"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.
WELCOME

VALUE OF SPACE SUMMIT 2023
Cyber Technical Keynote

Robert Metzger
Head of Washington Office
Rogers Joseph O'Donnell
Watch Center 2023 Trends Analysis and Presentation

Joel Francis, Watch Center Lead, Space ISAC
Watch Center 2023 Trends, Insights, and Observations

2023 Value of Space Summit – Technical Track
The Watch Center floor is organized by "cells" that correspond to functional areas related to use cases, tasking, and responsibilities.

The Coordination cell will be focused on facilitating communication between analysts and Space ISAC Members and approving reports.

There is a natural progression of physical and cyber analysis (All-Source) to Multi Domain Operations (MDO) including Signals and Space concepts.
Key Takeaways:

• China has continued to grow space and counterspace assets
• Russia has continued to display less advanced capabilities
• Iran has built one of the largest space programs in the middle east
• North Korea has increased space activity, including ISR capabilities

Key Takeaways:

• China seeks to supplant the US as the dominant power in space
• Competition has extended from near-earth orbits to cislunar and beyond
• Cislunar ambitions pose political, economic, and military implications
• The exploitation of outer space mirrors is integral to China’s national strategy

Key Takeaways:

• Threat actors leverage as-a-service offerings for phishing, identity theft and DDoS attacks
• Significant shift in cybercriminal tactics
• Russia has continued to display less advanced capabilities
• External remote services (RDP & VPNs) are among the most exploited vectors

Key Takeaways:

• Foreign Intelligence Entities (FIEs) see US space industry as vital to Economy, National Security, and Global competition
• FIEs use cyberattacks, strategic investment, and supply chain exploits
• Indicators include cyber activity and collection tactics
Nation State Actors

• Nation State Actors represent the most dangerous threat to the commercial space industry.
• Cyber actors are funded by state governments to conduct targeted, malicious cyber campaigns.
• State-sponsored cyber campaigns typically serve foreign intelligence and military objectives.
• Threat actors from China, Russia, Iran, and North Korea have demonstrated capability and intent to target space companies through a variety of methods.
• Motives are focused on establishing persistence and exfiltrating data for espionage and competitive advantage in the space sector – Living off the Land.
• Distinguished from financially motivated groups.

CHINA:
• China has doubled its number of satellites in orbit between 2019 and 2021.
• Leverages cyber & counterspace capability to target US space sector and critical infrastructure.
• China utilizes global investment (ex. BRI) to circumvent sanctions, grow global influence, and target the supply chain.

RUSSIA:
• Russia maintains cyber and counterspace capabilities.
• Threat actors use a diverse set of TTPs to disrupt organizations.
• Cyber campaigns focused on NATO member countries and military support of Ukraine.
• Several pro-Russian cybercrime groups have surfaced and routinely threaten the US defense and aerospace sectors.
Ransomware continues to be the leading category of cybercrime across all sectors. Threat groups have shifted to extortion-based tactics:

- Increased collaboration among threat actor groups: affiliate programs, as-a-service offerings, and the sale of toolkits to enable brute force attacks
- AI/ML is being leveraged for use in cyber attacks to bolster phishing and BEC attacks
- Compromised accounts are weaponized and constitute one of the most common TTP used to gain initial access
- The majority of ransomware attacks target SMBs, manufacturing and supply chain
- Darkweb marketplaces and clear web forums provide opportunities to advertise and sell stolen data
- Majority of attributed ransomware activity tied to Chinese and Russian state sponsored cyber threat actors

Hacktivists and cybercrime groups routinely leverage DDoS and defacement attacks to target websites and external assets:

- While denial of service attacks are less damaging to organizations, these attacks can be carried out by less sophisticated cybercrime groups
- Disruptive cyber activity in relation to regional conflicts (Russia/Ukraine > Israel/Hamas)
- As-a-service offerings are becoming more prominent for DDoS kits and botnet subscriptions, providing capabilities without the need to maintain botnets

Ransomware: Top Groups:
- Lockbit 3.0
- BlackBasta
- Royal Ransomware
- Akira
- BlackCat

On the Rise:
- 8Base
- NoEscape
- Cactus
- CL0P
- Play

Ransomware: Top Cybercrime Orgs:
- Lazarus
- Killnet / Killmilk
- Anonymous Sudan
- SelgedSec
- UserSec
- GhostSec

- Anonymous Russia
- REvil
Signals

- Consistent levels of interference in conflict areas, correlates to internet suppression
- Uptick in interference activities related to geopolitical conflicts (ex. Azerbaijan)
- Insights derived from FAA & ICAO NOTAMS – interference and 5G C-band testing
- Jamming activity near Baltic region, black sea observed from February - August 2023
- Verified uptick in GEO interference observations in October 2023

Space

- Increase in number of global launches, active satellites
- Uptick in Payload to Launch Ratio: ’22 = 12.68 / ’23 = 13.23
- Proliferation in LEO leading to an increase in conjunction assessment considerations
- Contested environments arise in Cislunar and VLEO
- Notice to Space Operators (NOTSOs) – Majority of maneuvers reported are from PRC owned assets.
- Satellites of interest include 41103 and 40258
- Increased solar weather in relation to solar maximum, minor impacts to satellites
Tactics, Techniques, and Procedures

Exploit Public Facing Application
- Attackers have shown the ability to infiltrate networks at the application layer through internet-facing services. This tactic is commonly used due to the prevalence of software vulnerabilities. Other applications include exploitation of VPNs and Firewalls.

Use of Valid Accounts
- Threat actors utilize valid credentials and domain accounts to obfuscate detection. The access and use of valid accounts has increased with the use of information stealers, credential harvesting, and as-a-service toolkits.

Living off the Land
- Techniques that involve using network administration tools fall under this category. Living off the Land TTPs bolster persistent access and defense evasion and are indicative of Advanced Persistent Threats.
CLOP Ransomware group exploited zero-day vulnerabilities in MOVEit file transfer software for initial access, leading to the largest string of successful ransomware attacks in 2023.

Tactics, Techniques, and Procedures

**Exploit Public Facing Application**
- Attackers have shown the ability to infiltrate networks at the application layer through internet-facing services. This tactic is commonly used due to the prevalence of software vulnerabilities. Other applications include exploitation of VPNs and Firewalls.

**Use of Valid Accounts**
- Threat actors utilize valid credentials and domain accounts to obfuscate detection. The access and use of valid accounts has increased with the use of information stealers, credential harvesting, and as-a-service toolkits.

**Living off the Land**
- Techniques that involve using network administration tools fall under this category. Living off the Land TTPs bolster persistent access and defense evasion and are indicative of Advanced Persistent Threats.
**Tactics, Techniques, and Procedures**

**Exploit Public Facing Application**
- Attacker - has shown the ability to infiltrate networks at the application layer through internet-facing services. This tactic is commonly used due to the prevalence of software vulnerabilities. Other applications include exploitation of VPNs and Firewalls.

**Use of Valid Accounts**
- Threat actors utilize valid credentials and domain accounts to obfuscate detection. The access and use of valid accounts has increased with the use of information stealers, credential harvesting, and as-a-service toolkits.

**Living off the Land**
- Techniques that involve using network administration tools fall under this category. Living off the Land TTPs bolster persistent access and defense evasion and are indicative of Advanced Persistent Threats.
Peach Sandstorm used commercial remote monitoring service AnyDesk to maintain access to victim networks. This activity was observed in a subset of a larger espionage campaign against satellite and defense sectors.

**Tactics, Techniques, and Procedures**

**Exploit Public Facing Application**
- Attackers have shown the ability to infiltrate networks at the application layer through internet-facing services. This tactic is commonly used due to the prevalence of software vulnerabilities. Other applications include exploitation of VPNs and Firewalls.

**Use of Valid Accounts**
- Threat actors utilize valid credentials and domain accounts to obfuscate detection. The access and use of valid accounts has increased with the use of information stealers, credential harvesting, and as-a-service toolkits.

**Living off the Land**
- Techniques that involve using network administration tools fall under this category. Living off the Land TTPs bolster persistent access and defense evasion and are indicative of Advanced Persistent Threats.
Tactics, Techniques, and Procedures

Exploit Public Facing Application
- Attackers have shown the ability to infiltrate networks at the application layer through internet-facing services. This tactic is commonly used due to the prevalence of software vulnerabilities. Other applications include exploitation of VPNs and Firewalls.

Use of Valid Accounts
- Threat actors utilize valid credentials and domain accounts to obfuscate detection. The access and use of valid accounts has increased with the use of information stealers, credential harvesting, and as-a-service toolkits.

Living off the Land
- Techniques that involve using network administration tools fall under this category. Living off the Land TTPs bolster persistent access and defense evasion and are indicative of Advanced Persistent Threats.
BlackTech threat actors were observed targeting network devices and modifying router firmware. They utilize custom malware and living off the land tactics to avoid endpoint detection.

<table>
<thead>
<tr>
<th>INITIAL ACCESS</th>
<th>PERSISTENCE</th>
<th>DEFENSE EVASION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Accounts</td>
<td>External Remote</td>
<td>Subvert Trust Controls</td>
</tr>
<tr>
<td>Exploit Public Facing</td>
<td>Scheduled Task/Job</td>
<td>Hijack Execution Flow</td>
</tr>
<tr>
<td>Application</td>
<td>Server Software</td>
<td>Indicator Removal</td>
</tr>
<tr>
<td></td>
<td>Component</td>
<td>Obfuscated Files or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>information</td>
</tr>
</tbody>
</table>

**Exploit Public Facing Application**
- Attackers have shown the ability to infiltrate networks at the application layer through internet-facing services. This tactic is commonly used due to the prevalence of software vulnerabilities. Other applications include exploitation of VPNs and Firewalls.

