



Small Step or Giant Leap? Cyber and Policy Progress Towards Satellite Security

William J. Malik

VP Infrastructure Strategies



Satellite History

Sputnik 1 – Oct 4, 1957



Echo 1 – Aug 12, 1960

N.A.S.A.



Telstar 1 – July 10, 1962



Skylab – May 14, 1973

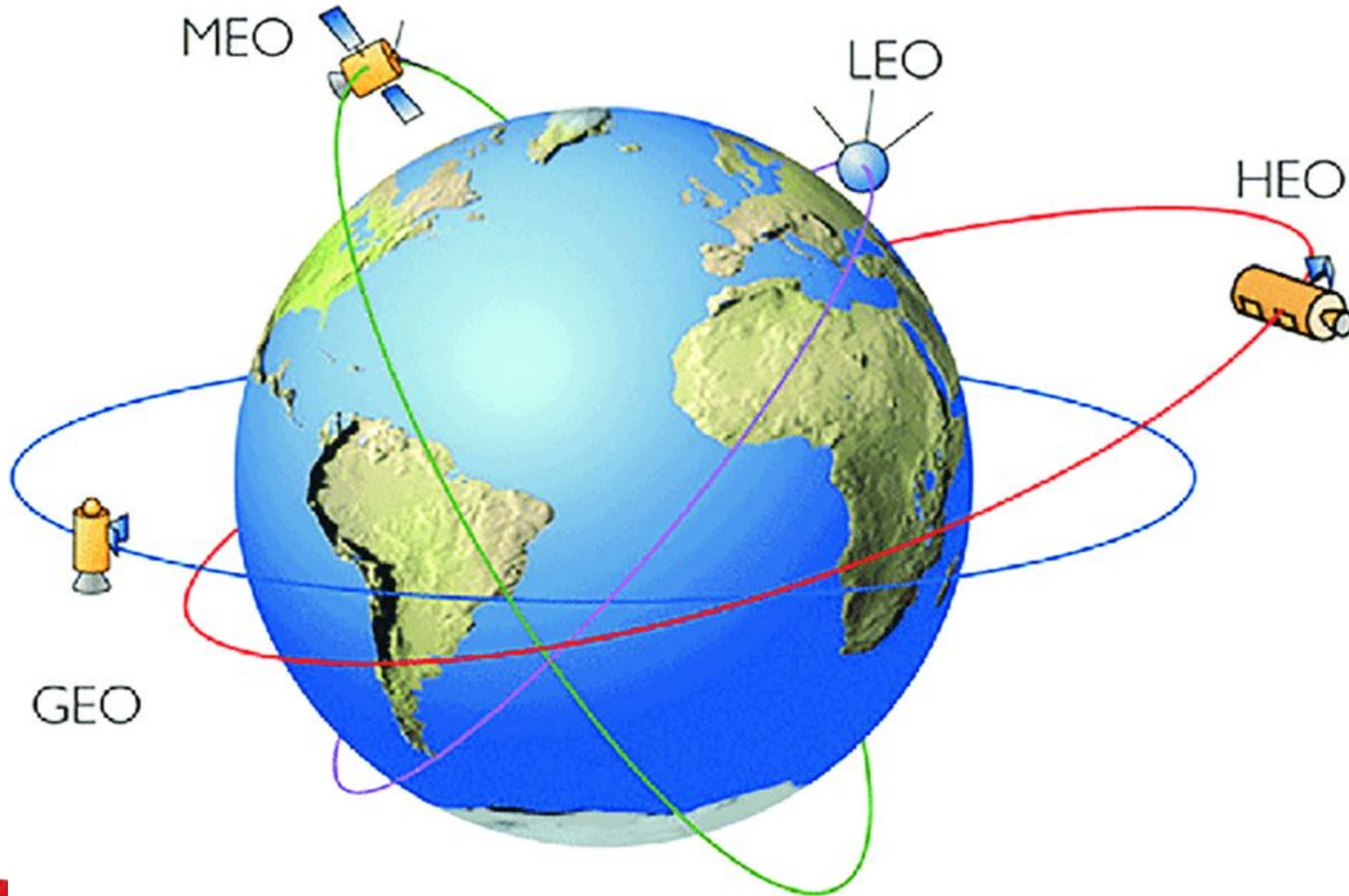


Voyager 1 – Sept 1977

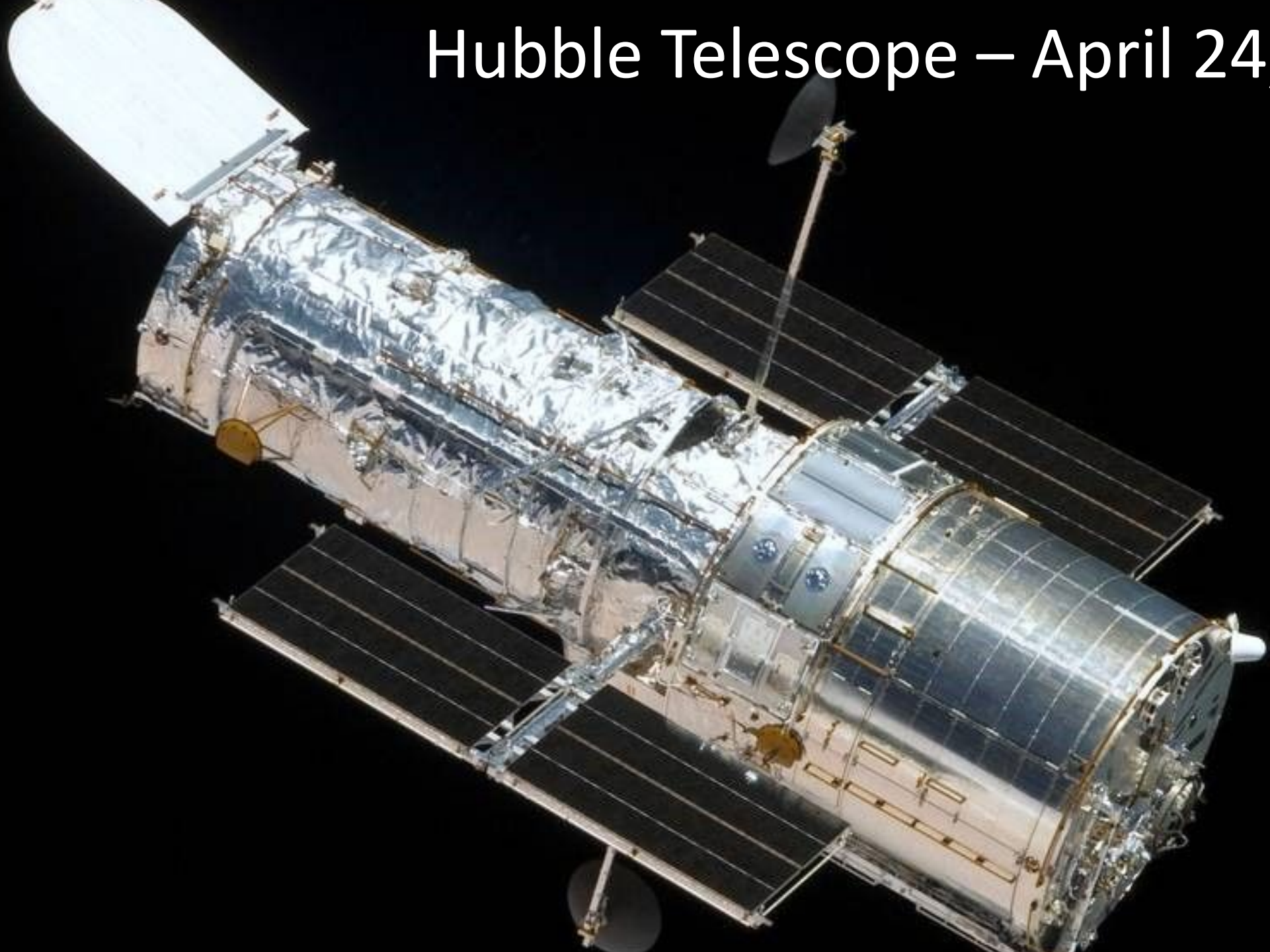


Illustration

Types of Satellite Orbits



Hubble Telescope – April 24, 1990



Hubble Support Systems



