OTR-2025-00018

Recommended Practices for Integrating TTP Frameworks to Secure and Defend Space Systems

October 10, 2024

Brandon T. Bailey[1], Joseph Daniel Painter[2]
[1]Cybersecurity and Advanced Platforms Subdivision, Information Systems and Cyber Division
[2]Cyber Assessments and Research Department, Cybersecurity and Advanced Platforms Subdivision

Prepared for:

CCSDS Security Working Group

Approved for public release. OTR 2025-00018.

Abstract

This paper presents a comprehensive approach to securing space systems by integrating multiple Tactics, Techniques, and Procedures (TTP) frameworks (e.g., MITRE ATT&CK®, SPARTA, and SPACE-SHIELD). By leveraging these frameworks in tandem, the paper addresses the cybersecurity challenges across the ground, link, and space segments of space missions, with a focus on tracking TTPs, developing Indicators of Compromise (IOCs), and facilitating intelligence sharing using STIX 2.1. The approach emphasizes the importance of understanding full attack chains and provides methodologies for combining frameworks to enhance risk analysis, testing, countermeasure development, and the automated exchange of cyber threat intelligence (CTI). Additionally, the paper explores how the frameworks can be mapped to regulatory standards like NIST 800-53 and ISO 27001, facilitating compliance while ensuring robust defenses. Practical use cases illustrate how integrating these frameworks supports resilient and secure space systems capable of withstanding evolving threats, and how sharing space-specific IOCs using STIX can enhance collaborative defense across the global space community.

Contents

Figures

Tables

No table of figures entries found.

1 INTRODUCTION

1.1 SCOPE

Space systems are integral to modern global infrastructure, supporting telecommunications, navigation, earth observation, and scientific research. However, they are increasingly becoming targets for cyber threats. A successful cyber-attack on a space system could lead to significant disruptions in global communications, navigation systems, and scientific data collection. This paper analyzes three cybersecurity tactic, technique, and procedure (TTP) frameworks, MITRE ATT&CK®, SPARTA, and SPACE-SHIELD, and offers guidance on their application to space system security. This document applies to the entire space system. Figure 1-1 depicts the main components of a space system. A space system is typically divided into three primary segments: the ground, space, and link segments. The **ground segment** comprises all Earth-based infrastructure responsible for controlling spacecraft, processing data, and maintaining communication with space assets. The ground segment includes mission control centers, ground stations, and network management of spacecraft operations. The **space segment** encompasses the spacecraft, including satellites, space probes, and space stations. This segment handles mission-specific operations such as navigation, communication, and data collection. Finally, the **link segment** is the communication pathways between the ground and space segments. The space segment includes uplinks (from ground to space) and downlinks (from space to ground), which transmit data, commands, and telemetry. Securing all three segments is crucial for the integrity and success of space missions, as vulnerabilities in any one segment could compromise the entire system.

