RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: MBS-W03

Attack Vectors in Orbit: The Need for IoT and Satellite Security

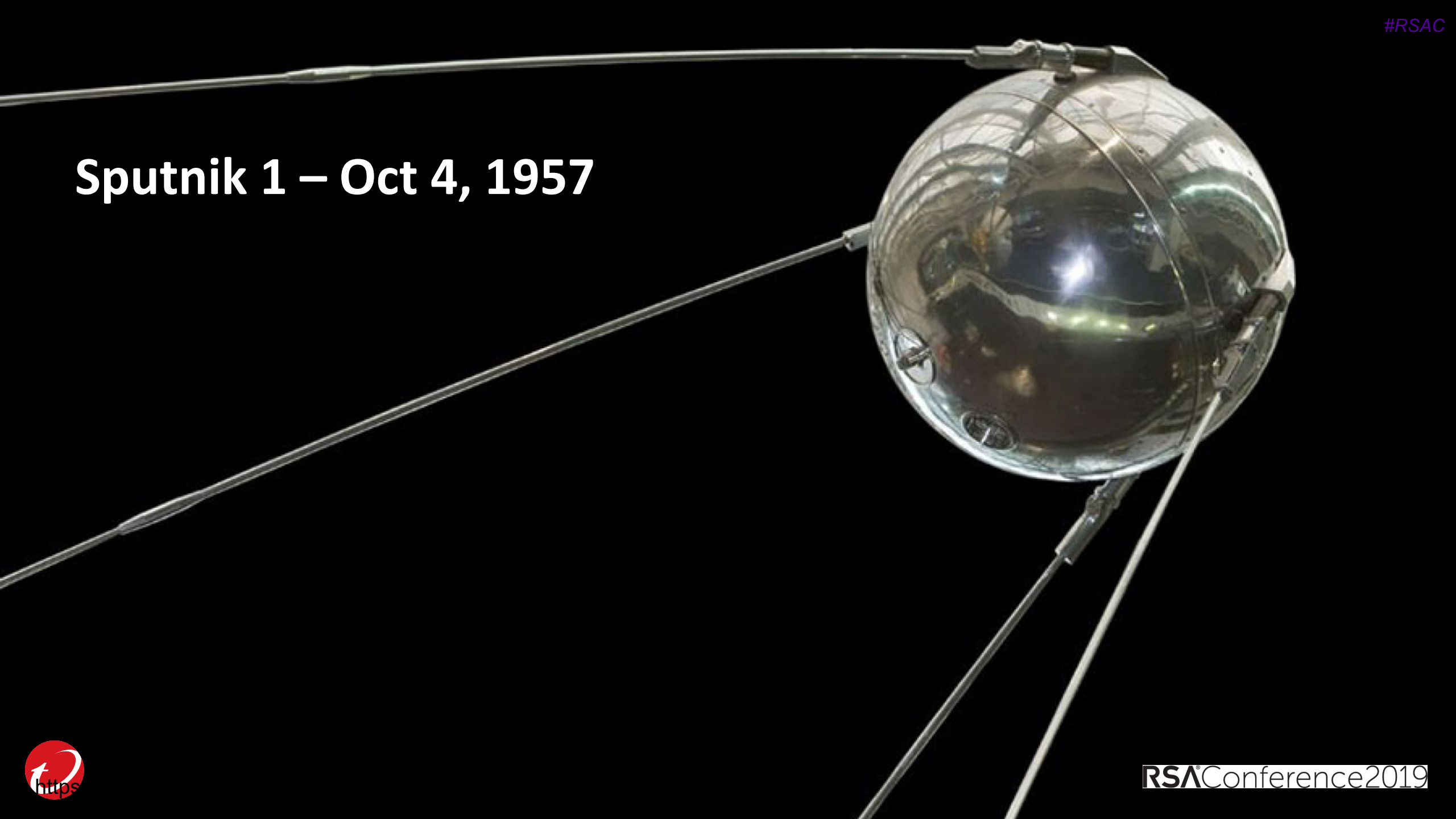
William J Malik, CISA

VP, Infrastructure Strategies
Trend Micro Inc.
@WilliamMalikTM