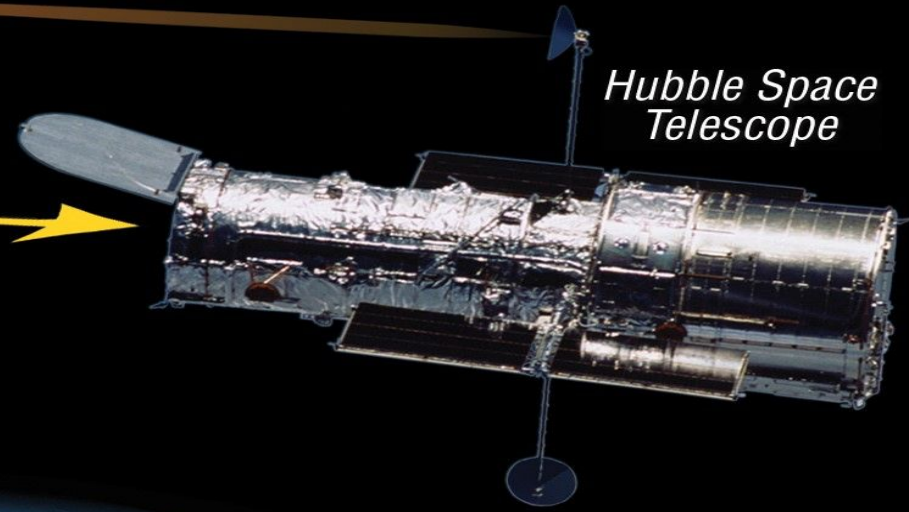
Tracking and Data Relay Satellite



DATA



LIGHT



Hubble Space Telescope

DATA



Ground Station
White Sands, NM



DATA



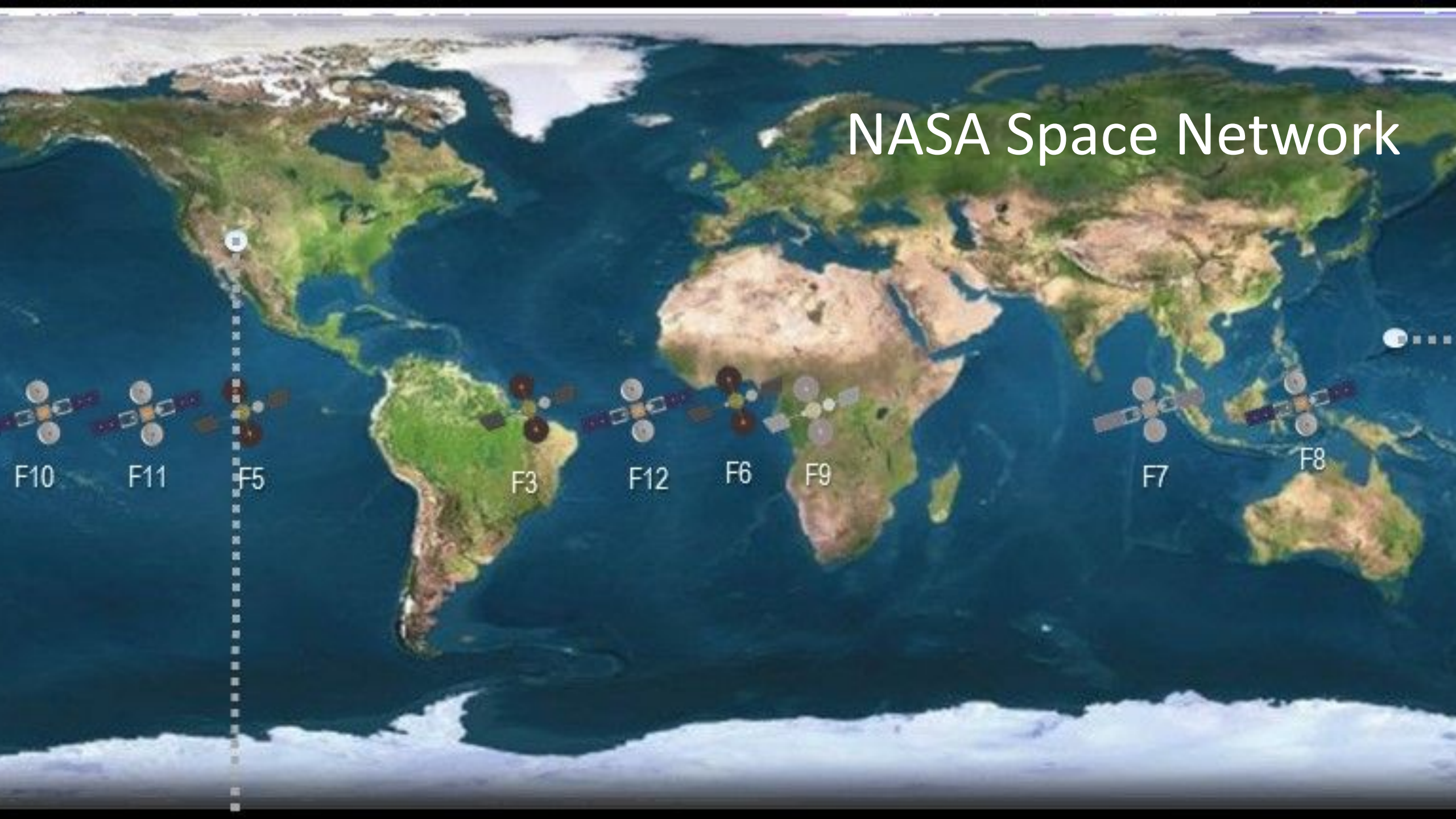
Space Telescope Science Institute
Baltimore, MD



