THE AEROSPACE CORPORATION

Space Enterprise Trends, Risks, and Securing the Future

Lori Gordon

November 2021

Approved for public release. OTR 2022-00078.

Abstract

Billions of people around the world rely on operations conducted across the space enterprise. Space systems support critical functions including navigation, communications, agriculture, financial exchange, and emergency services. Current and emerging markets for space services range from GPS and broadband connectivity to environmental monitoring and on-orbit manufacturing.

The volume of data travelling across information systems in satellite, ground, and user segments continues to escalate due to a range of factors and trends, including the commercialization of space with the transportation of cargo, experiments, and payload; human space flight; resupply to the International Space Station; Space as a Service (SaaS) and Ground Station as a Service (GSaaS); and the push to the moon and Mars.

Adversaries seek to exploit vulnerabilities and threats across this increased threat plane through unauthorized access, malware, denial of service, supply chain, and other opportunities. Guidance, best practices, and a defense-in-depth approach to protecting and securing data and information is a key priority and continues to evolve in the government and commercial sector to outpace the threat.

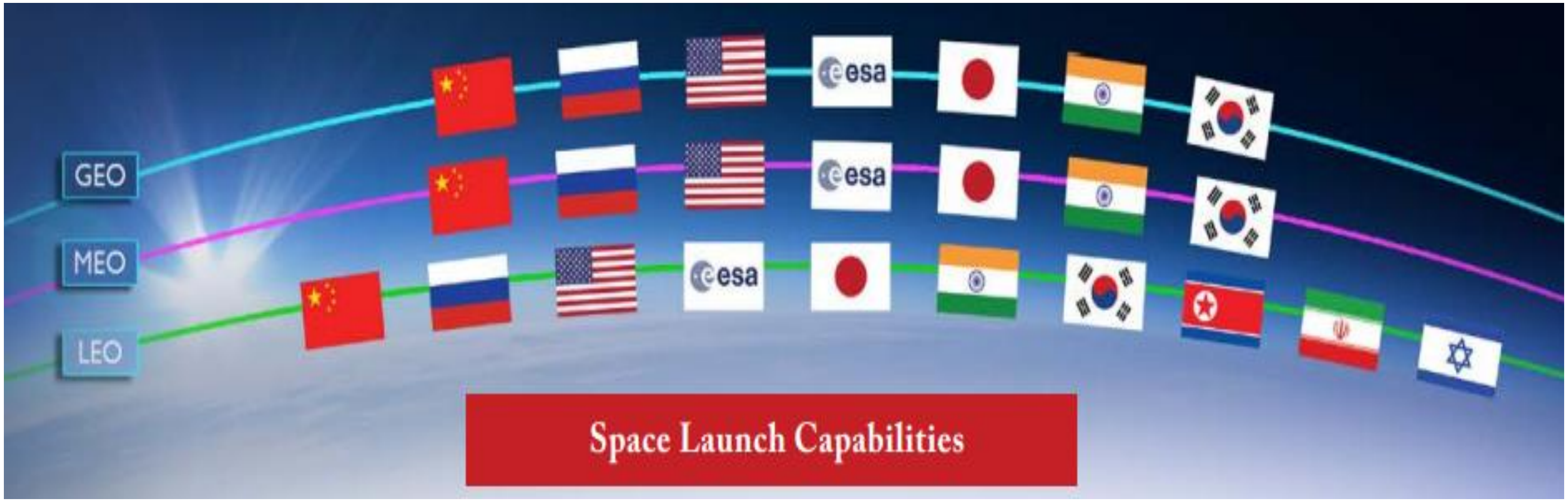
Overview

- At the national and global levels there is an increasing market for space services that ranges from GPS and broadband connectivity to emergency response and environmental monitoring
- Emerging factors and trends – such as commercialization of space - are leading to the escalation of data travelling across information systems in satellites, link, ground stations, and user equipment
- While once thought ‘off grid,’ some space systems are no longer immune to digital risk
- The space enterprise – which spans government and commercial operations that impact billions of people - is increasingly vulnerable to these risks
- Also at risk are National critical functions that space systems support – navigation, banking, communications, agriculture, emergency services
- Guidance and best practices are continuing to evolve; protecting and securing data and information across the space enterprise is critically important

