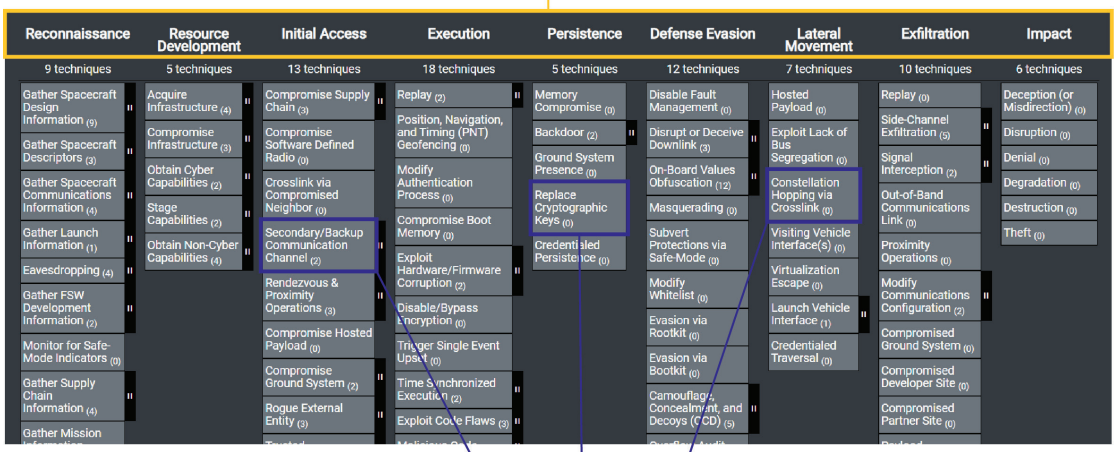
AEROSPACE

SPARTA: SPACE ATTACK RESEARCH & TACTIC ANALYSIS CYBERSECURITY FRAMEWORK

The Aerospace Corporation's SPARTA® is the first-of-its-kind body of knowledge on threats that emerge in the distinct and demanding space environment, filling a critical vulnerability gap for the U.S. space enterprise.

Tactics: The "why" of a SPARTA technique or sub-technique. It is the threat actor's tactical goal and the reason they are performing a technique.



Source: SPARTA website, https://sparta.aerospace.org

Techniques: Represent "how" a threat actor achieves a tactical goal by performing a threat action.

SPARTA is designed to support the protection of space systems from increasingly sophisticated cyber threats, aggregates cutting-edge research and practical intelligence to map and analyze attack chains using tactics, techniques, sub-techniques, and procedures. By linking cybersecurity with space operations, SPARTA empowers developers, owners, and operators to design defense-in-depth strategies that effectively secure critical space assets. SPARTA is publicly available and continually refined through community engagement, provides the essential insights and countermeasures needed to outpace adversaries in the modern space threat landscape.

THE AEROSPACE CORPORATION
SPARTA®
SPACE ATTACK RESEARCH & TACTIC ANALYSIS

Visit SPARTA.aero.org

Contact

sparta@aero.org

SPARTA Use Cases

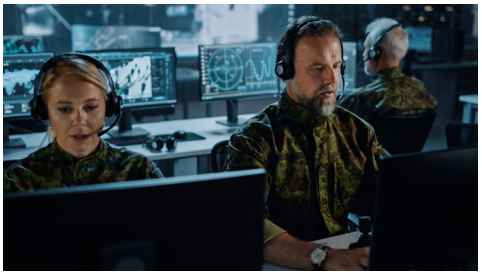
Developers, owners, and operators of spacecraft and space systems can leverage SPARTA to consider known adversarial cyber threats, techniques, and procedures to inform defense-in-depth design.

Potential use cases for SPARTA include:

- Space System Development
- Defensive Cyber Operations
- Threat Intelligence Reporting
- Tracking Tactics, Techniques, and Procedures (TTPs)
- Assessments and Tabletop Exercises

SPARTA Case Studies

Leading space organizations rely on SPARTA's advanced solutions to support mission-critical operations, ensuring operational excellence and pushing the boundaries of what's possible in space innovation.



TAILORED CYBERSECURITY CONTROLS FOR NATIONAL SECURITY

SPARTA delivers robust insights to produce actionable intelligence and support to critical space systems, bolstering national security efforts and ensuring strategic assets are safeguarded in an evolving threat landscape.

SPACE SECURITY STANDARDS DEVELOPMENT

By actively engaging with top industry leaders and contributing through key national committees and specialized working groups, SPARTA has significantly helped shape emerging standards in space security, laying the groundwork for innovative and reliable protocols.

ENHANCE INTELLIGENCE TRACKING AND REPORTING

With seamless information sharing across key defense and industry networks, including the Space Information Sharing and Analysis Center (ISAC), enhances situational awareness and optimizes collaborative responses in real time, elevating the space sector's cyber readiness and resiliency.

ONBOARD DEFENSIVE CYBER CAPABILITIES

SPARTA supports the integration of threat insights with real-time data generated through detection, reporting, and mitigation technologies, enabling new capabilities for protecting critical space assets during missions.
Photo courtesy NOAA/NASA.

SPARTA USER TESTIMONIAL

U.S. Government Agency Chief Information Officer (CIO)

"Using cybersecurity requirements derived from The Aerospace Corporation's SPARTA framework has been instrumental in reducing both schedule and technical risk for [our] acquisitions. By leveraging threat-informed technical cybersecurity requirements, rather than relying solely on traditional [risk management framework (RMF)] controls that get decomposed later post-contract award, SPARTA enables the integration of cyber-resilient features early in the system lifecycle.

By aligning SPARTA-derived cybersecurity requirements with RMF controls, the framework enables RMF processes and systems engineering to work in concert, ensuring that security is integrated early in the system development lifecycle, reducing both technical risk and the need for costly late-stage mitigations.

This approach enhances mission assurance through capabilities such as but not limited to onboard Intrusion Detection Systems (IDS) and Hardware-based Root of Trust (HWRoT), which ensure protection against evolving threats to spacecraft systems."

The Aerospace Corporation

The Aerospace Corporation is a leading architect for the nation's space programs, advancing capabilities that outpace threats to the country's national security while nurturing innovative technologies to further a new era of space commercialization and exploration. Aerospace's national workforce of more than 4,600 employees provides objective technical expertise and thought leadership to solve the hardest problems in space and assure mission success for space systems and space vehicles. For more information, visit www.aerospace.org.

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