4th Workshop on the Security of Space and Satellite Systems

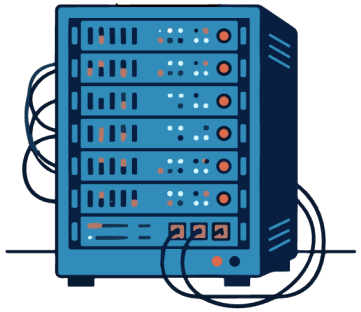
Temporal Risk on Satellites

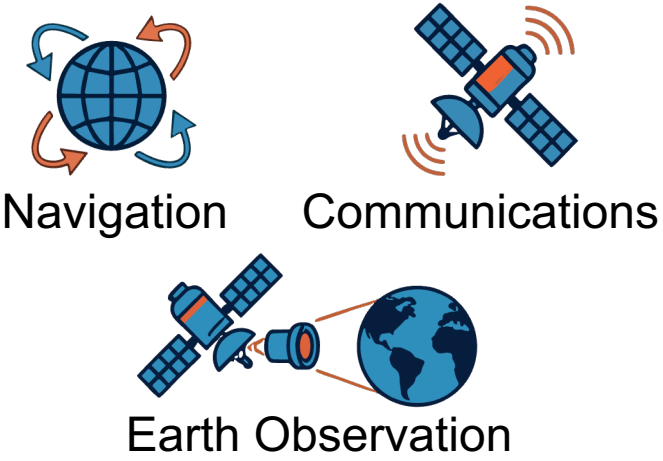
Shiqi Liu, Kun Sun

Center for Secure Information Systems, George Mason University

Background

- *Where* do threats in space occur?





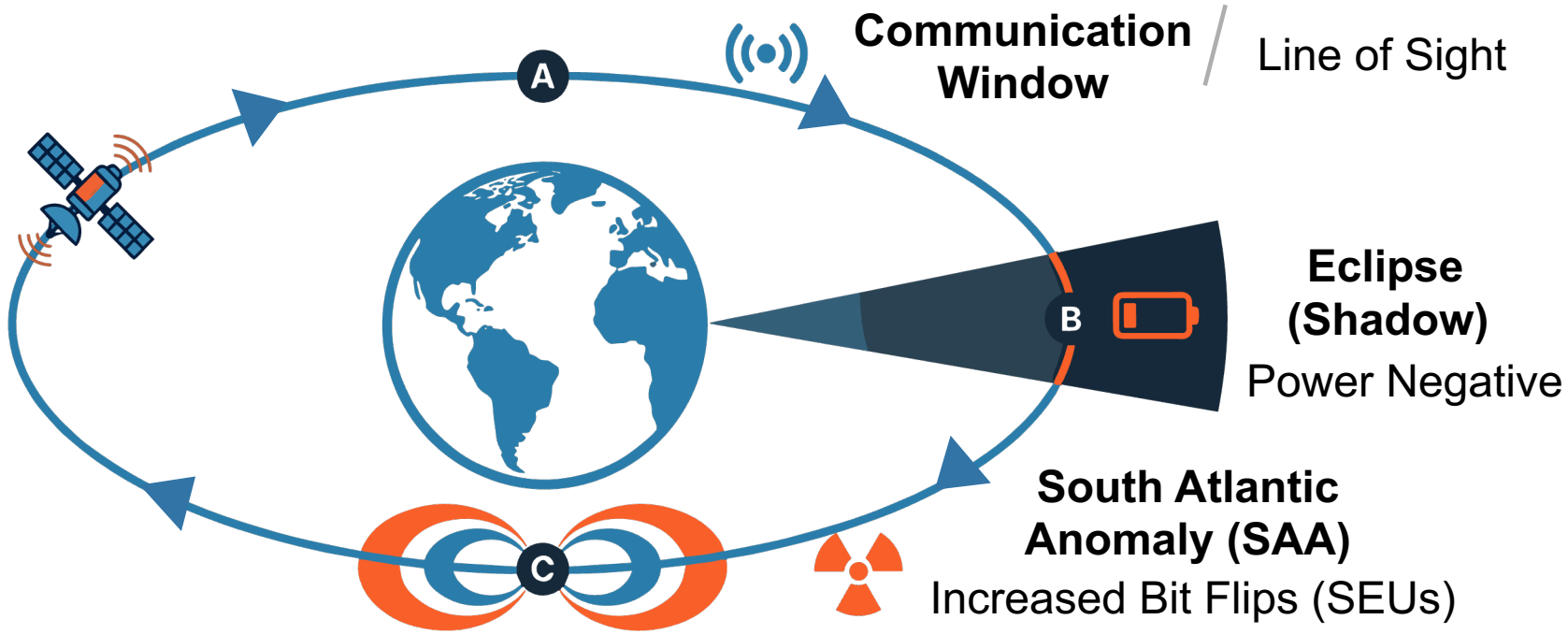
User / Ground Segment **Link Segment** **Space Segment**

