MAY 2025

NEEDED ADVANCEMENT FOR RESEARCH AND DEVELOPMENT IN SPACE CYBERSECURITY

BRANDON BAILEY
THE AEROSPACE CORPORATION

AEROSPACE

© 2025 The Aerospace Corporation. All trademarks, service marks, and trade names contained herein are the property of their respective owners. Approved for public release; distribution unlimited. OTR202500644

BRANDON BAILEY

Brandon Bailey is a principal engineer for the Cybersecurity and Advanced Platforms Subdivision (CAPS) at The Aerospace Corporation. In this role, Bailey has focused on developing a cyber range to support penetration testing training and in-the-lab evaluation of customers' implementations, performing vulnerability assessments and penetration testing activities for multiple customers as well as performing cybersecurity research on ground systems and spacecraft systems to better position the federal government with respect to protection of our critical space infrastructure. Bailey has also led the development of the space-focused tactic, technique, and procedures (TTPs) framework called Space Attack Research and Tactic Analysis (SPARTA). SPARTA is intended to provide unclassified information to space professionals about how spacecraft may be attacked. Bailey is a former civil servant at NASA, where he led various cybersecurity efforts and was awarded NASA's Exceptional Service Medal for his landmark cybersecurity work in 2019. He has extensive experience in the test and evaluation of systems and technology using high-fidelity digital twins with specialization in cybersecurity. Bailey graduated summa cum laude with a bachelor's degree in electrical engineering from West Virginia University and currently holds multiple certifications in the cybersecurity field.

Abstract

As space systems grow increasingly interconnected, autonomous, and mission-critical, the need for advanced cybersecurity capabilities has become paramount. This paper, developed by The Aerospace Corporation in collaboration with the Department of Homeland Security Science and Technology Directorate, outlines eight high-priority research and development areas aimed at improving the cyber resilience of space systems. These areas address key capability gaps related to on-orbit protection, zero trust (ZT) architectures, end-to-end security integration, space-tailored information technology and operational technology IT/OT measures, trustworthy operating systems, and secure interoperability. The work emphasizes the unique challenges faced in space environments, including size, weight, and power (SWaP) constraints, intermittent communications, and the lack of realtime forensics and response mechanisms. It advocates for the development of digital twins, cyber ranges, and formalized Secure-by-Design methodologies, while also promoting future-proof architectures that enable secure AI-driven autonomy. By focusing on these targeted research areas, the space ecosystem can proactively defend against evolving threats and ensure mission assurance in a contested and congested space domain.

Contents

Purpose

> ***"The United States considers unfettered freedom to operate in space vital to advancing the security, economic prosperity, and scientific knowledge of the Nation. Space systems enable key functions such as global communications; positioning, navigation, and timing; scientific observation; exploration; weather monitoring; and multiple vital national security applications. 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."***
>
> — Space Policy Directive 5 (SPD-5)[1]

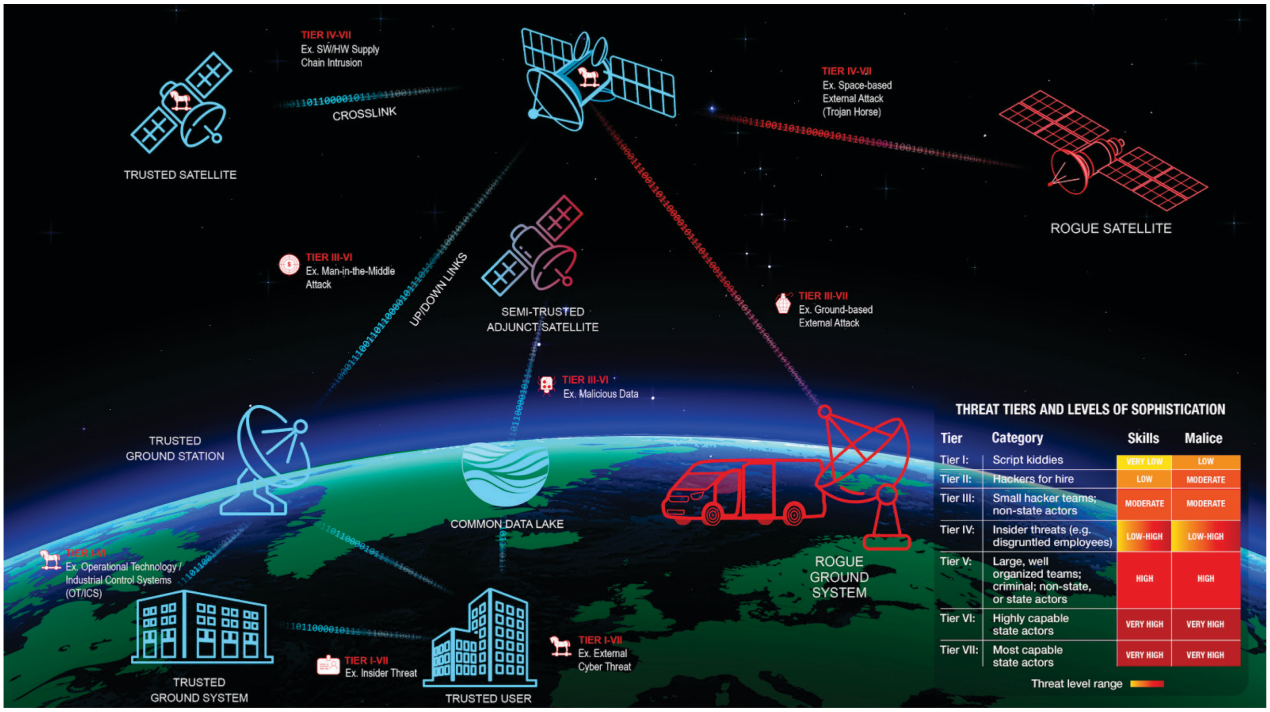
To enhance the protection of our nation's most critical space systems from cyber threats, The Aerospace Corporation, in collaboration with the Department of Homeland Security (DHS) Science and Technology Directorate (S&T), has identified eight high-priority research and development areas for advancing space cybersecurity. In alignment with SPD-5 and the Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity (EO 14144), action is required to accelerate the technology readiness of cybersecurity solutions in the space domain. By prioritizing these research areas, we can proactively mitigate emerging threats, ensure the resilience of space assets, and strengthen national security in an increasingly contested cyber landscape.

Background

Aerospace's report, *TOR-2021-01333-REV A: Cybersecurity Protections for Spacecraft: A Threat Based Approach, April 29, 2021*, recognized that space systems are leveraged by many government and commercial entities to provide global capabilities unique to the space domain. During a conflict, adversaries will seek to disrupt, deny, degrade, deceive, or destroy those capabilities. Cyberattacks are a complex but effective and increasingly prevalent attack vector in the space domain. To counter the threat posed by cyberattacks, cybersecurity and space operations are becoming inextricably linked. Space-centric cybersecurity standards and governance have been slow to materialize and are lagging the growth of the cyber threats. While P3349 - Space System Cybersecurity Working Group progresses with its secure-by-component methodology, there is still a need for advancement in research and technology readiness levels on many space-related cybersecurity countermeasures.

An example depiction of cyber threat vectors for space systems is visually represented in the Figure 1. The blue lines indicate normal expected communications/access, and the red lines indicate direct communications from adversary's infrastructure. Space systems face many well-known types of attack, including orbital, kinetic, and electronic warfare, and are vulnerable to many forms of cyber threat across multiple segments, space, communications link, and ground, within a space system architecture.

[1] Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems | Accessed September 4, 2020.



THREAT TIERS AND LEVELS OF SOPHISTICATION

Tier	Category	Skills	Malice
Tier I:	Script kiddies	VERY LOW	LOW
Tier II:	Hackers for hire	LOW	MODERATE
Tier III:	Small hacker teams; non-state actors	MODERATE	MODERATE
Tier IV:	Insider threats (e.g. disgruntled employees)	LOW-HIGH	LOW-HIGH
Tier V:	Large, well organized teams; criminal; non-state, or state actors	HIGH	HIGH
Tier VI:	Highly capable state actors	VERY HIGH	VERY HIGH
Tier VII:	Most capable state actors	VERY HIGH	VERY HIGH

Threat level range

Figure 1: Overview of cyber threat vectors for space systems.

Spacecraft are a combination of embedded hardware and software operating in the physically isolated environment of space, and cyberattacks can threaten spacecraft subsystems to include Attitude Determination and Control (AD&C), Telemetry, Tracking, and Command (TT&C), Command and Data Handling (C&DH), Electrical Power and Distribution Subsystem (EPDS), Thermal Control Subsystem (TCS), Structures and Mechanisms Subsystem (SMS), and Propulsion Subsystem (PS). A sample list of attacks against such systems includes:

- Ground-based attacks (subversion of the ground system capabilities) – using the ground system to maliciously interact with the spacecraft
- Communications hijacking on TT&C
- Embedded malicious feature during development, to include hardware-based trojans on application-specific integrated circuit (ASIC) and/or field programmable gate array (FPGA)
- Software design vulnerability exploits where designed-in features of the software are used for malicious purposes (i.e., direct memory writes to the spacecraft)
- Software-defined radio compromise
- Software weaknesses and vulnerabilities exploitation due to poor coding or inclusion of vulnerable libraries

Space Policy Directive-5 (SPD-5), released in September 2020, highlighted the following security measures that must be considered for space systems, but this list only accounts for a portion of the threat landscape:

- Physical security of TT&C environment
- TT&C protection using encryption or authentication
- Jamming and spoofing protections

- Supply Chain Risk Management
- Insider Threat

Examples of malicious cyber activities harmful to space operations include spoofing sensor data, corrupting sensor systems, jamming or sending unauthorized commands for guidance and control, injecting malicious code, and conducting denial-of-service attacks. Consequences of such activities could include loss of mission data; decreased lifespan or capability of space systems or constellations; or the loss of positive control of spacecrafts, potentially resulting in collisions that can impair systems or generate harmful orbital debris.

Cyber threats to space systems can be categorized into four segments: space, user, link, and ground (see Figure 2). Space systems must have cybersecurity protections applied to all four segments due to the unique attack surface of each segment.

