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.
"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.
VALUE OF SPACE SUMMIT 2023

Sponsors

CYWARE

KRATOS

Constellation

Deloitte

RADICL

ExC Analytic Solutions

RAPID ASCENT

thinklogical
Dr. Jennifer Sobanet,
Interim Chancellor
University of Colorado
Colorado Springs (UCCS)
Maj. Gen. (Ret) Kim Crider
Founding Partner
Elara Nova: The Space Consultancy
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)
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......
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 *despite*
  • 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 *during and after*
  • 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 *built* 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)
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
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
brandon.bailey@aero.org
240.521.4326 (c)

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

https://sparta.aerospace.org/resources/

Approved for public release. OTR 2022-01250 & OTR 2023-00989
Space Attack Research & Tactic Analysis (SPARTA) – Launched Oct 2022

Filling the TTP Gap for Space

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

SPARTA provides unclassified information to space professionals about how spacecraft may be compromised/impacted via cyber or traditional counterspace mean
SPARTA Use Cases – Impact Across Community & Lifecycle
USG, Commercial Space, International, Collaborations, etc.

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

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

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

Deeper Dive on Use Cases at https://sparta.aerospace.org/resources/SPARTA_Overview_InDepth_Nov22.pdf
Example: SPD-5 and SPARTA Relationship
Bridging the Technical Gap Between Policy and Implementation

SPD-5 PROVIDES SOME GENERIC SECURITY GUIDANCE FOR SPACE SYSTEMS
Implementation details on these principles – SPARTA provides guidance on SPD-5 principles and beyond

EXTRACTED SPD-5 PRINCIPLES (SECT 4b)

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}

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
  – 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
## Mapping to Standards

### NIST References

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

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
<th>SPARTA Countermeasures</th>
<th>ISO 27001</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.5</td>
<td>Organizational controls</td>
<td>None</td>
<td>CM0005</td>
<td>5.2, 5.3</td>
</tr>
<tr>
<td>A.5.1</td>
<td>Policies for information security</td>
<td></td>
<td>CM0005, CM0022, CM0024, CM0026, CM0027, CM0028, CM0034</td>
<td>7.5.2, 7.5.3</td>
</tr>
<tr>
<td>A.5.2</td>
<td>Information security roles and responsibilities</td>
<td></td>
<td>CM0005, CM0022, CM0041, CM0052, CM0054, CM0056, CM0057, CM0075</td>
<td>7.5.2, 7.5.3</td>
</tr>
<tr>
<td>A.5.3</td>
<td>Segregation of duties</td>
<td>None</td>
<td>AC-5</td>
<td></td>
</tr>
<tr>
<td>A.5.4</td>
<td>Management responsibilities</td>
<td></td>
<td>CM0005, CM0024, CM0025, CM0026, CM0027, CM0028, CM0041, CM0049</td>
<td>5.2, 5.3</td>
</tr>
</tbody>
</table>

### D3FEND Techniques

MTREs published Detection, Denial, and Disruption Framework Engineering 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 to provide the exact implementation of a countermeasure, but rather to provide a kernel and framework for defensive techniques. Similar to other frameworks (e.g., ATT&CK, SPARX, 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 no 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 action (COAs). Currently, SPARTA’s countermeasures provide a varying level of destruction on threats. 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.

### ID3FEND Techniques

- **ID3**: Asset Inventory
- **ID4**: Configuration Inventory
- **ID5**: Data Inventory
- **ID6**: Software Inventory
- **ID7**: Hardware Vulnerability Enumeration
- **ID8**: Network Node Inventory
- **ID9**: Hardware Component Inventory

### D3FEND Techniques

- **AC-1**: 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 the access control policy, coordinate and control access controls, and a. Designate an [Assignment: organization-defined official] to monitor and control access controls.