Increasing Market for Space Services

Innovation is accelerating in LEO, MEO, GEO… and now Cislunar

- 90+ countries and international organizations including US, China, Russia, UK, Japan, India, European Space Agency, Canada, and Germany have put objects on orbit and continue to increase investment

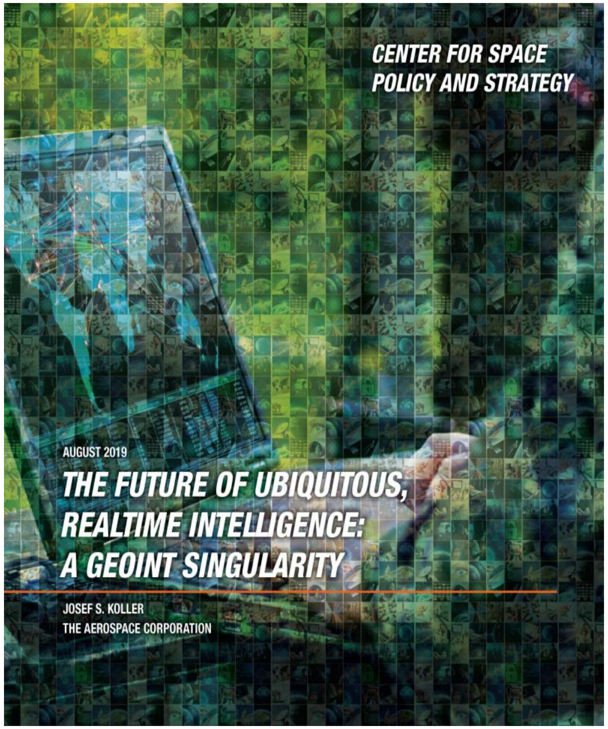


National Air and Space Intelligence Center, 'Competing in Space,' December 2018

Innovation and Opportunities Across the Space Enterprise

Trends, signals, and signposts indicate exciting current/future capabilities

- Expanded use of geoinformation and space technologies across sectors
- Race for satellite broadband services (SpaceX Starlink, Kuiper, OneWeb)
- Technology Integration
- Mega Constellations
- Smaller and more powerful satellites
- Space as a Service / Ground Station as a Service
- Orbital Congestion
- On-Orbit Manufacturing
- Real time Earth observations with analytics available globally to the average citizen



CENTER FOR SPACE
POLICY AND STRATEGY

AUGUST 2019

THE FUTURE OF UBIQUITOUS, REALTIME INTELLIGENCE: A GEOINT SINGULARITY

JOSEF S. KOLLER
THE AEROSPACE CORPORATION

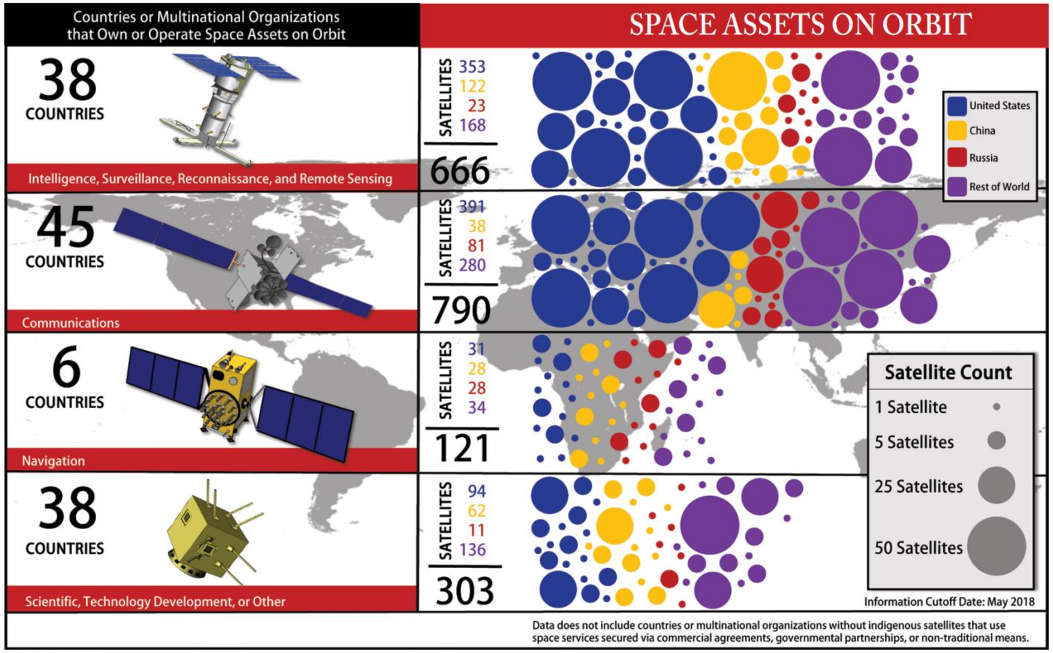
Josef Koller, "The Future of Ubiquitous, Realtime Intelligence: A GEOINT Singularity," The Aerospace Corporation, August 8, 2019

