SPACE ISAC

Space ISAC Artificial Intelligence & Machine Learning Community of Interest

DEVELOPING AI FOR SPACE CYBERSECURITY

Samuel Lefcourt, ReveillAI, Christine Black, The Aerospace Corporation, Daniel Westfall, The Aerospace Corporation, Max Spolaor Ph.D., The Aerospace Corporation, Ray Schouten, SQS, Dr. Larraine Brandt, P.E.

Developing AI for Space Cybersecurity

Space ISAC AI / ML COI

Executive Summary

The purpose of this paper is to educate and raise awareness of cyber threats in space and the potential use of new techniques in Artificial Intelligence (AI) for mitigating these threats as well as the vulnerabilities AI introduces.

This paper examines cybersecurity concerns related to space components, infrastructure, services, and operations, and assesses the application of MLSecOps, the Aerospace's SPARTA and MITRE ATLAS frameworks, and the use of AI for enhanced security.

Introduction

The burgeoning use of space technologies across the commercial, government, and international sectors has brought increased attention to the importance of space cybersecurity. As threats from leading-edge state actors grow more sophisticated, it becomes imperative to safeguard assets in the space domain.

Securing these vulnerable and high-impact targets from cyber threats is particularly challenging. Extended development and launch timelines, limited resources on the spacecraft, and the inaccessibility of the craft once in orbit are just some of the constraints that significantly hamper traditional cybersecurity methods. By the time a satellite arrives in orbit, new and advanced cybersecurity threats have been developed beyond the mitigation capabilities of that satellite. To keep pace with the rapidly evolving threat landscape, the space community has retroactively devised protective frameworks to help guide the community to suitable solutions.

However, the significant increase in satellite deployments and the rise in sophistication of cyber threats have highlighted the limitations of human ability to handle the complexity and sheer volume of attacks on space systems. Artificial Intelligence (AI) presents a promising solution to enhance human capabilities by accelerating threat detection and decision making. While offering exciting advancements, AI also introduces unique cybersecurity vulnerabilities, necessitating thoughtful security measures and following proper Machine Learning Security Operations (MLSecOps) procedures (Spolaor 2023).

Recognizing the industry's need for a comprehensive cybersecurity framework tailored for AI in space, we discuss the relevant components and vulnerabilities that must be considered.

Space Architecture

A traditional space system consists of four segments: a ground station, communication link, the space asset, and a user segment, shown in Figure 1. The ground station is responsible for driving the mission and sending commands, whereas the communication link, traditionally radio frequencies, enables these commands to be sent to the space device. The space asset (satellite) executes the commands to complete the mission(s). The user segment provides a mechanism for users to interface with the spacecraft and data. Each segment consists of unique vulnerabilities and entry points.

Space Cyber Threats

The space domain has increasingly become a target for sophisticated cyber attacks due to its critical role in global communications, military operations, and navigation systems. As more nations and private companies venture into space, the risk of cyber incidents has escalated. These threats can disrupt operations, lead to data breaches, and compromise national security.

Cyberthreats occur when adversaries infiltrate systems through vulnerabilities present in software and hardware dependencies that operators rely on. These threats can manifest in various forms, such as ransomware injection and supply chain attacks. Manipulated components could lead to indirect access to critical systems or introduce backdoors into secure networks. Advanced persistent threats (APTs) will engage in long-term and sophisticated hacking efforts targeting both government and commercial organizations to disrupt operations, engage in espionage, sabotage terrestrial conflicts, and more. Space components such as satellites, ground stations, and communication networks are prime targets for cyber adversaries. Notable frameworks that focus on the issues faced by space systems include the NIST IR 8270, which focuses on cybersecurity for commercial satellite operations, and the Space Attack Research and Tactic Analysis (SPARTA) framework, which outlines space threat tactics and techniques. These segments face threats such as signal jamming, hacking, data manipulation, and other attacks which are ripe for AI to have a positive impact. Table 1 describes some examples of cybersecurity risk mitigations that can be applied to various space segments. For a more in-depth review see Bailey (2021).