Goddard Space Flight Center
Greenbelt, MD



NASA Space Network



F10

F11

F5

F3

F12

F6

F9

F7

F8

TDRS

Multiple Access Antenna

- 32 receive antenna elements
- 15 transmit antenna elements
- S-band communications
- LHC polarization

AFT Omni Antenna

- S-band (TT&C)

Single Access Antenna

Solar Panels

Forward Omni Antenna

- S-band (TT&C)

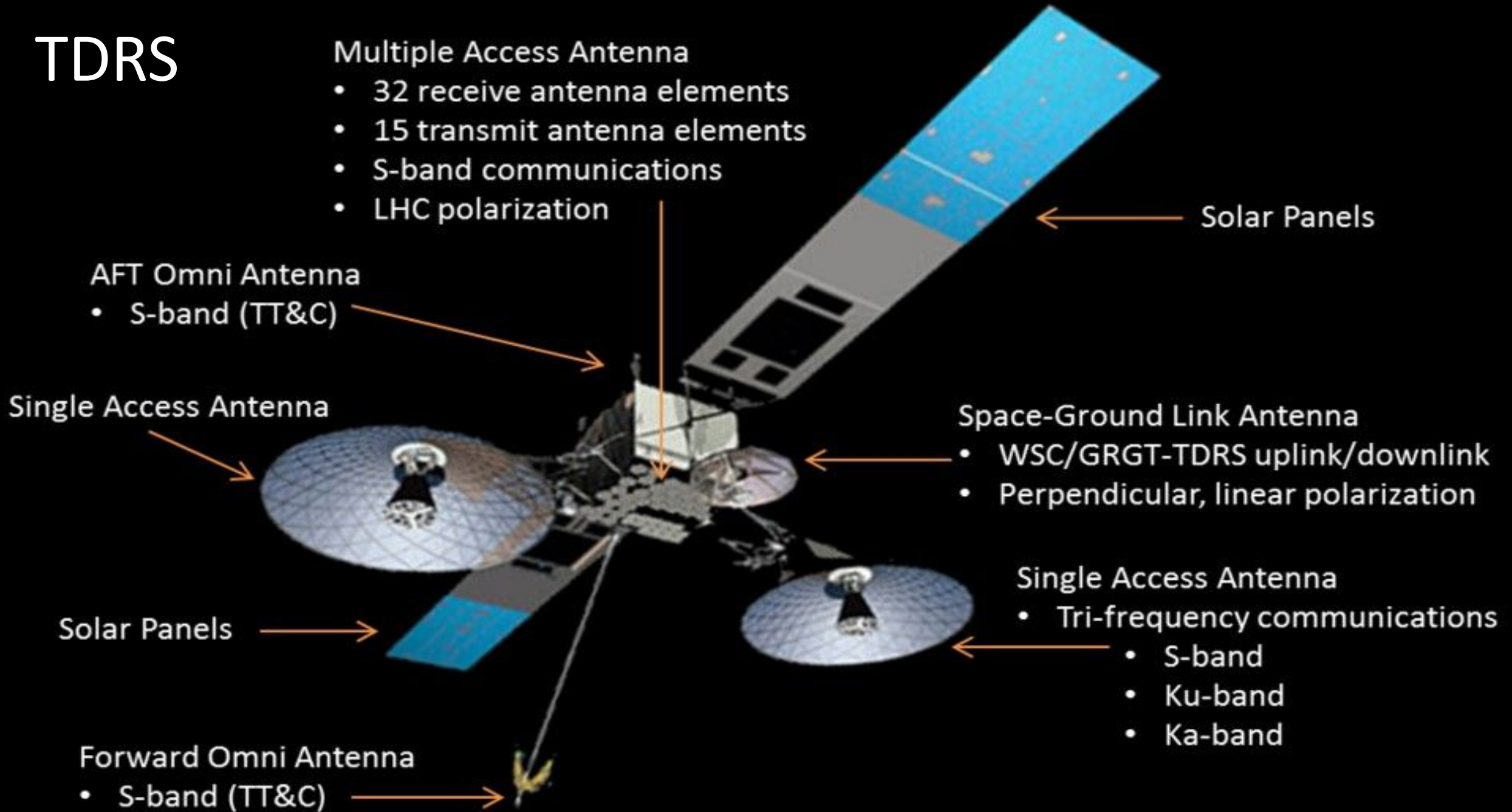
Solar Panels

Space-Ground Link Antenna