Aptly summarized in Aerospace's *Defending Spacecraft in the Cyber Domain, November 2019,*

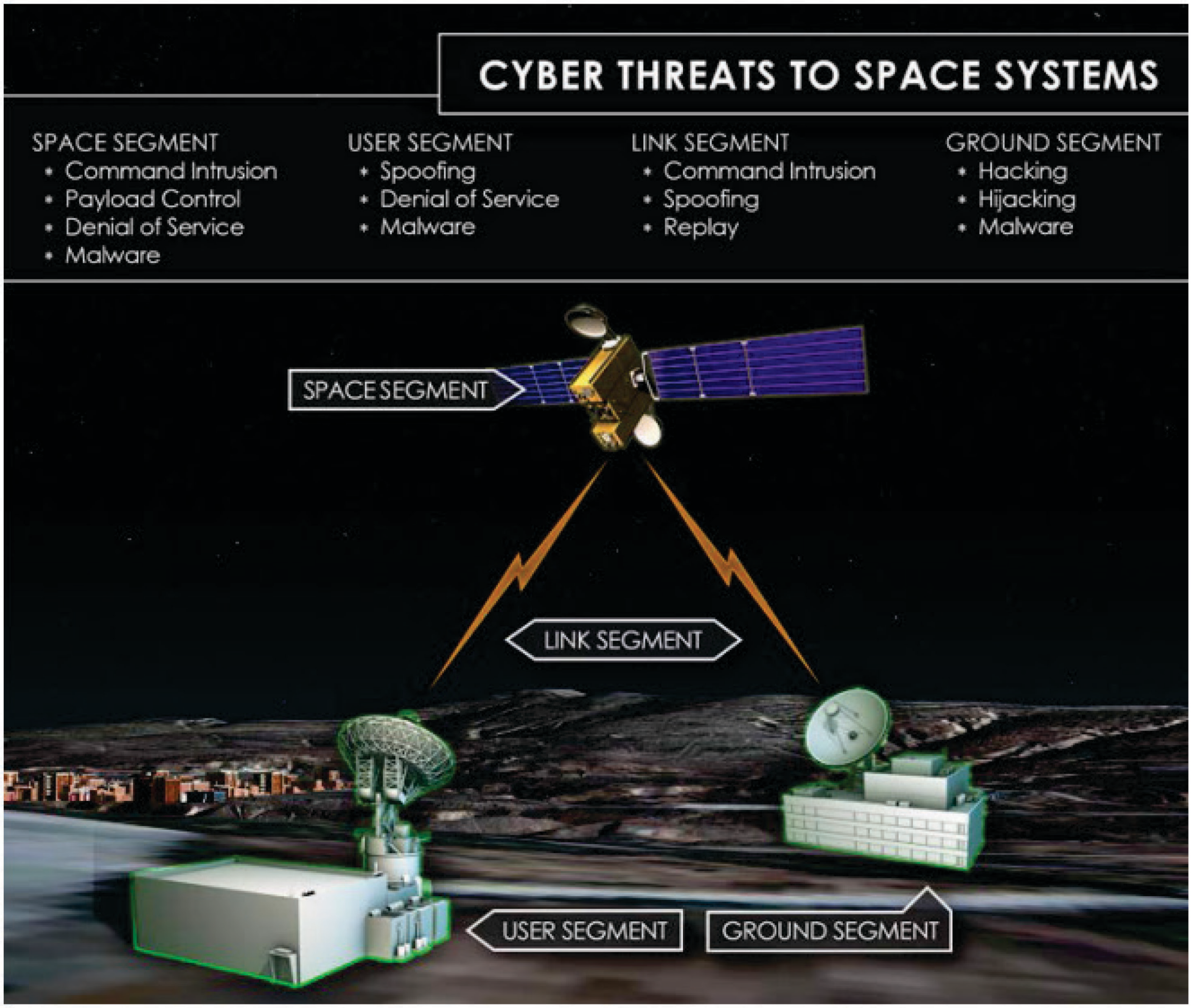


Figure 2: Cyber threats identified by the National Air and Space Intelligence Center (NASIC).

while research and open source intelligence on the vulnerabilities of space systems increase, so do the attacks. In recent years, researchers have published proof of concepts attacking satellite communication (e.g., Starlink and ViaSat ground terminals). In fact, research published by Oxford University catalogs 112 significant satellite hacking incidents, demonstrating the historic and ongoing threat to SATCOM.[2] Abstaining from action is not an option, and it is necessary for all national critical space systems to be appropriately hardened against cyber threats. According to a published research study titled Cyber Security in New Space, there has been a steady increase in attacks since the 1960s.

Defense-in-depth techniques for space system protection should be adopted across the government, industry, and international community to ensure space systems are resilient to cyber compromise. Space systems must be able to protect, detect, recover, and respond to threats, and new technologies like artificial intelligence and machine learning can aid detection and, further, inform response and recovery actions; however, specialized optimization may be required to fit within the computational and operational limits of the space system.

Needed Areas of Research

Specifically on the spacecraft, there are challenges with deploying some advanced cyber technology due to the limited technology readiness level (TRL) of solutions tailored for space systems. For example, implementing secure boot mechanisms may require radiation-hardened chips, which may not yet be widely available. Similarly, commercial off-the-shelf (COTS) intrusion detection systems (IDS) for spacecraft are in their infancy and often need customization for the unique constraints of space environments. Given these challenges posed by limited TRL solutions and the technical complexities of implementation, advancements are necessary to address the growing and sophisticated threats to space systems, which are critical to national security and global infrastructure.

The prioritization of the eight main research areas discussed in this section was informed by analysis that considered each capability's impact, feasibility, and expected timeline. While each main research area has been further decomposed into several example sub-areas, these are not intended to be exhaustive. Rather, they are illustrative of the types of research activities that could meaningfully advance progress in the broader category. The prioritization applies only to the main research areas and reflects both the urgency of the need and the practicality of implementation. Capabilities were evaluated based on their potential to significantly enhance cybersecurity, address unfilled gaps not currently covered by other initiatives, and transition feasibly into operational space systems. The result is a prioritized set of research and development (R&D) focus areas that balances strategic importance with technical viability where Areas 1 through 4 are designated as high priority due to their criticality and near-term applicability, and Areas 5 through 8 are considered medium priority based on their longer-term impact or implementation complexity. This prioritization framework is intended to guide the allocation of resources and innovation efforts toward the areas with the greatest potential to enhance mission resilience and space system cybersecurity.

One of the major challenges in space cybersecurity is the lack of sufficient modeling and simulation (M&S) capabilities for testing and validating adversarial tactics. To address this, cyber-focused digital twins and hardware-in-the-loop (HITL)

[2] Doctoral Thesis | James Pavur | University of Oxford | Securing New Space: on Satellite Cyber-Security | 2021 | page 271 | Accessed March 23, 2023.

testbeds should be developed to simulate real-world cyber threats. Additionally, model-based systems engineering (MBSE) should integrate cybersecurity elements to enhance early-stage security design for spacecraft. The expansion of space-specific cyber ranges will facilitate penetration testing, vulnerability assessments, and advanced training exercises, while some supply chain vulnerabilities can be mitigated through bug bounty programs leveraging digital twins and FlatSat environments.

Another priority is the end-to-end security integration for spacecraft and on-orbit systems, particularly in ensuring robust cryptographic protections and supply chain integrity. Research must explore heterogeneous versus homogeneous security models for proliferated low Earth orbit (pLEO) constellations, balancing interoperability with risk containment. The development of software-based cryptographic solutions with anti-tamper protections and over-the-air rekeying (OTAR) will help secure satellite communications. Furthermore, space-specific vulnerability research should be expanded by integrating known spacecraft security weaknesses into common vulnerabilities and exposures (CVEs) databases and leverage common weakness enumerations (CWEs) nomenclature. To enhance supply chain resilience, the implementation of black-box analysis and bill of materials (BOM) validation is important.

The implementation of zero trust architecture (ZTA) in space systems is a fundamental step toward cybersecurity resilience. Spacecraft require authentication and encryption models that account for latency; size, weight, and power (SWaP) constraints; and operational dependencies. Given the intermittent nature of space communications, delay-tolerant authentication and access control models should be developed to ensure that spacecraft maintain security even in disconnected states. The application of zero trust principles to spacecraft crosslinks, TT&C, and ground station interactions is essential to prevent unauthorized access and lateral movement across mission-critical networks. Additionally, high-assurance computing models leveraging formally verified hardware and software can reduce attack surfaces and protect against firmware exploitation.

A current gap in space cybersecurity is the lack of realtime on-orbit protection, detection, and response capabilities. Cyber Situational Awareness (CSA) frameworks should be established to define realtime security telemetry logging, anomaly detection, and automated threat response mechanisms. The development of on-orbit intrusion detection algorithms will improve spacecraft security by detecting unauthorized command execution, telemetry manipulation, and payload anomalies. Moreover, radio frequency (RF) detection and hardening techniques should be enhanced using AI-driven countermeasures to mitigate jamming, spoofing, and flooding attacks. To ensure mission continuity under cyberattack conditions, spacecraft should integrate autonomous response mechanisms, including the implementation of secure "cyber-safe mode" features that isolate compromised subsystems.

Expanding terrestrial IT/OT security measures into space operations is essential for improving cybersecurity in space-based infrastructures. Research should assess the suitability of security information and event management (SIEM) solutions for spacecraft to enable realtime threat detection and forensic analysis. Treating space vehicles as networked IT/OT nodes will facilitate structured access control, segmentation, and realtime security monitoring. Additionally, pre-launch cybersecurity testing protocols should be implemented to validate security patches, vulnerability assessments, and anomaly detection capabilities before spacecraft deployment. As virtualization and containerized security solutions become more prevalent in terrestrial cybersecurity, research must explore how these technologies can be adapted for space applications, ensuring secure execution environments, software isolation, and dynamic security policy enforcement.

To ensure long-term resilience, space architectures should be future proofed for adaptability, security, and autonomy. This requires the redesign of space architectures to support AI-driven decisionmaking, anomaly detection, and autonomous mission adaptation. A shift toward hardware-agnostic cybersecurity solutions can reduce reliance on rad-hardened computing while maintaining mission resilience. Additionally, distributed processing and AI-driven error correction models should be developed to allow non-rad-hardened components to operate reliably in radiation-prone environments. To enhance interoperability across space systems, modifications to spacecraft communication interfaces should be made, transitioning toward open, standardized architectures that facilitate secure data exchanges and cybersecurity intelligence sharing.

The development of trustworthy operating systems (OS) for space missions is a cornerstone of mission assurance and cybersecurity. A secure-by-design OS framework should be established, ensuring that spacecraft OS environments incorporate root-of-trust mechanisms, cryptographic integrity verification, and privilege separation. Given the harsh conditions and long-duration missions in space, OS architectures should be optimized for fail-safe, keep-alive, and self-healing operations to maintain mission continuity in the event of a cyberattack or system failure. Additionally, a suite of spacecraft OS variants should be developed to support single-satellite deep-space missions, pLEO constellations, and hybrid architectures. Finding the right balance between simplicity and complexity in OS designs is necessary to minimize attack surfaces while ensuring operational efficiency and adaptability.

The final area of focus is establishing standards for secure and interoperable space systems. As space networks evolve, the security of delay-tolerant networking (DTN) should be analyzed to protect high-latency communications from replay attacks, data corruption, and disruption. Key management protocols should be developed for intermittent communication paths, ensuring secure encryption in long-duration, air-gapped space operations. Space missions can also benefit from lessons learned in terrestrial ad hoc networks, leveraging dynamic trust models and autonomous cybersecurity protections for space-based networking. Additionally, establishing a secure-by-design framework (e.g., IEEE P3349) for space system engineering will provide structured cybersecurity validation from concept to deployment, ensuring that space systems are designed with security as a foundational requirement.

By focusing on these eight prioritized R&D areas, the space industry can accelerate the development of resilient, cyber-secure, and adaptable space systems capable of withstanding emerging threats. This strategic direction will help ensure that space assets remain protected, mission operations remain uninterrupted, and national security interests are preserved in an increasingly contested cyber environment. While each area includes representative subtopics to illustrate potential advancement paths, the prioritization applies to the main categories only. Based on impact, feasibility, and timing considerations, Areas 1 through 4 are designated as high priority, with Areas 5 through 8 identified as medium priority.