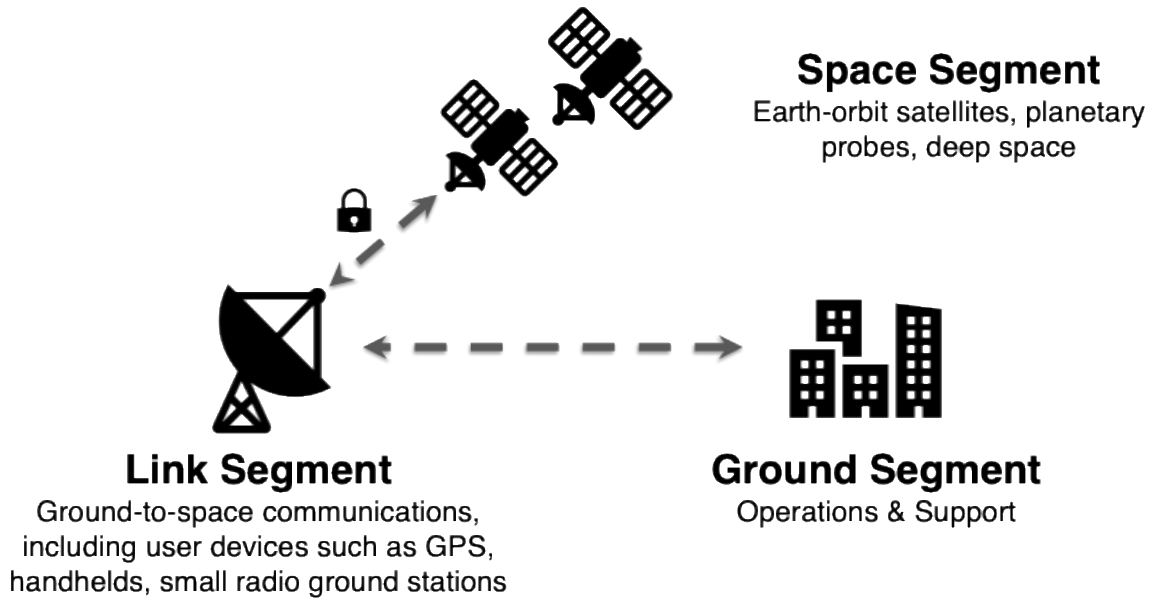


Figure 1-1: Basic Space System Segments

Each of the three cybersecurity frameworks, ATT&CK, SPARTA, and SPACE-SHIELD, addresses different aspects of space system security across the ground, link, and space segments. The ATT&CK framework is particularly relevant to the ground segment, offering guidance on mitigating threats like phishing, lateral movement, and privilege escalation within mission control centers and ground stations. It helps secure the enterprise infrastructure that supports space missions. The SPARTA framework applies to both the link and space segments**,** offering defense mechanisms against threats such as signal jamming, eavesdropping, and command injection attacks, which are critical for maintaining secure

communication channels and protecting the spacecraft from cyber threats. Similarly, the SPACE-SHIELD framework focuses on hybrid cyber and counter-space threats, providing protection strategies across the link and space segments by addressing vulnerabilities in satellite communications and the spacecraft itself. SPACE-SHIELD also emphasizes resilience against cyber intrusions and physical counter-space threats like signal interference and direct satellite attacks. Together, these frameworks provide comprehensive coverage across all three segments of a space system. This paper aims to articulate how these frameworks can help space system engineers and cybersecurity professionals build resilient space systems across the three critical segments: ground, link, and space. Below is a graphic showing where these frameworks apply to a generic space system architecture.