Table 1. Breakdown of space segment and sample cybersecurity risk mitigations

Space Segment	Function	Cybersecurity Risk Mitigations
Ground Stations	Command and control of space assets	Network segmentation, intrusion detection systems, secure hardware maintenance, etc.
Communication Networks	Networking infrastructure connecting space assets and ground stations	Multi-payer encryption, secure routing, real-time monitoring, etc.
Space Assets	Various communications, navigation, observation, scientific measurements, etc.	Encryption protocols and isolation techniques, Service-Level Agreements (SLAs), robust logging, and automated patch management, etc.
User Segment	End user of a space system	Encryption protocols, intrusion detection systems, secure routing, etc.

AI Space System Architecture

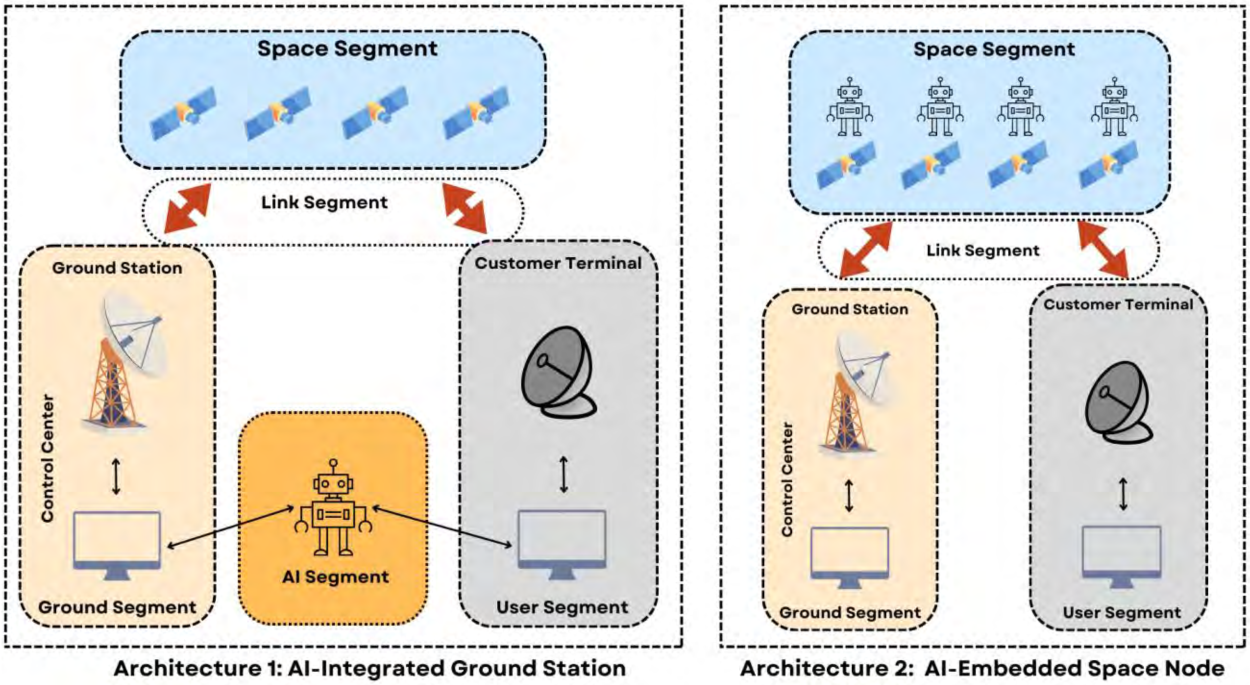

Figure 1. Depiction of the space system architecture and locations for AI integration.

Building an AI system for any domain requires a thorough understanding of its operational environment. Figure 1 highlights two architectures that offer a generalizable means of AI deployment within a space system: 1) AI systems embedded within the ground station and

2) AI on the edge. Architecture 1 allows for a variety of models to tackle problems like intrusion detection or fault management that can be layered and periodically updated to match current threats. For Architecture 2, the main advantage is speed. With the AI segment embedded on the spacecraft, communication latency and reaction times to potential attacks are significantly reduced.