**ID List**: CM0005, CM0022, CM0024, CM0026, CM0027, CM0028, CM0034

**ISO 27001**: 5.2, 5.3

**SPARTA Countermeasures**: CM0005

**NIST Rev 5**: None
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

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

Techniques
New Techniques

Modified Techniques
- REC-0001: Gather Spacecraft Design Information
- REC-0002: Gather Spacecraft Descriptions
- 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-0008: Exploit Hardware/Firmware Corruptions
- 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-0003.04: 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
- EXP-0003.02: Downlink Intercept

https://sparta.aerospace.org/contribute
SPARTA JSON Creator

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

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

Paste a comma delimited list of objects

Convert to JSON   Download JSON

Created JSON will be here
Building Spacecraft Attack Chains using Attack Chains / Attack Flow != Cyber Kill Chain

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

- Attack Chains using ATT&CK and or SPARTA are **more than a sequence** of attack tactics
  - Knowledge base that correlates environment-specific (IT, OT/ICS, Cloud, Space) cybersecurity information along a hierarchy of TTP, and other knowledge (detections, mitigations, countermeasures, etc.)

- Ex: building the attack chains in **Navigator** helps derive **countermeasures | mapper**
Building Spacecraft Attack Chains

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

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

**CySat 2023**
- ESA OPS-SAT Attack

**Theoretical Attack Chain in Backup**
- PCspooF

- [Hacking Spacecraft using Space Attack Research & Tactic Analysis](#) | Video (April 2023)
- Updated version presented at [DEF CON 31](#)
Many of these countermeasures likely not feasible for mission that are already launched
Combining the 4 Attack Chains

SPARTA Navigator – Extracting Countermeasures / NIST Controls

https://sparta.aerospace.org/navigator
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
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.

Control Mapper is Good for Comparing NIST 800-53 Control Baselines and their TTP Mitigation
<table>
<thead>
<tr>
<th>Reconnaissance</th>
<th>Resource Development</th>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Defense Evasion</th>
<th>Lateral Movement</th>
<th>Privilege Escalation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software</td>
<td>System</td>
<td>Controls</td>
<td>Controls</td>
<td>Controls</td>
<td>Controls</td>
<td>Controls</td>
<td>Controls</td>
</tr>
<tr>
<td>Firmware</td>
<td>Infrastructure</td>
<td>5</td>
<td>6</td>
<td>4</td>
<td>5</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>Cryptographic Algorithms</td>
<td>Host Network Security</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Edge Data</td>
<td>Terminals</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ethernet</td>
<td>Physical</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Face 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Space 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Commercial 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Government 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Defense 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Multi-Use 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Standard 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Non-Commercial 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Internal 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Confidential 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Commercial 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Government 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Defense 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Multi-Use 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Standard 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Non-Commercial 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Internal 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Confidential 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Commercial 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Government 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Defense 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Multi-Use 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Standard 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Non-Commercial 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Internal 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Confidential 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Commercial 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Government 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Defense 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Multi-Use 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Standard 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Non-Commercial 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Internal 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Confidential 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Commercial 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Government 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Defense 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Multi-Use 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Standard 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Non-Commercial 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Internal 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Confidential 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Commercial 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Government 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Defense 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Multi-Use 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Standard 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Non-Commercial 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Internal 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Confidential 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Commercial 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Government 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Defense 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Multi-Use 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Standard 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Non-Commercial 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Internal 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Confidential 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Commercial 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Government 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Defense 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Multi-Use 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Standard 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Non-Commercial 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Internal 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Confidential 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Commercial 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Government 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Defense 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Multi-Use 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Standard 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Non-Commercial 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Internal 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Confidential 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Commercial 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Government 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Defense 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Multi-Use 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Standard 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Non-Commercial 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Internal 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Confidential 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Commercial 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Government 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Defense 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Multi-Use 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Standard 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Non-Commercial 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Internal 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Confidential 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Commercial 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Government 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Defense 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Multi-Use 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Standard 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Non-Commercial 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Internal 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Confidential 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Commercial 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Government 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Defense 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Multi-Use 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Standard 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Non-Commercial 5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Only Using 800-53 Controls Mapped to NIST CSF v1.1.
Note: TOR in Development to drive CNSS Space Overlay Update
Notional Risk Scores

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

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
- 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


• 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
  – 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:
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 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.”
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.
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
• 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.
• 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.