RSAConference2019

Satellites

Sputnik 1 – Oct 4, 1957



Echo 1 – Aug 12, 1960

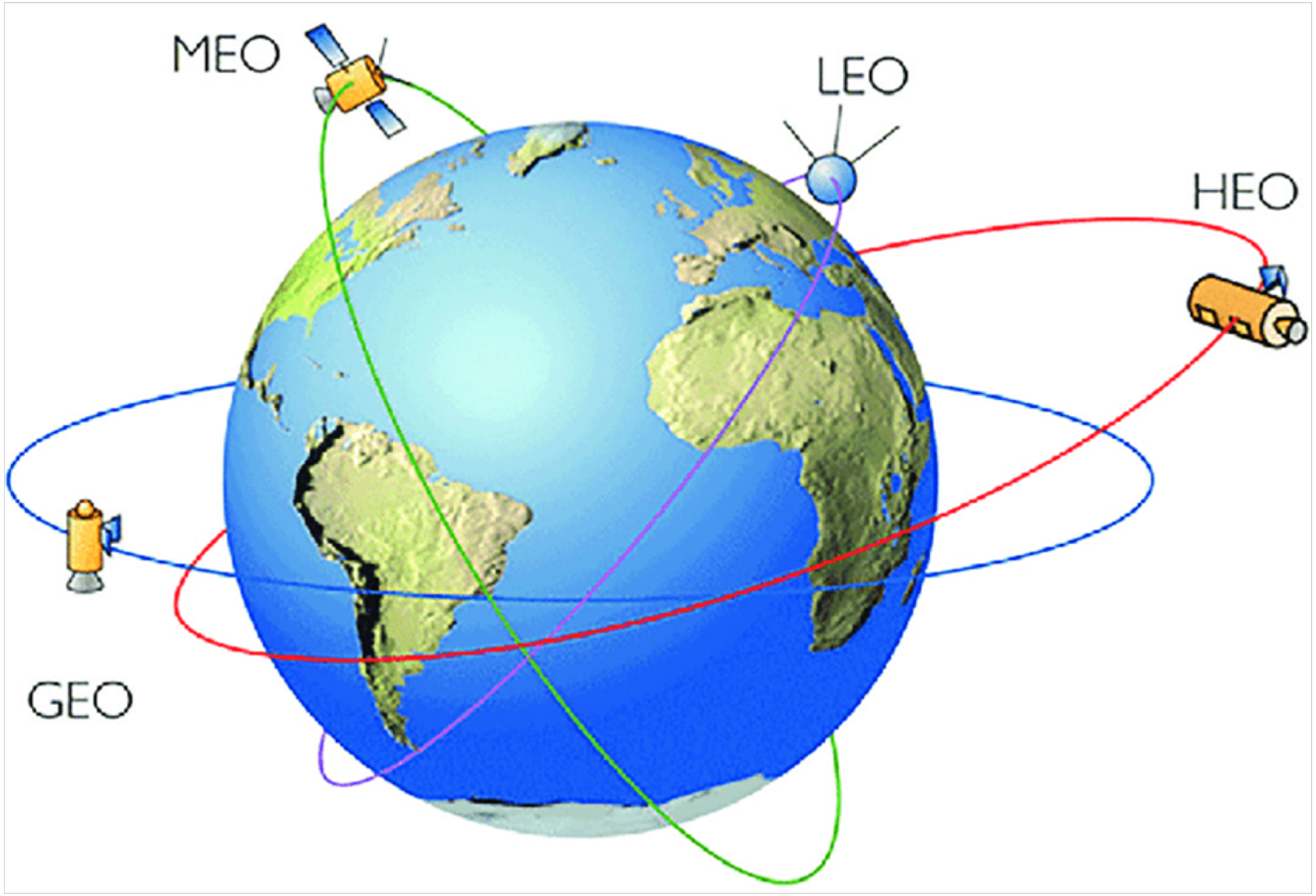
Telstar 1 – July 10, 1962

Skylab – May 14, 1973

Voyager 1 – Sept 1977

Illustration

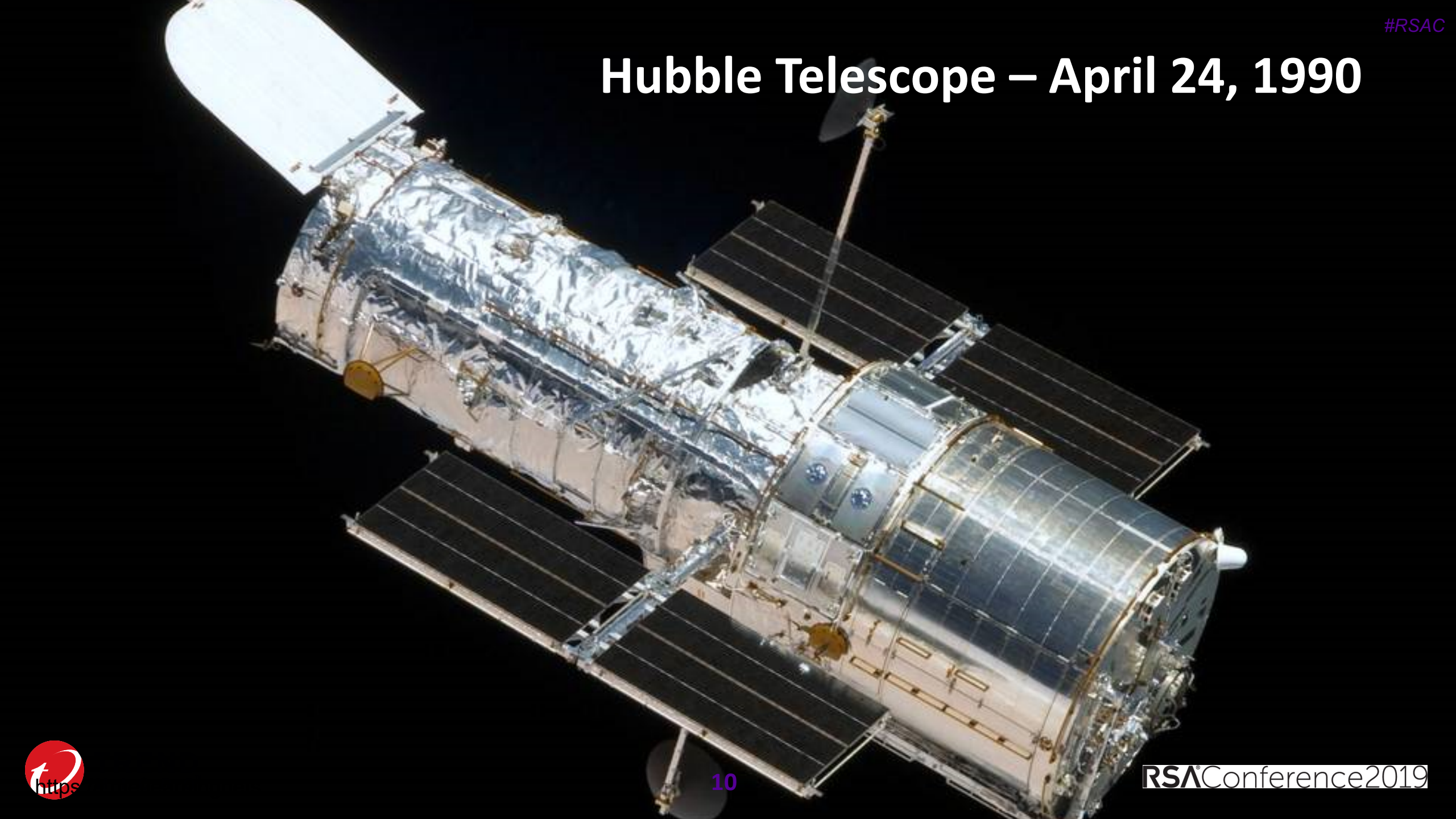
Types of Satellite Orbits