- WSC/GRGT-TDRS uplink/downlink
- Perpendicular, linear polarization

Single Access Antenna

- Tri-frequency communications
- S-band
- Ku-band
- Ka-band



Satellite Security Today

Primary Satellite Uses

- Communications

 - Earth to Satellite

 - Satellite to Satellite

 - Satellite to Earth

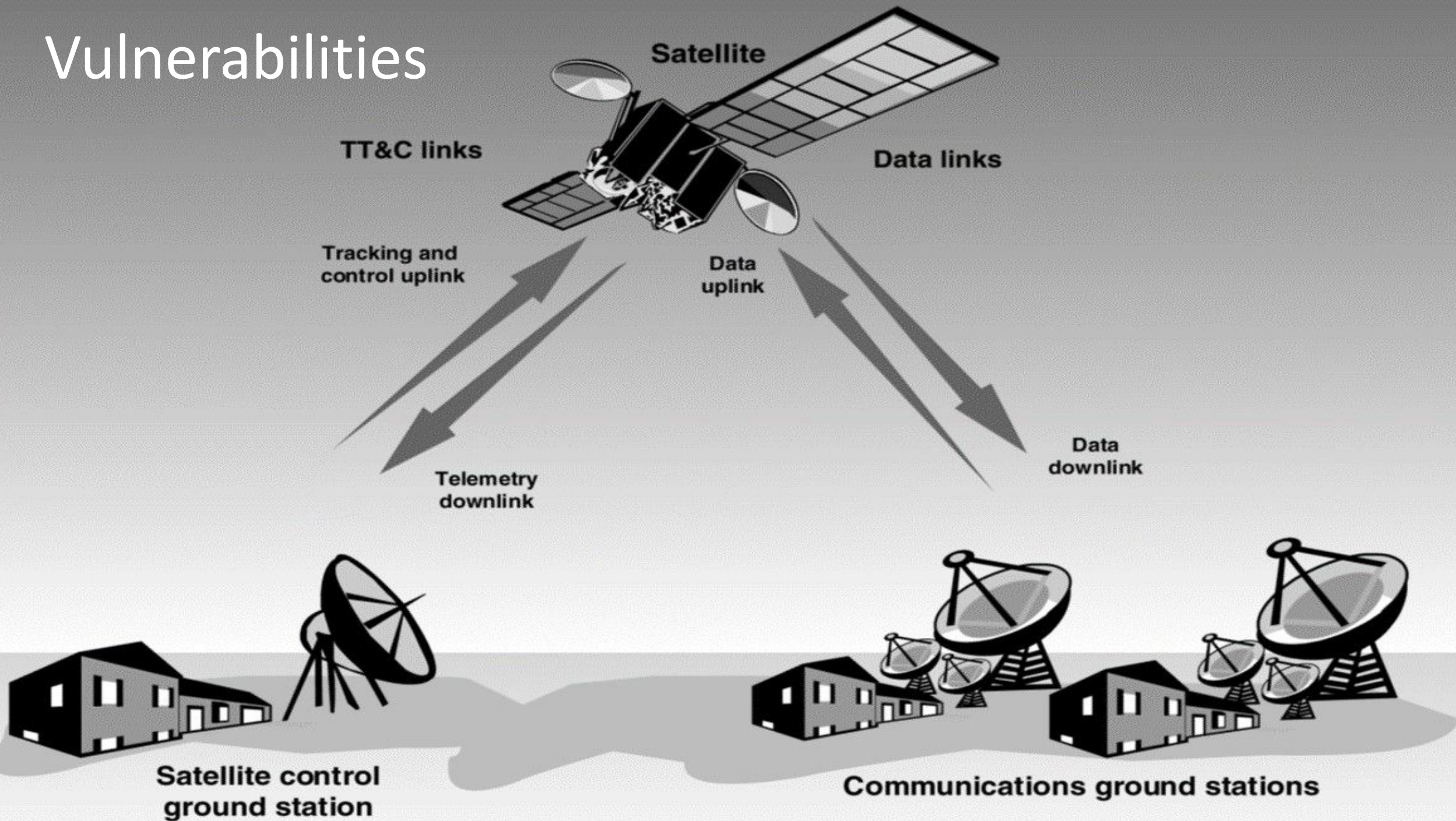
- Terrestrial Information

 - Beacons (GPS, time signals)

 - Observations (Weather, crops, disasters, spying)