**Use of Valid Accounts**
- Threat actors utilize valid credentials and domain accounts to obfuscate detection. The access and use of valid accounts has increased with the use of information stealers, credential harvesting, and as-a-service toolkits.

**Living off the Land**
- Techniques that involve using network administration tools fall under this category. Living off the Land TTPs bolster persistent access and defense evasion and are indicative of Advanced Persistent Threats.
Tactics, Techniques, and Procedures

Exploit Public Facing Application
- Attackers have shown the ability to infiltrate networks at the application layer through internet-facing services. This tactic is commonly used due to the prevalence of software vulnerabilities. Other applications include exploitation of VPNs and Firewalls.

Use of Valid Accounts
- Threat actors utilize valid credentials and domain accounts to obfuscate detection. The access and use of valid accounts has increased with the use of information stealers, credential harvesting, and as-a-service toolkits.

Living off the Land
- Techniques that involve using network administration tools fall under this category. Living off the Land TTPs bolster persistent access and defense evasion and are indicative of Advanced Persistent Threats.
PowerDrop, a malicious PowerShell script, surfaced in June 2023, used by suspected nation-state actors to target the US Aerospace and Defense sectors.

**Tactics, Techniques, and Procedures**

<table>
<thead>
<tr>
<th>INITIAL ACCESS</th>
<th>Valid Accounts</th>
<th>Exploit Public Facing Application</th>
<th>Phishing</th>
<th>Supply Chain Compromise</th>
</tr>
</thead>
<tbody>
<tr>
<td>PERSISTENCE</td>
<td>External Remote Services</td>
<td>Scheduled Task/Job</td>
<td>Server Software Component</td>
<td>Valid Accounts</td>
</tr>
<tr>
<td>DEFENSE EVASION</td>
<td>Subvert Trust Controls</td>
<td>Hijack Execution Flow</td>
<td>Indicator Removal</td>
<td>Obfuscated Files or information</td>
</tr>
<tr>
<td>EXECUTION</td>
<td>Command and Scripting Interpreter</td>
<td>PowerShell</td>
<td>Software Deployment Tools</td>
<td>System Services</td>
</tr>
</tbody>
</table>

**Exploit Public Facing Application**
- Attackers have shown the ability to infiltrate networks at the application layer through internet-facing services. This tactic is commonly used due to the prevalence of software vulnerabilities. Other applications include exploitation of VPNs and Firewalls.

**Use of Valid Accounts**
- Threat actors utilize valid credentials and domain accounts to obfuscate detection. The access and use of valid accounts has increased with the use of information stealers, credential harvesting, and as-a-service toolkits.

**Living off the Land**
- Techniques that involve using network administration tools fall under this category. Living off the Land TTPs bolster persistent access and defense evasion and are indicative of Advanced Persistent Threats.
Exploit Public Facing Application

- Attackers have shown the ability to infiltrate networks at the application layer through internet-facing services. This tactic is commonly used due to the prevalence of software vulnerabilities. Other applications include exploitation of VPNs and Firewalls.

Use of Valid Accounts

- Threat actors utilize valid credentials and domain accounts to obfuscate detection. The access and use of valid accounts has increased with the use of information stealers, credential harvesting, and as-a-service toolkits.

Living off the Land

- Techniques that involve using network administration tools fall under this category. Living off the Land TTPs bolster persistent access and defense evasion and are indicative of Advanced Persistent Threats.
Multiple nation-state actors have exploited vulnerabilities in ManageEngine software and firewalls to target space industry. The threat actors leveraged SSH protocols to communicate with C2 servers.

### Tactics, Techniques, and Procedures

**Exploit Public Facing Application**
- Attackers have shown the ability to infiltrate networks at the application layer through internet-facing services. This tactic is commonly used due to the prevalence of software vulnerabilities. Other applications include exploitation of VPNs and Firewalls.

**Use of Valid Accounts**
- Threat actors utilize valid credentials and domain accounts to obfuscate detection. The access and use of valid accounts has increased with the use of information stealers, credential harvesting, and as-a-service toolkits.

**Living off the Land**
- Techniques that involve using network administration tools fall under this category. Living off the Land TTPs bolster persistent access and defense evasion and are indicative of Advanced Persistent Threats.
Multiple nation-state actors have exploited vulnerabilities in ManageEngine software and firewalls to target space industry. The threat actors leveraged SSH protocols to communicate with C2 servers.

PowerDrop, a malicious PowerShell script, surfaced in June 2023, used by suspected nation-state actors to target the US Aerospace and Defense sectors.

BlackTech threat actors were observed targeting network devices and modifying router firmware. They utilize custom malware and living off the land tactics to avoid endpoint detection.

Peach Sandstorm used commercial remote monitoring service AnyDesk to maintain access to victim networks. This activity was observed in a subset of a larger espionage campaign against satellite and defense sectors.

Cl0p Ransomware group exploited zero-day vulnerabilities in MOVEit file transfer software for initial access, led to the largest string of successful ransomware attacks in 2023.

**Exploit Public Facing Application**
- Attackers have shown the ability to infiltrate networks at the application layer through internet-facing services. This tactic is commonly used due to the prevalence of software vulnerabilities. Other applications include exploitation of VPNs and Firewalls.

**Use of Valid Accounts**
- Threat actors utilize valid credentials and domain accounts to obfuscate detection. The access and use of valid accounts has increased with the use of information stealers, credential harvesting, and as-a-service toolkits.

**Living off the Land**
- Techniques that involve using network administration tools fall under this category. Living off the Land TTPs bolster persistent access and defense evasion and are indicative of Advanced Persistent Threats.
Timeline of Space Sector Targeting
March – September 2023

March
- Space Manufacturers Targeted by Lockbit 3.0 and Royal Ransomware
- Iranian Threat Actor "Peach Sandstorm" targets Satellite Industry with Password Spraying Attacks

April
- GhostSec Hackers Target Satellite Networks via GNSS Receivers

May
- MOVEit Transfer Zero-Day exploited by Clop Ransomware Group
- Hacker sells "Military Satellite Access" on Russian forum

June
- Hill Aerosystems Suffers Data Breach from BlackBasta Ransomware Group
- Threat Actors Exploit CITRIX CVE to Implant Webshells

July
- Russian Satellite Service Provider Dozor-Teleport Targeted in Cyber Attack
- Turk Hack Team Compromises Aerospace Company

August
- Verified Maneuvers from Russian-Owned satellite
- Hacker Compromises Airbus, exposing vendor information

September
- Moveit Transfer Targeted by Cl0p Ransomware Group
- Hacker sells "Military Satellite Access" on Russian forum
- Hacker Compromises Airbus, exposing vendor information
- Space Manufacturers Targeted by Lockbit 3.0 and Royal Ransomware
Timeline of Space Sector Targeting
March – September 2023

Trends and Observations:

• Increased targeting of **space supply chain**
Trends and Observations:

- Increased targeting of **space supply chain**
- State-sponsored threat actor targeting
### Timeline of Space Sector Targeting

**March – September 2023**

<table>
<thead>
<tr>
<th>Month</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>March</td>
<td>Space Manufacturers Targeted by Lockbit 3.0 and Royal Ransomware</td>
</tr>
<tr>
<td>April</td>
<td>Iranian Threat Actor “Peach Sandstorm” targets Satellite Industry with Password Spraying Attacks</td>
</tr>
<tr>
<td>May</td>
<td>GhostSec Hackers Target Satellite Networks via GNSS Receivers</td>
</tr>
<tr>
<td>May</td>
<td>PowerDrop Script Targets U.S. Aerospace and Defense Industries</td>
</tr>
<tr>
<td>May</td>
<td>Hill Aeronystems Suffers Data Breach from BlackBasta Ransomware Group</td>
</tr>
<tr>
<td>May</td>
<td>Threat Actors Exploit CITRIX CVE to Implant Webshells</td>
</tr>
<tr>
<td>June</td>
<td>Hacker sells “Military Satellite Access” on Russian forum</td>
</tr>
<tr>
<td>June</td>
<td>Threat Actors Exploit CIVEX CVEs to Target Aeronautical Company</td>
</tr>
<tr>
<td>June</td>
<td>RedHotel Targets Organizations in 17 Countries</td>
</tr>
<tr>
<td>July</td>
<td>MOVEit Transfer Zero-Day exploited by Clop Ransomware Group</td>
</tr>
<tr>
<td>July</td>
<td>Russian Satellite Service Provider Dozor-Teleport Targeted in Cyber Attack</td>
</tr>
<tr>
<td>July</td>
<td>Turk Hack Team Compromises Aerospace Company</td>
</tr>
<tr>
<td>July</td>
<td>Verified Maneuvers from Russian-Owned satellite</td>
</tr>
<tr>
<td>August</td>
<td>Hacker Compromises Airbus, exposing vendor information</td>
</tr>
<tr>
<td>September</td>
<td>Hacker sells “Military Satellite Access” on Russian forum</td>
</tr>
</tbody>
</table>

### Trends and Observations:
- Increased targeting of **space supply chain**
- State-sponsored threat actor **targeting**
- Exploitation of public-facing **application / software**
Impact of Zero Trust Architecture on Space Warfare

Altif Brown, Co-Founder, Constellation Network
Securing the Cosmos

The Integration and Impact of Zero Trust Architecture in Modern Space Warfare

Altif Brown
Co-Founder & Dir, Open Source Community
Constellation Network, Inc.
Agenda