Table 1: Prioritized Capability Gap and Areas of Potential Advancement

Capability Gap		Rationale	Areas of Potential Advancement
High Priority	Insufficient modeling and simulation (M&S)	Need for informed decisionmaking in evaluating security measures, assessing cyber threats, and optimizing resource allocation for R&D. Without robust M&S capabilities, identifying vulnerabilities, testing mitigations, and ensuring mission resilience remain significant challenges.	Research and publish results using adversarial tactics, techniques, and procedures (TTPs) for attacking spacecrafts
			LEO vs. deep space vs. cislunar vs. geosynchronous orbit (GSO) threat landscape
			Integrating cybersecurity into model-based systems engineering (MBSE)
			Creating space-specific cyber ranges for advanced penetration testing, vulnerability assessments, and red/blue/purple teams
			Developing open-architecture digital twins for cybersecurity assessments and research
			Funding bug bounty programs using digital twins or FlatSats
			Evaluating the role of commercial space assets in mission-critical government functions
			Government acquisition reform to demand better data rights for security research
	Addressing end-to-end security integration for spacecraft and on-orbit systems	There is also insufficient research on the interactions between cybersecurity measures and system reliability, which may introduce unintended operational risks. Integrated security is necessary to achieve a balance between cybersecurity, reliability, and resilience.	Designing and evaluating pLEO-specific security models that balance the benefits of homogeneous vs. heterogeneous security architectures
			Developing software-based cryptographic solutions with anti-tamper features, ensuring that OTAR and key distribution mechanisms are robust against adversary compromise
			Expanding space-specific vulnerability research and including into the existing comprehensive database of CVEs/CWEs
			Enhancing supply chain protections through black-box analysis and strengthening BOM validation processes for hardware and software
			Conducting scenario-based studies on supply chain compromise impacts and developing mitigation strategies
			Defining the intersection of security, reliability, and resilience to ensure mission continuity
	Lack of suitable zero trust architecture for	Zero trust is a promising approach for securing next-generation space architectures,	Designing space specific authentication and encryption models that account for latency, SWaP constraints, and operational requirements

Table 1: Prioritized Capability Gap and Areas of Potential Advancement

	Capability Gap	Rationale	Areas of Potential Advancement
🟥	on-Orbit components	particularly in multi-tenant, multi-orbit, and autonomous systems. However, alternative security models exist, and implementing zero trust in constrained on-orbit environments poses technical and operational challenges that require further research.	Developing delay/intermittent communications tolerant authentication mechanisms to ensure that access control decisions remain effective even in disrupted or degraded communication states
			Defining and implementing zero trust attributes tailored to different space architectures, ensuring seamless integration between ground, space, and crosslinks
			Building high-assurance computing models that utilize formally verified hardware and software components, reducing attack surfaces and improving spacecraft cybersecurity posture
			Adapting Industrial Control System (ICS) security best practices to space operations, preventing adversarial control over ground systems and spacecraft command pathways
	Advancing on-orbit protection, detection, and response for spacecraft cybersecurity	Current space systems lack layered defenses and are overly reliant on ground segments for security enforcement. This leaves spacecraft vulnerable to cyberattacks if the ground system is compromised. On-orbit detection and response mechanisms are essential for increasing autonomy and resilience.	Cyber situational awareness (CSA) and telemetry logging for space systems
			Algorithms for on-orbit cyber intrusion detection
			RF detection and hardening for space systems
			Defining and implementing autonomous cyber response mechanisms
			Standardizing on-orbit cybersecurity procedures and resilience measures
			Human factors in astronaut-involved missions (crew cyber behavior and human-machine interface risks)
			Exploring deceptive defense technologies for space systems
Med Priority	Advancing on-orbit implementations of terrestrial IT/OT cybersecurity measures for space systems	Feasible due to extensive experience with terrestrial IT/OT cybersecurity models. However, implementation is hindered by the risk-averse nature of space engineering and limited experience in adapting terrestrial security for on-orbit applications. There is a need to validate which IT/OT security controls are suitable for space systems given SWaP constraints, radiation exposure, and latency issues.	Evaluating the suitability of SIEM solutions for space cyber-situational awareness
			Evaluating the efficacy of treating spacecraft more like terrestrial network nodes
			Defining and evaluating secure rollouts of new security technologies and capabilities for space systems
			Evaluating the suitability and secure implementation of virtualized systems in space

Table 1: Prioritized Capability Gap and Areas of Potential Advancement

Capability Gap	Rationale	Areas of Potential Advancement
Future-proofing space architectures for adaptive, secure, and autonomous operations	Architectures optimized for evolving space operations (e.g., pLEO, multi-orbit networks, on-orbit servicing, and space-based AI/ML) will enable more scalable, efficient, and resilient security implementations. Security solutions should be architecturally integrated rather than bolted on to support long-term adaptability.	Reviewing, defining, and evaluating future space architectures for different space operations
		Investigating the impact of emerging technologies on space architectures
		Reinforcement learning (RL)
		Defining the "best" suite of future architectures and identifying capability gaps
		Defining and evaluating hardware-agnostic cybersecurity: a shift away from rad-hardened computing
		Defining and evaluating alternative architectural approaches to replace rad-hardened compute assets
		Determining the impact of architecture on computing resources, processing power, and latency
		Modifying communication interfaces (bus and payloads) to support open architecture
Developing trustworthy operating systems for secure and resilient space missions	A suite of trusted, space-optimized operating systems will reduce vulnerabilities, facilitate interoperability across different spacecraft platforms, and increase resilience against supply chain threats and software exploitation. Current OS options for space lack consistent security hardening, continuous patching, and built-in cyber resilience.	Defining and evaluating a suite of operating systems for bus, payloads, and components built on a root-of-trust
		Optimizing isolation and separation for space environments
		Designing fail-safe, keep-alive, and auto-recovery mechanisms
		Defining and evaluating software architectures optimized for space systems
		Evaluating the balance between simplicity and complexity in space OS designs
Establishing standards for secure and interoperable space systems	Standardization will improve interoperability, integration efficiency, and security assurance across space systems. However, adoption is slow due to proprietary architectures, differing operational needs, and a fragmented industry approach to security frameworks. Efforts should focus on open standards and industry collaboration.	Researching the security of DTN in space communications
		Developing secure key management protocols for intermittent communication paths
		Establishing interoperability standards for secure multi-network space operations
		Establishing a standardized process for secure-by-design space system development
		Open space network (OSN)

Appendix:
Details on the Eight Key Areas for Advancement in Space Cyber R&D

Area #1: Addressing the Insufficient Modeling and Simulation (M&S) Gap in Space Cybersecurity R&D

One of the most pressing gaps in space cybersecurity is the lack of robust modeling and simulation (M&S) capabilities to accurately assess cyber threats, develop effective countermeasures, and evaluate human and automated responses to attacks. Space systems operate in unique and highly constrained environments where traditional cybersecurity testing methodologies are insufficient. The high cost and impracticality of on-orbit testing make digital and simulated environments essential for understanding how space assets can be compromised and how they should respond in realtime to cyber threats.

To close these gaps, research and development efforts must prioritize building realistic, scalable, and accessible space cyber test environments, including both digital twins and physical testbeds (FlatSats), and ensure digital engineering initiatives (e.g., model-based systems engineering [MBSE]) include cybersecurity perspectives.

Areas of potential advancement could include:

- **Researching and publishing results using adversarial tactics, techniques, and procedures (TTPs) for attacking spacecrafts**
    - Validating and expanding the Space Attack Research and Tactic Analysis (SPARTA) library of space-specific adversarial TTPs is essential to ensure that the tactics used in cyberwarfare against spacecraft are accurately modeled and can be replicated in cybersecurity assessments or modeling and simulation.
    - Red team validation exercises should be conducted against spacecraft software and hardware to confirm the feasibility of known TTPs and identify gaps where SPARTA TTPs need refinement or additional sub-techniques should be added.
    - Research should include on-orbit attack simulation to test whether SPARTA's defined cyberattack sequences translate into real-world mission impact scenarios, such as compromising spacecraft command and control (C2) systems or disrupting telemetry.
    - Threat modeling techniques should be developed to correlate SPARTA TTPs to vulnerabilities mapped in common weakness enumerations (CWEs) and common vulnerabilities and exposures (CVEs), creating a repeatable process for assessing spacecraft security risks.
- **Low Earth orbit (LEO) vs. geosynchronous orbit (GSO) vs. deep space vs. Cislunar threat landscape**
    - Expand threat modeling tools to differentiate threat characteristics by orbital regime:
        - Model differential dwell time, signal exposure, and physical access vectors for LEO vs. GSO vs. deep space vs. cislunar.
        - Simulate latency and propagation effects in jamming, spoofing, and relay scenarios.

- Include orbital dynamics and mission durations in simulation of adversary kill chains.
- Validate resilience techniques against orbit-specific adversary capabilities.
- Correlate applicable techniques and publish threat models per orbital regime/location.

Integrating cybersecurity into MBSE

- Cybersecurity should be integrated into the early design phase of spacecraft systems, rather than added as a reactive layer after development. MBSE provides a structured approach to embedding security considerations into space system architectures from the start.
- Leveraging digital engineering frameworks (e.g., SysML, Cameo, Enterprise Architect) allows engineers to embed TTPs (e.g., SPARTA) directly into system architecture models, enabling security validation before implementation.
- Activity diagrams should be utilized to map out adversary attack sequences, allowing teams to visualize and simulate cyberattack paths, identify weak points, and preemptively implement security countermeasures where most effective.
- Swimlane diagrams should be developed to illustrate adversary-defender interactions, mapping out how an attacker's actions impact different spacecraft components and where countermeasures should be reinforced to disrupt adversary kill chains.
- Security-informed digital engineering will ensure that space mission designers understand attack vectors before deployment and can implement resilient architectures that withstand realistic cyber threats.

Creating space-specific cyber ranges for advanced penetration testing, vulnerability assessments, and red/blue/purple teams

- Traditional cyber ranges do not account for the physics-based constraints of space systems, making it difficult to accurately test attack methodologies against space architectures.
- Space-specific cyber ranges should replicate real-world spacecraft conditions, including radio frequency (RF) communications, on-orbit processing limitations, and command and telemetry protocols, allowing for comprehensive penetration testing in a realistic threat environment.
- Emulating space-based red and blue team exercises in cyber ranges will help train operators in detecting and mitigating real-world spacecraft cyberattacks before they occur on-orbit. Ideally, conduct purple team exercises in these space cyber ranges. Purple team exercises allow defenders (blue team) to improve realtime response to adversarial tactics, while collaborating with attackers (red team) to refine offensive cyber methodologies. By running live attack simulations against digital twins or FlatSat environments, security teams can assess how well defensive technologies detect and mitigate attacks.
- Threat intelligence gathered from purple teaming can be used to refine TTP mappings in frameworks like SPARTA, ensuring that new cyberattack techniques are systematically analyzed and incorporated into spacecraft cybersecurity frameworks.

- Realistic adversary emulation will help validate detection thresholds, alerting mechanisms, and automated defensive responses before an actual on-orbit incident occurs.

- Ensure security researchers have access to representative space technologies and systems for meaningful testing and research:

  - Provide controlled, sanitized versions of spacecraft firmware, bus protocols, radios, and interfaces to enable realistic emulation.

  - Establish government- and industry-sponsored programs that grant vetted researchers access to digital twins, FlatSats, or sandboxed subsystems.

  - Address current barriers to research—such as proprietary restrictions, ITAR constraints, or classified design artifacts—by developing clear policy frameworks for safe and ethical access.

- **Developing open-architecture digital twins for cybersecurity assessments and research**

  - Digital twins should serve as a universal testing environment for cybersecurity assessments, allowing for repeatable penetration testing, forensic analysis, and security validation before launching actual spacecraft. All spacecraft developments should include digital twin development as a default approach when developing or acquiring a spacecraft.

  - Open-architecture models should be developed to encourage industry collaboration, allowing organizations to exchange standardized spacecraft models for cyber resilience assessments.

  - Digital twins should include realistic spacecraft subsystems (e.g., command and data handling [C&DH], propulsion, payloads, communications) so that cyber range exercises can evaluate mission impact from adversary attacks.

  - Standardization of digital twin frameworks will ensure that government, commercial, and allied space entities can seamlessly integrate cybersecurity assessments into their mission planning workflows.

- **Funding bug bounty programs using digital twins or FlatSats**

  - Bug bounty programs incentivize ethical hackers to discover vulnerabilities before adversaries do, reducing the risk of mission-critical spacecraft being compromised post-launch.

  - Digital twins provide an ideal platform for running bounty programs, as vulnerabilities can be tested and patched without affecting operational spacecraft.

  - FlatSat test environments allow for real-world, hardware-level security testing, uncovering supply chain risks, firmware tampering, and side-channel attacks that might not be detected in purely software-based simulations.

  - Government and commercial space organizations should fund competitive security testing programs, encouraging researchers to identify and disclose vulnerabilities in exchange for structured rewards, thus improving the overall security of deployed spacecraft. This would expand upon proven concepts like Hack-a-Sat (HaS) but use more representative systems.

- **Evaluating the role of commercial space assets in mission-critical government functions**
  - U.S. government agencies are increasingly reliant on commercial satellites for mission-critical operations, yet there is no standardized oversight on the cybersecurity posture of commercial spacecrafts.
  - Simulating cyber dependencies on commercial spacecraft in mission exercises will allow for a better understanding of potential risks if commercial assets are compromised during conflict scenarios.
  - Assessing encryption standards, command authentication policies, and supply chain security in commercial spacecrafts will help identify where additional security measures are needed before these assets are integrated into national security operations.
  - Evaluating regulatory requirements for commercial space cybersecurity is crucial to establishing baseline security measures for government-used space services, ensuring that adversaries cannot exploit commercial spacecrafts as attack vectors against U.S. space operations.
- **Government acquisition reform to demand better data rights for security research**
  - Current government contracts often restrict independent security testing, limiting the ability of agencies to proactively identify vulnerabilities in the spacecraft they operate.
  - Reforming acquisition policies to mandate security data transparency will ensure that space assets can be continuously evaluated for cyber risks throughout their lifecycle.
  - Digital twin deliverables should be a contractual requirement, allowing government agencies to perform cyber risk assessments on their spacecraft, even post-launch.
  - Space cybersecurity assessments should be treated as an ongoing process, not a one-time certification, requiring flexible contracts that adapt to emerging threats and evolving cybersecurity standards.

By investing in comprehensive and standardized space cybersecurity M&S, the industry will proactively identify vulnerabilities, validate countermeasures, and enhance mission resilience before real-world adversaries exploit these gaps. The ability to simulate cyberattacks and human responses in a controlled environment will be a critical step in securing future space operations against increasingly sophisticated threats. These investments will enhance pre-launch testing, improve realtime detection, and ensure the security of both government and commercial space assets, protecting them from nation-state and non-state adversaries in an increasingly contested domain.

Area #2: Addressing End-to-End Security Integration for Spacecraft and On-Orbit Systems

Modern space architectures, particularly in proliferated low Earth orbit (pLEO), introduce new security challenges that require integrated, scalable, and resilient security systems across spacecraft, crosslinks, cryptographic infrastructures, and key management mechanisms. Unlike traditional monolithic spacecraft designs, pLEO constellations increase attack surfaces from a cyber perspective, making constellation-wide cybersecurity a top priority.

As pLEO systems scale, a key question is whether heterogeneous security solutions (which reduce the risk of a single vulnerability compromising an entire constellation) are necessary or if a homogeneous approach is feasible without increasing cyber risk.

Also, next-generation satellites will likely implement software-based cryptographic solutions with anti-tamper protections to prevent adversarial exploitation. Over-the-air rekeying (OTAR) is a critical capability to ensure cryptographic agility while maintaining secure key distribution across a constellation.

There needs to be a balance between security, reliability, and resilience. Cybersecurity measures can conflict with traditional spacecraft reliability and resiliency mechanisms. The industry lacks a formalized framework to optimize and resolve incompatibilities between these disciplines.

Areas of potential advancement could include:

- **Designing and evaluating pLEO-specific security models that balance the benefits of homogeneous vs. heterogeneous security architectures**
    - pLEO constellations introduce new security challenges due to the high number of interconnected spacecraft and the potential for a single vulnerability to compromise an entire network.
    - Research is needed to evaluate the risk trade-offs between homogeneity and heterogeneity, identifying the optimal level of security diversification that maximizes resilience while maintaining scalability, cost-effectiveness, and interoperability across large pLEO constellations.
        - Homogeneous security architectures provide standardized protection and simplified interoperability across a constellation but introduce systemic risk, where one successful cyberattack could propagate across the entire fleet.
        - Heterogeneous security architectures, where different spacecraft or subsystems have varying security implementations, can reduce the impact of widespread vulnerabilities but introduce complexity in integration, communication protocols, and key management.
    - Mission-driven security models should be explored, where spacecraft adapt security configurations based on operational context, dynamically shifting between secure communication modes and access control settings depending on mission priorities and threat conditions.
- **Developing software-based cryptographic solutions with anti-tamper features, ensuring that OTAR and key distribution mechanisms are robust against adversary compromise**
    - Traditional/Legacy hardware-based cryptographic modules (e.g., field programmable gate arrays [FPGAs] and secure elements) are difficult to update post-launch, making them vulnerable to advances in adversarial decryption capabilities.
    - Software-based cryptographic solutions should be designed to enable agile, post-deployment updates while maintaining high assurance levels against cyber threats.
    - OTAR mechanisms should be hardened against man-in-the-middle attacks, key compromise scenarios, and quantum computing threats to prevent adversaries from intercepting or replacing encryption keys used for spacecraft communications.

  - Cryptographic agility should be incorporated, allowing spacecraft to seamlessly switch encryption algorithms when vulnerabilities are detected in existing implementations.

  - Anti-tamper features should ensure that cryptographic software cannot be reverse engineered, modified, or bypassed by an adversary, even in the event of physical access or firmware exploitation.

  - Distributed key management approaches should be researched to determine whether centralized key authorities (e.g., ground-based key servers) or decentralized, self-sustaining key exchange models (e.g., peer-to-peer spacecraft key distribution) are more secure and resilient for future space networks.

- **Expanding space-specific vulnerability research and including into the existing comprehensive database of CVEs/CWEs**

  - As spacecraft systems become increasingly software-defined and interconnected, they lack information in existing vulnerability databases to help security teams track, assess, and mitigate potential cyber risks before adversaries can exploit them. Current vulnerability tracking systems (e.g., CVEs and CWEs) are largely focused on terrestrial information technology and operational technology (IT/OT) systems and fail to document weaknesses specific to spacecraft components. Some included examples are:

    - Star trackers, inertial measurement units (IMUs), reaction wheels, flight computers, and avionics systems that could be manipulated to disrupt navigation and stability.

    - Satellite buses and network protocols (e.g., MIL-STD-1553, SpaceWire, controller area network [CAN] bus) that lack built-in authentication or encryption mechanisms.

    - Software-defined radios (SDRs) and TT&C links that are vulnerable to signal manipulation, jamming, and spoofing attacks.

  - Research is needed to identify and document vulnerabilities specific to space systems, ensuring a comprehensive CVE/CWE repository that can be used by government agencies, commercial space operators, and security researchers to proactively harden space systems against known threats.

  - Space vulnerability research should be integrated with active threat intelligence, allowing operators to correlate real-world cyber events (e.g., attempted ground station breaches and RF interference incidents) with known space-specific vulnerabilities.

- **Enhancing supply chain protections through black-box analysis and strengthening bill of materials (BOM) validation processes for hardware and software**

  - Supply chain attacks pose a significant risk to space systems, as adversaries can insert vulnerabilities at the manufacturing stage, which then persist throughout the system's lifecycle. Black-box analysis techniques (e.g., binary analysis and fuzzing) should be developed to evaluate hardware and software components before integration into flight systems, allowing for comprehensive security assessments even when source code or design documentation is unavailable.

  - BOM validation for both hardware and software is critical to ensuring that all third-party components used in spacecraft systems are properly vetted and free from malicious implants or unintended vulnerabilities.

        - ◇ Software bill of materials (SBOM) validation should focus on tracking third-party libraries, dependencies, and firmware components, ensuring that spacecraft do not inherit vulnerabilities from external software supply chains. SBOM is not a unique attribute of space, but SBOM tools should ensure they can process space-based technologies.

        - ◇ Hardware BOM validation should include cryptographic attestation mechanisms to verify that components have not been tampered with during production or transit.

    - ▸ Supply chain risk modeling should be incorporated into digital twins, allowing for scenario testing to determine how different supply chain attack vectors could impact spacecraft operations.

- ◆ **Conducting scenario-based studies on supply chain compromise impacts and developing mitigation strategies**

    - ▸ Scenario-based studies are needed to analyze the real-world impact of compromised spacecraft components, evaluating how maliciously altered or vulnerable hardware/software affects mission outcomes. Example compromise scenarios could include:

        - ◇ A star tracker with an adversary-inserted corrupted star map, causing the spacecraft to drift off course.

        - ◇ A main processor vulnerability that cannot be patched remotely, leading to loss of spacecraft autonomy or execution of unauthorized commands.

        - ◇ A compromised FPGA or cryptographic module that allows an adversary to decrypt command and telemetry links, gaining unauthorized control over the spacecraft.

    - ▸ Mitigation strategies should be tested using digital twins, allowing operators to experiment with incident response plans and develop proactive safeguards for different attack scenarios.

    - ▸ Research should focus on redundancy strategies, automated fault isolation, and anomaly detection algorithms that allow spacecraft to self-correct when critical subsystems are compromised.

- ◆ **Defining the intersection of security, reliability, and resilience to ensure mission continuity**

    - ▸ Security, reliability, and resilience should be designed to reinforce, rather than conflict with, each other. Cybersecurity mechanisms may add complexity to spacecraft operations, which could reduce overall system reliability if not properly integrated.

    - ▸ Cyber protections should be aligned with fault-tolerant architectures, ensuring that security mechanisms do not interfere with automated failure recovery processes.

    - ▸ Autonomous recovery and redundancy strategies should be integrated with cybersecurity measures, enabling spacecraft to detect, isolate, and recover from cyber incidents without compromising mission execution.

- Research is needed to establish a structured approach to aligning cybersecurity, reliability, and resilience, ensuring that spacecraft systems:
    - ◇ Harden themselves against cyber threats (security).
    - ◇ Continue operating safely under attack or failure conditions (reliability).
    - ◇ Recover from cyber intrusions, system malfunctions, and unexpected anomalies (resilience).
- This framework should be mission-driven, allowing spacecraft to adapt their security postures based on operational risk assessments and evolving threat landscapes.

By integrating cybersecurity from the ground up in future space architectures, this research will enable secure-by-design constellations that are resilient to nation-state and non-state cyber threats, ensuring long-term operational integrity and mission success.

Area #3: Advancing Zero Trust Architecture (ZTA) for On-Orbit Components and Ground Systems

As space systems become more interconnected and autonomous, traditional perimeter-based security models are no longer sufficient to protect against evolving cyber threats. A zero trust architecture (ZTA) or even zero trust attributes for both on-orbit and ground systems are necessary to ensure that every access request, system component, and communication link is continuously verified and secured. Implementing zero trust in space environments, however, presents unique challenges, including size, weight, and power (SWaP) constraints, intermittent communication links, and mission-critical realtime operations that must remain unaffected by security mechanisms.

Many spacecraft operate under the assumption that commands originating from the ground are inherently trusted, making them susceptible to command injection attacks if the ground station is compromised. There is a need for secure command authentication mechanisms such as multi-factor authentication (MFA) for telemetry, tracking, and command (TT&C) systems and high-assurance software-based encryption to prevent unauthorized access. Unlike terrestrial networks, some space systems experience high-latency and intermittent communications, making traditional authentication and access control methods impractical. Research is needed to develop delay-tolerant authentication and authorization models that can function even when spacecraft experience long communication gaps.

