Project Proposal: TBD-Named (Secure Autonomous Command Integrity System)

---

1. Project Title:
TBD-Named: AI-Powered Command and Control Integrity for Space Missions

2. Mission Objective:
Develop an AI-driven platform that autonomously protects spacecraft command and control (C2) systems from unauthorized access, spoofing, and anomalies, especially during deep space missions with high communication latency.

3. Problem Statement:
Deep space missions face a high cybersecurity risk. Communication delays (up to 50 minutes) and lack of immediate human oversight create vulnerabilities. A successful attack on the C2 link could jeopardize billion-dollar missions and human lives. Traditional encryption is essential but insufficient without intelligent anomaly detection.

4. Proposed Solution:
SENTRY-AI will integrate:

- Command Authentication Verification
- Real-Time Anomaly Detection
- Adaptive Threat Response Mechanisms
- Threat Environment Adaptation Algorithms
- Immutable Audit Logging

5. Commercial Potential:
Beyond NASA, the platform can serve:

- Private satellite operators (SpaceX, Planet Labs)
- National defense space programs (U.S. Space Force)
- Lunar infrastructure (Artemis program partners)

6. Project Timeline Overview:

- Phase 1: Simulated attack scenarios + AI model training (0–9 months)
- Phase 2: Hardware-in-the-loop testing (10–18 months)
- Phase 3: LEO mission beta test (19–30 months)
- Phase 4: Deep space mission integration (31–48 months)

7. Project Team:

- Cybersecurity Engineers
- AI/ML Researchers
- Aerospace Systems Engineers
- Mission Operations Specialists

Detailed Solution Plan

Core Components:

Component	Purpose	Technology
Command Verification	Authenticate uplinked commands	Digital signatures, anomaly detection
Anomaly Detection	Detect suspicious command patterns	Supervised/Unsupervised ML (Autoencoders, Isolation Forests)
Adaptive Response	Quarantine, reject, escalate	Reinforcement Learning Decision Engines
Threat Prediction	Pre-emptive system hardening	Predictive threat modeling
Secure Logging	Immutable event records	Blockchain-based secure audit trails

System Flow:

1. Incoming command packet arrives.
2. Authenticate packet and verify signatures.
3. Analyze command pattern with AI models.
4. Accept/Quarantine/Reject command.
5. Log decision immutably.

Unique Innovations:

- Autonomous cybersecurity decisions without ground control delays.
- Dynamic threat adaptation based on environmental signals.
- Lightweight edge-optimized AI models for spacecraft hardware.

Testing Plan

Phase 1: Simulation-Based Testing

- Simulate normal and adversarial command traffic.
- Train supervised and unsupervised models on anomalies.
- Validate detection rates (>99% anomaly detection with <1% false positives).

Phase 2: Hardware-in-the-Loop Testing

- Integrate AI models with spacecraft-grade hardware.
- Conduct live simulation attacks (spoofed commands, timing attacks).
- Measure system response times and accuracy.

Phase 3: Low Earth Orbit (LEO) Testing

- Deploy a beta unit aboard a CubeSat.
- Monitor real-world telemetry and command integrity.

Phase 4: Deep Space Testing

- Deploy system on long-delay mission simulations.
- Test autonomous fallback procedures.

APA References:

NASA. (2021). *NASA Technical Memorandum: Space System Protection Standard*. NASA. https://ntrs.nasa.gov/api/citations/20210012886/downloads/NASA-TM-20210012886.pdf

Defense Innovation Unit. (2021). *Secure Command and Control for Space Assets*. U.S. Department of Defense. https://www.diu.mil/secure-space-c2

Consultative Committee for Space Data Systems (CCSDS). (2015). *Space Data Link Security Protocol*. https://public.ccsds.org/Pubs/355x0b1c2.pdf

National Institute of Standards and Technology. (2019). *Security Framework for Space Systems*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf