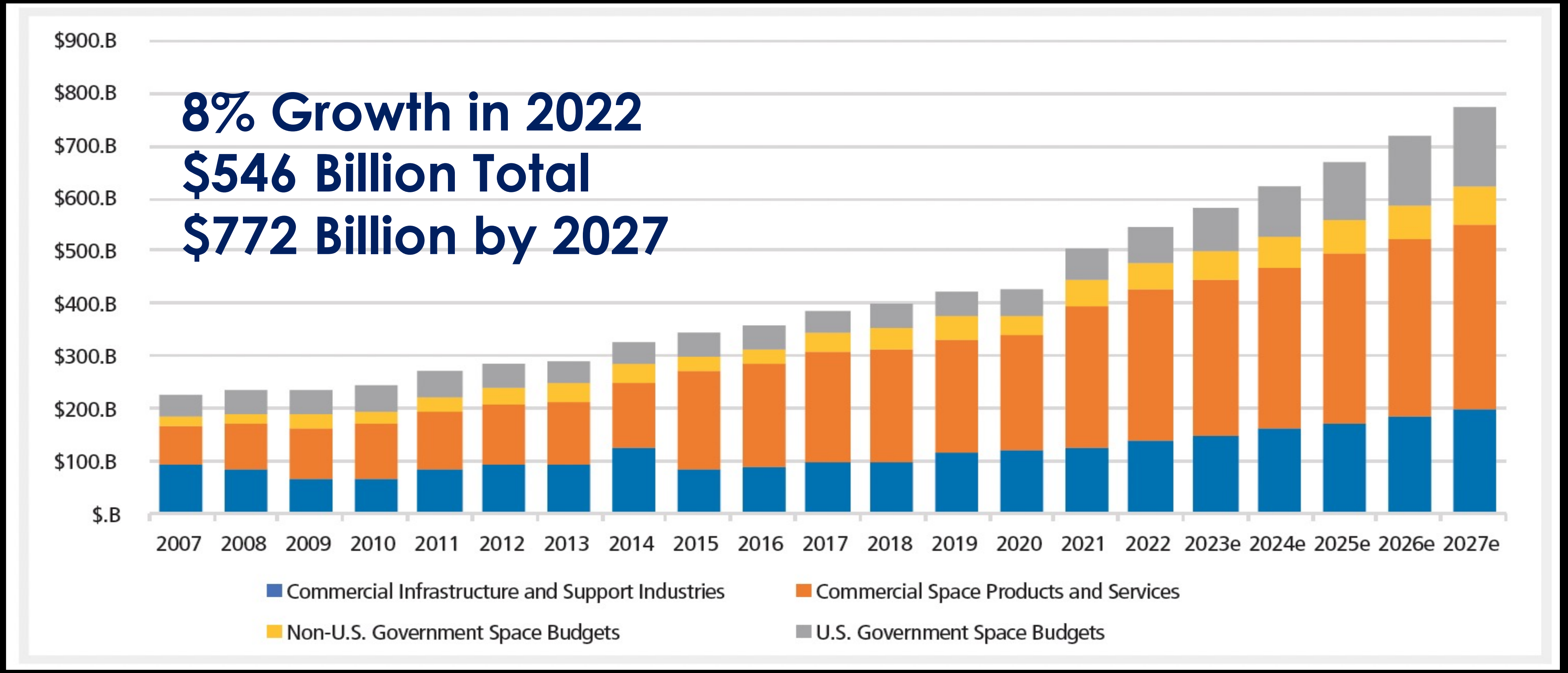
Kelli Kedis Ogburn, VP of Space Commerce, Space Foundation

