AEROSPACE

SPARTA: SPACE ATTACK RESEARCH & TACTIC ANALYSIS CYBERSECURITY FRAMEWORK

Space systems provide critical capabilities that power global industries and enable several facets of everyday life. During a conflict, adversaries may seek to deceive, deny, disrupt, degrade, or destroy those capabilities. Cyberattacks are a complex but effective and increasingly prevalent attack vector in the space domain. To counter cyber threats, cybersecurity and space operations are becoming inextricably linked. Though spacecraft have historically been considered relatively safe from cyber threats, they are squarely in the crosshairs within the modern threat landscape.

Cybersecurity matrices have become an industry-standard approach for providing a knowledge base of adversary behaviors, helping visualize and categorize threats, and serving as a taxonomy for adversarial actions across the attack lifecycle for a number of industry sectors. However, there has traditionally been no framework dedicated to address cyber threats to the spacecraft or space vehicles that are critical enablers of many of those sectors and important facets of daily life.

To fill this gap, The Aerospace Corporation (Aerospace) developed the Space Attack Research and Tactic Analysis (SPARTA) cybersecurity framework, the first cybersecurity threat identification and response framework purposefully designed to help spacecraft developers, owners, and operators outpace space-cyber threats.

Cyber Tactics, Techniques, and Procedures

Aerospace recognized that a dedicated security framework would help space developers and network defenders understand and address unique space-cyber threats. Introduced in 2022, SPARTA aggregates unclassified information and research from academia, space-cyber professionals, and federally funded research and development centers into a single resource to better educate the space community about how spacecraft may be compromised via cyber means, while also identifying associated countermeasures.

SPARTA, like preceding security matrices that inspired it, documents possible attack chains and visually organizes cyber tactics, techniques, subtechniques, and procedures (TTPs) that may compromise spacecraft. SPARTA catalogs TTPs that are either theoretically possible or have been proven in laboratories, on-orbit exercises, and hacking workshops, as well as countermeasures spacecraft can implement to outpace cyber threats.

- **Tactics** represent the threat actor's tactical goal and the reason(s) they are performing a technique. For example, a threat actor may want to achieve initial access on a spacecraft via cyber means. Other tactics include reconnaissance, resource development, execution, defense evasion, exfiltration, lateral movement, and impact.
- **Techniques** represent "how" a threat actor achieves a tactical goal by performing a threat action. For example, a threat actor may exploit trusted relationships to achieve initial access. SPARTA maps a range of techniques that threat actors can use to execute tactics.
- **Subtechniques** represent a variation or more specific instance of the threat actor's behavior used to achieve a goal. Subtechniques typically describe behavior at lower levels than a technique and are considered children of the parent technique. For example, a threat actor may compromise mission collaborators (academia, international, etc.) to achieve their initial access.
- **Procedures** represent the specific, step-by-step implementation plans that threat actors use for achieving their purpose through techniques or subtechniques.

THE AEROSPACE CORPORATION SPARTA SPACE ATTACK RESEARCH & TACTIC ANALYSIS

SPARTA Cybersecurity Framework

SPARTA is opensource, public, and free to use. Aerospace will continually update SPARTA with known or theoretical TTPs and aspires for SPARTA to continually improve through community participation.

To use the tool, visit sparta.aerospace.org. To recommend updates or adjustments to SPARTA, email **sparta@aero.org**.