- *What* are the threats to space?

User / Ground Segment	Link Segment	Space Segment
User terminal exploitation Ground-network compromise	Jamming & Spoofing	Unauthorized control On-orbit firmware exploitation

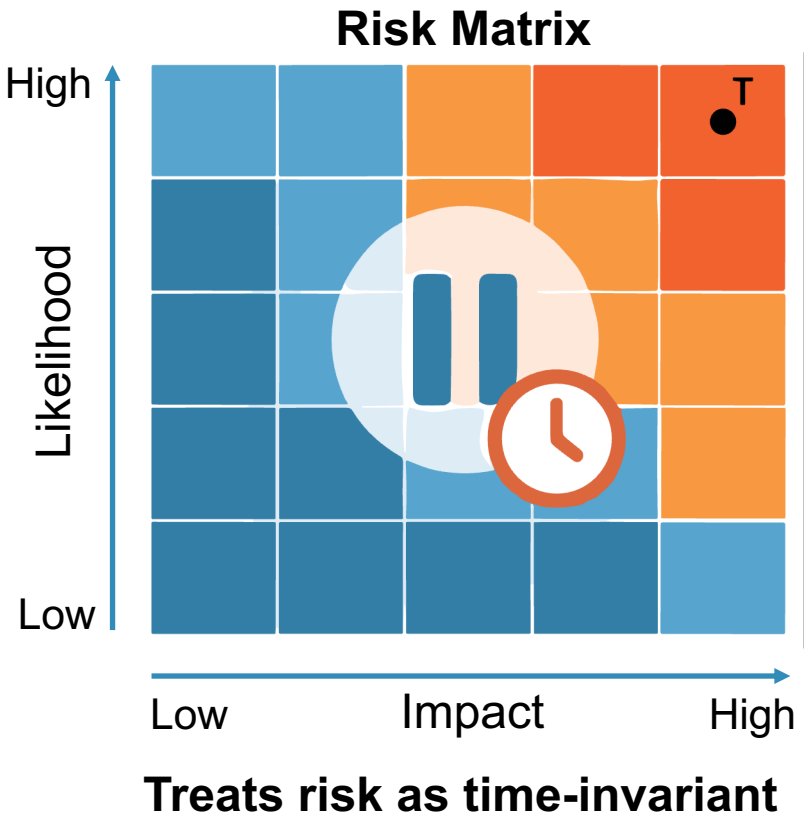
Observation

- *When* threats occur also matters!
  - The environment is changing over time.
- Threats are physically *predictable*.
  - Based on orbital mechanics and space weather.



Motivation: The Temporal Gap

Current Static Frameworks (e.g., SPARTA Approach[1])