While these provide a flexible architecture as a baseline, designing intelligent space technology is a rigorous process that must be tailored to specific requirements, such as data size, inference speed, the frequency of model updates, and SWAP (size, weight, and power) impacts.

Applications of AI for Space Cybersecurity

AI methods offer unique protection of space systems from cybersecurity threats. They can be used in the deployment of defense mechanisms and provide more responsive and adaptable countermeasures. For example, AI-based anomaly detection techniques can provide real-time intrusion detection and prevention. By automating threat detection and response, space agencies can mitigate risks attributed to sophisticated cyber-attacks.

A secure and trusted AI system will achieve and maintain a high level of performance in its operational environment. MLSecOps represents the convergence of machine learning and security operations to fortify cybersecurity efforts. This concept involves both utilizing AI methods for real-time threat detection/mitigation and securing the AI methods themselves within the MLOps framework.

MLOps is broken down into seven stages, allowing for thoughtful security implementations throughout the AI development process, shown in Figure 2.

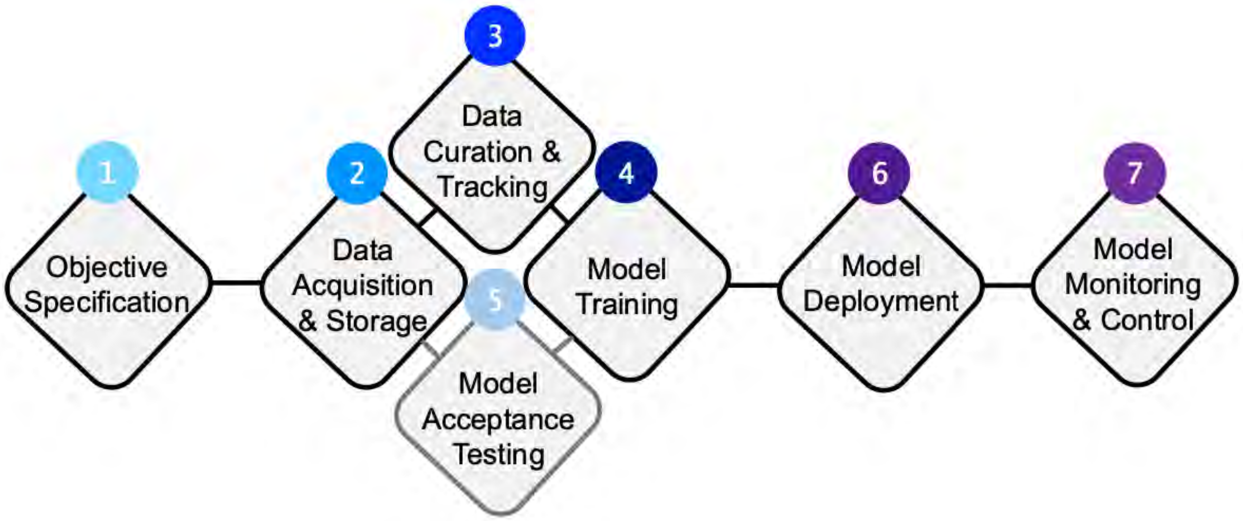

Figure 2. The seven stages of the MLOps workflow.

Tools, like the MITRE ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems) taxonomy, provide insight into the unique cyber threats faced by AI systems that should be considered during development.

A securely designed AI system for deployment within a space system should:

1. Maintain a level of transparency into the AI model operations so that potential failures can be easily diagnosed.
2. Be adaptable over time to respond to natural changes as well as evolving threats.
3. Be robust to a range of inputs to minimize instability caused by unfamiliar or manipulated data.
4. Have safety measures in place to monitor the model for out of distribution results.