- Space Exploration

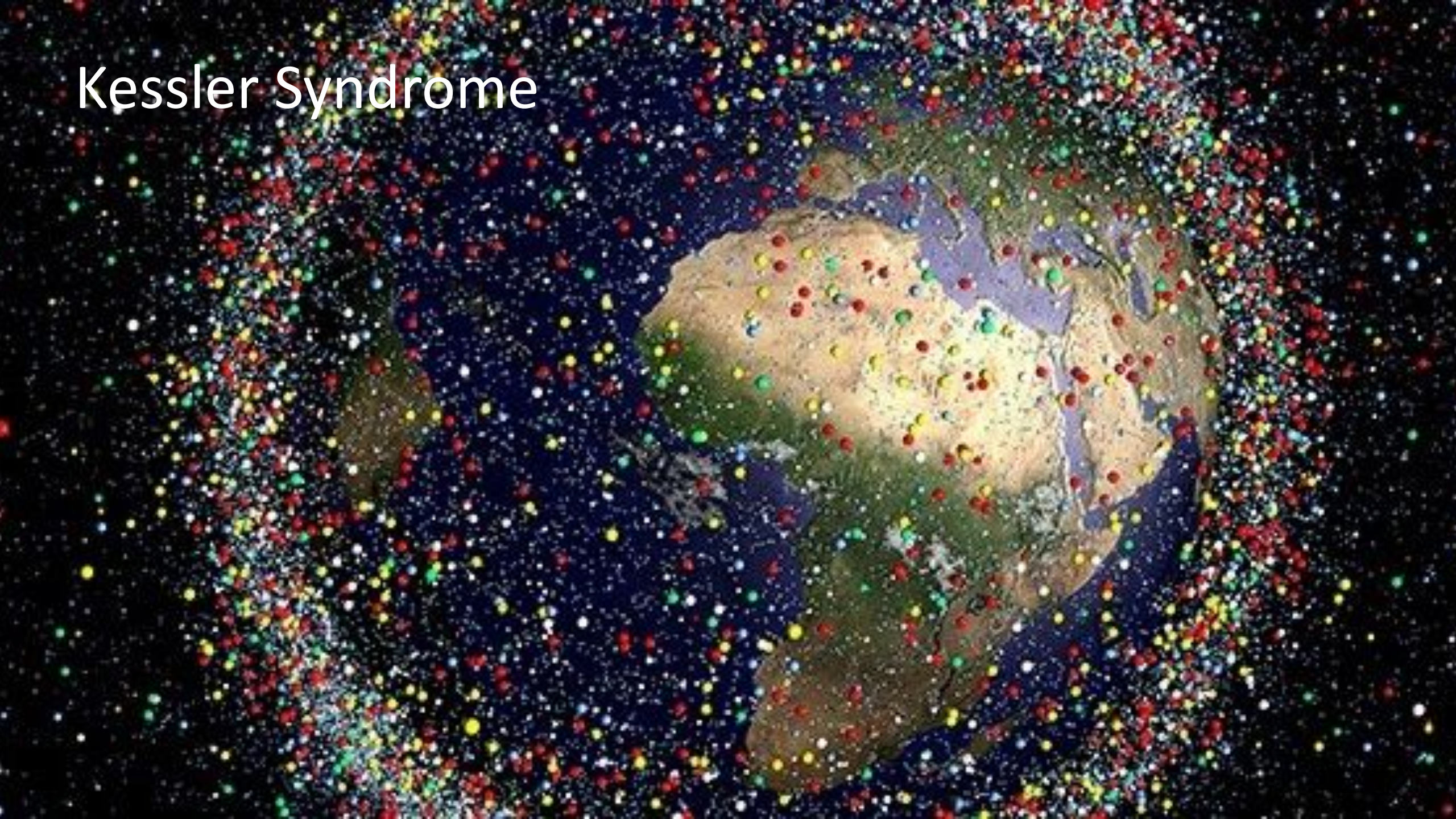
Vulnerabilities



Unintentional Threats to Satellites

| Type of threat | Vulnerable satellite system components |
|---|--|
| Ground-based: | |
| Natural occurrences (including earthquakes and floods; adverse temperature environments) | Ground stations; TT&C and data links |
| Power outages | |
| Space-based: | |
| Space environment (solar, cosmic radiation; temperature variations) | Satellites; TT&C and data links |
| Space objects (including debris) | |
| Interference-oriented: | |
| Solar activity; atmospheric and solar disturbances | Satellites; TT&C and data links |
| Unintentional human interference (caused by terrestrial and space-based wireless systems) | |

Kessler Syndrome



Intentional Threats to Satellites

| Type of threat | Vulnerable satellite system components |
|--|--|
| Ground-based: | |
| Physical destruction | Ground stations; communications networks |
| Sabotage | All systems |
| Space-based (anti-satellite): | |
| Interceptors (space mines and space-to-space missiles) | Satellites |
| Directed-energy weapons (laser energy, electromagnetic pulse) | Satellites; TT&C and data links |
| Interference and content-oriented: | |
| Cyber attacks (malicious software, denial of service, spoofing, data interception, and so forth) | All systems and communications networks |
| Jamming | All systems |

Types of Satellite Hacks

- Jamming
 - Flooding a communications channel to block information transfer (DDoS)
- Eavesdropping
 - Intercepting a communication channel
- Hijack
 - Replacing content (not taking over the satellite itself)
- Control
 - Taking over the TT&C ground station, bus, or payload
- Contamination
 - PCspooF – disable TTE (time sensitive messaging)