Treats risk as time-invariant

The *Missing* Dimension

The Resulting Gaps

Incomplete Likelihood

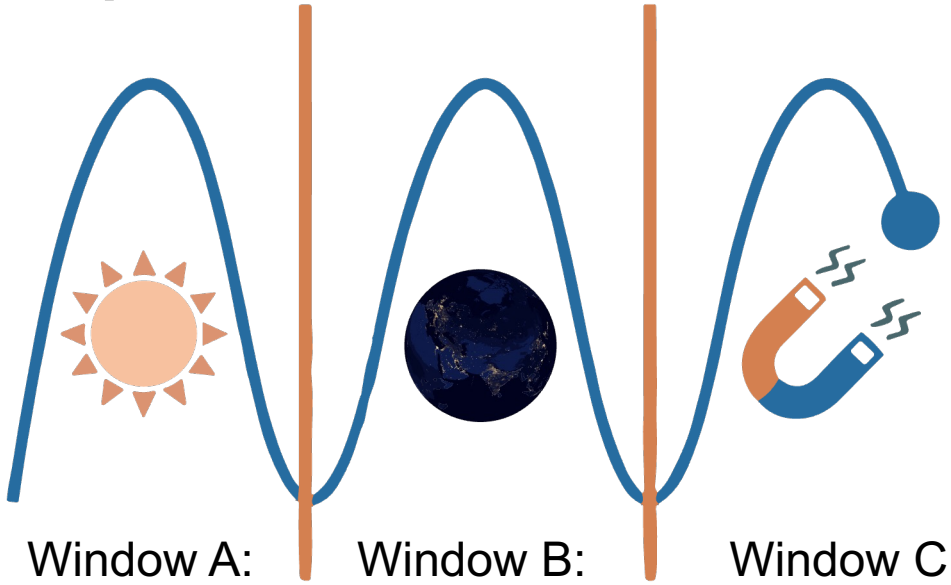
Impact Underestimation

Misaligned Defenses

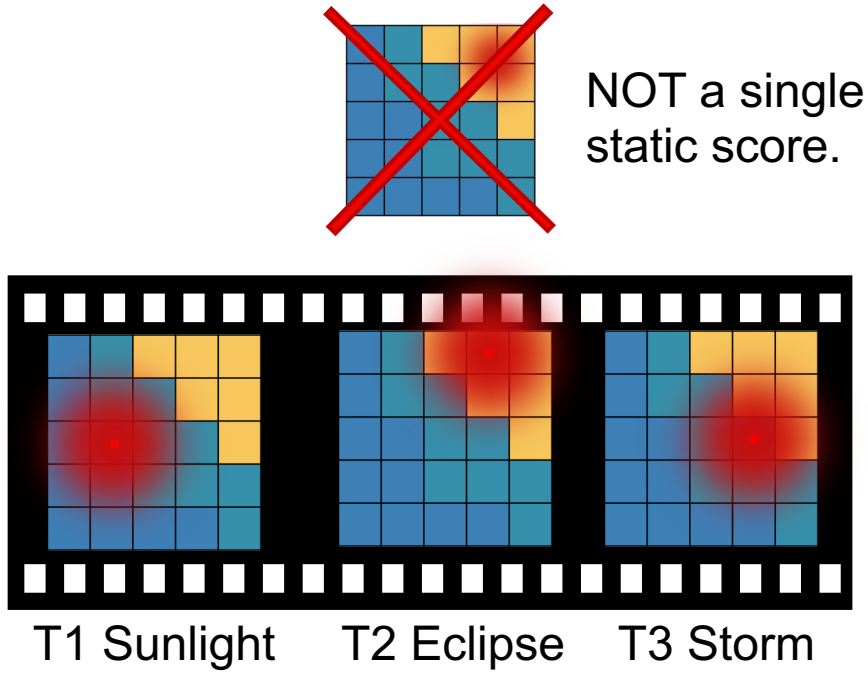
[1]Ear, Ekzhin, Brandon Bailey, and Shouhuai Xu. "Towards principled risk scores for space cyber risk management."

Solution: Temporal Risk Assessment

Input: Discretization Process



Output: Dynamic Risk Estimates



Step1: Divides continuous missions into meaningful time windows.