• 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
• 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
VALUE OF SPACE SUMMIT 2023

Co-hosted by AEROSPACE
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
Key drivers of space weather

- Electromagnetic Radiation
- Energetic Charged Particles
- Magnetic Field (Magnetized Plasma)
Solar Cycle
Approaching Solar Maximum

Experimental Solar Cycle 25 Prediction

International Sunspot Number
Predicted Max 141 - 181
Oct 2024 - Jan 2025

Space Weather Prediction Testbed
issued 6 Sep 2023
Space weather impacts on Satellites

- **Signal degradation**
- **Satellite drag**
The Sun: Magnetically Active Star

- Mostly well-behaved local star
- Periodically bristles with:
  - Sunspots/Magnetic Active Regions
    - Flares
    - Solar Energetic Particles
    - Coronal Mass Ejecta
- The results: Space Weather
  - Radio/Comms/GNSS Challenges
  - Radiations Storms
  - Geomagnetic Storms
  - Beautiful Aurora
- R/S/G scales 1-5
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
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

Long distance comm lines failed

Love (2022)
August 4 1972

- 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

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

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

Objects Including Debris

Monthly Number of Objects in Earth Orbit by Object Type

- Total Objects
- Fragmentation Debris
- Spacecraft
- Mission-related Debris
- Rocket Bodies

NASA
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?

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

Berger et al. (2020) SWE Journal
Why we need to improve Space Weather Forecasting
Interaction of the magnetosphere with the Ionosphere and Thermosphere, and the solar wind. From [Sarris, 2019]

**Why do we care?**

- **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

Auroral Electrojet (AE) Index

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

Moderate ($-50 \text{ nT} > \text{minimum of Dst} > -100 \text{ nT}$), intense ($-100 \text{ nT} > \text{minimum Dst} > -250 \text{ nT}$) or super-storm (minimum of Dst < −250 nT).

Observed changes in density

The problem!

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
+ 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
• 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
2. Birk/Guidi definition

Ecosystem transformations over time as a function of changes in available operating systems and functions.  
Linked system of systems, symbiotic functionalities, and the operating environments where they interact.  
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.  
Arrangement of parts or elements that together exhibit behavior or meaning that the individual constituents do not.  
Application of scientific knowledge to a practical means.

ENABLING SPACE ENTERPRISE EVOLUTION
Fit together >> Interoperate together >> Evolve together
ACHIEVING SPACE ENTERPRISE INTEGRATION
Across Owners/Operations of Space, Ground, and Decision Support Systems
QuantumNet provides data and mobility infrastructure
Consortium for Space Mobility and ISAM Capabilities (COSMIC)

Ronald Birk, Principal Director, The Aerospace Corporation
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?

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 information approved for unlimited public release
COSMIC Organization

Steering Committee
(USG + Industry + Academia)

Consortium Management Entity
PHASE 1: Execute day-to-day operations of the Consortium according to strategic guidance from the Steering Committee
PHASE 2: Integration across focus areas

Government Caucus

Industry Caucus

Academia Caucus

Research & Technology
Demonstration Infrastructure
Missions & Ecosystems
Policy & Regulation
Workforce Development

COSMIC information approved for unlimited public release
## Consortium Definition

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

COSMIC information approved for unlimited public release
COSMIC’s Proposed Role in the National ISAM Implementation Plan

- **NASA**
  - 2.1.2 Incorporate standards in govt SVs
  - 3.2.1 Convene a nationwide ISAM consortium
  - 6.1 Engage K-12 students in ISAM
  - 6.2 Increase access to education programs
  - 6.3 Expand multi-disciplinary education opportunities
  - 1.1.2 Launch an in-space ISAM test capability
  - 2.2.1 Close gaps in US testing capability
  - 3.2.2 Improve access to USG test facilities
  - 3.3.1 Adopt commercial modular infrastructure
  - 3.3.1 "Buy services" vs. "buy hardware"
  - 3.3.2 Create procurement documentation for ISAM

