POINT | SOLUTIONS GROUP

Securing Satellites: Cyber-Hardening Satellites in the Age of AI

September 11, 2024

Dr. Brian Hart

Astrophysicist / Space Data Scientist

WWW.POINTSOLUTIONSUS.COM

POINT | SOLUTIONS GROUP

KEYNOTE HIGHLIGHTS

1 **SETTING THE STAGE**
AI-driven threats and how AI can be leveraged for defense in satellite cybersecurity

2 **ADVERSARY'S PLAYBOOK**
AI-Driven Threats to Satellite Operations Across Orbits

3 **LEARNING FROM THE PAST**
Case studies to understand the implications for modern satellite security

4 **STRATEGIC DEFENSE MEASURES**
Integration of AI and the importance of innovation

5 **CLOSING THOUGHTS**
Key takeaways and a sense of direction – forward looking

Bio

- From Minneapolis / Saint Paul, MN
- Ph.D. Astrophysics, UC Irvine 2008
- Two-Time Military Veteran

U.S. Army

DA Civ Physicist, SMDC
Alabama Army National Guard Soldier
Redstone Arsenal, AL

U.S. Navy

Active Duty Officer 2018-21
Cyber Warfare Engineer
Fort Meade, MD

- Currently reside in Colorado Springs

Welcome

What we will cover today:

- AI's evolving threats to satellite security and unique challenges in defending these systems.
- Gain appreciation of the imperatives of ensuring security of satellite operations, enabling us to stay ahead of adversaries in this fast-evolving field.
- Explore real-world examples and discuss leveraging AI as a powerful tool for defense.

My goal is that you will leave this session with a deeper understanding of the current threat landscape and the need to safeguard Space assets.

1 SETTING THE STAGE

AI in Satellite Cybersecurity: Threats and Defense

Navigating the Dual Role of AI in Modern Satellite Security

AI Driven Attacks

- Predictive AI for Target Vulnerability Identification
- Generative AI for Satellite Operator Phishing and Social Engineering
- AI-Driven Signal Satellite Communications Jamming and Spoofing

AI Driven Satellite Defense

- Predictive AI for Threat Anticipation
- Heuristic AI for Anomaly Detection
- Generative AI for Adaptive Defense
- Autonomous Response and Recovery

AI Arms Race - Strategic Implications for Defense and Security

Satellite security must advance to counter AI-driven cyber threats. By utilizing AI's predictive, adaptive, and autonomous capabilities we can develop robust defense systems against a constantly changing threat environment.

Technical Solutions and Mitigation Strategies for Satellite Cybersecurity

Monitoring existing and emerging technologies, along with practical insights, is crucial for defending against AI-driven attacks on satellites.

Deployed Technologies on Satellites	Emerging and Future Technologies	Implementing Practical Insights
▪ End-to-End Encryption	▪ Quantum Key Distribution (QKD)	▪ Proactive Defense
▪ Intrusion Detection Systems (IDS)	▪ Supply Chain Risk Management	▪ Adapting to Emerging Threats
▪ Incident Response and Recovery Plans	▪ Regular Security Audits and Penetration Testing	▪ Continuous Improvement

Key Takeaway: While significant progress has been made in securing satellite systems, ongoing vigilance, innovation, and adaptation are essential to effectively counter the evolving cybersecurity landscape.

2 ADVERSARY'S PLAYBOOK

How Attackers Use AI in Cyberattacks

The landscape of attackers exploiting AI to breach satellite defenses.

1. **Predictive AI for Identifying Vulnerabilities**

   Used to identify vulnerabilities in systems, including satellite ground stations - already a concern in cybersecurity circles.

2. **Generative AI for Crafting Phishing Attacks**

   Enhanced by generative AI against ground stations and satellite operators

3. **AI-Driven Signal Jamming and Spoofing**

   AI-enhanced jamming and spoofing techniques are actively researched and deployed to disrupt satellite communications.

4. **Emerging Techniques**

   Heuristic AI for Adaptive Malware and AI for Automating Large-Scale Cyberattacks are emergent techniques.

Takeaway

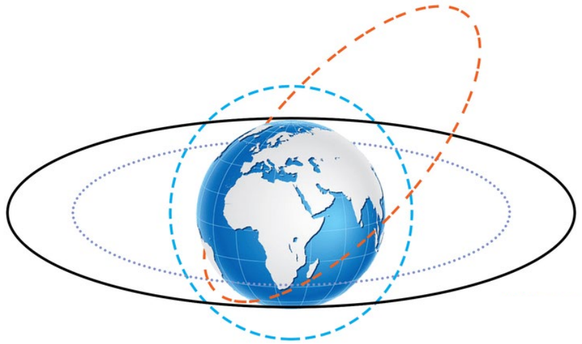
As attackers continue to refine and enhance their AI-driven techniques, it becomes imperative for satellite operators to develop equally advanced defense strategies to counter these evolving threats.

AI-Driven Threats to Satellite Operations Across Orbits

Addressing the Evolving Cybersecurity Challenges from LEO to HEO.

Low Earth Orbit

- **Threat**: Increased Cyber Exposure with Expanded Satellite Constellations



Medium Earth Orbit

- **Threat**: AI-Driven Disruption of Navigation System

Geosynchronous Orbit

- **Threat**: AI-Driven Attacks on Strategic Communication Assets

Highly Elliptical Orbit

- **Threat**: AI-Driven Threats to Specialized and Long-Duration Missions

Specific Challenges for Satellites

The challenges faced by satellite operators necessitate innovative approaches and technology solutions.