Control Takeover Hacks

- February 1999, SkyNet, UK. Hackers controlled one of four British military satellites, moving its position and demanding ransom
- 2000, US Abrams and British Challenger tank trials in Greece meaconed by French intelligence agencies – GPS takeover

Analyzed Satellite Identified Vulnerabilities

| Satellite | Orbit | Form | Launch | OBC | TCs | Strongest Attack Path |
|---------------|-------|-------------|--------|-------|-----------|---|
| ESTCube-1 | 665km | 1U CubeSat | 2013 | ARM | Cortex-M3 | Unprotected External Attack → Seize Control |
| OPS-SAT | 515km | 3U CubeSat | 2019 | AVR32 | AT32UC3 | Unprotected External Attack → Seize Control |
| Flying Laptop | 600km | 60x70x90 cm | 2017 | Leon3 | SPARC V8 | Encrypted Semi-Privileged Insider → TC Alteration |

Countermeasures

Threat-specific Detection and Response

- Anti-jamming
 - Spread-spectrum
- Hardening
 - EMP and radiation shielding
 - GPS Authentication
- Embedded security processor
 - Encryption
 - Digital signing
 - Identity management – authentication and authorization
- Detection and blocking

Systemic Detection and Response

- Deploy security orchestration
 - Real-time anomaly detection and response
- Apply ISO 7498-2
 - Authentication
 - Authorization
 - Encryption
 - Data Integrity
 - Non-repudiation
- Expand monitoring and logging
- Exploit secure chip architectures

Hybrid Satellite Network Cybersecurity Framework

Identify

- Asset Management Category
- Business Environment
- Governance
- Risk Assessment
- Risk Management
- Supply Chain Risk Management

Protect

- Identity Management, Authentication, and Access Control
- Awareness and Training
- Data Security
- Information Protection Processes and Procedures
- Maintenance
- Protective Technology

