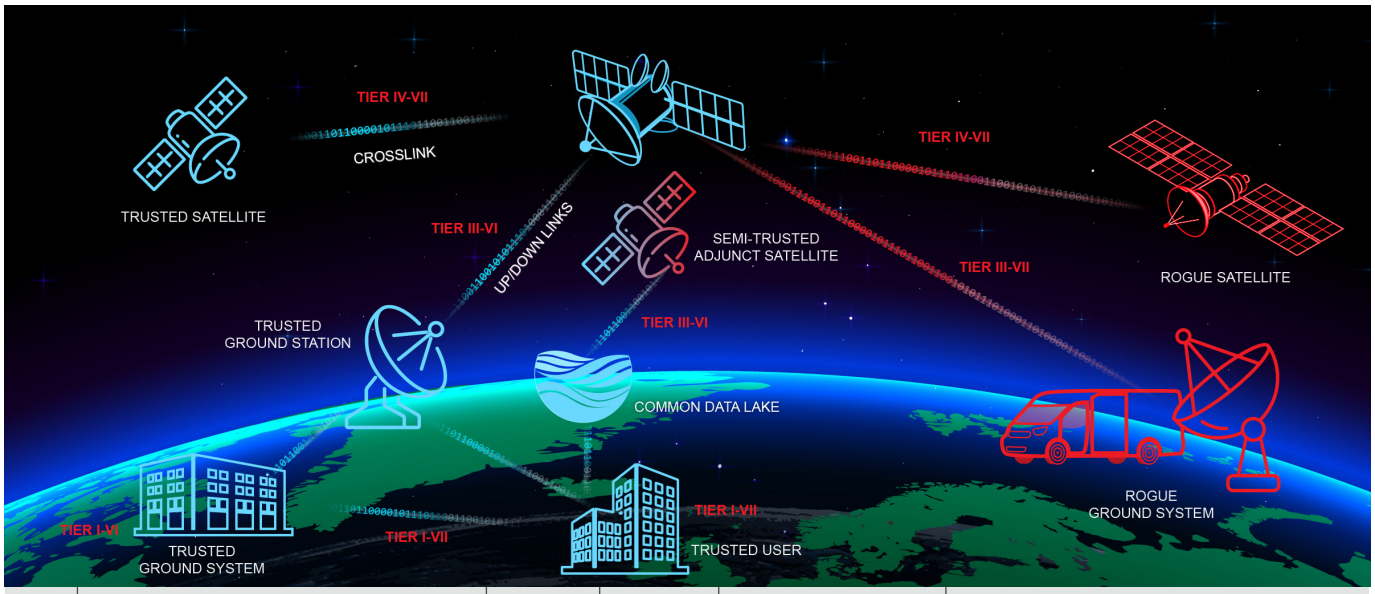
AEROSPACE

SPACE CYBER

Cyber threats pose a significant and complex challenge due to the absence of warning, the speed of an attack by an adversary, the difficulty of attribution, and the complexities associated with carrying out a proportionate response. Space systems face many well-known types of attack, including orbital, kinetic, and electronic warfare, but are also vulnerable to other forms of cyber threat. Applying defense-in-depth principles throughout each segment is imperative to defending our space assets.

Cyberattacks can occur across multiple segments within the architecture — space, link, and ground — and space systems are often overlooked in wider discussions of cyber threats to critical infrastructure. All critical national space systems must be appropriately hardened against cyber threats; forgoing preventative measures is not an option.

THREAT AGENTS AND LEVELS OF SOPHISTICATION



Tiers	Name	Skills	Malice	Motive	Methods
I	Script Kiddies	Very low	Low	Boredom, thrill seeking	Download and run hacking scripts known as “toolkits”
II	Hackers for Hire	Low	Moderate	Prestige, personal gain, thrill seeking	Write scripts, engage in malicious acts, brag about exploits
III	Small Hacker Teams: Non-State Actors OR Disorganized/State Actors	Moderate	Moderate	Power, prestige, intellectual gain, respect	Write scripts and automated tools
IV	Insider Threats (e.g. disgruntled employees)	Very low – Very high	Very low – Very high	Unwitting, ideology, politics, espionage	Insider knowledge; Methods can range from inadvertent to sophisticated.
V	Large, Well-Organized Teams: Non-State OR State Actors	High	High	Personal gain, greed, revenge	Sophisticated attacks by criminals; “guns for hire” or organized crime
VI	Highly-Capable State Actors	Very high	Very high	Ideology, politics, espionage	State sponsored cyberattacks against enemy nations
VII	Most Capable State Actors				

