DEFENDING SPACECRAFT IN THE CYBER DOMAIN

Cyber threats pose a significant and complex challenge due to the absence of a warning and speed of an attack by an adversary, the difficulty of attribution, and the complexities associated with carrying out a proportionate response. Applying defense in depth throughout the space enterprise, particularly on the space vehicle themselves is imperative.

In lieu of structured governance and standards being available, a threat informed DiD approach can be used to manage cyber risk for the spacecraft. Industry and government alike can begin to apply defenses at all segments within the space system to build a more robust security posture. To mitigate risks, decision makers must ultimately determine what kinds of Defense in Depth principles to apply. Not all risks can be eliminated, and no decision maker has unlimited budget or enough personnel to combat all risks. However, decision makers, acquisition professionals, program managers and system designers can consider the following key principles when acquiring or designing a cyber-resilient spacecraft:

- **Intrusion detection and prevention** leveraging signatures and machine learning to detect and block cyber intrusions onboard spacecraft
- **A supply chain risk management program** to protect against malware inserted in parts and modules
- **Software assurance methods** within the software supply chain to reduce the likelihood of cyber weaknesses in flight software and firmware
- **Logging onboard the 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
- **Lightweight cryptographic solutions** for use in SmallSats

Abstaining from action is not an option and it is necessary for all national critical space systems to be appropriately hardened against cyber threats.

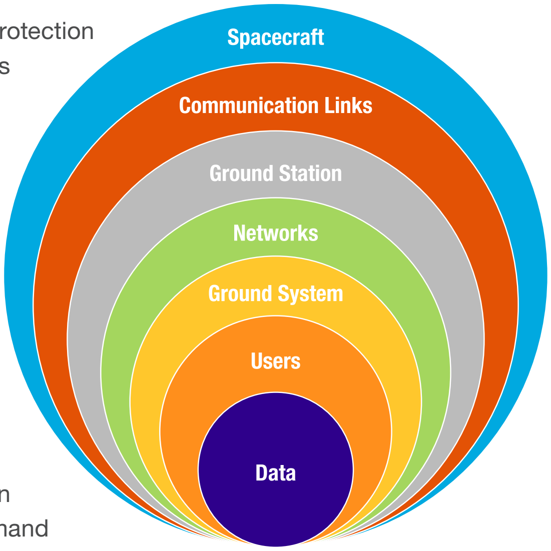
› The space domain is a complex integration of many government and commercial components where cybersecurity and space security are inextricably linked.

› The vulnerability of satellites and other space assets to cyberattack is often overlooked in wider discussions of cyberthreats to critical national infrastructure.

› Neither space policy nor cybersecurity policy is prepared for the challenges created by the meshing of space and cyberspace, especially for the spacecraft.

Defense in Depth

The fundamental problem for space systems is that they are designed assuming protection at their boundaries will be enough. Little internal protection exists if the boundary is breached. Similar schools of thought existed in the beginning days of traditional cybersecurity where border firewalls were providing the only protection from intrusion. This approach proved to be faulty and well-protected IT systems are now designed with DiD principles. Similarly, current and future space system designs must overcome the risk of an adversary breaching the boundary and operating unhindered inside the system using these principles. Both large traditional developments and more modern rapidly developed space systems should ensure that they have a cyber hardened design with DiD throughout.



DiD Principles for a Cyber Resilient Spacecraft

INTRUSION DETECTION AND PREVENTION SYSTEMS

The backbone of a cyber resilient spacecraft should be a robust intrusion detection system (IDS). The IDS should consist of continuous monitoring of telemetry, command sequences, command receiver status, shared bus traffic, and flight software configuration and operating states. The IDS system should be integrated into the existing onboard spacecraft fault management system (FMS) because the FMS has its own fault detection and response system built in.

SUPPLY CHAIN

Spacecraft developers must ensure that each of their vendors handle hardware and software appropriately and with an agreed upon chain of custody. Critical units and subsystems should be identified and handled with different rigor and requirements than non-critical units and subsystems. Parts should be sourced from reputable vendors and checked for signs of counterfeiting. Proper configuration management must be implemented for all software and firmware residing in any system on a spacecraft.

LOGGING

Both the spacecraft and ground should independently perform command logging and anomaly detection of command sequences for cross validation. Commands received may be stored and sent to the ground through telemetry and automatically checked to verify consistency between commands sent and commands received. Alternatively, command sequence hashes can be used to verify consistency if telemetry link bandwidth is a concern.

SMALL SATELLITE CONSIDERATIONS

Due to the increased usage and capabilities of smaller satellites, both the complexity and availability of satellite technology are growing, making the space infrastructure even more vulnerable. The future of the space enterprise is moving towards large constellations of small satellites in low Earth orbit. As designs are being developed, several considerations should be undertaken. Many of the aforementioned DiD principles apply to small satellites, but with these new technologies there are new security considerations. For example, lightweight software cryptography solutions should be considered acceptable.

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.