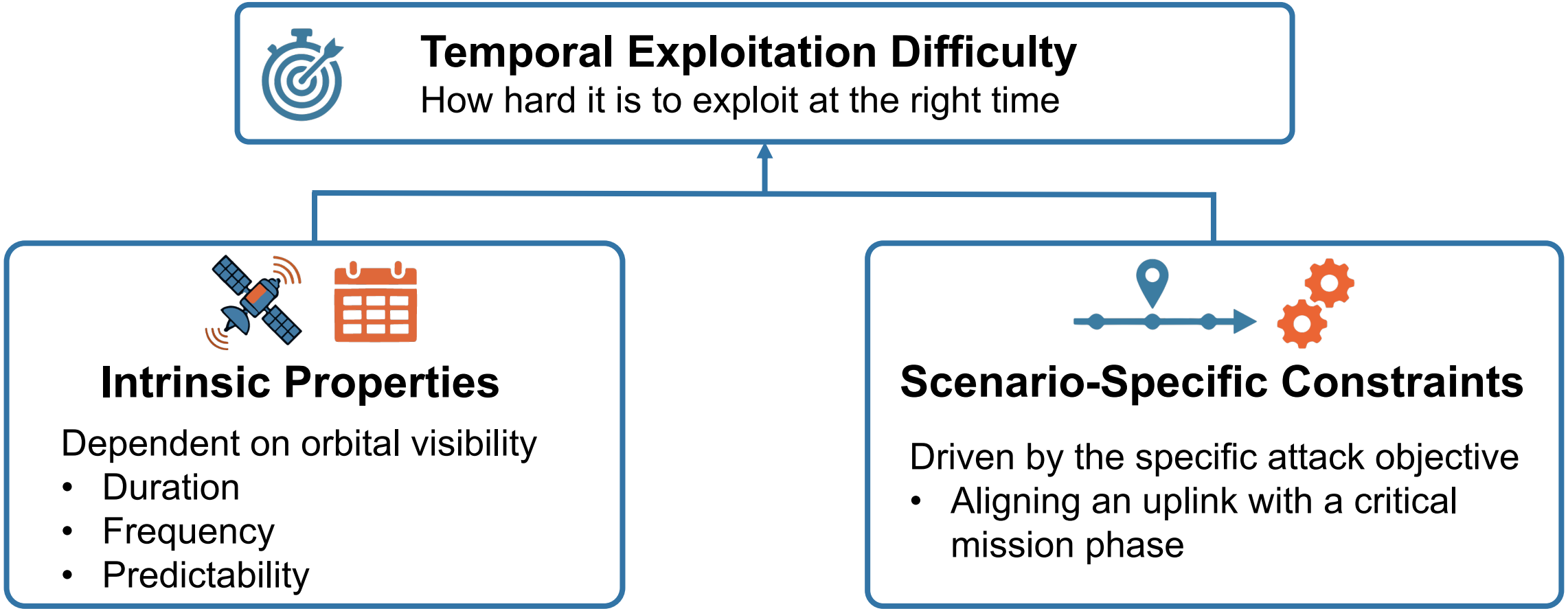
Step2: Generates a series of time-indexed matrices reflecting changing vulnerabilities.

Key Idea: Treat timing as a primary concern in threat assessment.