National Air and Space Intelligence Center, 'Competing in Space,' December 2018

Innovation by the Numbers

Year-over-year the number of satellites launched is increasing

- In 2020, 114 launches carried 1,300 satellites to space, surpassing the 1,000 new satellites per year mark for the first time
- 2021 surpassed the 2020 record – as of September 2021, approximately 1,400 new satellites had launched
- To date there are more than 3,400 active satellites in orbit
- With SpaceX's Starlink, Amazon's Kuiper, OneWeb, etc. the number of satellites on orbit is expected to increase exponentially



National Air and Space Intelligence Center, "Competing in Space," December 2018

Geospatial World, "How Many Satellites Are Orbiting the Earth in 2021?," May 28, 2021

Space.Com, "How Many Satellites Are Orbiting Earth?," September 25, 2021

Concerning Trends and Challenges

Technological and security factors are increasing risk to the space enterprise

- Increasing access to space is creating a larger threat surface and additional threat vectors
- Commercial and government space-based communications platforms are creating dependencies that could potentially be exploited
- We must assume our adversaries are evolving ransomware, cyberwarfare, cyber terrorism, etc.

Other significant issues are arising from:

- Supply chain and insiders
- Failure to design-in security in early development phases
- Lack of secure configuration
- Age and system maturity of the space ecosystem
- Lack of threat intelligence sharing
- Lack of knowledge or regard for security standards

Space Operations

Interdependent elements across the space enterprise ensure continuous space and space-enabled capabilities

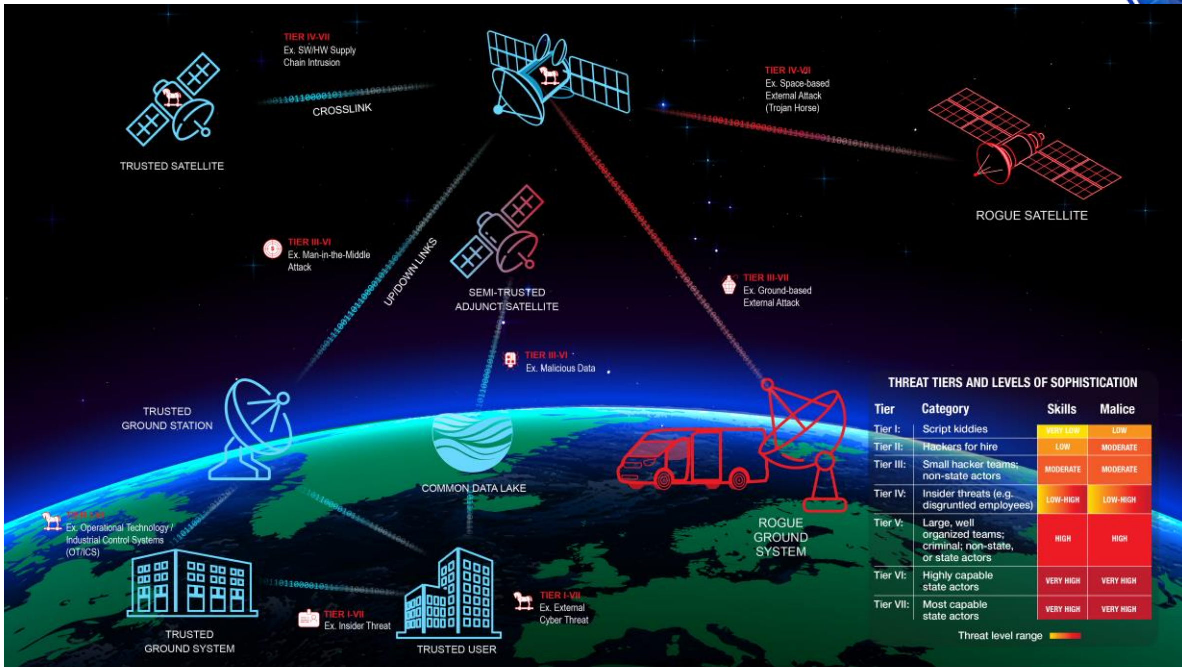
- Research & Development and Space System Manufacturing
- Space Launch facilities including Air Force bases, missile range facilities, spaceports, space stations/centers
- Ground Stations used to control spacecraft flight systems and payload
- Satellites which include flight systems and payload systems to help them reach orbit and maneuver
- Space Exploration Vehicles provide surface mobility and transportation
- Space Transportation Vehicle which port cargo and human space flight, including resupply to international space station, our return to moon and Mars, and the life support systems that are required
- Electromagnetic Spectrum radio frequencies – a finite resource that must be assigned and deconflicted – used by satellites to support a range of capabilities, from weather to combatant command