- Welcome and Introduction
- Constellation Overview
- Intro to ZTA
- Why ZTA Matters
- Emerging Technologies
- Challenges
- Use Case
- The Way Forward
Remember this number:

11
Company Overview

Fall 2023
Constellation is a 3rd generation Blockchain infrastructure that fulfills the promise of secure decentralization. We combine fast communications speeds, easy implementation and low operational costs.
Company Highlights

US Based Blockchain Infrastructure Company
- Base Layer Protocol - DAG Architecture - Custom Consensus - L0 Interoperability - Open Source

A Feeless & Scalable Network Built Around the Validation & Management of Data
- Hypergraph Transfer Protocol (HGTP) - 80k Transaction in 7 Seconds - Highly Energy Efficient

Web3 Tooling for Developers & Support for Legacy Systems
- Euclid SDK (Metagraphs) - Stargazer Multi-Currency Wallet - Node Management Support - DeFi Platform

100+ Projects from Legacy to Emerging, Engaged in Building on Constellation
- Business Accelerator Program - Web3 Legal LaunchKit - 100k+ Community Members & Wallet Holders

Native Cryptocurrency $DAG - Utility Validates Complex Data and Transactions
- #250 Market Cap Ranking - Focused on Complex Data Types VS Basic Transfer of Value (BTC, ETH, Etc.)
Threat Landscape
### Changing Landscape of Space Warfare

Increased reliance on digital systems leading to new vulnerabilities.

<table>
<thead>
<tr>
<th>External Threats</th>
<th>Development and deployment of anti-space asset weaponry</th>
<th>Global Implications</th>
</tr>
</thead>
<tbody>
<tr>
<td>➢ State-sponsored cyberattacks that target critical space infrastructure.</td>
<td>➢ Rapid development of anti-satellite weapons by major powers.</td>
<td>➢ Disruptions affecting global communication and navigation systems.</td>
</tr>
<tr>
<td>➢ Non-state actors/ Independent groups with varied motives.</td>
<td>➢ Electronic warfare: jamming, spoofing, and SATCOM interference techniques.</td>
<td>➢ Economic implications: satellite-based services, GPS, supply chains, and more.</td>
</tr>
<tr>
<td></td>
<td>➢ Dual-use technologies: Commercial tech with potential military applications.</td>
<td>➢ Geopolitical tensions arising from contested space domains.</td>
</tr>
</tbody>
</table>

### Internal Threats

- Insider sabotage
- Compromised updates
- Human errors
Introduction to Zero Trust Architecture
Origins

★ Authentication and trust have been foundational for centuries. Ancient civilizations employed seals, symbols, and other methods to validate and authenticate messages.

★ **1980s-1990s:** The dawn of digital networking brought a perimeter-based security approach, where everything inside the network was trusted, and external entities were not.

★ **2000s:** With the rise of mobile computing and cloud services, the traditional network perimeter began to erode. The need for a new security model became evident.

★ **2010:** John Kindervag, while at Forrester Research, introduced the concept of "Zero Trust". It was a revolutionary approach that suggests never trusting and always verifying, regardless of whether the resource is inside or outside the network.
What is Zero Trust Architecture?

1. **No Implicit Trust**: Trust is not based on location (e.g., inside or outside the corporate network).
2. **Least Privilege**: Users/access devices are given the minimum access required to perform their tasks.
3. **Microsegmentation**: Breaks the network into smaller zones to maintain separate access for separate segments.
4. **Continuous Verification**: Requires validation of all entities and requests, regardless of source.

NEVER TRUST, ALWAYS VERIFY
Why Zero Trust Architecture Matters?

- **Enhanced Security**: Reduces the attack surface and limits lateral movement.
- **Flexibility**: Adapts to various digital environments, from cloud to on-premises.
- **Improved Compliance**: Helps organizations meet stringent regulatory requirements.
- **Proactive Defense**: Shifts from reactive security measures to proactive defenses.

Executive Order (EO) 14028
The Nexus of ZTA & Emerging Technologies
Do You Remember That Number?
Decentralization:
No single point of trust. Trust is distributed across the network nodes.

Cryptography:
Every transaction is cryptographically signed. Block hashes ensure data integrity and prevent tampering.

Consensus Algorithms:
Transactions/data transfers are only added to the blockchain after network consensus, ensuring authenticity and reliability.

Key Takeaways

**Trustless Environment:** Blockchains are inherently designed to function in a trustless environment. Trust is generated through protocol & math, not through intermediaries.

**Security:** Zero Trust minimizes attack vectors, and blockchain’s inherent zero trust properties add an additional layer of security against malicious actors.

**Decentralized Verification:** Blockchain’s verification process is distributed, ensuring that trust isn’t centralized.
Other Emerging Technologies

Quantum Resistance

- Quantum computing poses threats to current encryption.
- Quantum-resistant algorithms in development to protect against quantum breaches.

Artificial Intelligence/Machine Learning

- Forefront of threat modeling.
- Predictive analysis & real-time responses.
- AI growth predicted at $1.3 Trillion by 2032.
- Challenges: Quality data reliance & space systems integration.
Other Emerging Technologies

**Edge Computing**

- Process data at its source.
- Advantages: Reduced latency & data exposure alignment with ZTA

**Remote Security Posture Attestation**

- Lightweight, scalable way to implement security across large, dynamic SATCOM ecosystems containing diverse devices with varying capabilities
- Ensures device trustworthiness for risk management in HSN (Hybrid Space Network)
- Not constrained by SWaP
Key Challenges in ZTA Implementation

Real-time Authentication Challenges
Need for instantaneous decisions based on real-time data.
Balancing rigorous ZTA authentication without introducing operation-impeding latencies.

Micro-segmentation in Satellite Networks
Complex interactions among satellites, ground stations, and military assets.
Ensuring a security breach in one segment doesn’t compromise the entire system.

Threat of Advanced Persistent Threats (APTs)
APTs: Stealthy and long-term cyberattacks.
Amplified implications in space warfare due to potential for intelligence gathering and large-scale assaults.

Continuous Oversight and Evolution
Post-ZTA deployment isn’t the endgame.
Constant surveillance and adaptive security protocols needed to address ever-changing threats.

Synchronizing ZTA with Legacy Infrastructures
Challenges due to extended operational lifecycles of space assets.
Issues range from software incompatibilities to hardware constraints.
Use Case
USAF, AMC, and 618 AOC (the air component to USTRANSCOM) have a national defense-related mission need in the area of securing their legacy and future C2 and mission planning systems and data exchanges with their commercial partners and lay foundation for transition to big data cloud infrastructure using a unique scalable, secure end-to-end, multi-source, smart contracts, and big data Blockchain solution.
Iron SPIDR Deployment Approach

Blockchain to Blockchain Communications with a Smart Contracting Framework Enabling Secure Information Sharing for Mission Execution

- USTRANSCOM Private Permissioned Blockchain Network
- Craf Private Permissioned Blockchain Network
- Secure Smart Contracting Application for CRAF & TCAQ Communications & Mission Orchestration
- Node Operators (Virtual Machines) Powering Multiple Blockchain Networks Enforcing Security of All Data-in-Transit Transactions
- Data at Rest is Securely Stored Using Kinnami’s Encrypted Sharding Approach
Benefits & Impact
FOR BOTH USTRANSCOM & CRAF

★ Secure Intelligence Sharing Between Government and Industry
★ Protection from Spoofing, Corruption, Jamming & Man-in-the-Middle Attacks
★ Robust Cyber Intelligence to Inform Cyber Actions for Mission
★ End-to-End Encrypted Data Transmission and Storage Protection Procedures
★ Quantum Attack Protected Communications to Ensure Global Navigation
★ Ease of Deployment - Leverages Existing Infrastructure Investments
★ Highly Scalable, Fast and Uses Less Energy for Computational Use than Existing Systems
★ Real-Time Mission Progress - Secure Monitoring of Content Updates & Mission Movement
★ CRAF IP and Data is Protected Using Blockchain to Blockchain with Smart Contracting
★ All Contract Events Notarized Providing Proof of Ownership & Advanced Analytics
The Way Forward
The Way Forward

**Human Training**

- **Training & Development**: Vital despite ZTA's technological advancements.
- **Tailored Programs**: From basic ZTA courses to advanced workshops.
- **Simulated Environments**: Offer hands-on experience, replicating actual space operations.
- **Periodic Assessments**: Ensure personnel remain updated with ZTA advancements and evolving threats.

**Global Collaboration**

- **Joint R&D**: Exploring novel authentication protocols, threat detection, and seamless integration.
- **Shared Testing**: Establish environments for rigorous evaluations, simulating real-world scenarios.
- **Universal Standards**: Crucial for consistent ZTA application; should be dynamic and reviewed regularly.
- **Collaborative Platforms**: Sharing real-time threat intelligence for quick identification & mitigation.
Key Takeaways

**Evolving Threat Landscape:** Space warfare has transitioned from primarily physical threats to sophisticated cyber threats, requiring adaptive security measures.

**Limitations of Traditional Security:** Perimeter-based defenses, once effective, now show vulnerabilities against modern cyber threats, especially in the dynamic realm of space.

**ZTA's Role:** Zero Trust Architecture (ZTA) offers a proactive, adaptive, and granular approach to security, addressing both external and internal threats.

**Emerging Technologies:** Technologies like blockchain, AI, and quantum-resistant algorithms play a pivotal role in enhancing ZTA's effectiveness in space warfare.

**Collaboration is Crucial:** Given the global nature of space warfare, international collaboration, shared standards, and joint R&D initiatives are essential for effective ZTA implementation.

