AEROSPACE

AEROSPACE CYBER CAPABILITIES

Operational Space Systems are similar to complex terrestrial systems like power grids, industrial plants, large ocean-going vessels and aircraft systems. One common factor in all modern, intelligent systems is the inextricable linkage between the physical systems and the electronic and increasingly cyber enabled systems. It is critical to ensure that robust security principles are present for traditional designs as well as new SmallSat constellations, and to apply defense in depth throughout the space enterprise. Aerospace's Cyber Security Subdivision (CSS) has capabilities across a variety of areas within space systems with focus on the user, ground and space segments.

Designing a Cyber Resilient Space System

Ground and user segments and any other interface must be properly secured. As IT systems have over the last few decades, spacecraft should implement defense-in-depth (DiD) principles, which include detecting, deterring, and attributing attacks at various places across ground and space systems. CSS has a robust assessment and testing approach for ground systems and networks to test cyber resiliency using threat-informed tactics, techniques, and procedures. CSS assesses design against credible threats and adheres to Spacecraft DiD principles when assessing spacecraft design which include Intrusion Detection and Prevention Systems, Supply Chain Risk Management, Onboard Logging Root-of-Trust (RoT) & Trusted Boot, MIL-STD-1553 Separation, and other considerations for SmallSats (software updates, software crypto, and memory monitoring).

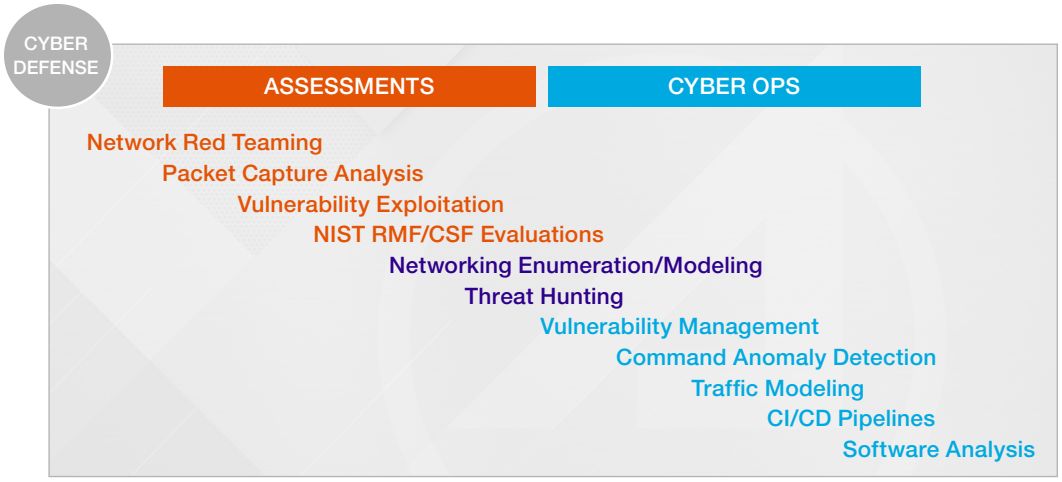


Figure 1: Aerospace Areas of Focus in Cyber Defense for Space Systems

Cyber Assessment & Testing

- Pen Testing & Cyber Assessments
- ICS/SCADA Architecture Design, Review, and Assessments
- Air-Gapped Network Security
- Crypto Engineering

Hardware & Embedded Cyber

- Embedded & Trusted Computing
- Integrated Circuit Supply Chain Risk Management, FPGA/ASICs

Space Cyber Software & Tools

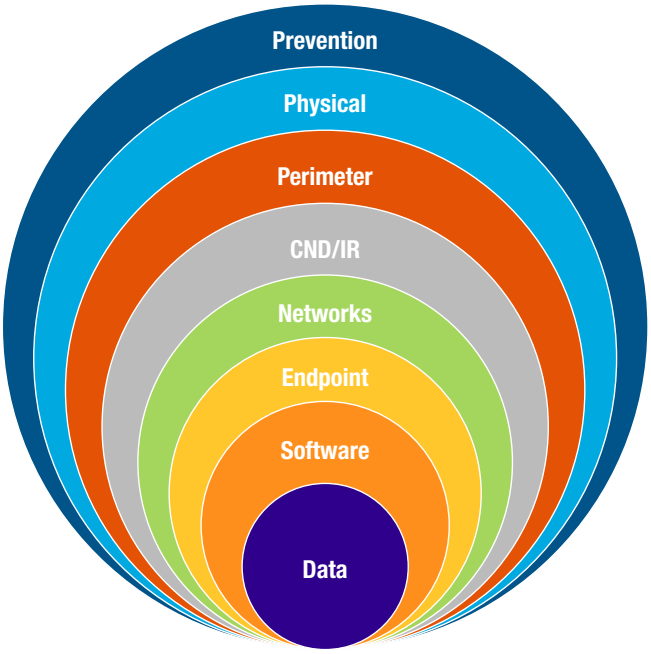
- Spacecraft Cyber Defense
- Static & Dynamic SW Analysis
- Space Cyber Lab and Test Range
- SW Assurance Framework & Tools