RSAConference2019

Deep Dive on Hubble

Hubble Telescope – April 24, 1990

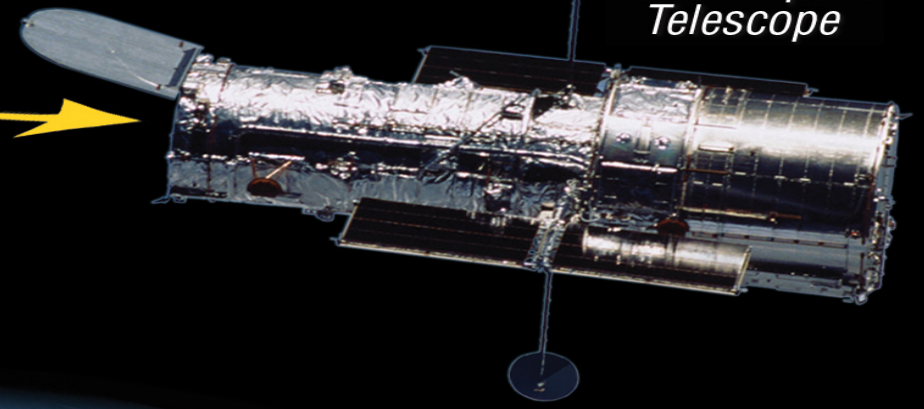


Hubble Support Systems

Tracking and Data Relay Satellite

DATA

LIGHT



Hubble Space Telescope

DATA

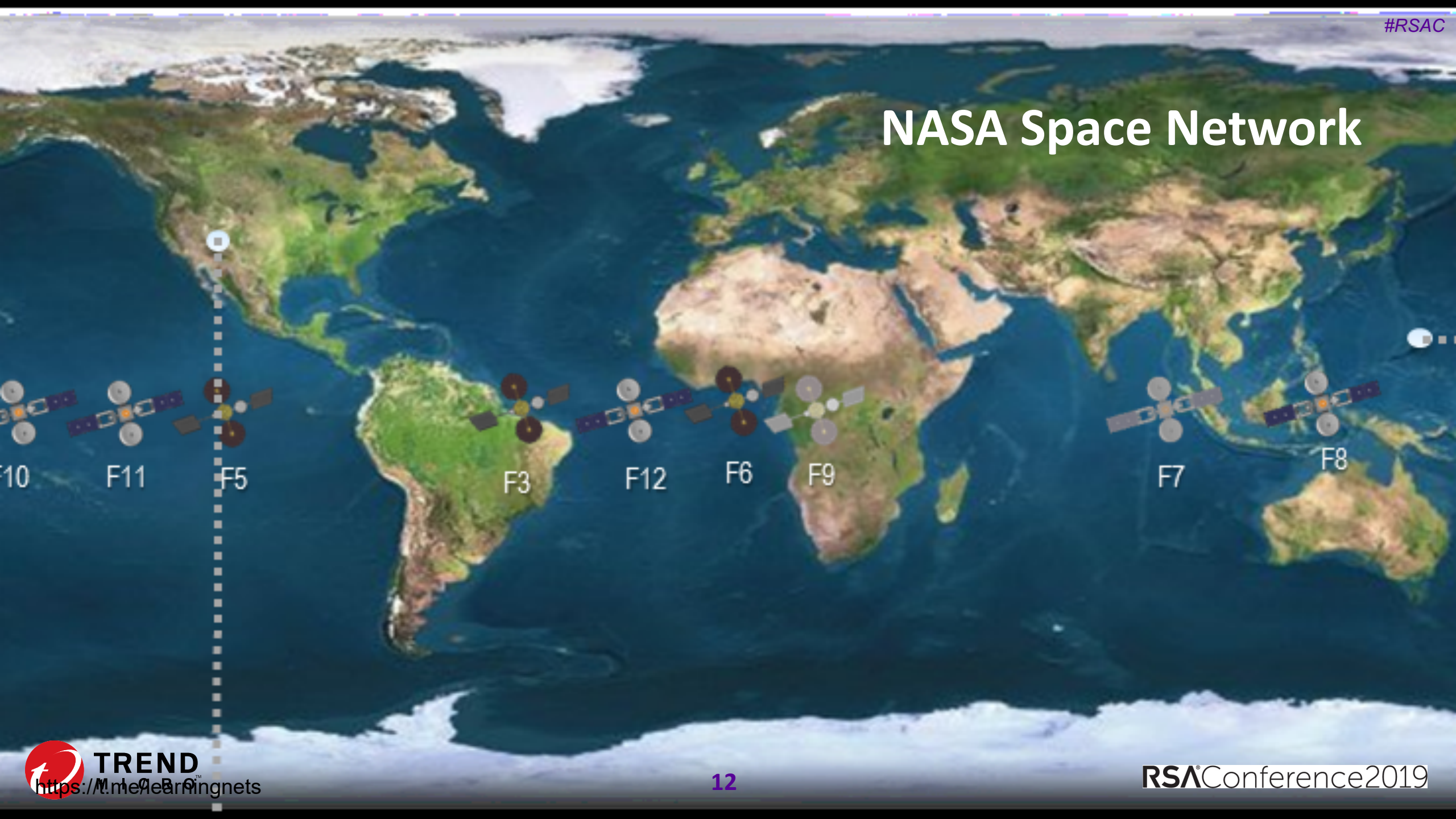
Space Telescope Science Institute
Baltimore, MD

DATA

Goddard Space Flight Center
Greenbelt, MD

Ground Station
White Sands, NM

NASA Space Network



TDRS

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

Solar Panels

AFT Omni Antenna
- S-band (TT&C)