SPACE FOUNDATION

Charting the Path to Prosperity: Navigating the Future of the Space Economy

Value of Space Summit 2023

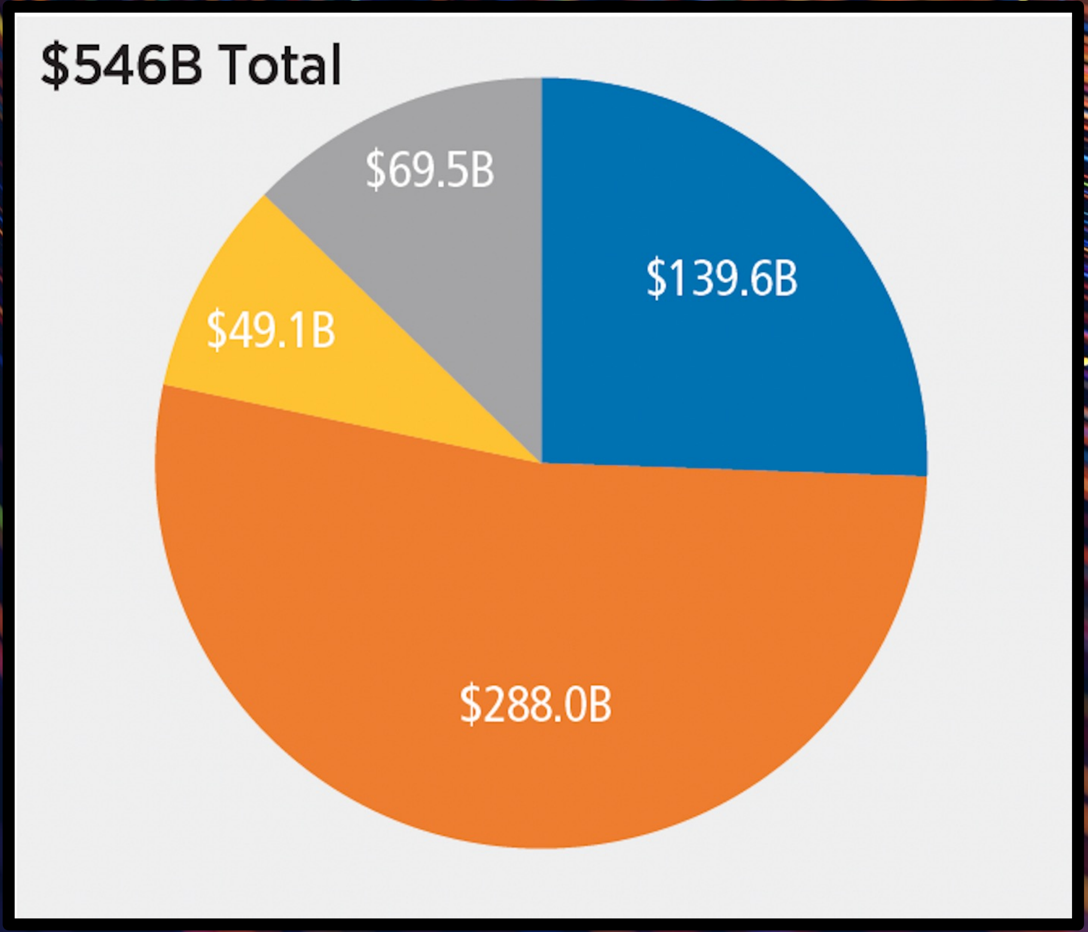
Global Space Forecast, 2022-2027



SPACE FOUNDATION

Four Key Sectors

- Commercial Infrastructure and Support
- Commercial Space Products and Services
- U.S. Government Space
- Non-U.S. Government