**Human Element:** While technology is vital, training and skill development for personnel are equally crucial to ensure the successful adoption and management of ZTA protocols.
"Trust is a vulnerability."

– John Kindervag

The father of Zero Trust
Thank You

The full length paper will be made available to the full SpaceISAC when this conference concludes.

Feel free to reach out to me:

altif@constellations.com

Special Thanks to:

- Brian Thamm
- Sophinea
- James Gallegos
- Deloitte
- William Mattull
- Viasat
Space Systems Critical Infrastructure

Nick Reese, Co-Founder and COO, Frontier Foundry

Erin Miller, Executive Director, Space ISAC
Fortifying Space: Building Cyber Resilience with Smart Design Principles

Irby Thompson, Chief Executive Officer (CEO), OP[4]
Fortifying Space: Building Cyber Resilience

SMART DESIGN PRINCIPLES FOR SPACE SYSTEMS

https://op4.io
hello@op4.io
[703] 574.0280
Agenda

- The cacophony of cybersecurity
- A lesson from thermodynamics
- Grand unifying theory
- Top 10 Smart design principles for secure space systems
- The path to cyber resilience
The "guidance" is overwhelming

Whitehouse Executive Orders

CISA guidance, DOD Instructions, IC Directives

NIST requirements

Thousands of requirements – don’t miss one!
And then reality strikes

System security posture naturally degrades over time
The currency of cybersecurity can be summed up in one word

Access

“the ability, right, or permission to approach, enter, speak with, or use”

1 Definition source: https://dictionary.com
SMART DESIGN PRINCIPLES™
FOR SECURE IOT

Design
Data-at-Rest Protection
Secure Boot
Compartmentalization
Secure Communications

Development
Secure Development Practices
Attack Surface Reduction
Mandatory Access Control

Deployment
Identity and Asset Management
Secure Software Update
Lifecycle Security Management

Download the OP[4] Smart Design Principles Whitepaper
NSA and CISA – Top Ten Cybersecurity Misconfigurations

**System Operations**

- Default configurations of software & applications
- Improper separation of user/admin privileges
- Insufficient internal network monitoring
- Lack of network segmentation
- Poor patch management
- Bypass of system access controls
- Weak or misconfigured multifactor authentication
- Insufficient access control lists (ACLs) on network
- Poor credential hygiene
- Unrestricted code execution

Source: cisa.gov
The path towards cyber resilience

Start by assuming the attacker has root access to every subsystem

Confidentiality
Solvable by inverting the privilege hierarchy
Make an attacker’s access inconsequential

Integrity
Solvable using cyber-fault-tolerant designs
Turn the attacker’s access into a “don’t care”

Availability
About the OP[4] Team

OP[4] was founded by established cybersecurity experts and industry leaders with a unique specialty performing offensive security assessments for embedded mission systems. The founder’s groundbreaking research for DARPA has catalyzed *Automated Program Analysis* for commercial cybersecurity applications.

Don’t Let the Enemy W[in]!
Take the next step
https://op4.io
hello@op4.io
[703] 574.0280
Supply Chain Risk Management Survey, Space ISAC SCRM COI

Megan Moloney, Associate Director, Defense and Security Segment, Guidehouse
PURPOSE

INFORM SPACE ISAC SCRM WORKING GROUP
• Vision: To promote a more secure space infrastructure through increased community engagement, information sharing, supply chain visibility, and cyber survivability.

ILLUMINATE SPACE SCRM ENVIRONMENT
• February 2023 Pilot Survey
• 18 October 2023 Live Survey

➢ INTENDED OUTCOMES:
• Shared infographic and insights
• Starting point for collective understanding of SCRM environment
• SCRM Working Group priorities
LEVEL SETTING

- You need a cell phone or laptop with connectivity
- One survey per person
- Answer based upon your experience
- Please answer all questions to allow for robust analysis
- Discussion around questions will not occur nor will there be livestreaming
- Survey will be open until end of day if extra time is needed
- Formal results will be shared
- Survey responses will be treated as anonymous, but it is requested that you provide your contact information on sign-in sheet, chat, and/or on survey if you’d like a copy of the results
LIVE COMMUNITY
SCRM SURVEY

YOUR VOICE MATTERS

You can also vote at Slido.com with the code #1336294

Go to “Polls” tab on the top right
Question 1

Which best characterizes your organization?

- Industry
- Government
- FFRDC
- Academia
- Other
What is the size of your organization?

1-50 People
51-250 People
251-500 People
501-2,000 People
2,001-10,000 People
10,000+ People
Question 3

On which space segments does your organization concentrate? (Mark all that apply)

- Ground Segment
- Launch Segment
- Link Segment
- Space Segment
Question 4

Which part of the space lifecycle does your organization concentrate on? (Mark all that apply)

- Research & Development
- Manufacturing
- Launch
- On-Orbit Operations
- End-of-Life/Recovery
- Other
Question 5

Which of the following best describes the organization of SCRM efforts within your organization?

- Centralized enterprise-wide program
- Centralized oversight, decentralize execution
- Siloed
- Minimal/None
- Other
Question 6

How would you describe your SCRM maturity?

Ad-hoc: *Not formalized; activities are ad-hoc, reactive*

Defined: *Policies, procedures, and strategies are formalized/documentated but not consistently implemented*

Consistently Implemented: *Consistently implemented but no effectiveness measures are lacking*

Managed and Measurable: *Quantitative and qualitative measures of effectiveness collected across the organization and used to assess and make changes*

Optimized: *Fully institutionalized, repeatable, consistently implemented, and regularly updated based on changing needs*
Which of the following are barriers to the successful implementation of SCRM within your organization? (Mark all that apply)

Lack of Resources
Lack of Senior Leadership Support
Lack of Capability/Technology
Unclear Roles & Responsibilities
Lack of Authority
Lack of Awareness
Lack of User Buy-In
Other
Questions 8-10: Lifecycle Ranking

Risk = Vulnerability x Threat x Severity of Impact

Question 8:
Rank each stage of the supply chain lifecycle from most vulnerable to least

Question 9:
Rank each stage of the supply chain lifecycle from most threatened to least

Question 10:
Rank each stage of the supply chain lifecycle from most likely to experience to most severe impacts to least
Question 11

Which of the following disruptive actors poses the most threat to your supply chain? (Mark all that apply)

State Actors – Intelligence
State Actors – Economic
Hybrid State/Non-state actors – Intelligence
Hybrid State/Non-state actors – Economic
Natural Disaster
Public Health Crisis
Other
Which of the following disruptions poses a threat to your supply chain? (Mark all that apply)

- Sourcing interruptions
- Counterfeit materials
- Limited supply
- Limited supplier diversity
- Malicious intrusion
- Anti-tamper insufficiencies
- Lack of Supplier Modularity
- Geopolitical Instability (non-conflict)
- War/Conflict
- Other
Question 13

Which risk do you perceive as the greatest to your organization? (Mark all that apply)

- Financial
- Operational
- Information and Security
- Software
- Reputational
Question 14

What does your organization need to strengthen supply chain risk management?

Please provides 1-3 word response(s)
THANK YOU FOR PARTICIPATING!

YOUR VOICE MATTERS

Continue to vote at Slido.com with the code #1336294

Megan M. Moloney
mmoloney@guidehouse.com
Linkedin.com/in/mmmoloney
Critical Challenges to Protecting Human Habitats On Orbit, On The Moon, And Beyond

Laura Winter, Editor & Host, Defense & Aerospace Report, The DownLink Podcast

Jason Aspiotis, Director, In-Space Infrastructure & Logistics, Axiom Space

Samuel Visner, Fellow, The Aerospace Corporation
Space ISAC AI/ML COI
"Machine Learning Security Operations – MLSecOps"

Max Spolaor, Ph.D., Sr. Engineering Specialist – Advanced Autonomy, The Aerospace Corporation

Michelle Archuleta, Ph.D., Director of Data Science, RS21
Carnegie Mellon Sei
Research on Securing Cyber-physical Systems in Space

Dionisio de Niz, Technical Director
Assuring Cyber Physical Systems Directorate, Carnegie Mellon University
Cyber Threat Analysis as-a-Service (CTAaaS)

William Belei, Aerospace Corporation, Cyber Operations and Resiliency Department (CORD)
An Automated Supplemental Cyber Risk Assessment Tool that Leverages Open-Source Cyber Threat Intelligence (CTI)

William Belei,
Aerospace Corporation,
Cyber Operations and Resiliency Department (CORD)

2023-10-18
Canaries were iconically used in coal mines to detect the presence of carbon monoxide. The bird’s rapid breathing rate, small size, and high metabolism, compared to the miners, led birds in dangerous mines to succumb before the miners, thereby giving the miners time to take action.

Border Fancy Canary
Virtual Canaries in Global Cybercoalmines

The world and its massive network of "virtual canaries in global cybercoalmines" are reporting more and more. The industry is becoming more open and more collaborative due to collective recognition in the value and need in sharing cyber threat information and regulatory and legal pressures mandating such sharing. The more the better, right? Not so easy.

- Scale: 200 plus pages
- Format: all over place
- Usage for analysis (not made for mental/manual)
Air Force Customer Turned to Aerospace For Help In Developing a Pragmatic Way of Leveraging Real-World Cyber Threat Intel (CTI)

• Customer: Authorizing Official (AO) office with significant resource limitations and looking to significantly increase the efficacy of their Cyber Risk Assessments. The approach had the following requirements/limitations:
  – Must be mostly automated
  – Measure a given system’s strategic level cyber risk posture
  – Use the system’s non-compliant security controls to represent the system’s vulnerabilities
  – Use existing open-source CTI to represent real-world Threat Sources and Threat Events (no-classified sources (at first))

Note: need to compress a pretty complex topic into 30 minutes. Happily available for follow on engagements to explain the methodology in more detail!
What Did Aerospace Learn and How Did We Apply That to a Solution?