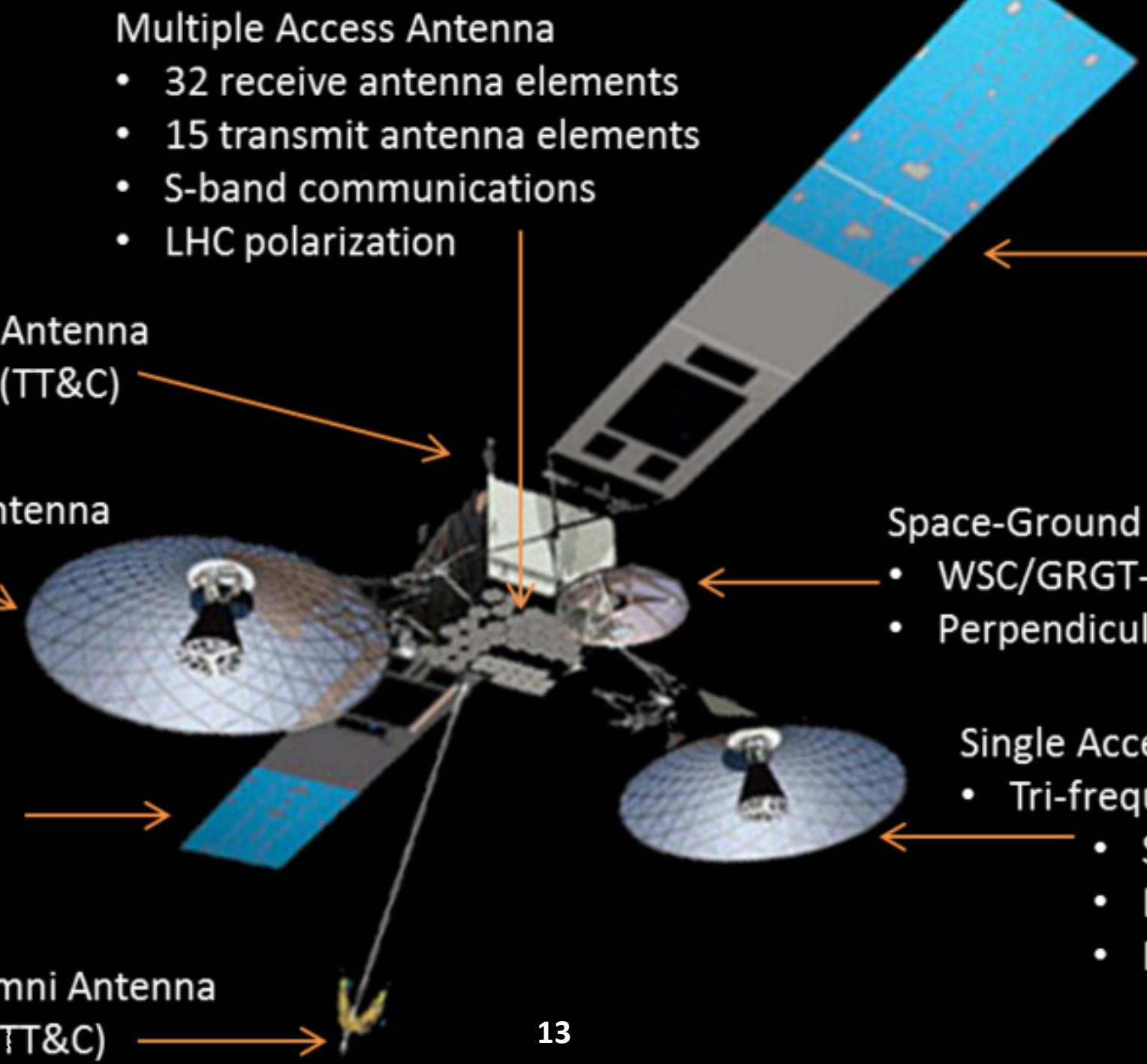
Single Access Antenna

Space-Ground Link Antenna
- WSC/GRGT-TDRS uplink/downlink
- Perpendicular, linear polarization

Single Access Antenna
- Tri-frequency communications
  - S-band
  - Ku-band
  - Ka-band

Solar Panels

Forward Omni Antenna
- S-band (TT&C)