Solution: Temporal Adversary Capabilities

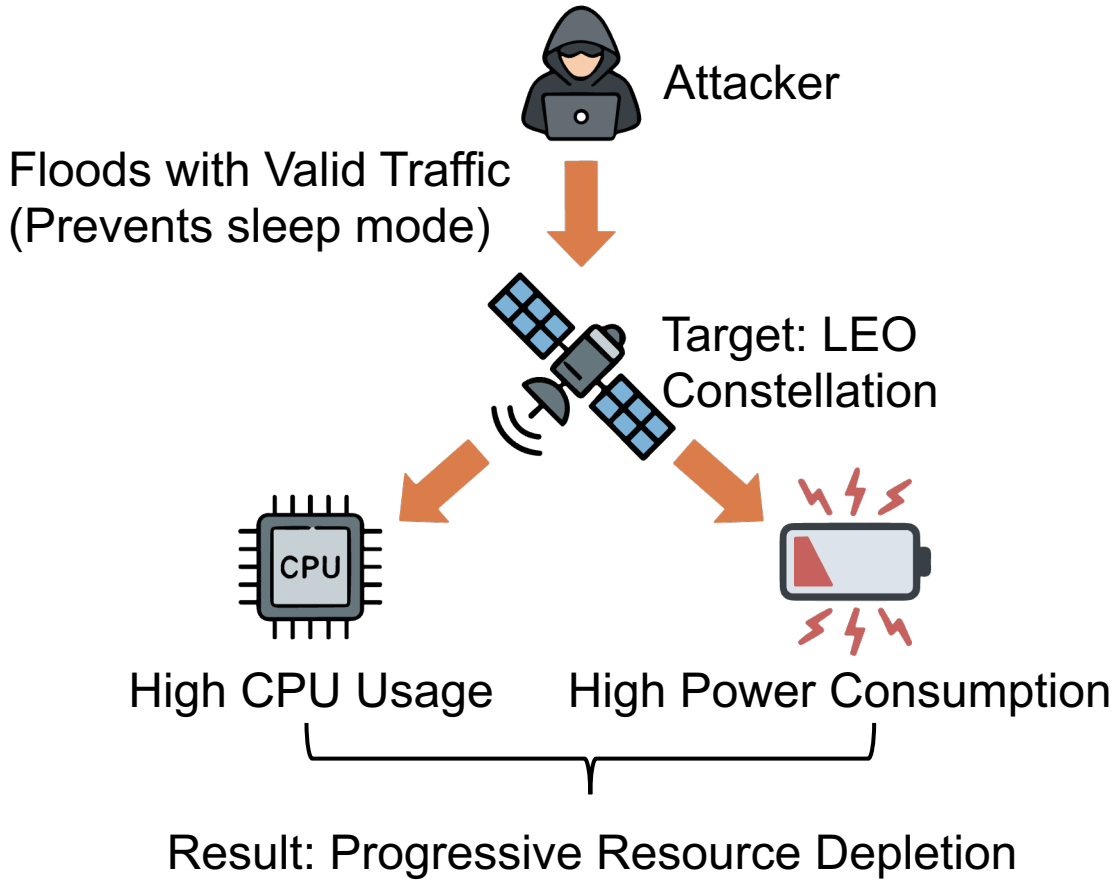
Script kiddies	Hackers for hire	Small hacker teams	Insider threats	Large well-organized teams	Highly capable state actors	Most capable state actors	
✓	✓	✓	✓	✓	✓	✓	**Actuation** Causing effects within a given access window.
–	✓	✓	✓	✓	✓	✓	**Forecasting** Predicting future access windows and environment states.
–	–	✓	✓	✓	✓	✓	**Sensing** Near-real-time awareness of the system's state.
–	–	–	✓	✓	✓	✓	**Synchronization** Aligning actions with a chosen time window.
–	–	–	–	✓	✓	✓	**Hiding** Timing actions to blend in with natural noise or space weather.

Solution: Temporal Exploitation Difficulty



Case Study: The STARMELT Attack

Attack Anatomy



Static Framework Risk Score

SPARTA Mapping

EX-0013.01: Valid Commands

Issues legitimate actions to progressively deplete resources (e.g., battery energy).

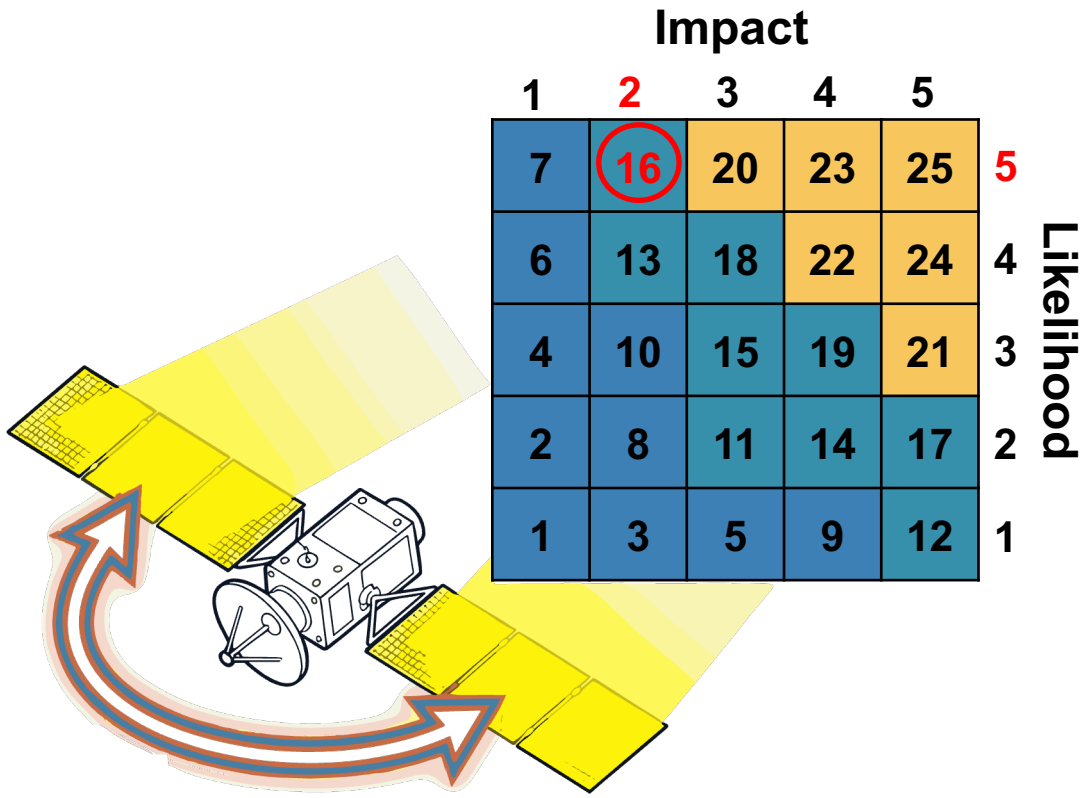
⚠ Static NRS Score (High-Criticality)