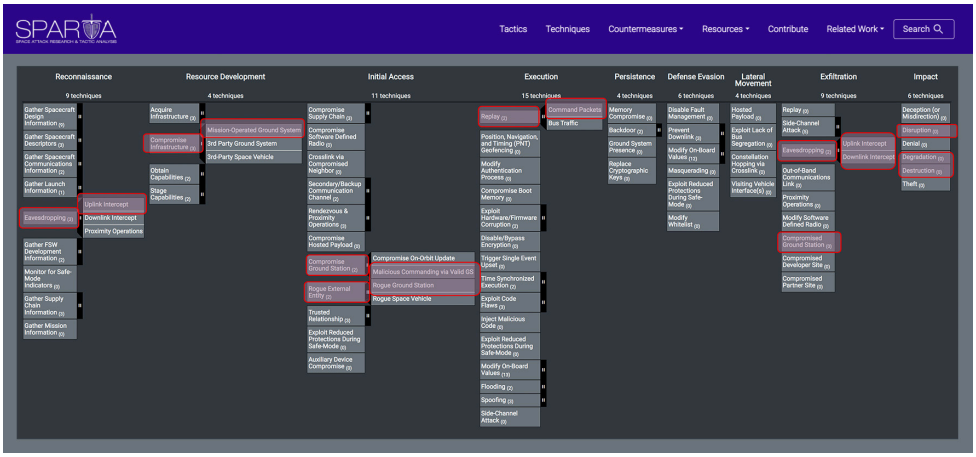
SPARTA Use Cases

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 (DiD)-based 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

The National Cybersecurity Strategy issued in March 2023 continues the commitment to enhance the security and resilience of U.S. space systems, including the implementation of Space Policy Directive-5, "Cybersecurity Principles for Space Systems," which established a set of principles to protect the nation's valuable space assets from an increasing number of cyber threats.

Aerospace's **Cybersecurity and Advanced Platforms Subdividision** uses space cyber ranges and digital twins to perform research on TTPs and countermeasures to better inform the space enterprise through cyber products like SPARTA.



This SPARTA attack chain emulates a "man-in-the-middle" attack scenario which Aerospace demonstrated at DEF CON 28 in 2020.

Learn more:
Leveraging the SPARTA Matrix

Using SPARTA to Simulate Attack Chains and Countermeasures

Attacks can occur across all segments of space systems (including ground systems and sensor networks). Countermeasures represent security concepts and classes of technologies that can be used to prevent tactics, techniques, and subtechniques from being successfully executed. Countermeasures may be implemented or deployed in space segments, ground segments, or the spacecraft development environment. SPARTA countermeasures, which are grounded in experience and industry standards, will be enhanced as new TTPs are published and space-cyber defensive technology matures.

Space system developers, engineers, owners, and operators can use SPARTA to visually represent various theoretical or proven attack chains and articulate the ideal place(s) to deploy possible countermeasures. The following steps can be used to address threats early in the space system lifecycle or any time after a system becomes operational:

1. Enumerate end-to-end systems during all phases of mission development and operations.
2. Review each threat, technique, and subtechnique and determine applicability based on the specific mission or system contexts for each space segment identified in Step 1.
3. Evaluate current design choices to identify potential gaps that would leave an element(s) vulnerable to applicable threats or techniques, as determined in Step 2.

SPARTA has successfully demonstrated real and theoretical attack chains from Aerospace research and space security conferences. The Space Information Sharing and Analysis Center (Space ISAC), which facilitates collaboration across the global space industry to prepare for and respond to vulnerabilities, incidents, and threats, has also announced it will integrate the SPARTA framework into the future threat information sharing capabilities of its Space Watch Center in Colorado Springs.

Securing Space Systems with Defense-in-Depth Design Principles

Space system engineers and developers will ultimately need to understand multiple cybersecurity matrices and how threat actors can leverage TTPs depending on their designs. Understanding TTPs will help inform spacecraft design decisions and where detection and/or countermeasures can be deployed within the system-of-systems context. Space systems should have a cyber-hardened design with defense-in-depth (DiD) applied throughout, including ground and space segments, to reduce the likelihood of successful cyberattacks. SPARTA leverages Aerospace's DiD model for space systems. Strong collaboration between offense and defense teams greatly improves a space system's ability to detect and stop a cyberattack. Ideally, engineers and defenders will work together to determine if and how their system-of-systems is vulnerable to specific TTPs and develop methods to detect or enact countermeasures within the attack chain to protect the spacecraft.

Contribute to SPARTA

SPARTA's usefulness relies on community engagement and collaboration, and Aerospace aspires for SPARTA to continually improve through community participation. Members of the space community who wish to recommend a TTP, countermeasure, or other data sources or use cases for SPARTA may do so by emailing **sparta@aero.org**.

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