RSAConference2019

Satellite Applications

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

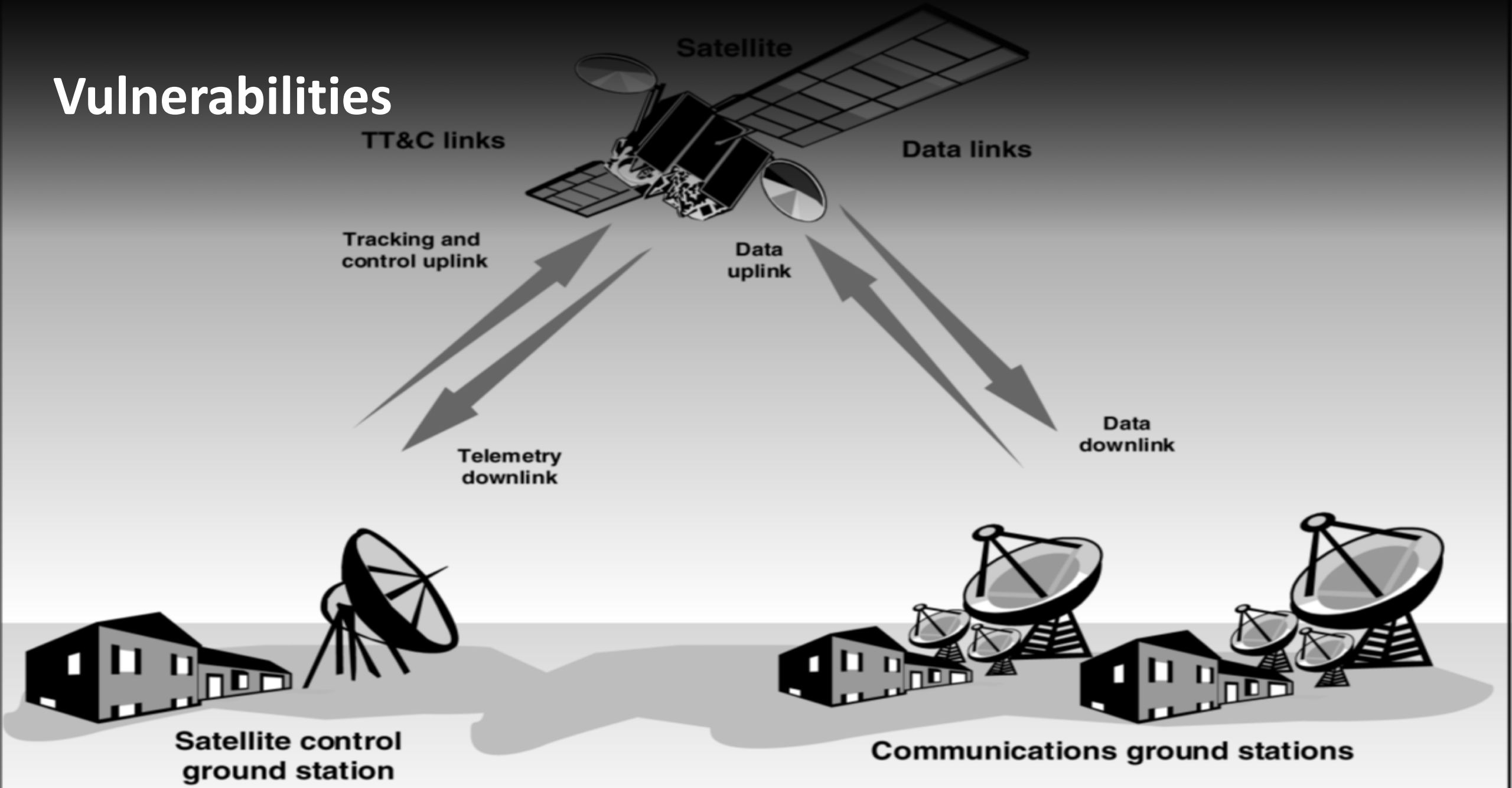
Satellite Role in 5G and IoT

- 5G Backhaul
  - High data capacity
  - Remote coverage areas
  - Latency an issue
- Industrial IoT
  - SIM/firmware updates
  - N-tier backhaul
  - Latency an issue