Applying zero trust attributes spacecraft should be distinct from ground-based ZTA models, as spacecraft operate in resource-constrained environments and rely on highly specialized protocols. On-orbit message encryption, hardware-based root of trust, and realtime security verification should be integrated without degrading system performance or operational reliability. As spacecraft rely more on software-defined functionality, it is critical to formally verify the security of onboard software, operating systems, and hardware components. Research is needed to validate the security of the spacecraft operating system (OS) kernel and its fundamental building blocks, ensuring that spacecraft can defend against firmware tampering, supply chain attacks, and persistent backdoors.

Areas of potential advancement could include:

- **Designing space specific authentication and encryption models that account for latency, SWaP constraints, and operational requirements**
  - Spacecraft communication links experience high latency, intermittent availability, and strict power limitations, making traditional authentication and encryption models unsuitable for on-orbit applications.
  - Research must focus on lightweight cryptographic algorithms that can operate efficiently within the SWaP constraints of spacecraft while still providing robust security protections against eavesdropping, replay attacks, and unauthorized command injection.
  - Command authentication and encryption for TT&C links must ensure only authorized operators can issue commands, even if an adversary has intercepted and replayed valid transmissions.
  - Post-quantum cryptography (PQC) research is needed to ensure that space systems remain secure against emerging quantum computing threats, particularly for long-duration missions where legacy encryption may become obsolete before the spacecraft is decommissioned.
  - Key management and distribution mechanisms (e.g., OTAR) should be optimized for space environments to allow for secure key rotation and update capabilities without requiring excessive ground intervention or additional hardware modifications.
  - Authentication models must incorporate multifactor authentication (MFA) techniques tailored for space systems, including physical layer authentication (e.g., signal fingerprinting) and time-based cryptographic challenges that account for delayed and asymmetric communications. Protecting against the malicious use critical commands is imperative (e.g., secure command mode).
- **Developing delay/intermittent communications tolerant authentication mechanisms to ensure that access control decisions remain effective even in disrupted or degraded communication states**
  - Traditional authentication mechanisms rely on realtime connectivity, but spacecraft often operate in degraded communication conditions, making reauthentication and access control verification complex.
  - Delay-tolerant authentication models must allow spacecraft to store, verify, and enforce access control policies autonomously, ensuring continued security protections even when disconnected from ground control for extended periods.
  - Threshold-based authentication could be developed, where multiple partially transmitted authentication tokens are used to validate commands, ensuring secure operation even with packet loss or high-latency uplinks.
  - Self-healing access control models should be designed so that if a spacecraft is temporarily compromised or disconnected, it can automatically restore secure authentication mechanisms once communication is reestablished.
  - Machine-learning-based anomaly detection should be incorporated to recognize authentication attempts that deviate from

normal mission operations, allowing autonomous spacecraft security protocols to differentiate between legitimate delayed commands and malicious injection attempts.

- Research is needed to determine how ZT can be applied when spacecraft operate in full "radio silence" mode, ensuring they can autonomously detect and reject adversary attempts to gain control when ground communications are unavailable.

- **Defining and implementing ZT attributes tailored to different space architectures, ensuring seamless integration between ground, space, and crosslinks**

  - ZT is not a one-size-fits-all model, and space systems require architecture-specific ZT implementations for each operational domain, including ground control stations, crosslinks between satellites, and spacecraft subsystems.

  - On-orbit ZT must focus on identity-centric security, ensuring commands, data transfers, and inter-satellite communications are continuously verified and authorized before execution.

  - Crosslink authentication and encryption models should be designed to prevent adversarial control of satellite mesh networks, ensuring that compromising one spacecraft does not provide lateral movement access to an entire constellation.

  - Ground station ZTA implementations should incorporate role-based access control (RBAC), continuous authentication, and AI-driven monitoring to detect and mitigate unauthorized access attempts before commands reach the spacecraft.

  - Mission-tailored ZT policies must define how access control should change based on operational scenarios, such as autonomous deep-space operations, emergency recovery situations, or adversary-compromised ground control environments.

  - Adaptive trust mechanisms should be built to ensure that different mission phases (e.g., launch, on-orbit operations, and deorbiting) have customized ZT security policies, allowing spacecraft to modify security postures dynamically based on environmental and operational conditions.

- **Building high-assurance computing models that utilize formally verified hardware and software components, reducing attack surfaces and improving spacecraft cybersecurity posture**

  - Traditional computing models rely on assumptions of trust, but mission-critical spacecraft components should be designed with high-assurance, formally verified security to eliminate vulnerabilities before deployment.

  - Formal verification of hardware components, such as the operating system kernel, cryptographic processors, and command execution modules, ensures that low-level system functions are free of exploitable bugs and backdoors.

  - Red teaming against hardware-based security controls (e.g., trusted platform modules [TPMs] and secure enclaves) is needed to assess how well they resist supply chain tampering, firmware manipulation, and on-orbit side-channel attacks.

- Autonomous recovery from hardware/ software faults should be built into high-assurance spacecraft architectures, ensuring that cyber compromises or radiation-induced errors do not result in permanent mission loss.

- Fault-tolerant and security-hardened embedded computing architectures should be designed to mitigate single-event upsets (SEUs) and total ionizing dose (TID) failures, preventing cyber threats from masquerading as environmental failures.

- Rigorous supply chain validation mechanisms should be developed to ensure that all flight software and firmware undergo formal security audits before integration, reducing the risk of malicious implants or unauthorized code execution in space assets.

◆ **Adapting Industrial Control System (ICS) security best practices to space operations, preventing adversarial control over ground systems and spacecraft command pathways**

- Space systems increasingly rely on ICS/OT infrastructure, including mission control centers, ground station networks, and spacecraft bus control systems, but most ICS security best practices have not been adapted for space operations.

- Research is needed to apply ZT to ICS networks, ensuring that all control system interactions are continuously monitored, authenticated, and validated against a baseline of expected behavior.

- Space-ground communications should be protected against ICS-specific attack vectors, including man-in-the-middle attacks, command spoofing, and replay attacks that could disrupt spacecraft operations.

- ICS segmentation for space operations should be implemented, ensuring that vulnerabilities in one mission segment (e.g., ground control) cannot be exploited to effect on-orbit assets.

By integrating ZT principles into spacecraft and mission control systems, space agencies and commercial operators can ensure continuous authentication, strict access control, and end-to-end encryption, significantly reducing the risk of cyberattacks that could compromise critical space operations.

Area #4: Advancing On-Orbit Protection, Detection, and Response for Spacecraft Cybersecurity

As space systems become increasingly networked and autonomous, the lack of on-orbit cybersecurity protections, detection mechanisms, and response capabilities presents a vulnerability. Spacecraft constellations are reliant on terrestrial infrastructure for cyber defense, leaving them exposed to attacks that could disable, manipulate, or take control of mission-critical space assets. Currently, on-orbit cyber situational awareness (SA) is limited, and most spacecraft lack the ability to detect and respond to cyber intrusions in realtime, increasing the risk of mission failure, data corruption, or adversary exploitation. This research aims to bridge this gap by developing enhanced on-orbit monitoring, attack detection, and autonomous response mechanisms, ensuring resilience against cyber threats without full reliance on ground station intervention.

Many spacecrafts do not have comprehensive telemetry collection and logging to detect cyber intrusions in realtime. Without event capture and logging, operators cannot effectively attribute attacks, assess mission impact, or coordinate response actions. Attribution is also critical for establishing proof of cyber aggression and determining if a defensive response is warranted. Unlike terrestrial systems, there is no established baseline of spacecraft telemetry (TLM) indicators that could signal a cyber intrusion. Without predefined detection metrics, attacks may go undetected or be mistaken for routine anomalies. Modern pLEO constellations and distributed space architectures require cyber-SA across multiple satellites, not just on individual spacecraft. Currently, there is no standardized method to aggregate telemetry across a constellation to detect coordinated or multi-vector cyberattacks.

Additionally, spacecraft lack autonomous self-protection capabilities, meaning that, if an attack occurs, the spacecraft must rely on ground teams for mitigation, which may introduce delays or gaps in response due to latency, communication degradation, or adversary interference.

Areas of potential advancement could include:

- **Cyber situational awareness (CSA) and telemetry logging for space systems**
  - Research, document, and publish indicators of malicious behavior or compromise. TTP frameworks exist that document the methods of attack, but more research is needed on how to detect the TTPs.
  - Spacecraft currently lack realtime cyber telemetry logging, making intrusion detection and response difficult once an attack has occurred. This research would aim to define and capture key spacecraft telemetry points that could indicate a cyber intrusion or an attempted attack. These could include:
    - Logical telemetry data (e.g., unauthorized command execution, firmware modifications, software anomalies, and unexpected data modifications).
    - Physical telemetry indicators (e.g., unexplained power consumption fluctuations, unexpected thermal spikes, attitude sensor misalignment, or sudden changes in radio frequency transmission patterns).
  - With pLEO constellations becoming the norm, CSA must extend beyond a single spacecraft to enable realtime threat sharing across an entire fleet. This research could focus on:
    - Developing secure, low-latency telemetry-sharing architectures that allow spacecraft to collectively monitor cyber anomalies and report unusual patterns to other spacecraft and ground operators.
    - Utilizing constellation-wide AI-driven analytics to correlate cyber incidents across multiple space assets, identifying large-scale cyber campaigns or coordinated adversary operations.
  - Develop machine-learning-driven anomaly detection algorithms that monitor spacecraft commands, data transmission patterns, and system performance for signs of cyber threats, such as:
    - Unauthorized command injection attempts that deviate from normal mission execution.
    - Unexpected changes in inter-satellite communication traffic, indicating potential adversarial eavesdropping or data exfiltration.

        - Abnormal sensor outputs that may indicate cyber manipulation of positioning, navigation, and timing (PNT) data.

- **Algorithms for on-orbit cyber intrusion detection**

    - Unlike terrestrial networks, many spacecraft do not have dedicated intrusion detection systems (IDS) to flag cyber anomalies in realtime. This research would develop and validate onboard IDS algorithms that monitor behaviors that could be malicious, for example:

        - Monitor files, memory, telemetry, bus traffic, and process data.

        - Unexpected bus or payload behavior or unauthorized sensor or actuator activations.

        - Anomalous command sequences or unusual instruction patterns that do not align with mission objectives.

        - Sudden communication loss or degradation or disruptions that could indicate adversary interference, signal hijacking, or protocol attacks.

        - Power or thermal irregularities or spikes or inconsistencies that may suggest cyber-induced sabotage of key spacecraft components.

    - Software-defined radios are highly versatile but are also susceptible to RF-based cyberattacks, including jamming, spoofing, and signal injection. May need to develop AI/ML-powered RF intrusion detection models to identify and differentiate between natural RF interference and malicious signal manipulation.

        - Training spacecraft SDRs to autonomously recognize and adapt to hostile RF environments, mitigating the impact of attempted spacecraft hijacking or command injection attacks.

    - Building tailored behavioral models for each spacecraft, allowing deviation detection without excessive false positives. Implementing spacecraft anomaly profiles that adapt over time as mission parameters evolve, reducing reliance on static cybersecurity rules.

- **RF detection and hardening for space systems**

    - Most spacecrafts rely on highly predictable RF communication channels, making them vulnerable to signal interference, spoofing, and hijacking. This research should:

        - Develop RF-based intrusion detection sensors that continuously scan for unusual signal patterns, allowing spacecraft to detect anomalous RF activity before an attack escalates.

        - Explore passive RF monitoring techniques that allow spacecraft to identify hostile signals without actively transmitting, reducing the risk of detection by adversaries.

    - Spacecraft should be able to withstand RF-based attacks by implementing:

        - Advanced filtering algorithms to reduce susceptibility to jamming and signal flooding.

        - Adaptive modulation techniques that allow spacecraft to change frequencies dynamically when a channel is compromised.