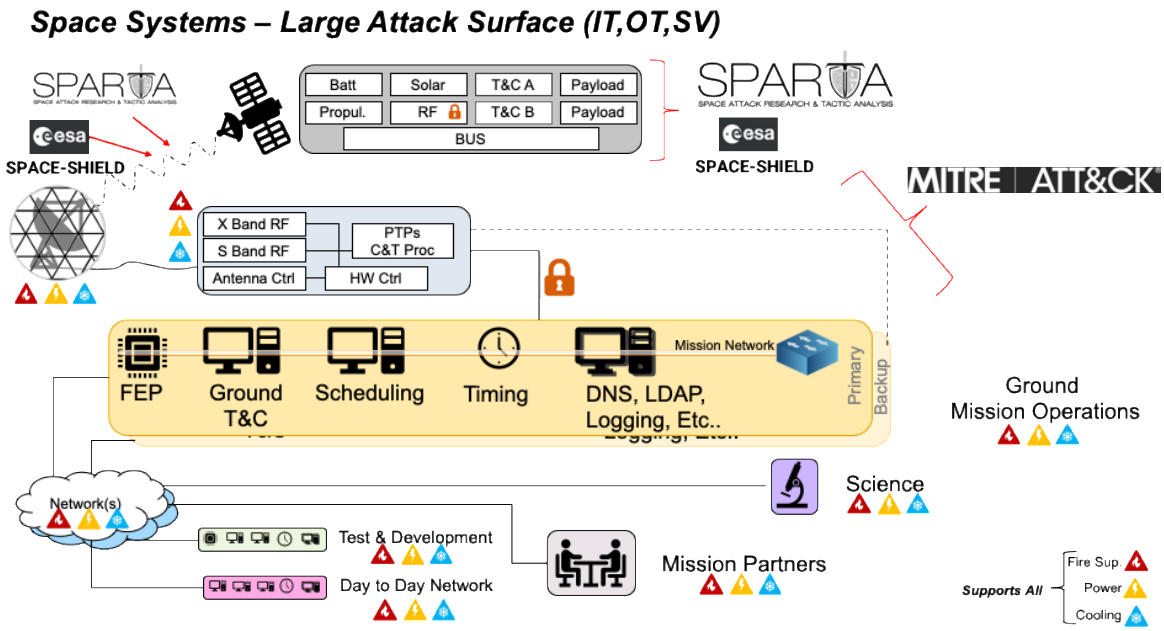


Figure 1-2: Frameworks Application Across the Space Architecture

1.2 PURPOSE AND APPLICABILITY

TTP frameworks are widely adopted within the broader cybersecurity community and are gaining increasing traction within the space industry for various use cases. This paper's objective is to educate space system engineers and cybersecurity professionals on the application of the ATT&CK, SPARTA, and SPACE-SHIELD frameworks, which represent state-of-the-art methods for addressing cyber threats in the space domain and serve as a resource for the generation of a Magenta Book for CCSDS and provide recommended practices for using TTP frameworks for designing secure space systems.

This paper provides structured guidelines to be turned into a CCSDS Magenta Book for incorporating security into the space systems engineering lifecycle, including functional decomposition, threat modeling, and the iterative refinement of security controls. It maps threats from TTP frameworks to specific security controls (such as those in NIST 800-53 and ISO 27001 and/or standards from CCSDS) and provides clear, actionable steps for organizations to enhance their security posture.

Additionally, this paper captures the recommended practices and state-of-the-art methods for addressing space system cybersecurity. It provides guidelines, grounded in consensus, on how to apply these methods and standards in real-world mission environments. These guidelines are intended to assist space system engineers and cybersecurity professionals in navigating the complex security landscape of space missions and provide organizations with an efficient path to securing space systems while meeting regulatory standards. This paper was written using recommended practices like language to enable smother translation into a CCSDS Magenta Book.

This paper will serve as a valuable recommended practice for Mission Planners. It offers a combination of threat modeling, standardized security controls, and community-driven recommended practices to protect future space missions from the evolving cybersecurity landscape. It is intended to serve as practical guidance for space system stakeholders including system engineers, cybersecurity analysts, standards developers, and mission assurance professionals seeking to adopt threat-informed defense strategies grounded in operational reality. It specifically addresses the application of TTPs to spacecraft and space-ground architectures, emphasizing the value of mapping adversary behavior to system-level defensive responses using frameworks like SPARTA, ATT&CK, and SPACE SHIELD.

The applicability of this document extends across the lifecycle of space system development and operations, particularly in contexts where:

- Threat modeling and defensive engineering need to be integrated early in the design process
- Cyber-resilience must be demonstrated in mission assurance documentation
- Cross-segment protections (space, link, and ground) must be evaluated from an adversarial perspective
- Stakeholders require justification for the inclusion of specific countermeasures or mitigations tied to observable behaviors or known threat techniques
- Mission variability, such as short-lifecycle technology demonstrators, long-lived constellations, or national security payloads, introduces diverse design patterns and threat exposures

1.3 RATIOINALE

Integrating security into the systems engineering process for space systems presents numerous challenges that must be addressed to ensure that these systems are functional but also secure and resilient against a wide range of evolving threats. Designing spacecraft that meet stringent security requirements adds significant complexity to an intricate task, requiring a collaborative effort between cybersecurity professionals and systems engineers. This collaboration often encounters barriers due to differences in technical language, priorities, and methodologies. Security experts may focus on risk mitigation and threat prevention, while systems engineers prioritize performance, reliability, and mission success. Bridging these gaps is critical for building space systems that are both secure and operationally effective.

Effective security engineering for space systems requires the integration of security practices throughout the entire system development lifecycle. Security considerations must be incorporated from the initial design phase through manufacturing, launch, operation, and decommissioning. This approach differs from traditional systems engineering, where security is often seen as an afterthought or a supplementary feature. In space systems, security must be woven into the fabric of the system's architecture to address the unique challenges posed by the space environment, such as radiation, extreme temperatures, long mission lifespans, and limited physical access. These environmental constraints further complicate ensuring security, as traditional security solutions may not be directly applicable or require significant adaptation for space-grade applications.

Moreover, the rapidly evolving nature of the threat landscape presents additional challenges. Spacecraft must remain resilient to the current array of threats and those that will emerge over the mission's lifetime. Implementing robust security measures, such as those outlined in mitigation/countermeasure areas of TTP frameworks can help mitigate these threats. However, doing so can introduce cost, schedule, and system performance trade-offs. Incorporating advanced countermeasures such as encryption, secure boot, and intrusion detection and prevention may increase system complexity, potentially affecting mission timelines and budgets. The need for robust security measures can create tension between maintaining a secure system, meeting tight development schedules, or adhering to limited financial resources.