- Limited Computational Resources
- Long Lifespan with Outdated Technology
- Dependency on Ground Station Security
- AI-Induced Vulnerabilities
- Increased Attack Surface Due to Interconnectivity
- Challenges in Real-Time Threat Detection and Response
- Regulatory and Compliance Challenges
- Supply Chain Security

3 LEARNING FROM THE PAST

Case Study: *ROSAT* Incident

Overview: The *ROSAT* (*Röntgensatellit*) was a pioneering X-ray observatory that, through its study of X-ray emissions, contributed significantly to understanding the universe.

Pioneering Mission: The satellite had a successful operational period, making critical discoveries in X-ray astronomy before it ceased operations in 1999.

Importance: *ROSAT*'s mission underscored the strategic importance of space-based assets in scientific research and their contribution to technological advancements.

Incident: *ROSAT* experienced a critical failure that rendered it unusable due to inadvertently pointing its X-ray imager toward the sun - overheating and irreparably damaged the imager.

Significance: Though unproven whether an intrusion directly led to the satellite's damage, the incident highlights vulnerabilities in space systems and the potential for cyber exploitation.

Case Study Analysis: Strategic Implications

Enhancing Cybersecurity and Operational Integrity in Space Missions

Vulnerabilities in Satellite Operations

- **Speculative Concerns:** Although no definitive evidence of external interference present, the event highlights the inherent vulnerabilities in Space assets.
- **Cybersecurity Relevance:** Need for rigorous measures to protect against software errors and potential cyber threats.

Strategic Lessons for Modern Satellite Operations

- **Operational Safeguards and Redundancy:** Ensuring satellite systems are resilient against both accidental failures and potential cyberattacks.
- **Continuous Monitoring and Adaptation:** Ability to adapt to emerging threats in real-time.

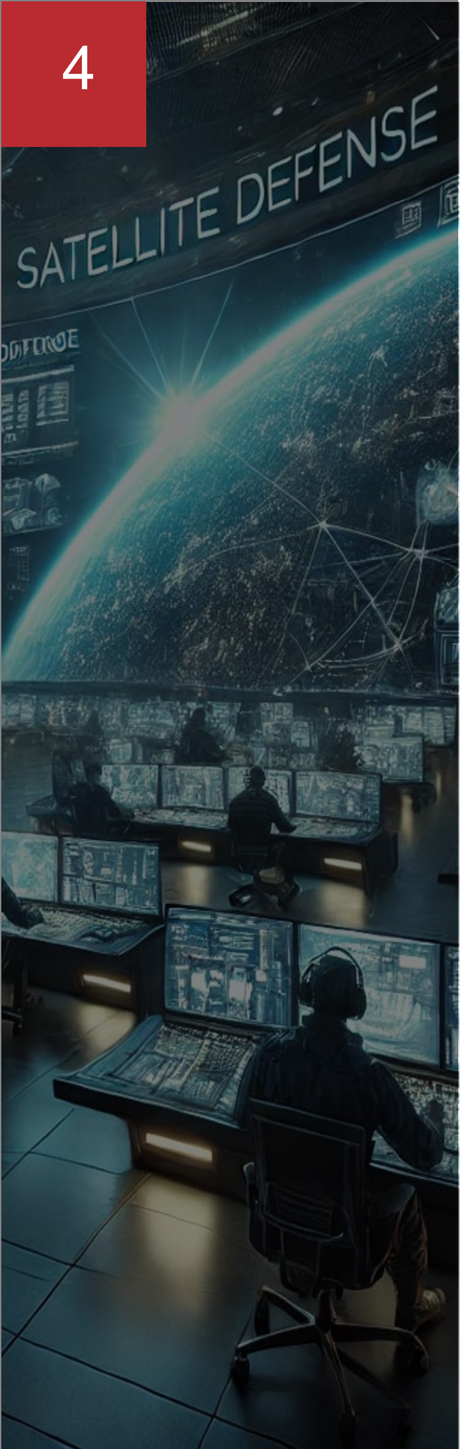
Strategic Implications for DoD and Military Satellites

- **Enhancing Cyber Posture:** Reminder of ensuring operational protocols must withstand technical and malicious threats.
- **Collaboration and Intelligence Sharing:** Sharing intelligence and best practices for securing satellite operations against threats.

Takeaway

By learning from this event, we can enhance our operational safeguards, integrate cybersecurity from the design phase, and ensure the resilience of our space-based assets against both accidental and intentional threats.

4 STRATEGIC DEFENSE MEASURES



Strategic Defense Measures in Satellite Cybersecurity

Ensuring Resilience and Security in the Age of AI

Predictive Defense

- AI for Threat Intelligence
- Collaborative Intelligence Sharing

Resilient Systems

- Collaboration
- AI-Enhanced Defensive Architectures

Training

- Advanced Training Programs
- AI Attack Simulation

R & D

- Next-Generation AI
- Partnerships for Innovation

By integrating these measures, we can ensure the continued security and operational readiness of our critical satellite assets.

5 CLOSING THOUGHTS

CLOSING THOUGHTS

SECURITY IMPERATIVE

In the age of AI, securing satellites is not just an option but a necessity to ensure the continuity and reliability of global communication, navigation, and data integrity.

EVOLVING THREATS

The threat landscape is rapidly evolving, with AI-driven attacks and sophisticated malware presenting new and complex challenges specifically targeting satellite systems.

PROACTIVE DEFENSE

By leveraging AI for defense, we can significantly enhance our capabilities to predict, detect, and mitigate cyber threats, staying one step ahead of potential adversaries.

LOOKING FORWARD

Our approach to cybersecurity must evolve in tandem with AI, ensuring that we safeguard not just the satellites themselves but the critical infrastructure they support.

POINT | SOLUTIONS GROUP

THANK YOU

Point Solutions Group

Dr. Hart LinkedIn Profile

Feedback for this Talk

ISSA-COS Website

WWW.POINTSOLUTIONSUS.COM