    - Spread spectrum and frequency-hopping approaches to ensure that critical telemetry and command data cannot be easily intercepted or blocked.

  - Instead of static defenses, spacecraft should use AI/ML-driven RF countermeasures to:

    - Dynamically adjust communication parameters in response to RF-based attacks, preventing adversaries from maintaining consistent signal interference.

    - Enable spacecraft to recognize and block command signals from unauthorized sources, preventing spacecraft hijacking attempts.

- **Defining and implementing autonomous cyber response mechanisms**

  - Better defining a "cyber-safe mode" for spacecraft to be able to enter a secured operational mode when under attack. Define the requirements for an automated cyber-safe mode, allowing spacecrafts to contain cyber threats while preserving mission functionality. Explore how spacecraft can autonomously isolate compromised systems, preventing an attacker from accessing critical payloads or subsystems.

  - Need to develop autonomous threat containment strategies to prevent mission-wide failures. Spacecraft should be able to respond to cyberattacks in realtime without relying on ground intervention. This research should:

    - Enable spacecrafts to block unauthorized critical commands in realtime, ensuring that malicious payload activations cannot succeed.

    - Develop subsystem-level isolation techniques, preventing malicious code from propagating across interconnected spacecraft components.

    - Allow spacecraft to disable compromised communication pathways, cutting off unauthorized remote access before attackers can escalate their control.

  - Researching appropriate cyberattack response actions since different mission types require different responses to cyber incidents. Spacecraft response actions based on mission phase and orbit type, ensuring that cyber defenses do not interfere with mission objectives. Acceptable countermeasures for different levels of cyber threats, ensuring that spacecraft can mitigate attacks without compromising safety or operational readiness.

    - Investigate the interaction between safety and cybersecurity responses, ensuring that automated cyber defenses (e.g., isolation, reboot, and mode switching) do not conflict with life-critical or mission-critical safety protocols—particularly in human spaceflight, propulsion events, or time-sensitive science operations.

- **Standardizing on-orbit cybersecurity procedures and resilience measures**

  - Establish clear operational guidelines for cyber intrusions. Space operators currently lack a unified framework for responding to on-orbit cyber incidents. Develop standardized response protocols that guide operators in handling suspected cyber intrusions efficiently and consistently.

        - ◇ Ensure mission-critical functions remain operational while attack containment measures are implemented.

    - ▸ Develop on-orbit recovery methods to self-recover from cyberattacks. Create automated rollback mechanisms, allowing spacecraft to restore modified system files, executables, and configurations to pre-attack conditions.

        - ◇ Integrate self-healing cybersecurity architectures, enabling spacecraft to autonomously repair compromised software and resume normal functions.

- ◆ **Human factors in astronaut-involved missions (crew cyber behavior and human-machine interface risks)**

    - ▸ Incorporate astronaut behavior modeling into on-board cyber telemetry baselines:

        - ◇ Monitor command timing, usage patterns, physical interface interactions, and mission task context.

        - ◇ Define behavioral baselines for expected astronaut interaction with avionics, diagnostics, or payload control interfaces.

    - ▸ Correlate astronaut-initiated anomalies with potential cyber-relevant system effects.

        - ◇ Misconfigurations or deviations due to fatigue, distraction, or emergency conditions.

        - ◇ Interfaces used in unintended ways due to ambiguity, user interface (UI) complexity, or degraded crew cognition.

    - ▸ Expand onboard anomaly detection to recognize potential insider threats or unintentional misuse.

        - ◇ Role-based deviations (e.g., noncommand crew attempting privileged actions).

        - ◇ Time-of-use or command sequence anomalies inconsistent with mission plan or crew responsibilities.

    - ▸ Integrate behavior-aware alerting into cyber-safe mode and mission abort logic.

        - ◇ Include astronaut-in-the-loop alerts that prompt crew verification before executing potentially anomalous or high-risk commands.

        - ◇ Develop thresholds and response models tailored for mixed-initiative human-machine environments.

    - ▸ Promote cyber-physical training data sets based on realistic human error, degraded cognition, or malicious insider scenarios.

        - ◇ Incorporate data from analog missions, human-in-the-loop simulations, and astronaut training programs.

        - ◇ Use training data to improve AI/ML models for cyber resilience in crewed spacecraft and habitats.

    - ▸ Design interfaces and procedures with cognitive security in mind:

        - ◇ Reduce likelihood of inadvertent system compromise by enhancing clarity, context-awareness, and safeguard prompts.

        - ◇ Apply user-centered design principles to mitigate ambiguous command entry or irreversible actions.

- **Exploring deceptive defense technologies for space systems**

    - In the terrestrial world, deceptive cyber defenses are highly effective at misleading adversaries and collecting intelligence on their attack methods. Explore the feasibility of deploying space honeypots to attract and identify adversarial cyber actors.

        - ◇ Develop techniques for deceptive spacecraft signals, forcing adversaries to waste resources on false targets while real spacecraft operate securely.

    - Deploy honeypots within spacecraft bus systems, allowing spacecrafts to trap and analyze malicious commands without risking mission integrity.

    - Need to explore optical communication jamming techniques. Optical communication channels are assumed to be more secure than RF, but adversaries may develop new disruption methods. May need to investigate ways to detect and mitigate jamming of optical data links before adversaries exploit them.

By developing advanced monitoring, intrusion detection, RF hardening, autonomous response, and deception-based cyber defenses, space assets can become more resilient against emerging cyber threats. These efforts will ensure that spacecraft remain operational, secure, and self-defending even in the face of highly sophisticated attacks.

Area #5: Advancing On-Orbit Implementations of Terrestrial IT/OT Cybersecurity Measures for Space Systems

As spacecraft networks become increasingly interconnected, they inherit many of the same cybersecurity risks that exist in terrestrial IT and OT environments. However, unlike terrestrial systems, spacecraft operate in resource-constrained environments with limited processing power, intermittent communications, and extreme physical conditions, making direct application of traditional IT/OT security measures sometimes impractical. Many cybersecurity architectures for spacecraft do not incorporate modern security monitoring, virtualized defenses, or realtime threat intelligence sharing, leaving spacecrafts vulnerable to persistent cyber threats, unauthorized access, and remote exploitation.

This research would aim to evaluate and adapt terrestrial cybersecurity principles for space environments, ensuring that on-orbit assets can benefit from robust IT/OT security protections while accounting for the unique constraints of space operations. Some focus areas would include security information and event management (SIEM) solutions, spacecraft network architecture, secure technology rollouts, and virtualization strategies.

There is currently limited security monitoring and threat intelligence sharing in space systems. Unlike terrestrial IT/OT environments, space systems lack centralized threat monitoring solutions such as SIEM platforms, making it difficult to detect, analyze, and respond to cyber intrusions in realtime. The absence of on-orbit telemetry aggregation and security event correlation increases the risk of undetected cyberattacks that could disrupt space missions. Ground-based SIEMs often need to be expanded to process space specific protocols and information.

Terrestrial cybersecurity relies on structured IT and OT networks, where devices are actively monitored, patched, and secured through established protocols. Spacecraft, however, are not typically treated as networked nodes, leading to fragmented security controls.

Virtualization and containerization are widely used in terrestrial cybersecurity to improve system flexibility, redundancy, and rapid recovery from cyber incidents, but their applicability to space remains somewhat unexplored. Without virtualization, space systems lack secure ways to isolate critical processes, deploy updates dynamically, or create sandbox environments for security testing.

Areas of potential advancement could include:

- **Evaluating the suitability of SIEM solutions for space cyber-situational awareness**

  As cyber threats against space systems become more sophisticated, there is a growing need to integrate spacecraft security telemetry into SIEM platforms. SIEM solutions aggregate security data, detect anomalies, and generate realtime alerts, allowing missions to rapidly respond to cyber incidents. However, current space architectures lack the ability to seamlessly integrate on-orbit telemetry with SIEM frameworks, limiting realtime threat detection and forensic analysis for space-based systems.

  This gap indicates research should focus on:

  - Defining key spacecraft security telemetry data points because space-based SIEM implementations require clear definitions of security-relevant telemetry that can be monitored, logged, and analyzed for potential cyber threats.
    - Enabling spacecraft to retain cyber incident logs for forensic evaluation without compromising mission operations.
  - Advancing space vehicle forensics capabilities to support incident investigation and post-event analysis.
    - Develop onboard forensic logging mechanisms that preserve critical data (e.g., command sequences, memory state, and bus activity) for analysis after suspected cyber incidents.
    - Research lightweight, tamper-evident forensic frameworks that operate within SWaP constraints and can withstand reboots, radiation events, and degraded communications (e.g., black box).
    - Define standardized forensics data schemas to ensure compatibility with ground-based SIEM platforms and facilitate cross-mission comparison of attack patterns.
    - Explore techniques for remote forensic triage of compromised or anomalous space vehicles (SVs) in scenarios where physical access is impossible and downlink bandwidth is limited.
  - Developing space-specific log aggregation methods. Due to bandwidth limitations and intermittent connectivity, spacecraft cannot continuously stream all security telemetry to the ground. Research should focus on:
    - Prioritizing essential security logs to be sent during scheduled data transfers.
    - Developing lightweight on-orbit log aggregation mechanisms that filter, compress, and summarize security events before transmission.

        - Exploring edge processing solutions where spacecraft perform preliminary anomaly detection locally before relaying security insights to ground-based SIEMs.

    - Enhancing realtime threat intelligence sharing across space networks and/or organization (e.g., space information sharing analysis center [Space-ISAC]). If a cyber threat is detected on one spacecraft, the entire constellation should be able to respond dynamically. Research should focus on:

        - Establishing secure telemetry-sharing protocols that allow spacecraft to exchange threat intelligence updates without introducing new vulnerabilities.

        - Automating fleet-wide anomaly detection, allowing multiple spacecraft to correlate security events and identify coordinated attacks across the constellation.

        - Developing interoperability standards to ensure that space SIEM data can be seamlessly integrated with ground-based cybersecurity operations centers.

        - Developing procedures to share information with information sharing analysis centers (ISACs)

- **Evaluating the efficacy of treating spacecraft more like terrestrial network nodes**

  Traditional space architectures are not designed to function as networked nodes in a larger security infrastructure. However, as space systems grow in complexity, treating spacecraft as fully integrated network endpoints, like terrestrial IT and OT environments, could enhance security visibility, enable realtime monitoring, and improve overall cyber resilience. Concepts for research to explore could be:

    - Defining segmentation strategies that prevent compromised components from affecting entire spacecraft operations.

    - Implementing software-defined access controls, ensuring that only authorized processes and operators can interact with different spacecraft functions. Exploring software-defined networking concepts in space that allow for dynamic network reconfiguration and centralized security policy enforcement.

    - Integrating spacecraft security telemetry into mission cybersecurity dashboards, allowing analysts to monitor space-based assets alongside terrestrial networks.

    - Determining the risks and benefits of active threat hunting on spacecraft networks, ensuring that cybersecurity teams can detect adversary movements.

- **Defining and evaluating secure rollouts of new security technologies and capabilities for space systems**

  Unlike terrestrial systems, spacecraft cannot afford to experience system failures due to faulty security updates or misconfigured cyber defenses. New cybersecurity tools and capabilities should be carefully validated before deployment to avoid unintended mission disruptions.

    - Developing pre-launch cybersecurity testing protocols. Cybersecurity updates should be tested in realistic environments before implementation. Using digital twins and hardware-in-the-loop (HITL) simulations to replicate on-orbit conditions before rolling out security updates.

    - Creating automated penetration testing environments where security vulnerabilities can be identified and mitigated before launch.
    - Evaluating mission-specific cyber risks, ensuring that security updates do not introduce operational instability.