Cloud & Network Security

- Cloud Infrastructure Security
- CND in the Cloud
- CI/CD Pipeline Security

Fully Understanding Mission, Data Flow, and All Supporting Assets

Comprehensive ground system cyber evaluations require a full understanding of the Mission environment. To achieve this understanding requires tapping a range of robust capabilities to characterize architecture, systems, and facilities; identify mission critical, mission essential, and mission-support assets across network infrastructure, workstations/servers, SCADA/ICS/OT, custom software, and cloud; detect abnormal flows through machine learning; and to test strategies to identify vulnerabilities and risk without impacting mission operations.



PREVENTION
Personnel mgt/awareness
Risk management
Security assessments
Threat modeling
Training

PHYSICAL
Badging/doors
Fire supression
Gates/fences
Logging
Single points of failure
Surveillance

PERIMETER
DLP
DMZ/security names
Firewall

CND/IR
Forensics
Hunting
IDS/IPS
Sensors
TAPs
SIEM
SOC
Policy procedures

NETWORKS
ACL
Path diversification
Firewall
Port security
Segmentation
Wireless
Authentication

ENDPOINT
Authentication
Hardening
HDS/MPS
AV/AM
CM/baseline
DLP
File integrity
Vulnerability scanning
Patch management

ENDPOINT
Authentication
Hardening
HDS/MPS
AV/AM
CM/baseline
DLP
File integrity
Vulnerability scanning
Patch management

SOFTWARE
Coding standards
CWE prevention
Static analysis
Origin analysis
Dynamic analysis

DATA
Encryption
Leakage
OSINT
Permissions/access

Testing Environments and Capabilities

Due to the fragility of some environments, assets can be difficult to test on live networks. Aerospace has diverse labs across the country to passively test in these fragile environments. Capabilities include:

- **Network Modeling:** Creates powerful ground truth network models and cyber-attack simulation
- **DCO 2.0 (Irene Sceptre):** Flexible toolkit for cyber defense & orchestration
- **Immortal Snail:** Cloud-native, extensible, scalable tool that creates a fingerprint of their networks and tracks cyber vulnerabilities offline and educates customers to new vulnerabilities that may impact their deployments
- **Static (Source & Binary) and Dynamic Testing:** Perform code analysis and dynamic testing on custom mission software
- **Network Traffic Analysis:** Post process network traffic (PCAP) looking for IOCs, misconfigurations, and confirm data flows
- **Hardware Trojan Identification (ASIC and FPGA Trust Assurance (AFTA) Government Microelectronics Assessment for Trust (GOMAT)):** Identify Trojans within ASIC and FPGA chipsets

Figure 3: Select Aerospace Cyber Capabilities include DCO 2.0 (Irene Sceptre), Immortal Snail, Hardware Trojan Identification

Aerospace Assessment Differentiators

Aerospace's work is strengthened by our vast knowledgebase of space systems and research. Leveraging this depth and breadth in understanding space and ground systems, we continue to evolve our research as the threat environment becomes more complex. These areas include bulk capture of network traffic data using a network tap or spanned port, creating data models of traffic using tailored dimensions of data to "teach" the model a representative baseline, using machine learning to assess gigabytes to terabytes of network traffic in a fraction of the time, and orchestrating response to cyber incidents. We continue to innovate in particularly challenging or distinct areas in determining risk and exposure of discovered vulnerabilities, analyzing mission custom software using static and dynamic analysis, assessing the impacts of Industrial Control Systems and Operational Technology on mission, and ensuring assessments are threat-informed, to include use of real attacker TTPs in simulations.

The Aerospace Corporation

The Aerospace Corporation is a national nonprofit corporation that operates a federally funded research and development center (FFRDC) and has approximately 4,000 employees. The Aerospace FFRDC is aligned to support the most critical programs of the Department of Defense and the nation, and to serve as its customers' innovation partner across the space enterprise. Consistent with the competencies outlined in our sponsoring agreement, Aerospace provides strategic value through independent, intellectually rigorous, relevant, and timely products and services. With major locations in El Segundo, Calif., Albuquerque, N.M., Colorado Springs, C.O., and Washington, D.C., Aerospace addresses complex problems across the space enterprise and other areas of national significance.

The Aerospace Corporation | 2310 East El Segundo Boulevard, El Segundo, California 90245-4609 USA | www.aerospace.org