RSAConference2019

Threats to Satellites

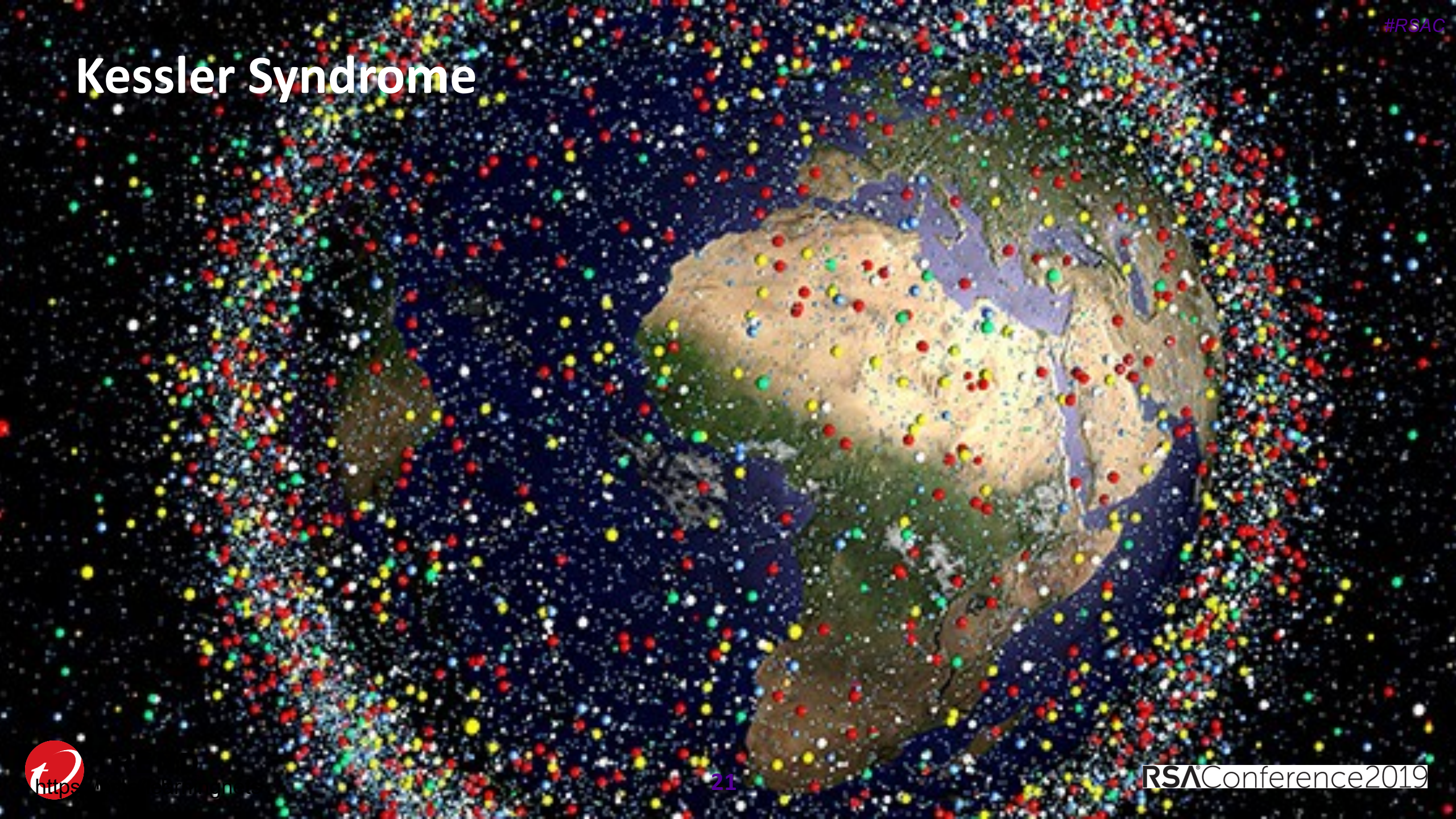
Vulnerabilities



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)	