Integrating security into space systems is further complicated by the need to comply with a range of regulatory requirements and industry standards, which may mandate specific security protocols or design principles. These regulations place necessary constraints on the design and development process, but they can also create challenges if security measures are treated as an afterthought rather than a foundational element. Retrofitting security into systems not originally designed with it in mind often proves costly and complex, underscoring the need for a "secure-by-design" approach.

Leveraging TTP frameworks supports this "secure-by-design" philosophy by embedding security considerations from the earliest stages of engineering. These frameworks provide detailed mappings of potential threats, vulnerabilities, and mitigation strategies tailored to space systems, allowing design teams to integrate security elements from the start. This approach helps ensure that security requirements align with mission functionality and regulatory standards while reducing the need for costly retrofits. By building on the structured insights and countermeasures outlined in these frameworks, space systems are equipped to meet security needs proactively, achieving a robust and resilient design from inception.

A comprehensive approach that integrates security as a core component of the systems engineering lifecycle is essential to overcome these challenges. A successful approach involves fostering a culture

prioritizing security and promoting collaboration between systems engineers and cybersecurity experts. Risk-based techniques must be adopted to evaluate and prioritize threats based on their potential impact on the mission, ensuring that limited resources are directed toward mitigating the most critical risks. Furthermore, leveraging established TTP frameworks can provide a structured methodology for integrating security into space systems. These frameworks offer detailed mappings of potential adversarial tactics and countermeasures, enabling engineers to identify relevant threats and design resilient systems against them.

Mission Planners should incorporate security into the systems engineering process, it is essential for ensuring space missions' long-term success and resilience. By treating security as a foundational element of system design rather than an afterthought, Mission Planners can develop more robust, secure, and resilient systems better equipped to face the growing range of cyber and counter-space threats.

1.4 DOCUMENT ORGANIZATION

This document is organized into six main sections and one appendix that collectively guide space system stakeholders in understanding and applying adversary TTP frameworks across the space domain.

- **Section 1** provides introductory material, including document scope, intended audience, definitions, nomenclature, and distinctions between normative and informative content.
- **Section 2** introduces TTP frameworks, ATT&CK, SPARTA, and SPACE-SHIELD, providing rationale for their use, their unique applicability to space mission segments, and foundational concepts such as threat modeling.
- **Section 3** outlines a mission-centric methodology for applying these frameworks across ground, link, and space segments, emphasizing cross-domain threat analysis and pivot-point identification.
- **Section 4** presents practical guidance on translating TTP-informed insights into system requirements, test cases, architectural protections, acquisition artifacts, and red/blue team engagements.
- **Section 5** focuses on cyber threat intelligence (CTI) and information sharing, describing how TTP frameworks improve observability, STIX-based exchange, and cross-mission collaboration.
- **Section 6** discusses future challenges and opportunities, including low-TRL countermeasures, evolving attacker tradecraft, and how the space community can use frameworks to enable proactive defense and inform future standards.

The appendix contains a full list of recommended practices extracted from the body of the document. The following conventions apply for the specifications in this recommended practices document:

a) the words ‘shall’ and ‘must’ imply a binding and verifiable specification;

b) the word ‘should’ implies an optional, but desirable, specification;

c) the word ‘may’ implies an optional specification;

d) the words ‘is’, ‘are’, and ‘will’ imply statements of fact.

Recommended practices will be denoted with stylistic text via ***bold*** and ***italics*** and labeled with unique identifier {section.number}

2 OVERVIEW OF FRAMEWORKS

2.1 TTP FRAMEWORKS

TTP frameworks are powerful tools in cybersecurity designed to help organizations and engineers understand and counteract the behavior of cyber attackers. These frameworks categorize the methods that attackers commonly use to breach systems, exploit vulnerabilities, and disrupt operations. By mapping out these attack methods, TTP frameworks provide a structured way to anticipate threats, identify weaknesses, and implement appropriate defensive measures. The value of TTP frameworks lies in their ability to give cybersecurity teams a clearer picture of how attacks unfold, allowing them to develop proactive strategies to detect, mitigate, and respond to threats before they escalate. They are especially beneficial because they offer a common language for cybersecurity professionals, enabling more effective collaboration and information sharing across teams and organizations. This shared understanding helps improve overall security posture by aligning defense strategies with real-world attack scenarios, ultimately enhancing the resilience of systems against evolving cyber threats.