Without any one of these elements, space missions or systems – and anything other systems reliant on them - could be degraded or fail to operate

Vulnerabilities, Threats, Consequences to Space Systems

As space becomes more contested, information systems must be a protection priority

- Vulnerabilities include ICS/SCADA, engineering and design, insufficient logging and monitoring, configuration control, supply chain security
- Threats include unauthorized commands for control, spoofing sensor data, corrupting sensor systems, injecting malicious code, conducting DoS attacks
- Consequences include loss of mission data, decreased lifespan or capability of space systems, or loss of control of space vehicles resulting in collisions that can impair systems or create orbital debris

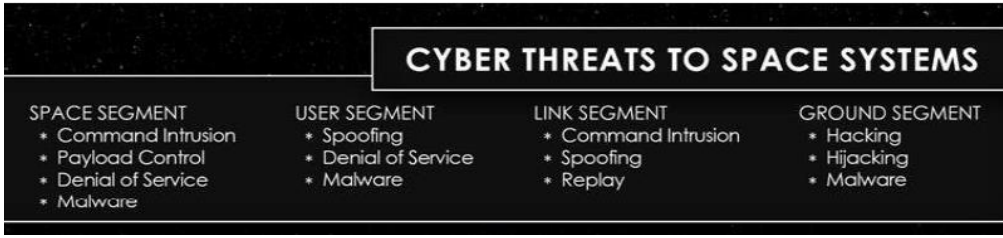


THREAT TIERS AND LEVELS OF SOPHISTICATION

Tier	Category	Skills	Malice
Tier I:	Script kiddies	VERY LOW	LOW
Tier II:	Hackers for hire	LOW	MODERATE
Tier III:	Small hacker teams; non-state actors	MODERATE	MODERATE
Tier IV:	Insider threats (e.g. disgruntled employees)	LOW-HIGH	LOW-HIGH
Tier V:	Large, well organized teams; criminal; non-state, or state actors	HIGH	HIGH
Tier VI:	Highly capable state actors	VERY HIGH	VERY HIGH
Tier VII:	Most capable state actors	VERY HIGH	VERY HIGH

Threat level range

A satellite systems OV-1 illustrates segments to operations – ground, link, user, space - where threat actors could potentially impact those segments



CYBER THREATS TO SPACE SYSTEMS

SPACE SEGMENT
- Command Intrusion
- Payload Control
- Denial of Service
- Malware