- Spacecraft security updates should be deployed incrementally, minimizing risk. Controlled deployment methodologies, where security updates are first tested on select spacecraft before fleet-wide implementation.
    - Fallback contingency plans, ensuring that spacecraft can revert to a stable configuration if a new security feature introduces issues.
        - To prevent mission failure from faulty updates, spacecraft should be able to restore previous configurations. Develop automated rollback procedures, allowing spacecraft to detect and undo harmful security updates.
    - Ensure spacecraft maintain multiple secure boot environments, enabling recovery from cyber-induced software corruption.

- **Evaluating the suitability and secure implementation of virtualized systems in space**

Virtualization offers security, scalability, and isolation benefits, but spacecraft have yet to fully integrate virtualized architectures due to concerns about performance impact, system complexity, and compatibility with legacy hardware. Research should focus on:

- Developing space-ready hypervisors and containerized security applications.
    - Investigating lightweight virtualization techniques, such as containerization, to isolate spacecraft processes and reduce attack surfaces (e.g., process isolation).
    - Defining hardware-assisted virtualization approaches, ensuring that virtualization overhead does not negatively impact spacecraft performance.
- Studying the impact of virtualization on spacecraft performance.
    - Ensuring virtualization does not introduce latency or degrade mission execution.
    - Developing energy-efficient virtualization techniques that work within the SWaP constraints of spacecraft.
- Developing dynamic sandboxing environments for spacecraft.
    - Creating virtualized test environments onboard spacecraft to allow for secure execution of unverified updates, AI-based security algorithms, or third-party applications before full deployment.

By adapting and implementing terrestrial IT/OT cybersecurity measures for space systems, we can enhance spacecraft security monitoring, improve network resilience, standardize technology rollouts, and introduce virtualization-based protections to reduce cyber risk. These advancements will enable a more proactive, scalable, and autonomous approach to space cybersecurity, ensuring that next-generation space assets remain secure, adaptive, and resilient against evolving threats.

Area #6: Future-Proofing Space Architectures for Adaptive, Secure, and Autonomous Operations

As space operations evolve with the rise of pLEO constellations, autonomous systems, and AI-driven space applications, traditional space architectures are no longer sufficient to meet modern security, operational, and performance demands. Existing spacecraft designs often rely on highly specialized, proprietary, and hardware-dependent architectures, making them inflexible, costly, and difficult to upgrade over long mission durations. Furthermore, these architectures do not inherently support cybersecurity resilience, machine learning (ML), or ZT models, leaving them vulnerable to emerging cyber and electronic warfare threats. This research would aim to define, evaluate, and develop future-proof space architectures that can adapt to evolving mission needs, integrate cutting-edge technologies, and enhance security without adding excessive hardware requirements.

Many current space system designs do not efficiently support next-generation mission paradigms, such as realtime inter-satellite networking, autonomous spacecraft decisionmaking, or dynamic reconfiguration in contested environments. Emerging technologies, including AI, ML-driven anomaly detection, software-defined payloads, and ZT security models, require architectural changes to support realtime processing and adaptive security enforcement. There is no defined "best" suite of future space architectures, making it difficult for government, commercial, and defense organizations to align on cybersecurity and operational design principles. Current space cybersecurity measures often rely on rad-hardened computing assets, which are expensive, power-intensive, and difficult to upgrade, leading to stagnation in space security innovation. Most spacecraft are not designed to natively collect and analyze cybersecurity telemetry, making on-orbit cyber defense and forensic analysis challenging. Many spacecraft rely on proprietary communication interfaces that hinder integration with broader space networks and delay the adoption of open, flexible security standards.

Areas of potential advancement could include:

- **Reviewing, defining, and evaluating future space architectures for different space operations**

  As space operations evolve, modular and scalable spacecraft architectures are needed to support a variety of mission profiles while ensuring security, adaptability, and operational efficiency. Traditional monolithic spacecraft designs lack flexibility, making it difficult to integrate new technologies, upgrade cybersecurity defenses, and support autonomous networked operations. Some key areas of research could be:

  - Ensuring architectures are customizable based on mission objectives, whether for deep-space exploration, pLEO mega-constellations, or intelligence, surveillance, reconnaissance spacecraft.

    - Enabling plug-and-play compatibility with future payloads, onboard processing units, and communication systems.

  - Designing self-organizing inter-satellite networks with automated routing and data-sharing capabilities to enhance distributed mission execution.

  - Embedding ZT security models, advanced authentication mechanisms, and realtime intrusion detection directly into spacecraft architecture.

  - Integrating realtime, edge-based AI/ML processing to support autonomous anomaly detection, spacecraft self-defense, and intelligent task allocation.

- **Investigating the impact of emerging technologies on space architectures**

  Future spacecraft must integrate cutting-edge technologies to enhance security, resilience, and operational efficiency. However, new advancements should be carefully evaluated to ensure compatibility, security, and reliability within resource-constrained environments.

  - Studying how software-defined payloads, AI-driven automation, and advanced encryption technologies impact traditional space architectures.

  - Exploring the integration of post-quantum cryptography into architectures to protect against future quantum-based attacks.

  - Assessing the architectural requirements for deploying AI/ML models directly on spacecraft for autonomous anomaly detection, predictive maintenance, and cyberattack mitigation.

  - Investigating new energy-efficient computing architectures that allow greater onboard processing capabilities while minimizing power consumption. High-performance computing solutions that enable realtime security analysis and mission processing while remaining resilient to space radiation.

- Reinforcement learning (RL)

  - Research reinforcement learning for adaptive cyber defense in space environments:

    - Develop RL-based agents for dynamic routing, access policy updates, or anomaly detection tuning.

    - Simulate adversarial AI scenarios to train spacecraft responses.

  - Validate RL models within constrained on-orbit computing environments using digital twins.

  - Explore RL for optimizing onboard resource allocation under attack or anomaly conditions.

- **Defining the “best” suite of future architectures and identifying capability gaps**

  There is no universally accepted framework for next-generation spacecraft architecture. Research is needed to define a standardized reference architecture that ensures security, flexibility, and seamless integration across government, commercial, and allied space assets. Research could aim to address some of the following:

  - Developing a standardized reference architecture for future spacecraft. Establishing universal security and interoperability standards to streamline spacecraft integration across different missions.

    - Ensuring architectures support long-term software and hardware upgradeability to extend spacecraft lifespan.

  - Identifying technology gaps and pinpointing architectural limitations that prevent current spacecraft from adopting autonomous operations, advanced cryptography, and adaptive security models.
    - Creating roadmaps for closing gaps, ensuring future architectures remain agile, cyber-resilient, and cost-effective.
  - Long-duration mission support with reconfigurable software and hardware. Investigating in-space reconfigurable computing to allow spacecraft to adapt to mission changes without requiring new hardware.

- **Defining and evaluating hardware-agnostic cybersecurity: a shift away from rad-hardened computing**

  Rad-hardened computing adds cost and complexity, and limits hardware flexibility, leading to stagnation in cybersecurity innovation. Research is needed to explore software-based security mechanisms that reduce reliance on dedicated rad-hardened security chips while maintaining mission resilience. Some potential key research areas:

  - Exploring software-based security mechanisms that reduce dependence on rad-hardened, purpose-built cybersecurity components while maintaining resilience. Software-based security mechanisms may exist where designing cryptographic and authentication solutions will operate without requiring specialized security chips.
  - Evaluating secure enclave computing models for spacecraft.
  - Developing software-defined encryption that allows spacecraft to upgrade cryptographic protocols dynamically.
  - Developing trusted execution environments (TEEs) that ensure secure execution of mission-critical software without relying on hardware-dependent security protections.

- **Defining and evaluating alternative architectural approaches to replace rad-hardened compute assets**

  To reduce costs and increase flexibility, spacecraft should explore new error correction and distributed processing methods that reduce dependence on rad-hardened CPUs.

  - AI-driven, software-defined error correction, which could enable the use of commercial off-the-shelf hardware to operate in radiation-prone environments with AI-based error mitigation.
  - Investigating how computing workloads can be distributed across multiple spacecraft in a constellation, reducing reliance on individual hardened processors (e.g., voting schema).
  - Investigating the application of error-tolerant AI algorithms that allow non-rad-hardened computing assets to adaptively correct errors caused by space radiation. Developing adaptive ML-based error correction to compensate for radiation-induced faults without needing dedicated rad-hard computing hardware.

- **Determining the impact of architecture on computing resources, processing power, and latency**

  Spacecraft architectures must balance computational power, realtime processing needs, and energy efficiency to support AI, ML, and security monitoring. Potential research areas could include:

  - Evaluating tradeoffs between centralized and decentralized computing models, ensuring that architectures are optimized for realtime processing vs. high-latency deep-space operations.
  - Assessing the feasibility of AI-driven workload balancing, where computationally intensive security tasks are offloaded to ground stations or distributed across interlinked spacecraft.
  - Modeling power consumption impacts of AI/ML security monitoring, ensuring that future architectures prioritize efficiency without sacrificing security.
    - Ensuring that security architectures prioritize energy efficiency while maintaining robust threat detection.
  - Developing autonomous task scheduling models that optimize onboard computing resources while reducing power consumption.

- **Modifying communication interfaces (bus and payloads) to support open architecture**
  - Transitioning from closed, proprietary spacecraft interfaces to open, flexible architectures can improve security, interoperability, and mission adaptability.
    - Ensuring spacecraft from different manufacturers can exchange cybersecurity intelligence seamlessly.
  - Defining standards for secure inter-satellite communications, ensuring that spacecraft from different manufacturers can seamlessly exchange mission-critical data and cybersecurity intelligence.

Future space architectures should be scalable, cyber-resilient, AI-capable, and adaptable to evolving mission needs. This research ensures that next-generation spacecraft designs are security-first, hardware-agnostic, and optimized for AI-driven automation, allowing for autonomous security enforcement and adaptive mission execution. By transitioning to hardware-agnostic cybersecurity, AI-supported anomaly detection, and open architecture communication interfaces, future spacecraft will be more secure, interoperable, and mission-flexible than ever before. These advancements will enable a new generation of space operations that prioritize cybersecurity, autonomy, and resilience against emerging threats.

Area #7: Developing Trustworthy Operating Systems for Secure and Resilient Space Missions

As spacecraft become more software-defined and autonomous, their OS play a critical role in mission success, security, and resilience. However, current spacecraft OS architectures lack a standardized, security-first design, making them vulnerable to cyber threats, software failures, and operational disruptions. Many of the in-use OS contain unnecessary features and binaries that increase their attack surface. Unlike terrestrial systems, where OS security can be patched and updated dynamically, space-based systems operate in isolated environments, where software failures can lead to mission failure, data loss, or spacecraft inoperability. Additionally, most existing spacecraft OS implementations lack built-in root-of-trust (RoT) mechanisms, leaving them vulnerable to unauthorized modifications, tampering, and system exploitation.

To address these challenges, this research would aim to define, develop, and evaluate a suite of trustworthy OS tailored for different space architectures, ensuring secure execution environments, fault tolerance, and built-in resilience against cyber threats. This effort will focus on secure OS architectures for spacecraft buses, payloads, and mission-critical components, while balancing operational complexity with security and reliability.

Some of the problems being addressed by focusing on secure OS are:

- Lack of secure-by-design OS frameworks for spacecraft since many OS are not built with inherent security mechanisms, leaving them vulnerable to malicious code execution, unauthorized command injections, and system corruption.
- Inadequate isolation and separation between critical spacecraft functions. Many space OS implementations do not enforce strict separation between mission-critical processes, meaning compromised applications or payload software could impact spacecraft core functions.
- Limited built-in resilience, fail-safe mechanisms, and auto-recovery capabilities. Spacecraft OS must continue functioning even under extreme conditions, including cyberattacks, radiation-induced faults, or software corruption, but existing architectures lack automated self-healing mechanisms.
- No standardized OS architectures across different space missions. There is no universally accepted suite of operating systems for spacecraft, meaning that different mission types require custom-built/tailored OS solutions, increasing development complexity and security risks.