Considerations for Maintaining Space Cybersecurity Integrity with AI

Because necessary AI resources, like compute power and data storage, can be significantly restricted in a space system, creative work arounds are needed to achieve nominal results. However, this comes with the cost of pairing down the AI architecture in ways that can make it more vulnerable to attack than a more robust, traditional system. Table 2 offers a way to approach combining MLSecOps practices, Aerospace's SPARTA, Mitre ATLAS in order to assess the security and integrity of an AI model in a space system throughout the development process. Note that the "Impacted Segment" (Ground, Space, User) can be dependent on where the AI model is deployed.

Table 2. Example method for documenting potential security vulnerabilities and possible mitigations to employ for a given space system

TRL	Impacted MLOps Stages (2-7)	Space System Vulnerabilities (SPARTA)	AI Segment Vulnerabilities (ATLAS)	Possible Mitigations	Impacted Segment
2/3	2, 3, 4, 5	1) REC-0001: Gather Spacecraft design 2) RD-0001: Acquire Infrastructure	1) AML.T0004: Search Application Repositories 2) AML.T0010: ML Supply Chain Compromise	Monitor for significant deviation from expected performance	All
4/5	2, 3, 4, 5, 6, 7	1) IA-0011: Auxiliary Device Compromise 2) IA-0009: Trusted Relationship	1) AML.T0019: Publish Poisoned Datasets 2) AML.T0020: Poison Training Data	Outlier Detection for poisoned data Small verified batch	Ground, Space
6/7	4, 5, 6	1) EX-0010: Malicious Code 2) EXF-0002: Side-Channel Attack	1) AML.T0040: ML Model Inference API Access 2) AML.T0031: Erode ML Model Integrity	1) Human in the loop oversight 2) Data Drift Identification 3) Explainability / Transparency in decision-making	User
8/9	6, 7	1) DE-0003: Modify On-Board Values 2) EX-0013: Flooding	1) AML.T0051: LLM Prompt Injection 2) AML.T0015: Evade ML Model	1) Incorporate closed-loop adversarial training. 2) Identify select threats to build resiliency to	Space, User

This paper highlights the current threats to space cybersecurity across its various components, while introducing recommended guidelines to potential AI solutions. While

AI provides a promising means of defense to the threat landscape, it also introduces risks which must be addressed. Understanding this gap in standards, we analyze Aerospace's SPARTA, MITRE ATLAS, and MLSecOps frameworks to present viable attack surfaces and suggest guidelines towards developing protection for AI systems. Future work should expand upon the attack vectors discussed and prepare for an increasingly autonomous shift to threats. It must be acknowledged that the development of cyber threats will continue to increase, and this work does not provide a comprehensive body of knowledge, but a foundational starting point for next efforts.

References

Bailey, B. 2021. "Cybersecurity Protections for Spacecraft: A Threat Based Approach". The Aerospace Corporation, TOR-2021-01333-REV A. https://aerospace.org/sites/default/files/2022-07/DistroA-TOR-2021-01333-Cybersecurity%20Protections%20for%20Spacecraft--A%20Threat%20Based%20Approach.pdf

MITRE. "MITRE ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems)." Accessible online at: https://atlas.mitre.org/

Scholl, M., & Suloway, T. (2023). Introduction to Cybersecurity for Commercial Satellite Operations. National Institute of Standards and Technology, Gaithersburg, MD. NIST Interagency or Internal Report (IR) NIST IR 8270. DOI: 10.6028/NIST.IR.8270. https://csrc.nist.gov/pubs/ir/8270/final

Spolaor, M., Miller, T., Archuleta, M., & Wilson, D. 2023. "Machine Learning Security Operations: MLSecOps". Space ISAC: Artificial Intelligence and Machine Learning Community of Interest. https://spaceisac.org/wp-content/uploads/2023/08/Space-ISAC-MLSecOps-White-Paper-08.04.2023.pdf

The Aerospace Corporation. "SPARTA (Space Attack Research and Tactic Analysis)." Accessible online at: https://sparta.aerospace.org/