A Virtual Global Network of Canaries in Cyber Coal Mines Exists!

Challenges Have Driven Organizations to Use Junk Science

Aerospace Developed a Methodology to Leverage ATT&CK, a CTID Mapping, and NIST SP 800-30
A Virtual Global Network of Canaries in Cyber Coal Mines Exists!
What Did Aerospace Learn and How Did We Apply That to a Solution?

A Virtual Global Network of Canaries in Cyber Coal Mines Exists!

Challenges Have Driven Organizations to Use Junk Science

Aerospace Developed a Methodology to Leverage ATT&CK, a CTID Mapping, and NIST SP 800-30
Challenges Have Driven Organizations to Use Junk Science
What Did Aerospace Learn and How Did We Apply That to a Solution?

A Virtual Global Network of Canaries in Cyber Coal Mines Exists!

Challenges Have Driven Organizations to Use Junk Science

Aerospace Developed a Methodology to Leverage ATT&CK, a CTID Mapping, and NIST SP 800-30
Aerospace Developed a Methodology to Leverage ATT&CK, a CTID Mapping, and NIST SP 800-30
NIST says to employ a risk model to accomplish these 3 steps:

1) Document all relevant: VUs, TEs, and TSS.

2) Analyze every possible combination to determine LI, IM, and resulting risk of each.

3) Aggregate and analyze results.
NIST says to employ a risk model to accomplish these 3 steps:

1) Document all relevant: **VUs**, **TEs**, and **TSs**.
2) Analyze every possible combination to determine **LI**, **IM**, and resulting **risk** of each.
3) Aggregate and analyze results.
NIST says to employ a risk model to accomplish these 3 steps:

1) Document all relevant: VUs, TEs, and TSs.
2) Analyze every possible combination to determine LI, IM, and resulting risk of each.
3) Aggregate and analyze results.
NIST says to employ a risk model to accomplish these 3 steps:

1) Document all relevant: VUs, TEs, and TSs.
2) Analyze every possible combination to determine LI, IM, and resulting risk of each.
3) Aggregate and analyze results.
NIST says to employ a risk model to accomplish these 3 steps:

1) Document all relevant: VUs, TEs, and TSs.
2) Analyze every possible combination to determine LI, IM, and resulting risk of each.
3) Aggregate and analyze results.

A single example of combining risk factors into a risk scenario and algorithmically scoring the resulting risk value:

```
Risk Scenario #001 = TEs * VUs = 12.34 * 8 = 98.72
```

Repeat and generate all known possible risk scenarios.
NIST says to employ a risk model to accomplish these 3 steps:

1. Document all relevant: VUs, TEs, and TSs.
2. Analyze every possible combination to determine LI, IM, and resulting risk of each.
3. Aggregate and analyze results.

A single example of combining risk factors into a risk scenario and algorithmically scoring the resulting risk value:

Risk Scenario #001 = 12.34 * 8 = 98.72

Repeat and generate all known possible risk scenarios.
Risk Scenario #001  APT 1 | NetDOSAttack | NonComp SC-7 | LI-12.34 | IM-8 – 98.72
<table>
<thead>
<tr>
<th>Risk Scenario #</th>
<th>Threat Actor</th>
<th>Impact Type</th>
<th>NonComp Control</th>
<th>LI</th>
<th>IM</th>
</tr>
</thead>
<tbody>
<tr>
<td>#001</td>
<td>APT 1</td>
<td>NetDOSAttack</td>
<td>NonComp SC-7</td>
<td>12.34</td>
<td>8</td>
</tr>
<tr>
<td>#002</td>
<td>APT 3</td>
<td>Phishing</td>
<td>NonComp Ctrl 2,10</td>
<td>2.12</td>
<td>2</td>
</tr>
<tr>
<td>#003</td>
<td>APT 29</td>
<td>UserExecution</td>
<td>NonComp Ctrl 1</td>
<td>29.31</td>
<td>10</td>
</tr>
<tr>
<td>#004</td>
<td>AquaticPanda</td>
<td>ModifyExecution</td>
<td>NonComp Ctrl 83</td>
<td>8.29</td>
<td>2</td>
</tr>
<tr>
<td>#005</td>
<td>Chimera</td>
<td>NetReconScan</td>
<td>NonComp Ctrl 49,91,139</td>
<td>4.43</td>
<td>8</td>
</tr>
<tr>
<td>#006</td>
<td>APT 1</td>
<td>HijackExecutionFlow</td>
<td>NonComp Ctrl 82,77</td>
<td>0.72</td>
<td>2</td>
</tr>
<tr>
<td>#007</td>
<td>APT 29</td>
<td>ImplantImage</td>
<td>NonComp Ctrl 4,9,37,111</td>
<td>22.81</td>
<td>4</td>
</tr>
<tr>
<td>#008</td>
<td>DarkHotel</td>
<td>ModifyExecution</td>
<td>NonComp Ctrl 1,3,78,317</td>
<td>11.41</td>
<td>2</td>
</tr>
<tr>
<td>#009</td>
<td>APT 41</td>
<td>HijackExecutionFlow</td>
<td>NonComp Ctrl 96,229</td>
<td>3.86</td>
<td>2</td>
</tr>
<tr>
<td>#010</td>
<td>APT 29</td>
<td>ModifyExecution</td>
<td>NonComp Ctrl 1,10,29,119</td>
<td>18.29</td>
<td>10</td>
</tr>
<tr>
<td>#011</td>
<td>Sandworm</td>
<td>Rootkit</td>
<td>NonComp Ctrl 1,72,73,88</td>
<td>1.86</td>
<td>6</td>
</tr>
<tr>
<td>#012</td>
<td>APT 29</td>
<td>Rootkit</td>
<td>NonComp Ctrl 1,3,233</td>
<td>12.38</td>
<td>16.52</td>
</tr>
<tr>
<td>#013</td>
<td>Machete</td>
<td>HijackExecutionFlow</td>
<td>NonComp Ctrl 166,167</td>
<td>5.13</td>
<td>10</td>
</tr>
<tr>
<td>#014</td>
<td>WizardSpider</td>
<td>ModifyExecution</td>
<td>NonComp Ctrl 201,229</td>
<td>38.86</td>
<td>2</td>
</tr>
<tr>
<td>#015</td>
<td>APT 29</td>
<td>HijackExecutionFlow</td>
<td>NonComp Ctrl 1,89,121</td>
<td>45.75</td>
<td>4</td>
</tr>
</tbody>
</table>

How can we analyze this aggregated cyber risk information and thereby turn that CTI into actionable information?
<table>
<thead>
<tr>
<th>Risk Scenario #001</th>
<th>APT 1</th>
<th>NetDOSAttack</th>
<th>NonComp SC-7</th>
<th>LI-12.34</th>
<th>IM-8 – 98.72</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Scenario #002</td>
<td>APT 3</td>
<td>Phishing</td>
<td>NonComp Ctrl 2,10</td>
<td>LI-2.12</td>
<td>IM-2 – 4.23</td>
</tr>
<tr>
<td>Risk Scenario #003</td>
<td>APT 29</td>
<td>UserExecution</td>
<td>NonComp Ctrl 1</td>
<td>LI-29.31</td>
<td>IM-10 – 293.06</td>
</tr>
<tr>
<td>Risk Scenario #004</td>
<td>AquaticPanda</td>
<td>ModifyExecution</td>
<td>NonComp Ctrl 83</td>
<td>LI-8.29</td>
<td>IM-4 – 33.17</td>
</tr>
<tr>
<td>Risk Scenario #005</td>
<td>Chimera</td>
<td>NetReconScan</td>
<td>NonComp Ctrl 49,91,139</td>
<td>LI-4.43</td>
<td>IM-8 – 35.46</td>
</tr>
<tr>
<td>Risk Scenario #006</td>
<td>APT 1</td>
<td>HijackExecutionFlow</td>
<td>NonComp Ctrl 82,77</td>
<td>LI-0.72</td>
<td>IM-2 – 1.44</td>
</tr>
<tr>
<td>Risk Scenario #007</td>
<td>APT 29</td>
<td>ImplantImage</td>
<td>NonComp Ctrl 4,9,37,111</td>
<td>LI-22.81</td>
<td>IM-4 – 91.27</td>
</tr>
<tr>
<td>Risk Scenario #008</td>
<td>DarkHotel</td>
<td>ModifyExecution</td>
<td>NonComp Ctrl 1,3,78,317</td>
<td>LI-11.41</td>
<td>IM-2 – 22.83</td>
</tr>
<tr>
<td>Risk Scenario #009</td>
<td>APT 41</td>
<td>HijackExecutionFlow</td>
<td>NonComp Ctrl 96,229</td>
<td>LI-3.86</td>
<td>IM-2 – 7.22</td>
</tr>
<tr>
<td>Risk Scenario #010</td>
<td>APT 29</td>
<td>ModifyExecution</td>
<td>NonComp Ctrl 1,10,29,119</td>
<td>IM-18.29</td>
<td>IM-10 – 182.89</td>
</tr>
<tr>
<td>Risk Scenario #011</td>
<td>Sandworm</td>
<td>Rootkit</td>
<td>NonComp Ctrl 1,72,73,88</td>
<td>LI-1.86</td>
<td>IM-6 – 11.18</td>
</tr>
<tr>
<td>Risk Scenario #012</td>
<td>APT 29</td>
<td>Rootkit</td>
<td>NonComp Ctrl 1,3,233</td>
<td>LI-12.38</td>
<td>LI-16.52</td>
</tr>
<tr>
<td>Risk Scenario #013</td>
<td>Machete</td>
<td>HijackExecutionFlow</td>
<td>NonComp Ctrl 166,167</td>
<td>LI-5.13</td>
<td>IM-10 – 51.26</td>
</tr>
<tr>
<td>Risk Scenario #014</td>
<td>WizardSpider</td>
<td>ModifyExecution</td>
<td>NonComp Ctrl 201,229</td>
<td>LI-38.86</td>
<td>IM-2 – 77.72</td>
</tr>
<tr>
<td>Risk Scenario #015</td>
<td>APT 29</td>
<td>HijackExecutionFlow</td>
<td>NonComp Ctrl 1,89,121</td>
<td>LI-45.75</td>
<td>IM-4 – 183.82</td>
</tr>
</tbody>
</table>