USER SEGMENT
- Spoofing
- Denial of Service
- Malware

LINK SEGMENT
- Command Intrusion
- Spoofing
- Replay

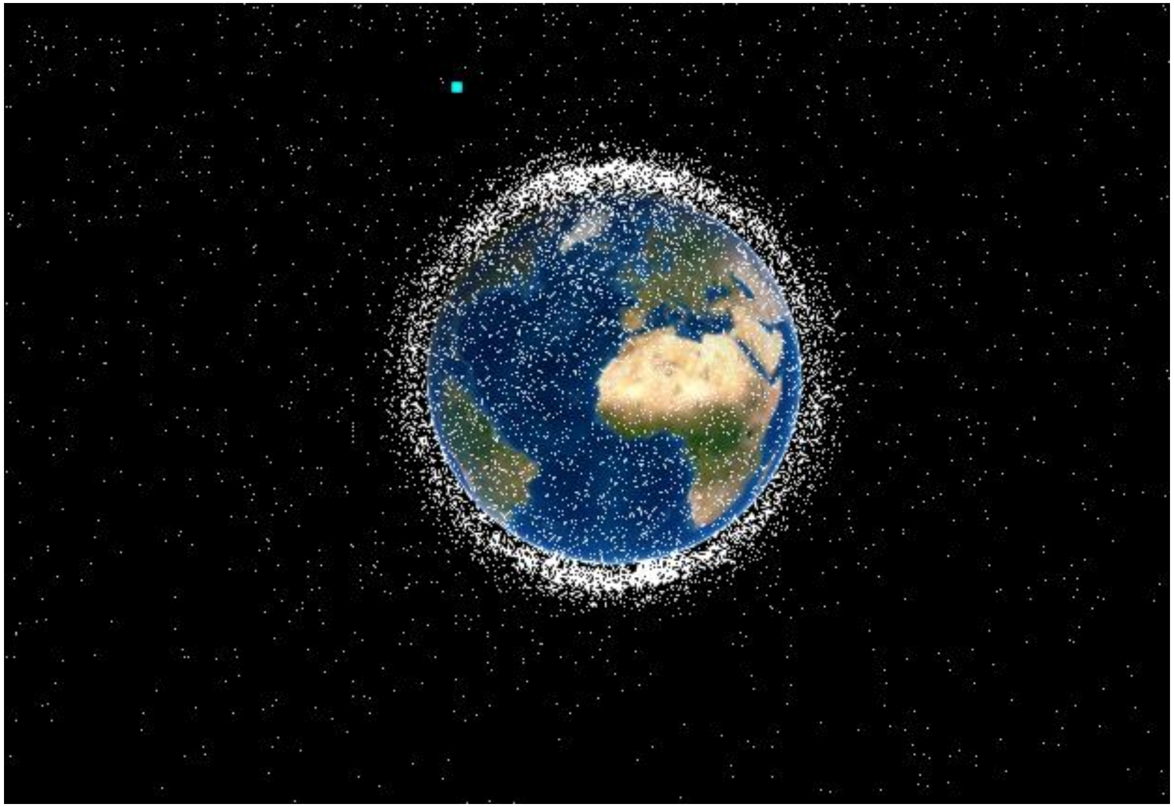
GROUND SEGMENT
- Hacking
- Hijacking
- Malware

The Aerospace Corporation, « Space Cyber, » June 2021

National Air and Space Intelligence Center, "Competing in Space," December 2018

Space Enterprise Integration for Safety and Security

Agencies coordinate policy, regulatory, and cross-cutting technical initiatives to support national security, civil, & commercial space



Agencies are coordinating around common opportunities (as well as risk management) in space – these include space traffic management, space-based environmental monitoring, and orbital debris management

Information Systems and Cybersecurity Guidance

National and International standards development organizations develop guidance to increase space systems security and resilience

- NIST
  - *Cybersecurity Framework and Implementation Guide, Risk Management Framework*
  - *SP 800-171, SP 800-53, SP 800-161*
- ISO
  - *27001, 27016, 27034*
- FIPS-199
- Cybersecurity Model Certification
- Consultative Committee for Space Data Systems (CCSDS)
  - *Space Data Link Security Protocol, Others*
- Committee on National Security Systems Instruction (CNSSI)
  - *Security Categorization and Control Selection for National Security Systems, Others*
- DoD, IC, NASA, and other agencies’ Software Engineering Requirements