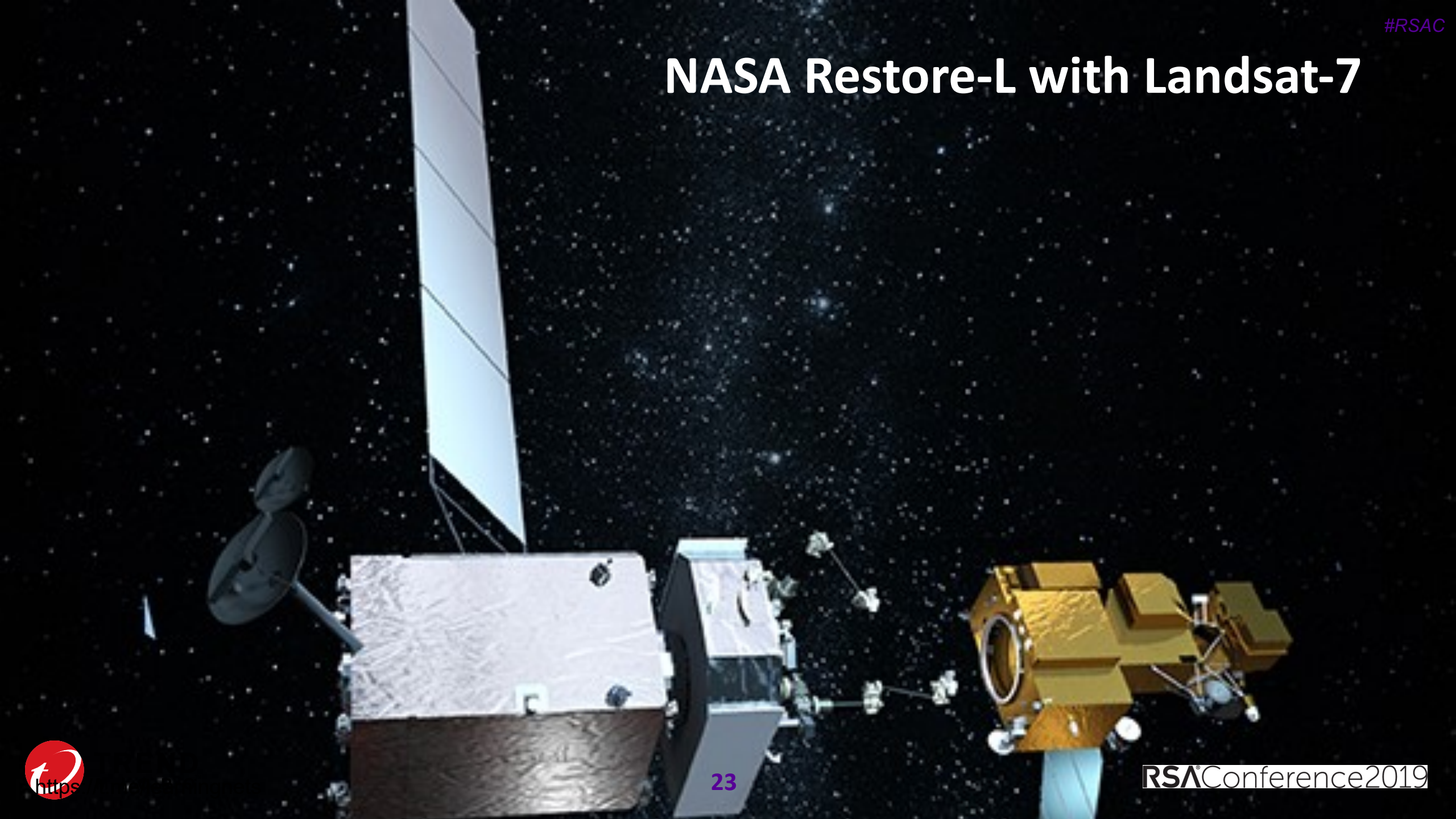
Kessler Syndrome



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

NASA Restore-L with Landsat-7



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

Intrusions into NASA Systems

1997, Goddard Space Flight Ctr, data exfil
1998, US-German ROSAT blinded by unplanned turn towards the Sun (RU)
2002, Huntsville, engine design (CN)
2003 – 2006, data exfil propulsion systems
2004, Ames Research supercomputer shut down to halt intrusion
2005, Kennedy VAB. Johnson Space Ctr, data exfil (TW)
2006, NASA HQ, phishing, data exfil satellite design
2006. NASA bans Word attachments
2007, Goddard, EOS network compromised (CN)
2007, Landsat-7 12 minute interference
2008, Landsat-7 another 12+ minute takeover
2008, Terra EOS AM-1, 2+ minute takeover
2008, Terra EOS AM-1, 9+ minute TT&C takeover
2008, Johnson Space Ctr, Trojan disrupted ISS and infected obsolescent on-board computers
2010, seven NASA systems compromised, Chinese national detained
2010, China Telcom routed 15% of Internet traffic through Chinese servers, including .gov and .mil sites
2011, NASA and ESA identity and authentication data hacked and published

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

RSAConference2019

Remediation

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

Long Term Solutions

- View satellite as just another communication channel
- Use comprehensive information security, privacy, and identity management across appropriate layers
- Imbed security and privacy by design (both IT and OT)

Conclusions and 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

Apply What You Have Learned Today

- Next week you should:
  - Extend your information security architecture to include OT – and possibly satellites. Upgrade to 13-bit “week” counter by April 6
- In the first three months following this presentation you should:
  - Assess the potential value to satellite infrastructure for your Industrial IoT deployments
- Within six months you should:
  - Train your architectural, infrastructure, and procurement teams to include enhanced information security criteria in design, deployment, and acquisition

References

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

“Emerging 5G Technology Could Compromise SIM-Card Dependent IoT Devices on a Massive Scale.” https://blog.trendmicro.com/trendlabs-security-intelligence/emerging-5g-technology-could-compromise-sim-card-dependent-iot-devices/

“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/

Radar Course 3 - Electromagnetic Spectrum, European Space Agency, from: https://earth.esa.int/web/guest/missions/esa-operational-eo-missions/ers/instruments/sar/applications/radar-courses/content-3/-/asset_publisher/mQ9R7ZVkKg5P/content/radar-course-3-electromagnetic-spectrum

“Introduction to the Electromagnetic Spectrum”, NASA Science, https://science.nasa.gov/ems/01_intro

Toll Fraud, International Revenue Share Fraud and More: How Criminals Monetize Hacked Cellphones and IoT Devices for Telecom Fraud, Craig Gibson, Europol, 2018.

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

RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID:

Attack Vectors in Orbit: The Need for IoT and Satellite Security

William J Malik, CISA

VP, Infrastructure Strategies
Trend Micro Inc.
@WilliamMalikTM