25 (HIGH)

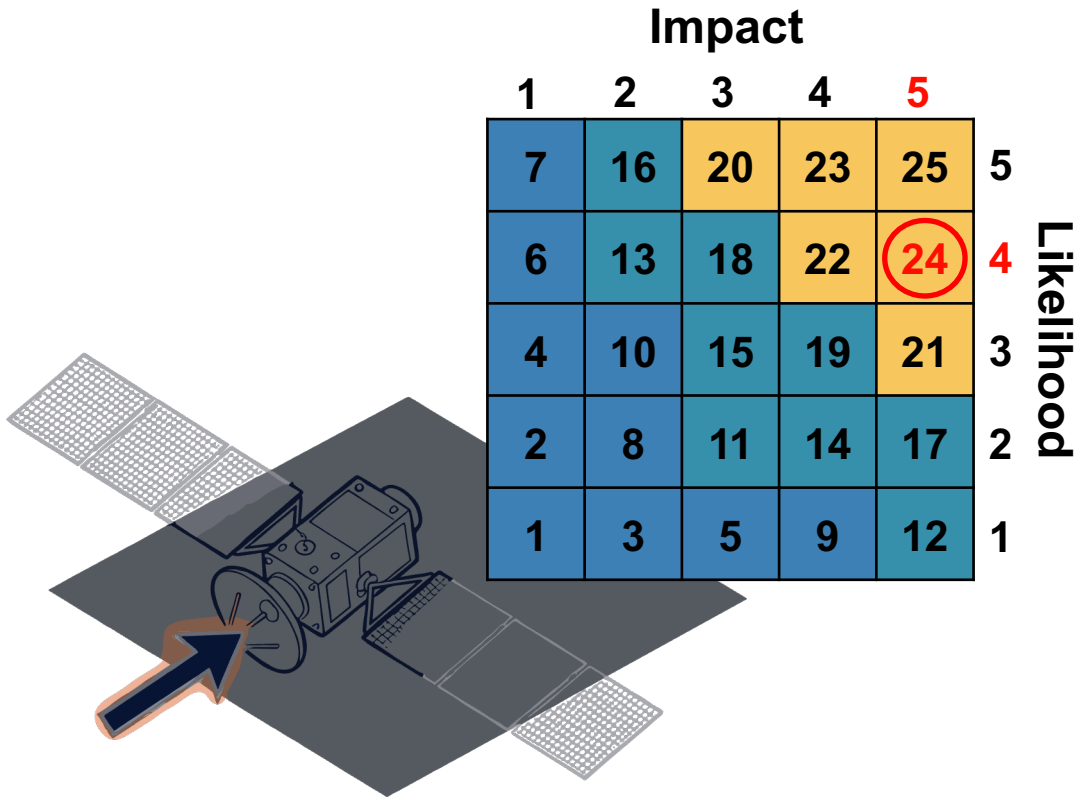
Likelihood:5/5 **Impact:5/5**

[2]Zhang, Yaoying, et al. "Energy drain attack in satellite internet constellations."

Case Study: Sunlight vs. Eclipse Risk



Risk: Medium



Risk: High

Takeaways

- Don’t treat space risk as static.
- Timing is a capability for attackers.
- Timing constraints directly affect likelihood of risks.
- Time-aware scheduling can be a mitigation.

Q & A

Feedback: sliu38@gmu.edu