Areas of potential advancement could include:

- **Defining and evaluating a suite of operating systems for bus, payloads, and components built on a RoT**
    - Developing spacecraft OS architectures built on a secure RoT to ensure that only authenticated and verified software can execute on mission-critical systems.
    - Ensuring cryptographic integrity checks at the OS level, allowing spacecraft to validate their software images at boot and detect unauthorized modifications.
    - Investigate secure an OS architecture's ability to be tailored for different spacecraft subsystems (buses, payloads, components, etc.).
- **Optimizing isolation and separation for space environments**
    - Ensuring strict process isolation to prevent malicious or malfunctioning applications from affecting mission-critical functions.
    - Developing microkernel-based architectures where essential spacecraft functions run in isolated execution environments, reducing the risk of software corruption affecting core system stability.
    - Implementing secure privilege separation, ensuring that unprivileged software components cannot modify protected OS kernel functions or system memory.
    - Exploring the use of hypervisors and containerized environments in space OS architectures to enhance isolation while allowing dynamic mission updates.

- **Designing fail-safe, keep-alive, and auto-recovery mechanisms**

  - Developing automated OS self-healing mechanisms, allowing spacecraft to detect, isolate, and recover from software failures or cyber incidents.

  - Implementing redundant execution paths, ensuring that critical OS functions can automatically restart if they fail without disrupting mission execution.

  - Defining autonomous failure detection algorithms that analyze system health metrics (e.g., unexpected CPU loads, memory corruption events, or abnormal command execution patterns) and initiate automated recovery procedures.

  - Exploring the feasibility of rollback mechanisms, where spacecraft can restore a previously known-good OS state in case of software corruption or cyberattack-induced failures.

- **Defining and evaluating software architectures optimized for space systems**

  - Developing realtime OS architectures optimized for low-latency spacecraft operations, ensuring that mission-critical tasks execute with deterministic timing guarantees.

  - Designing OS architectures that support AI/ML-driven security monitoring, enabling spacecraft to autonomously detect and respond to anomalies in realtime.

  - Ensuring that OS architectures support post-launch reconfiguration, allowing for on-orbit software updates, security patches, and adaptive mission profile changes.

  - Evaluating how existing OS architectures (e.g., real-time executive for multiprocess systems [RTEMS], VxWorks, Linux, and emerging secure OS frameworks) can be modified for modern space cybersecurity and resilience needs.

  - Extend secure OS frameworks to protect payload and mission-specific software:

    - Define secure application containerization models for user space applications.

    - Implement privilege boundaries and runtime validation for mission applications.

  - Incorporate application-level patching, audit logging, and anomaly response mechanisms.

  - Promote inclusion of mission software in software bill of materials (SBOM) and validation pipelines.

- **Evaluating the balance between simplicity and complexity in space OS designs**

  - Assessing the tradeoffs between minimal OS designs and feature-rich OS, ensuring that spacecraft:

    - Maintain lightweight, resource-efficient execution without introducing security vulnerabilities due to unnecessary complexity.

    - Incorporate essential cybersecurity features without overloading the system's processing capabilities.

    - Can operate in degraded conditions, where failures in one component do not compromise the entire OS stack.

- Determining the best architectural approach for balancing OS security, reliability, and mission adaptability based on spacecraft mission profiles, risk tolerance, and expected operational lifespan.

Developing trustworthy OS for space is essential to enhancing spacecraft security, resilience, and autonomy. By building OS architectures with RoT mechanisms, strong process isolation, and automated fail-safe mechanisms, future spacecraft will be better equipped to withstand cyber threats, system failures, and mission disruptions. Furthermore, by ensuring flexibility, interoperability, and scalable security features, space OS frameworks will enable next-generation missions to operate securely across diverse architectures, from standalone deep-space probes to interconnected LEO constellations. This research should ensure that space OS designs prioritize cybersecurity, mission reliability, and adaptability, providing a robust foundation for future space exploration and defense initiatives.

Area #8: Establishing Standards for Secure and Interoperable Space Systems

As space operations grow more complex and interconnected, the lack of standardized security and engineering frameworks poses a challenge to mission interoperability, resilience, and cybersecurity. Unlike terrestrial IT and OT systems, where security best practices are well established, space systems operate under unique constraints, including intermittent communication paths, long latency delays, and highly heterogeneous architectures. The absence of standardization in development methodology, secure networking, key management, and system interoperability increases the risk of fragmented security policies, inefficient mission coordination, and vulnerabilities across multi-organization space operations.

This research seeks to define and advance standardization efforts in space and security engineering, ensuring that space systems can seamlessly interoperate, securely exchange mission-critical data, and maintain robust cybersecurity postures across diverse mission architectures.

Areas of potential advancement could include:

- **Researching the security of delay-tolerant networking (DTN) in space communications**

  Originally developed by NASA, DTN enables spacecraft to communicate across disrupted, high-latency environments, allowing for store-and-forward data transmission between nodes that are intermittently connected. However, DTN security is not yet fully standardized, which could create vulnerabilities in data integrity, authentication, and availability.

  - Evaluating the cryptographic security of DTN-based protocols to prevent data tampering, replay attacks, and unauthorized interception of delayed transmissions.

  - Developing intrusion detection mechanisms tailored for DTN networks, ensuring that spacecraft can detect and mitigate cyber threats even when operating under long latency constraints.

  - Hardening DTN implementations against cyber-physical attacks, preventing adversaries from disrupting message relays, injecting false telemetry, or delaying mission-critical communications.

- **Developing secure key management protocols for intermittent communication paths**

  Unlike terrestrial networks, where continuous connectivity allows for realtime cryptographic key exchange, space networks experience long durations without contact, requiring new approaches to key generation, distribution, and authentication. Without secure key management, adversaries could intercept or manipulate spacecraft communications, inject false commands, or decrypt mission-sensitive data.

- Defining key pre-distribution models that allow spacecraft to generate and securely store cryptographic keys before launch, enabling secure data exchanges even when disconnected from ground control.
- Exploring threshold cryptography for space missions, where distributed trust models allow spacecraft to self-authenticate and securely establish session keys without relying on ground-based key servers.
- Developing post-quantum key management strategies to ensure that spacecraft remain protected against future quantum-based decryption threats, particularly for long-duration missions.
- Implementing resilient key rotation and rekeying mechanisms, ensuring that spacecraft can automatically update encryption keys when reestablishing contact with mission control or peer spacecraft.

◆ **Establishing interoperability standards for secure multi-network space operations**

Modern space missions involve collaborations between government agencies, commercial spacecraft operators, and allied nations, requiring standardized security frameworks to ensure seamless interoperability across diverse mission assets. However, many organizations still rely on proprietary architectures, leading to fragmented security models, communication incompatibilities, and cybersecurity gaps. On the civil space side, the Consultative Committee for Space Data Systems (CCSDS) is a group working on interoperability standards, but these have not been universally adopted.

- Defining universal security protocols for inter-satellite networking, ensuring that different spacecraft fleets can securely share mission data, relay commands, and exchange security updates without introducing interoperability risks.
- Developing standardized authentication and encryption frameworks for spacecraft-to-ground and spacecraft-to-spacecraft communications, ensuring end-to-end data protection across multi-organization missions.
- Building secure application programming interface (API) interfaces for cross-platform spacecraft collaboration, enabling federated security monitoring, joint anomaly detection, and shared threat intelligence capabilities across mission partners.
- Implementing ZT security principles in space networking, ensuring that all data exchanges are continuously authenticated and monitored, even between trusted entities.

◆ **Establishing a standardized process for secure-by-design (SbD) space system development**

The lack of a standardized process for designing, developing, and validating secure space systems has led to fragmented security implementations, inconsistencies across missions, and vulnerabilities in mission-critical space assets. Without a unified, industry-wide SbD framework, space system manufacturers, government agencies, and commercial operators risk inadequate security controls, insufficient testing, and difficulty in integrating cybersecurity measures across mission phases.

A formalized SbD framework, such as what is being proposed by IEEE P3349, would establish a structured process for building, testing, and verifying security measures in space systems from concept to deployment. This research would focus on refining, expanding, and advocating for the adoption of standardized SbD processes, ensuring that future space systems are engineered with cybersecurity at the forefront rather than as an afterthought.

Some example key areas of research:

- Formalizing as a baseline for secure space system engineering.
    - ◇ Establishing process-driven security engineering methodologies that integrate cyber risk assessments, threat modeling, and security validation throughout design and development.
    - ◇ Defining minimum security requirements based on their operational risk profile and threat exposure.
    - ◇ Ensuring that security engineering principles align with existing space industry standards such as NIST SP 800-160 (Volume 1, "Engineering Trustworthy Secure Systems," and Volume 2, "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach") and CCSDS cybersecurity guidelines.
- Developing a secure-by-design certification process for spacecraft.
    - ◇ Establishing a standardized cybersecurity certification and compliance process that spacecraft must meet before launch, ensuring that all mission-critical systems are hardened against cyber threats.
    - ◇ Defining a structured testing and validation framework that includes penetration testing, vulnerability scanning, and secure software assurance for flight systems.
    - ◇ Implementing a modular security validation approach, ensuring that spacecraft can evolve and maintain compliance as cybersecurity threats change.
- Building a standardized repository of secure-by-design best practices and lessons learned.
    - ◇ Collecting historical data on spacecraft cyber incidents, vulnerabilities, and mitigations to inform future mission designs and security engineering improvements.
    - ◇ Establishing a cross-agency, international knowledge-sharing framework, ensuring that lessons from commercial, military, and scientific missions are applied consistently across the space industry (e.g., Space-ISAC).

    - ◇ Advocating for widespread adoption of secure-by-design methodologies across government, industry, and academic institutions, ensuring long-term commitment to space cybersecurity.

- **Open space network (OSN)**
  - Develop architectural and security standards for OSN environments:
    - ◇ Secure inter-satellite and inter-provider routing protocols with federated trust.
    - ◇ Mission data and telemetry exchange agreements across domains with ZT enforcement.
  - Establish APIs and access control models that support multi-tenant, cross-mission operations.
  - Define cryptographic interoperability mechanisms for coalition and commercial OSN participants.
  - Expand OSN concepts to support cooperative space situational awareness (SSA) and collision avoidance, like ADS-B in aviation:
    - ◇ Enable spacecraft to broadcast telemetry beacons (e.g., position, velocity, and intent/maneuver planning) on secure, authenticated channels.
    - ◇ Facilitate peer-to-peer awareness between spacecraft (crosslinks), enabling decentralized conflict detection and resolution.
  - Develop interoperable beacon protocols and standards for spacecraft-to-spacecraft and spacecraft-to-ground visibility:
    - ◇ Leverage secure broadcast messages for orbital state, health status, and proximity alerts.
    - ◇ Incorporate cryptographic authentication to prevent spoofing or adversarial manipulation of space traffic data.

By establishing standardized security frameworks for space systems, this research hopes to enhance cybersecurity resilience in delay-tolerant space networks, preventing adversarial manipulation of high-latency communications. Ensure secure cryptographic key management for spacecraft operating in intermittent connectivity environments, preventing data breaches and command hijacking. Define universal interoperability standards, allowing spacecraft from different organizations to securely communicate, share intelligence, and collaborate on mission objectives. By addressing these standardization challenges, future space missions will benefit from enhanced security, seamless interoperability, and greater mission assurance in an increasingly contested space domain.