2,527 total risk
<table>
<thead>
<tr>
<th>Risk Scenario #</th>
<th>Technique</th>
<th>Compromised System</th>
<th>LI</th>
<th>IM</th>
</tr>
</thead>
<tbody>
<tr>
<td>#001 APT 1</td>
<td>NetDOSAttack</td>
<td>NonComp SC-7</td>
<td>12.34</td>
<td>98.72</td>
</tr>
<tr>
<td>#002 APT 3</td>
<td>Phishing</td>
<td>NonComp Ctrl 2,10</td>
<td>2.12</td>
<td>4.23</td>
</tr>
<tr>
<td>#003 APT 29</td>
<td>UserExecution</td>
<td>NonComp Ctrl 1</td>
<td>29.31</td>
<td>293.06</td>
</tr>
<tr>
<td>#004 AquaticPanda</td>
<td>ModifyExecution</td>
<td>NonComp Ctrl 83</td>
<td>8.29</td>
<td>33.17</td>
</tr>
<tr>
<td>#005 Chimera</td>
<td>NetReconScan</td>
<td>NonComp Ctrl 49,91,139</td>
<td>4.43</td>
<td>35.46</td>
</tr>
<tr>
<td>#006 APT 1</td>
<td>HijackExecutionFlow</td>
<td>NonComp Ctrl 82,77</td>
<td>0.72</td>
<td>1.44</td>
</tr>
<tr>
<td>#007 APT 29</td>
<td>ImplantImage</td>
<td>NonComp Ctrl 4,9,37,111</td>
<td>22.81</td>
<td>91.27</td>
</tr>
<tr>
<td>#008 DarkHotel</td>
<td>ModifyExecution</td>
<td>NonComp Ctrl 1,3,78,317</td>
<td>11.41</td>
<td>22.83</td>
</tr>
<tr>
<td>#009 APT 41</td>
<td>HijackExecutionFlow</td>
<td>NonComp Ctrl 96,229</td>
<td>3.86</td>
<td>7.22</td>
</tr>
<tr>
<td>#010 APT 29</td>
<td>ModifyExecution</td>
<td>NonComp Ctrl 1,10,29,119</td>
<td>18.29</td>
<td>182.89</td>
</tr>
<tr>
<td>#011 Sandworm</td>
<td>Rootkit</td>
<td>NonComp Ctrl 1,72,73,88</td>
<td>1.86</td>
<td>11.18</td>
</tr>
<tr>
<td>#012 APT 29</td>
<td>Rootkit</td>
<td>NonComp Ctrl 1,3,233</td>
<td>12.38</td>
<td>99.09</td>
</tr>
<tr>
<td>#013 Machete</td>
<td>HijackExecutionFlow</td>
<td>NonComp Ctrl 166,167</td>
<td>5.13</td>
<td>51.26</td>
</tr>
<tr>
<td>#014 WizardSpider</td>
<td>ModifyExecution</td>
<td>NonComp Ctrl 201,229</td>
<td>38.86</td>
<td>77.72</td>
</tr>
<tr>
<td>#015 APT 29</td>
<td>HijackExecutionFlow</td>
<td>NonComp Ctrl 1,89,121</td>
<td>45.75</td>
<td>183.82</td>
</tr>
</tbody>
</table>

*How about finding out which TE Techniques our system is the most risk exposed to (again, based on the data in ATT&CK) so we can prioritize mitigations?*
<table>
<thead>
<tr>
<th>Risk Scenario #005</th>
<th>Chimera</th>
<th>NetReconScan</th>
<th>NonComp Ctrl 49,91,139</th>
<th>LI-4.43</th>
<th>IM-8 – 35.46</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Scenario #006</td>
<td>APT 1</td>
<td>NonComp Ctrl 82,77</td>
<td>LI-0.72</td>
<td>IM-2 – 1.44</td>
<td></td>
</tr>
<tr>
<td>Risk Scenario #007</td>
<td>APT 29</td>
<td>ImplantImage</td>
<td>NonComp Ctrl 4,9,37,111</td>
<td>LI-22.81</td>
<td>IM-4 – 91.27</td>
</tr>
<tr>
<td>Risk Scenario #008</td>
<td>DarkHotel</td>
<td>ModifyExecution</td>
<td>NonComp Ctrl 1,3,78,317</td>
<td>LI-11.41</td>
<td>IM-2 – 22.83</td>
</tr>
<tr>
<td>Risk Scenario #009</td>
<td>APT 41</td>
<td>NonComp Ctrl 96,229</td>
<td>LI-3.86</td>
<td>IM-2 – 7.22</td>
<td></td>
</tr>
<tr>
<td>Risk Scenario #010</td>
<td>APT 29</td>
<td>ModifyExecution</td>
<td>NonComp Ctrl 1,10,29,119</td>
<td>IM-18.29</td>
<td>IM-10 – 182.89</td>
</tr>
<tr>
<td>Risk Scenario #011</td>
<td>Sandworm</td>
<td>Rootkit</td>
<td>NonComp Ctrl 1,72,73,88</td>
<td>LI-1.86</td>
<td>IM-6 – 11.18</td>
</tr>
<tr>
<td>Risk Scenario #012</td>
<td>APT 29</td>
<td>Rootkit</td>
<td>NonComp Ctrl 1,3,233</td>
<td>LI-12.38</td>
<td>LI-16.52</td>
</tr>
<tr>
<td>Risk Scenario #013</td>
<td>Machete</td>
<td>NonComp Ctrl 166,167</td>
<td>LI-5.13</td>
<td>IM-10 – 51.26</td>
<td></td>
</tr>
<tr>
<td>Risk Scenario #014</td>
<td>WizardSpider</td>
<td>ModifyExecution</td>
<td>NonComp Ctrl 201,229</td>
<td>LI-38.86</td>
<td>IM-2 – 77.72</td>
</tr>
<tr>
<td>Risk Scenario #015</td>
<td>APT 29</td>
<td>NonComp Ctrl 1,89,121</td>
<td>LI-45.75</td>
<td>IM-4 – 183.82</td>
<td></td>
</tr>
</tbody>
</table>

And how about using the above to inform our Red and Blue Teams as to which TTPs to prioritize for cyber training and exercises?

How about finding out which TE Techniques our system is the most risk exposed to (again, based on the data in ATT&CK) so we can prioritize mitigations?

And, what kind of help can ATT&CK provide towards the pragmatic steps to address these techniques?
How about objectively prioritizing cyber mitigations investments. Ex. Should we focus resources on mitigating risks by implementing security Ctrl 1 or Ctrl 2? Which is the higher priority?
<table>
<thead>
<tr>
<th>Risk Scenario #001</th>
<th>APT 1</th>
<th>NetDOSAttack</th>
<th>NonComp SC-7</th>
<th>LI-12.34</th>
<th>IM-8 – 98.72</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Scenario #002</td>
<td>APT 3</td>
<td>Phishing</td>
<td>NonComp Ctrl 2,10</td>
<td>LI-2.12</td>
<td>IM-2 – 4.23</td>
</tr>
<tr>
<td>Risk Scenario #003</td>
<td>APT 29</td>
<td>UserExecution</td>
<td>NonComp Ctrl 1</td>
<td>LI-29.31</td>
<td>IM-10 – 293.06</td>
</tr>
<tr>
<td>Risk Scenario #004</td>
<td>AquaticPanda</td>
<td>ModifyExecution</td>
<td>NonComp Ctrl 83</td>
<td>LI-8.29</td>
<td>IM-4 – 33.17</td>
</tr>
<tr>
<td>Risk Scenario #005</td>
<td>Chimera</td>
<td>NetReconScan</td>
<td>NonComp Ctrl 49,91,139</td>
<td>LI-4.43</td>
<td>IM-8 – 35.46</td>
</tr>
<tr>
<td>Risk Scenario #006</td>
<td>APT 1</td>
<td>HijackExecutionFlow</td>
<td>NonComp Ctrl 82,77</td>
<td>LI-0.72</td>
<td>IM-2 – 1.44</td>
</tr>
<tr>
<td>Risk Scenario #007</td>
<td>APT 29</td>
<td>ImplantImage</td>
<td>NonComp Ctrl 4,9,37,111</td>
<td>LI-22.81</td>
<td>IM-4 – 91.27</td>
</tr>
<tr>
<td>Risk Scenario #008</td>
<td>DarkHotel</td>
<td>ModifyExecution</td>
<td>NonComp Ctrl 1,3,78,317</td>
<td>LI-11.41</td>
<td>IM-2 – 22.83</td>
</tr>
<tr>
<td>Risk Scenario #009</td>
<td>APT 41</td>
<td>HijackExecutionFlow</td>
<td>NonComp Ctrl 96,229</td>
<td>LI-3.86</td>
<td>IM-2 – 7.22</td>
</tr>
<tr>
<td>Risk Scenario #010</td>
<td>APT 29</td>
<td>ModifyExecution</td>
<td>NonComp Ctrl 1,10,29,119</td>
<td>IM-18.29</td>
<td>IM-10 – 182.89</td>
</tr>
<tr>
<td>Risk Scenario #011</td>
<td>Sandworm</td>
<td>Rootkit</td>
<td>NonComp Ctrl 1,72,73,88</td>
<td>LI-1.86</td>
<td>IM-6 – 11.18</td>
</tr>
<tr>
<td>Risk Scenario #012</td>
<td>APT 29</td>
<td>Rootkit</td>
<td>NonComp Ctrl 1,3,233</td>
<td>LI-12.38</td>
<td>LI-16.52</td>
</tr>
<tr>
<td>Risk Scenario #013</td>
<td>Machete</td>
<td>HijackExecutionFlow</td>
<td>NonComp Ctrl 166,167</td>
<td>LI-5.13</td>
<td>IM-10 – 51.26</td>
</tr>
<tr>
<td>Risk Scenario #014</td>
<td>WizardSpider</td>
<td>ModifyExecution</td>
<td>NonComp Ctrl 201,229</td>
<td>LI-38.86</td>
<td>IM-2 – 77.72</td>
</tr>
<tr>
<td>Risk Scenario #015</td>
<td>APT 29</td>
<td>HijackExecutionFlow</td>
<td>NonComp Ctrl 1,89,121</td>
<td>LI-45.75</td>
<td>IM-4 – 183.82</td>
</tr>
</tbody>
</table>
Based on the 3 non-compliant controls entered (explicit and known Vulnerabilities (VU)), CTAaaS analysis has determined the following:

- Your system is exposed to 8 MITRE ATT&CK Threat Event Techniques (TE Techniques) and are subsequently referred to in this report as “Menacing TE Techniques.”

- Of those 8 Menacing TE Techniques, there are currently 11 MITRE ATT&CK Threat Source Groups (TS Groups) that are known by MITRE to employ those specific Menacing TE Techniques and are subsequently referred to in this report as “Menacing TS Techniques.”

- CTAaaS has assembled all the possible combinations of those Menacing TE Techniques and Menacing TS Techniques into 15 of known-possible Risk Scenarios.

- Each of these 15 Risk Scenarios have been quantified by CTAaaS employing NIST SP 800-30R1 guidance on semi-quantitative assessments and have been documented in the Cyber Risk Register (CRR) contained within the CRR tab of this CTAaaS report.

- And finally, the overall cyber risk posture of this system is considered to be the total score of all the risk scenarios in the CRR which for this system is: 2,527.
CTAaaS For the Space ISAC Community

• How is CTAaaS is a service (vice software tool to be distributed)?:
  – Aerospace to keep spreadsheet tool up to date with continually updated MITRE ATT&CK data/structure
  – Will provide refreshed spreadsheets to CTAaaS users

• Why was CTAaaS functionality made available to users as a spreadsheet vice website?
  – Avoids having to deploy software to countless user environments
  – Many users were unwilling to enter their sensitive security control status information into a CTAaaS website
  – Avoids need for ATO by relying on a standard MS Office product (note: MS Excel Spreadsheet uses no-macros)

• Status of Availability to Space ISAC and Members/Partners
  – Going through Aerospace legal to obtain terms of use language and permission to distribute CTAaaS functionality
  – Adding SPARTA techniques into methodology
  – Plan to imbed CTAaaS reports/analysis into Space Watch Center reports
  – Will host subsequent Q&A sessions with interested users

For more information, contact William.d.belei@Aero.org
Backup Content Past This Point
System Information Discovery

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from System Information Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Tools such as Systeminfo can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the 'appexec' configuration tool on macOS. As an example, adversaries with user-level access can:

- Make modifications to the system configuration
- Install malicious software
- Gain escalated privileges

Procedure Examples:

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00085</td>
<td>41 RAT</td>
<td>41 RAT sends an OS version identifier in its beacon.</td>
</tr>
<tr>
<td>01220</td>
<td>Action RAT</td>
<td>Action RAT has the ability to collect the hostname, OS version, and OS architecture of an infected host.</td>
</tr>
<tr>
<td>00018</td>
<td>admin338</td>
<td>admin338 actors used the following commands after exploiting a machine with LOWBALL: malware to obtain information about the OS processes.</td>
</tr>
<tr>
<td>00468</td>
<td>ADVSTORESHELL</td>
<td>ADVSTORESHELL can run Systeminfo to gather information about the victim.</td>
</tr>
<tr>
<td>05311</td>
<td>Agent Tools</td>
<td>Agent Tools can collect the victim’s computer name and also has the capability to collect information on the processes, memory, OS, and video card from the system.</td>
</tr>
<tr>
<td>01255</td>
<td>Amnsea</td>
<td>Amnsea has collected the computer name and OS version from a compromised machine.</td>
</tr>
<tr>
<td>01084</td>
<td>AppleX</td>
<td>AppleX has collected the victim host information after infection.</td>
</tr>
<tr>
<td>05622</td>
<td>AppleSag</td>
<td>AppleSag can identify the OS version of a targeted system.</td>
</tr>
<tr>
<td>00036</td>
<td>APT18</td>
<td>APT18 can collect system information from the victims’ machines.</td>
</tr>
<tr>
<td>00071</td>
<td>APT19</td>
<td>APT19 collected system architecture information, APT19 used an HTTP malware variant and a Port 22 malware variant to gather the hostname and CPU information from the victims’ machines.</td>
</tr>
<tr>
<td>00016</td>
<td>APT29</td>
<td>APT29 used masstox to check available free space before executing actions that might create data.</td>
</tr>
<tr>
<td>00022</td>
<td>APT3</td>
<td>APT3 has a tool that can obtain information about the local system.</td>
</tr>
</tbody>
</table>

Return to background/details
## Enterprise Techniques

Techniques represent how an adversary achieves a tactical goal by performing an action. For example, an adversary may dump credentials to achieve credential access.

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1548</td>
<td>Abuse Elevation Control Mechanism</td>
<td>Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can perform on a machine. Authorization has to be granted to specific users in order to perform tasks that can be considered of higher risk. An adversary can perform several methods to take advantage of built-in control mechanisms in order to escalate privileges on a system.</td>
</tr>
<tr>
<td>.001</td>
<td>Setuid and Setgid</td>
<td>An adversary may abuse configurations where an application has the setuid or setgid bits set in order to get code running in a different (and possibly more privileged) user's context. On Linux or macOS, when the setuid or setgid bits are set for an application binary, the application will run with the privileges of the owning user or group respectively. Normally an application is run in the current user's context, regardless of which user or group owns the application. However, there are instances where programs need to be executed in an elevated context to function properly, but the user running them may not have the specific required privileges.</td>
</tr>
<tr>
<td>.002</td>
<td>Bypass User Account Control</td>
<td>Adversaries may bypass UAC mechanisms to elevate process privileges on system. Windows User Account Control (UAC) allows a program to elevate its privileges (tracked as integrity levels ranging from low to high) to perform a task under administrator-level permissions, possibly by prompting the user for confirmation. The impact to the user ranges from denying the operation under high enforcement to allowing the user to perform the action if they are in the local administrators group and click through the prompt or allowing them to enter an administrator password to complete the action.</td>
</tr>
<tr>
<td>.003</td>
<td>Sudo and Sudo Caching</td>
<td>Adversaries may perform sudo caching and/or use the sudders file to elevate privileges. Adversaries may do this to execute commands as other users or spawn processes with higher privileges.</td>
</tr>
<tr>
<td>.004</td>
<td>Elevated Execution with Prompt</td>
<td>Adversaries may leverage the AuthorizationExecutionWithPrivileges API to escalate privileges by prompting the user for credentials. The purpose of this API is to give application developers an easy way to perform operations with root privileges, such as for application installation or updating. This API does not validate that the program requesting root privileges comes from a reputable source or has been maliciously modified.</td>
</tr>
<tr>
<td>T1134</td>
<td>Access Token</td>
<td>Adversaries may modify access tokens to operate under a different user or system security context to perform</td>
</tr>
</tbody>
</table>
### Associated Group Descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRON RITUAL</td>
<td></td>
</tr>
<tr>
<td>IRON HELMET</td>
<td></td>
</tr>
</tbody>
</table>

#### Techniques Used

<table>
<thead>
<tr>
<th>Domain</th>
<th>ID</th>
<th>Name</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>NobleBaron</td>
<td>T148</td>
<td>Abuse Elevation Control Mechanism: Bypass User Account Control</td>
<td>APT29 has bypassed IAC.</td>
</tr>
<tr>
<td>Dark Halo</td>
<td>T1007</td>
<td>Account Discovery</td>
<td>APT29 obtained a list of users and their roles from an Exchange server using ( \text{ENCRYPTED} ) ( \text{METHODS} ).</td>
</tr>
</tbody>
</table>

### Software

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>References</th>
<th>Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>S0677</td>
<td>AADInternals</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### References

CRAs should be based on risk models, include explicit formulas and algorithms for combining risk factors, and result in scores/values.