Detect

- Anomalies and Events



Black Hat Las Vegas

Houston, We Have a Problem: Analyzing the Security of Low Earth Orbit Satellites

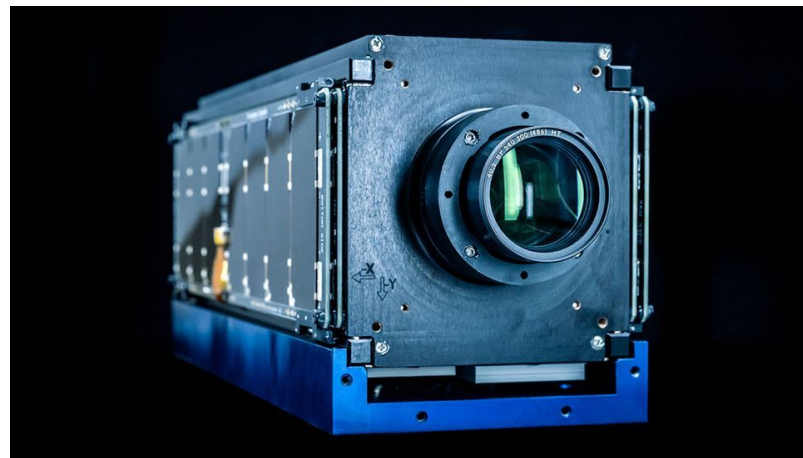
Johannes Willbold | Doctoral Student, Ruhr University Bochum

Date: Thursday, August 10 | 1:30pm-2:10pm (South Seas AB, Level 3)

Format: 40-Minute Briefings

Tracks:  Cyber-Physical Systems & IoT,  Hardware / Embedded

USAF Hack-a-Sat



Next Steps

Costs plummeting per Moore's law

- Both satellite costs and hacker RF attack kit

Attack surfaces widening

5G fringe coverage will require satellites

Industrial IoT firmware updates via satellites

Private sector regulation required

Satellite Network Hacking and Security Analysis, Adam Ali. Zare Hudaib, International Journal of Computer Science and Security (IJCSS), Volume (10) : Issue (1) : 2016

“Attack Vectors in Orbit: The Need for IoT and Satellite Security in the Age of 5G,”

<https://blog.trendmicro.com/trendlabs-security-intelligence/attack-vectors-in-orbit-need-for-satellite-security-in-5g-iot/>

GPS Flaw: Security Expert Says He Won't Fly April 6, Paul Wagensell, Tom's Guide, <https://www.tomsguide.com/us/gps-mini-v2k-rsa2019,news-29583.html>

Satellite Hacking: A Guide for the Perplexed, Jason Fritz, Culture Mandala: Bulletin of the Centre for East-West Cultural and Economic Studies, Vol. 10, No. 1, December 2012- May 2013, pp21-50.

Satellite Hijack 'Impossible', BBC News, Sci/Tech, Mar 2, 1999 <http://news.bbc.co.uk/2/hi/science/nature/288965.stm>

Critical Infrastructure Protection: Commercial Satellite Security Should be More Fully Addressed, GAO-02-781, Aug 30, 2002. <https://www.gao.gov/products/GAO-02-781>

Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN), NIST IR 8441, McCarthy, J. et al. Sept 2023. <https://doi.org/10.6028/NIST.IR.8441>

Space Odyssey: An Experimental Software Security Analysis of Satellites, IEEE Symposium on Security and Privacy, <https://www.youtube.com/watch?v=WPTwk9rML9c>

PCSPPOOF: Compromising the Safety of Time-Triggered Ethernet, Loveless, A. et al. IEEE Symposium on Security and Privacy, 2023.

<https://web.eecs.umich.edu/~barisk/public/pcspooof.pdf> talk at <https://www.youtube.com/watch?v=UtKJLrUzRQ0>

These 3 teams just hacked a US Air Force satellite in space ... and won big cash prizes, Brett Tingley, Space.com. Aug 2023.

<https://www.space.com/satellite-hacking-hack-a-sat-competition-winners>

Houston, We Have a Problem, Johannes Willbold, Black Hat Las Vegas, Aug 10 2023..

<https://www.blackhat.com/us-23/briefings/schedule/#houston-we-have-a-problem-analyzing-the-security-of-low-earth-orbit-satellites-32468>



Small Step or Giant Leap? Cyber and Policy Progress Towards Satellite Security

William J. Malik

VP Infrastructure Strategies