- **DOD**
  - 1.1.1 Evaluate ISAM cost/benefit
  - 1.2.1 Maintain ISAM State of Play
  - 2.2.2 Create propellant purchasing strategy
  - 2.1.3 Flight qualify standard hardware
  - 5.1 Develop ISAM procurement options

- **ODNI**
  - 1.2.3 Research power technologies
  - 1.2.4 Research autonomy technologies

- **ED**
  - 5.3 Evaluate EOL disposal policies

- **NSF**

- **DOT**
  - 2.1.1 Coordinate on standards development
  - 5.2 Revise US policy for RPO

- **FCC**
  - 4.1 Encourage international cooperation on norms

- **DOC**
  - 4.2 Assess ISAM national security risks
  - 4.3 Inform ISAM regulations
  - 4.4 Promote US regulatory intent

- **DOS**
  - 4.5 Promote international cooperation

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-OHORO
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
COSMICspace.org
University of Maryland
College Park, MD
CONSORTIUM FOR SPACE MOBILITY AND ISAM CAPABILITIES

cosmicspace.org
# COSMIC Responds to the National Need

<table>
<thead>
<tr>
<th>Tasking</th>
<th>Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>This OSAM consortium should focus on developing technologies needed by the commercial space industry (as a potential user; not just as a provider).</td>
<td>✓ 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.</td>
</tr>
<tr>
<td>To this end, the OSAM consortium should consider co-funding partners from the commercial space industry.</td>
<td>✓ Government, industry, and academic members fund their own participation.</td>
</tr>
<tr>
<td>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).</td>
<td>✓ 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&amp;D for ISAM applications.</td>
</tr>
<tr>
<td>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.</td>
<td>✓ 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.</td>
</tr>
<tr>
<td>This OSAM consortium should collaborate where there may be possible synergies and to avoid unnecessarily overlapping or duplicative federal efforts.</td>
<td>✓ Identified potential USG partners based on existing interests, expressed via membership in the OSAM National Initiative, ISAM Interagency Working Group, and other community forums.</td>
</tr>
</tbody>
</table>
## COSMIC and CONFERS: Invigorating the Community

### 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

### 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

#### 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

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

### Funding

#### NO MEMBERSHIP DUES
- Management entity funded by NASA to support whole-of-nation needs
- Members fund their own participation

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

Value of Space Summit 2023
Global Space Forecast, 2022-2027

8% Growth in 2022
$546 Billion Total
$772 Billion by 2027
Four Key Sectors

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

$546B Total

- $288.0B
- $139.6B
- $69.5B
- $49.1B
Sectors Now Showing Strong Growth

- Satellite Communication
- Earth Observation
- Launch Services

Future Sectors
- AI and Big Data
- New Space Stations
- Cislunar
## Top Government Space Spending

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

<table>
<thead>
<tr>
<th>Nation/Agency</th>
<th>Spending (USD)</th>
<th>2021-22 Change (USD)</th>
<th>2021-22 Change (national currency)</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>$69.5B</td>
<td>13.6%</td>
<td>13.6%</td>
</tr>
<tr>
<td>China</td>
<td>$16.1B</td>
<td>0.7%</td>
<td>4.5%</td>
</tr>
<tr>
<td>ESA*</td>
<td>$5.4B</td>
<td>11.6%</td>
<td>0.1%</td>
</tr>
<tr>
<td>Russia</td>
<td>$3.7B</td>
<td>19.7%</td>
<td>10.5%</td>
</tr>
<tr>
<td>Japan</td>
<td>$3.1B</td>
<td>11.8%</td>
<td>7.8%</td>
</tr>
<tr>
<td>European Union</td>
<td>$2.3B</td>
<td>21.4%</td>
<td>11.0%</td>
</tr>
<tr>
<td>India</td>
<td>$1.3B</td>
<td>20.6%</td>
<td>15.6%</td>
</tr>
</tbody>
</table>
Kelli Kedis Ogborn
VP of Space Commerce and Entrepreneurship
kkedisogborn@spacefoundation.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
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.
VALUE OF SPACE SUMMIT 2023

Co-hosted by AEROSPACE