- Page 16: “The expectation set forth in Special Publications 800-39 and 800-30 is that each organization or community will define a risk model appropriate to its view of risk (i.e., formulas that reflect organizational or community views of which risk factors must be considered, which factors can be combined, which factors must be further decomposed, and how assessed values should be combined algorithmically).”
- Page 28: “Organization-specific risk models include algorithms (e.g., formulas, tables, rules) for combining risk factors” (page 28)
- “Combinations of factors such as targeting, intent, and capability thus can be used to produce a score representing the likelihood of threat initiation; combinations of factors such as capability and vulnerability severity can be used to produce a score representing the likelihood of adverse impacts; and combinations of these scores can be used to produce an overall likelihood score.” (page G-1)

Guide for Conducting Risk Assessments appendices provide extensive tools

- 36 taxonomy guides, semi-quantitative assessment tables, assessment process exemplars, etc that are routinely ignored by organization risk assessment approaches

Now let’s look at some animations to explain how CTAaaS operationalizes 800-30 guidance to meet this CRA use case
Challenge 3: Profound Complexity in Deciphering Relevancy of CTI

Let’s look at how many organizations attempt to manually analyze CTI.

Ex. Commodity CTI sources:
- MITRE CVEs
- MITRE CWEs
- CISA KEVs
- Comm. Reports
- CTI feeds
- ISAC Reports

Example CTI finding:
“Threat Source (cyber group) A employed Threat Event (technique) B on [org, system, asset] C”

Is Threat Source A a cyber attacker who would be likely to attack any of my systems?

Is Threat Event B an attack technique that my systems’ are even vulnerable to?

Is [org, sys, asset] Z a similar target as the systems I’m concerned with protecting?

I’ve already got a 100 other cyber concerns, should this become my #1 or #101 concern?

If this data drives me to generate a new cyber priority, how do I find the time to mitigate this new one?

AKA – is Threat Source X contextually relevant? There are 138 Threat Sources, how do you know which are relevant and which are not?

AKA – is Threat Source X contextually relevant? There are 607 attack techniques, they map to ~7,000 different vulnerabilities. Can you determine if relevant and how relevant?

You need to know if Threat Source X is targeting same or similar targets so you can determine if relevant.

In a sense every potential cyber attack is a concern but you can’t defend against everything so understanding your priorities is KEY! So how do you measure and adjust your priorities every time CTI like this floats in?

Rarely do cyber problems have a nice and neat single solution to eliminate the risk. They typically have many different ways to mitigate (aka reduce) the risk. How can you determine the right mitigation or combination of mitigations?

So much to think about … yet so little time to do so …
Space ISAC Cislunar Affinity Group Discussion

Gabrielle Hedrick, Ph.D, Aerospace Engineer, The MITRE Corporation
Strategic Earthshot Initiative

Robert Katz, Founder, CEO & Executive Director, World Innovation Network
PPPs

[Logos of various organizations]
# Solution

## People

<table>
<thead>
<tr>
<th>Public</th>
<th>Private</th>
<th>Pupil</th>
<th>Press</th>
<th>Promises</th>
<th>Pride</th>
<th>Propagation</th>
<th>Proclamation</th>
<th>Proliferation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Promulgation</td>
<td>Prosperity</td>
<td>Projects</td>
<td>Processes</td>
<td>Planet</td>
<td>Programs</td>
<td>Partnerships</td>
<td>Partners</td>
<td>Presentations</td>
</tr>
<tr>
<td>Productivity</td>
<td>Platforms</td>
<td>Pledges</td>
<td>Plans</td>
<td>Pronouncement</td>
<td>Procurement</td>
<td>Prolongation</td>
<td>Practices</td>
<td>Proposals</td>
</tr>
<tr>
<td>People</td>
<td>Patents</td>
<td>Planning</td>
<td>Providers</td>
<td>Pipelines</td>
<td>Packaging</td>
<td>Promotion</td>
<td>Publications</td>
<td>Prospectuses</td>
</tr>
<tr>
<td>Productization</td>
<td>Perseverance</td>
<td>Power</td>
<td>Patience</td>
<td>Perspective</td>
<td>Protection</td>
<td>Perspiration</td>
<td>Prediction</td>
<td>Persepolis</td>
</tr>
<tr>
<td>Preparation</td>
<td>Politics</td>
<td>Profits</td>
<td>Persistence</td>
<td>Personality</td>
<td>Policies</td>
<td>Performance</td>
<td>Purpose</td>
<td>Passion</td>
</tr>
</tbody>
</table>
Problem

The space sector is facing a skills shortage

The space industry's looming workforce problem

Labor supply is the 'biggest challenge' facing the space industry

Labor shortage still pinching aerospace and defense sector

Space Report: Decade High in Employment, But Still Not Enough

The Space Industry Faces a Workforce Shortage Threatening its Growth

A Space Workforce Initiative Launches Amid Concerns NASA Has Insufficient Stalling for Artemis Moon Missions

Space Industry Is Growing Faster Than Its Workforce, Analysts Say

Space industry struggling to attract more skilled workers

Advice for NASA on solving its workforce shortage

SPECIAL REPORT: Defense Companies Face Post-Pandemic Workforce Shortages

Space Force: 100,000 Jobs, 100,000 Hiring

The future of the space workforce: How to attract and retain the best talent
Solution
<table>
<thead>
<tr>
<th>Educate</th>
<th>Employ</th>
<th>Energize</th>
<th>Engage</th>
<th>Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community Colleges</td>
<td>Companies</td>
<td>Defense Installations</td>
<td>Community</td>
<td>Foundations</td>
</tr>
<tr>
<td>4-Year Institutions</td>
<td>Associations</td>
<td>Defense Innovation</td>
<td>Social</td>
<td>Providers</td>
</tr>
<tr>
<td>Technical Training</td>
<td>Chambers</td>
<td>National Laboratories</td>
<td>Military</td>
<td>Professionals</td>
</tr>
<tr>
<td>K-12 Programs</td>
<td>Centers</td>
<td>Resources</td>
<td>Non-Traditional</td>
<td>Media</td>
</tr>
</tbody>
</table>
Initiative 1 - Interconnection: Holistic Hyper-Connectivity

Takes a Village
Initiative 2 - Identification: Hunt & Gather Resources

- Tools
- Tips
- Tactics
- Techniques
- Tricks
- Talent
## Initiative 3 - Information:

### National Space Month

<table>
<thead>
<tr>
<th>January</th>
<th>February</th>
<th>March</th>
<th>April</th>
</tr>
</thead>
<tbody>
<tr>
<td>su</td>
<td>mo</td>
<td>tu</td>
<td>we</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

### May

**Space Month**

<table>
<thead>
<tr>
<th>June</th>
<th>July</th>
<th>August</th>
</tr>
</thead>
<tbody>
<tr>
<td>su</td>
<td>mo</td>
<td>tu</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

### September

<table>
<thead>
<tr>
<th>October</th>
<th>November</th>
<th>December</th>
</tr>
</thead>
<tbody>
<tr>
<td>su</td>
<td>mo</td>
<td>tu</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>
Initiative 4

First Autonomous Vehicle?
Initiative 4 - Incubation: ASTROpreneurship
Initiative 5 - Invigoration: Designated Critical Infrastructure
Initiative 6
Initiative 6

Key Pillars

Human Life

Key Sustainability Factor

SUSTAINABILITY

ABUNDANT RESOURCES

ENVIROMENTAL RELIEF
Initiative 6 - Interconnection: UN SDGs
Initiative 7
Initiative 7

Operational Components
CBP – U.S. Customs and Border Protection
CISA – Cybersecurity and Infrastructure Security Agency
FEMA – Federal Emergency Management Agency
ICE – U.S. Immigration and Customs Enforcement
TSA – Transportation Security Administration
USCG – U.S. Coast Guard
USCIS – U.S. Citizenship and Immigration Services
USSS – U.S. Secret Service

Support Components
CWMD – Countering Weapons of Mass Destruction Office
DMO – Departmental Management and Operations
FLETC – Federal Law Enforcement Training Centers
I&A – Office of Intelligence and Analysis
OIG – Office of Inspector General
OPS – Office of Operations Coordination
S&T – Science and Technology Directorate
Initiative 7
Initiative 7
Initiative 8
Initiative 8
Star corps
Initiative 9 - Inclusion:

Inclusive of:
- Every Demographic
- Every Non-STEMer
- Every Background
- Every Community
- Every Experience
- Every Affiliation
- Every Discipline
- Every Diversity
- Every STEMer
- Every Domain
- Every Interest
- Every Subject
- Every Identity
- Every Profile
- Every Ability
- Every Talent
- Every Grade
- Every Major
- Every Level
- Every Field
- Every Skill
- Every Gift
- Every Age
- Everyone!

Fun for:
- All Aerospace-Fans
- All Problem-Solvers
- All Flight-Engineers
- All Videographers
- All Nature-Lovers
- All Entrepreneurs
- All Technologists
- All Star-Gazers
- All Journalists
- All Storytellers
- All Developers
- All Innovators
- All Musicians
- All Designers
- All Dreamers
- All Engineers
- All Scientists
- All Creatives
- All Thinkers
- All Builders
- All Aviators
- All Gamers
- All Makers
- All Writers
- All Coders
- All Artists
- All You!
There's a Place In Space For Every Face
Strategic Earthshot Initiative

- Educate
- Employ
- Energize
- Engage
- Enable
May the cyber - Space Work Force Be with You

Thank You
The Sky’s the Limit...Anymore

Robert S. Katz
rsk@win.ngo
+1.301.983.6700

https://win.ngo/li
https://www.linkedin.com/in/robert-scott-katz/
VALUE OF SPACE SUMMIT 2023