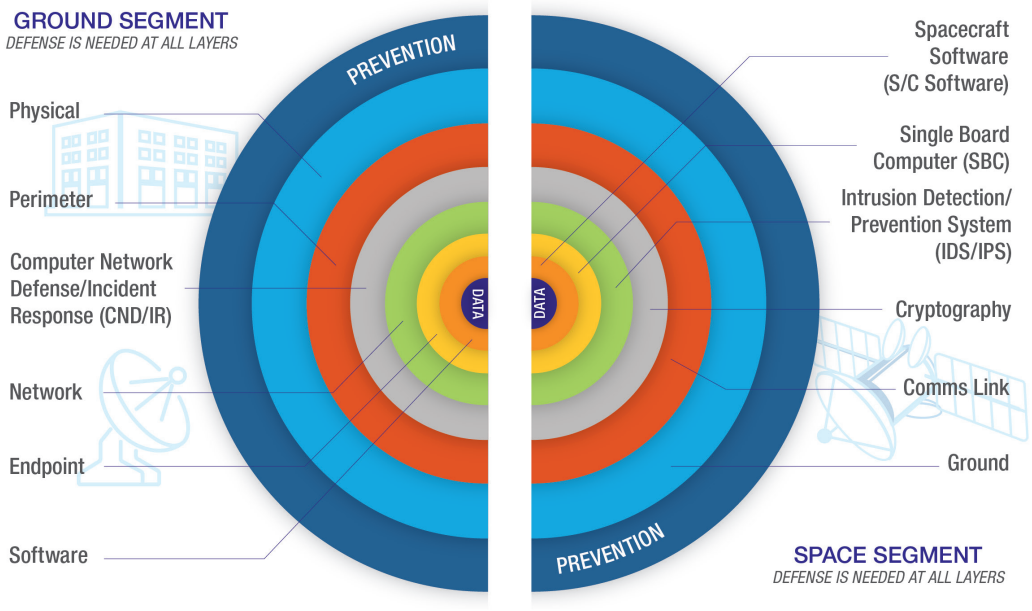
Defense-in-Depth Principles

Without structured governance of security requirements, policies, and practices, a threat-informed, defense-in-depth approach should be used to manage space cyber risk. No risk can be eliminated entirely, but decision makers, acquisition professionals, program managers, and system designers can consider some key principles when acquiring or designing a cyber-resilient space system to mitigate appropriate risk. Application of defenses at all segments will build a more robust security posture.

- Include threat emulation/modeling on the ground segment, expanding the cyber strategy beyond physical or logical isolation when the goal is mostly accreditation and compliance
- Link segment protection by applying the desired level of Communications Security (COMSEC) and/or Transmission Security (TRANSEC), i.e., authentication and encryption, along with consideration of jamming and spoofing protections
- Intrusion detection and prevention leveraging signatures and machine learning to detect and block cyber intrusions onboard spacecraft in addition to traditional ground-based monitoring
- A Supply Chain Risk Management (SCRM) program to protect against counterfeit parts, hardware trojans, or malware
- Logging onboard spacecraft to verify legitimate operations and aid in 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 or unintentional insider threats affecting mission operations or the supply chain

Similar to early firewall protections, space systems are designed assuming external boundaries are sufficient, with little internal protection if a boundary is breached. Designs must now anticipate an adversary operating unhindered within a system. All systems must ensure they have a cyber-hardened design with defense-in-depth throughout.

Cost and schedule as well as spacecraft size, weight, and power restrictions are key to architecting a secure space system. Threat-informed risk management addresses threats and vulnerabilities within a system, the impacts on the system, and the risk to an overall mission. Operational environments must be considered when classifying threats and vulnerabilities; each applicable cyber threat for a mission must be evaluated to determine its likelihood and mission impact.



The Aerospace Corporation

The Aerospace Corporation is a national nonprofit corporation that operates a federally funded research and development center and has more than 4,600 employees. With major locations in Chantilly, Virginia; El Segundo, California; Albuquerque, New Mexico; and Colorado Springs, Colorado, Aerospace addresses complex problems across the space enterprise and other areas of national and international significance through agility, innovation, and objective technical leadership. For more information, visit www.aerospace.org.

The Aerospace Corporation | 14745 Lee Road, Chantilly, VA 20151 USA | www.aerospace.org