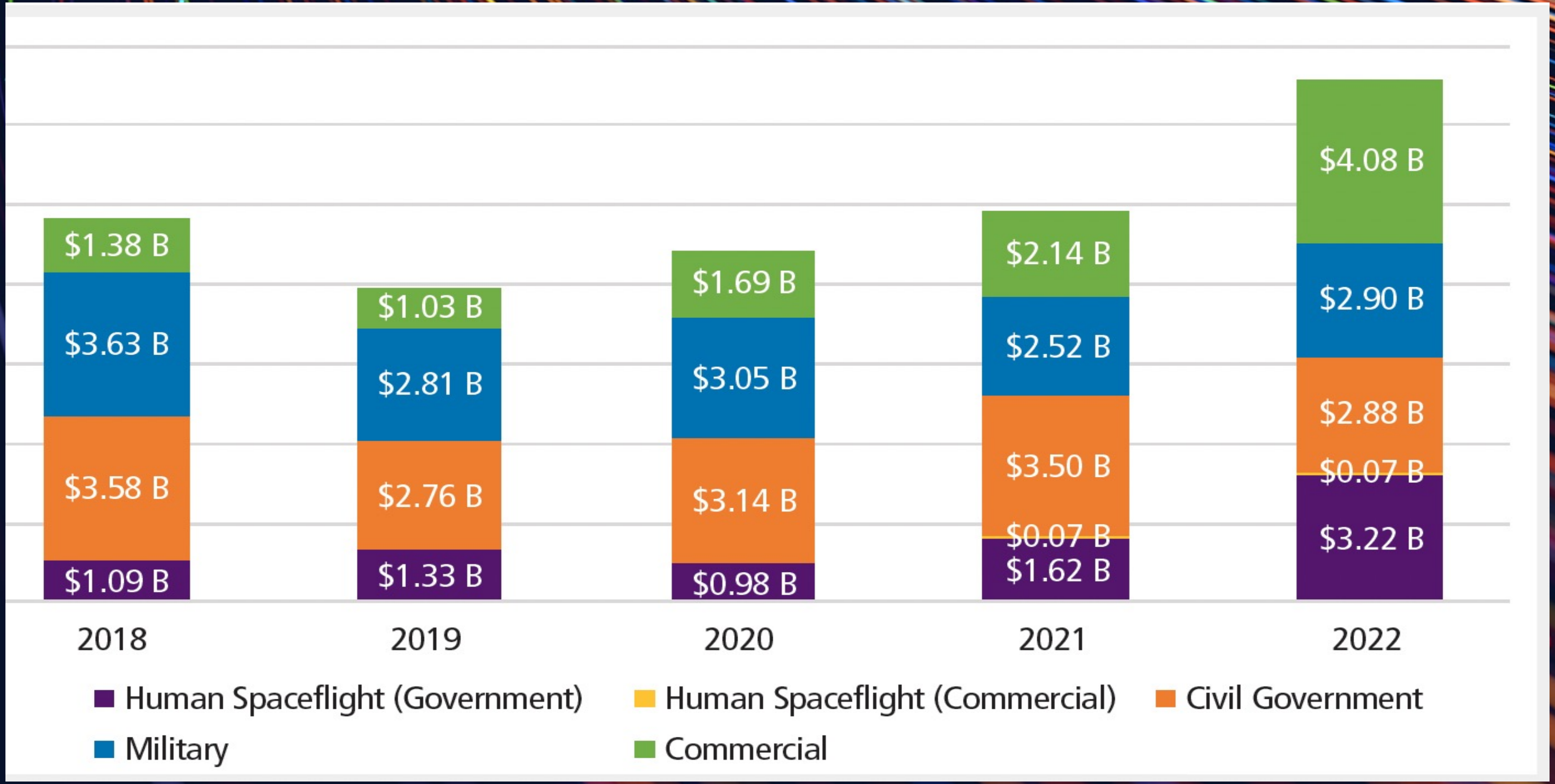
SPACE FOUNDATION

Sectors Now Showing Strong Growth

- Satellite Communication
- Earth Observation
- Launch Services

Future Sectors

- AI and Big Data
- New Space Stations
- Cislunar



SPACE FOUNDATION

Top Government Space Spending

Nation/Agency	Spending (USD)	2021-22 Change (USD)	2021-22 Change (national currency)
United States	$69.5B	13.6%	13.6%
China	$16.1B	0.7%	4.5%
ESA*	$5.4B	11.6%	0.1%
Russia	$3.7B	19.7%	10.5%
Japan	$3.1B	11.8%	7.8%
European Union	$2.3B	21.4%	11.0%
India	$1.3B	20.6%	15.6%

- $119B in 2022
- $52B in Global Defense
- $26B U.S. non-military spending

SPACE FOUNDATION

Kelli Kedis Ogborn
VP of Space Commerce and Entrepreneurship
kkedisogborn@spacefoundatioin.org

Lesley Conn
Director, Research & Digital Programming
lconn@spacefoundation.org
thespacereport.org

Gretchen Bliss,

Director of Cybersecurity Programs
University of Colorado Colorado Springs (UCCS)

Space ISAC Interview with the Fellows

Bernadette Maisel, Workforce Development Director, Space ISAC

Lydia Siramdane, Cyber Systems Engineer, Peraton

Xavier Foster, Fellow, Space ISAC

VALUE OF SPACE SUMMIT 2023

Co-hosted by AEROSPACE

Erin Miller

Executive Director, Space ISAC

Erin boasts a decade of experience fostering high-impact tech collaborations across government, industry, and academia for national security and warfighter support. She currently leads as Executive Director of the Space Information Sharing and Analysis Center (ISAC), the key security information hub for the public and private space sector. Erin's career revolves around non-profit leadership, including her role as Managing Director at the Center for Technology, Research and Commercialization (C-TRAC).

Her achievements include establishing AFCyberWorx, the Air Force's first cyber design studio, and Catalyst Accelerator, a pioneering space-focused accelerator in collaboration with the Air Force Research Laboratory and AFWERX. Erin received the Woman of Influence award in 2020 and the Mayor's Young Leader (MYL) of the Year Award for Technology in 2018, along with the Southern Colorado Women's Chamber of Commerce Award for Young Female Leader. Her expertise spans intellectual property, technology transfer, export control/ITAR, secure facilities, and rapid prototyping collaborations.

SPACE ISAC

VALUE OF SPACE SUMMIT 2023

Co-hosted by AEROSPACE