Best Practices

Organizations in the Space Enterprise employ best practices to enhance or fill gaps in guidance

- Training & Education
  - *Continuous Education to all employees across various cybersecurity topics*
  - *Diverse Space Mission Resiliency Studies*
  - *Supplier Webinars and Tracking*

- Exercises
  - *Cyber Table-Top Exercises*
  - *Space Cyber Capabilities for continuous monitoring, testing, and tracking*
  - *Cyber Incident Response Team (CIRT)*

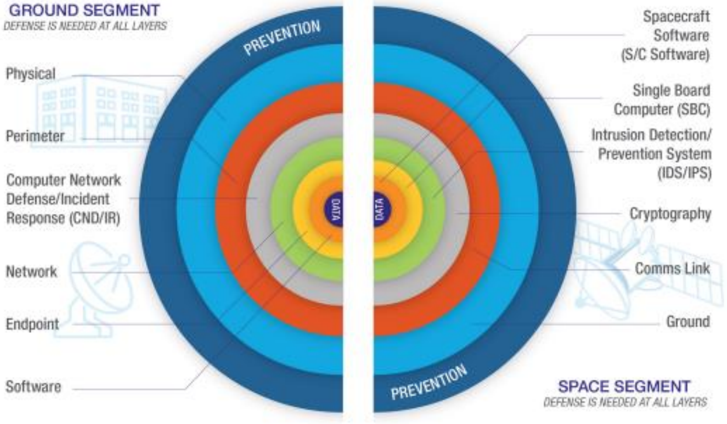
- Threat Intelligence
  - *Security Intelligence Center (SIC)*
  - *Insider Threat Program*
  - *Space Vulnerability Management Council*
  - *Space and cyber information sharing partnerships*

- Standards & Tools
  - *JWICS-like environment for intellectual property development*
  - *Cyber Resiliency Reference Architectures model*
  - *Zero Trust Framework*
  - *Toll-gates into the engineering and PM processes*
  - *IT systems cybersecurity per corporate standards*
  - *Product development methodology to minimize non-secure technology protocol/process*

Defense-in-Depth

A defense-in-depth approach can build a more robust security posture and help address challenges

- Threat emulation/modeling on ground segment, expanding cyber strategy beyond physical or logical isolation when goal is accreditation and compliance
- Linking segment protection by applying Communications Security (COMSEC) and/or Transmission Security (TRANSEC), i.e., authentication and encryption; jamming and spoofing protections
- Intrusion detection, prevention, leveraging signatures and ML to detect and block cyber intrusions onboard spacecraft + traditional ground-based monitoring
- Supply Chain Risk Management program to protect against counterfeit parts, hardware trojans, malware
- Logging onboard spacecraft to verify legitimate operations, aid forensic investigations after anomalies
- Root of Trust to protect software and firmware integrity
- A tamper-proof means to restore the spacecraft to a known-good cyber-safe mode
- Protections against intentional/unintentional insider threat affecting mission operations or supply chain


GROUND SEGMENT
DEFENSE IS NEEDED AT ALL LAYERS
Physical
Perimeter
Computer Network Defense/Incident Response (CND/IR)
Network
Endpoint
Software
PREVENTION
DATA
DATA
PREVENTION
Spacecraft Software (S/C Software)
Single Board Computer (SBC)
Intrusion Detection/ Prevention System (IDS/IPS)
Cryptography
Comms Link
Ground
SPACE SEGMENT
DEFENSE IS NEEDED AT ALL LAYERS

Aerospace research focuses on layered prevention across ground and space segments.
“Space Cyber,” The Aerospace Corporation, June 2021

Bailey et al, “Defending Spacecraft in the Cyber Domain,” November 2019, The Aerospace Corporation

Conclusion

- With the commercialization of space and a range of other accelerating trends, the market for space services is projected to increase in future decades
- This means that the volumes of data and information across the enterprise in satellites, ground stations, and user equipment will escalate
- The vast opportunities and the scale of infrastructure that this offers means that this is a growing threat plane that can be exploited
- Without exception, risk management must be a priority
- Evolving guidance, best practices, and a layered defense-in-depth approach to protect and secure data and information across the space enterprise is critical to outpace the threat