In 2013, MITRE created the ATT&CK framework to document common TTPs used by adversaries against enterprise networks. While the framework assists organizations in better understanding, visualizing, anticipating, and defending against cyber-attacks, its taxonomy of offense and defense also provides cyber security disciplines, from threat intelligence to network defense, with a common language.

The “new space” evolution, more players, new technology, and a dramatically reduced barrier for entry has only underscored the critical gaps that TTP frameworks serve to address, as all these factors now collide with our modern and substantially adversarial information environment. These gaps range from lapses in harmonization between far-flung catalogs of potential threats and incomplete TTPs to a lack of information dissemination and ways to communicate information in a machine-digestible manner (i.e., STIX-compliant). In the same way that Information Technology and Operational Technology stakeholders have done before, the growing number of space-cyber practitioners from all sectors can learn from the past and use these frameworks to normalize taxonomy, countermeasures, and best practices across the space community.

TTP frameworks are a living capability; they will evolve and advance over time through cyber incidents, community input, and aggregation of unclassified research from academia and Federally Funded Research and Development Centers (FFRDCs. It is essential to understand the nuance of TTP frameworks. ATT&CK focuses on documented incidents from past attacks where SPARTA and SPACE-SHIELD take a view to the “art of the possible” and will include TTPs of potential attack utility, not just observed or likely behavior. This fundamental difference enables a shift from retroactive analysis into proactive analysis for the link and space segment. The space community will be better positioned to understand TTPs, identify associated countermeasures, and defend spacecraft and space missions. The frameworks can also be used to test the efficacy of security solutions in development environments, ground systems, and spacecraft subsystems.

These frameworks are organized around the pre-attack, attack, and post-attack stages: reconnaissance, resource development, initial access, execution, exfiltration, persistence, defense evasion, lateral movement, and impact. Each step lists several techniques and sub-techniques to provide more specific information about the various stages of an attack. It also includes information on the tools and infrastructure that might be used to support an attack.

Tactics: These represent the "why" of a technique or sub-technique the threat actor's tactical goal and the reason they are performing a technique. For example, a threat actor may want to achieve initial access to a spacecraft via cyber means.

Techniques: These 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.

Sub-techniques: These represent a variation or more specific instance of the threat actor's behavior used to achieve a goal. Sub-techniques typically describe behavior at a lower level than a technique and are considered children of the parent technique. For example, a threat actor may compromise mission collaborators (academia, international partners, suppliers, etc.) to achieve their initial access.

Procedures: These represent specific implementations the threat actor uses for techniques or sub-techniques. Procedures are step-by-step descriptions of how the threat actor plans to achieve its purpose. They detail how the general techniques/sub-techniques will be carried out.

Pre-Attack: The Pre-Attack phase includes information about the reconnaissance and resource development activities that attackers typically conduct before launching an attack. Pre-attacks include gathering relevant space system design information, social engineering, malware research/development, and compromising initial infrastructure.

Attack: The Attack phase includes information about the different types of attacks that can be carried out and the tools and techniques that are typically used. For example, these attacks may involve leveraging initial access through a compromised ground station or hosted payload to execute an attack, such as denial-of-service, arbitrary code execution, or data exfiltration.

Post-Attack: Once an attacker has begun an attack, the Post-Attack phase includes information about the persistence, evasion, and movement techniques an attacker may employ. Post-attacks may include compromising memory or installing a backdoor, disabling fault management systems, and/or moving to a new target in a constellation.

Mission Planners should integrate these TTP frameworks into their cybersecurity methodologies to proactively identify the potential threats across all phases of attack chains, enabling a robust defense throughout the entire lifecycle. {2.1.1}

2.2 ATT&CK FRAMEWORK

The MITRE ATT&CK®*{Adversarial Tactics, Techniques and Common Knowledge}* framework is a comprehensive, open-source knowledge base that details adversarial TTPs observed in real-world cyberattacks. Originally developed to aid enterprise security teams in defending their networks, ATT&CK has become an essential tool across multiple domains, including space systems, particularly for safeguarding the ground segment. ATT&CK catalogs the various stages of an attack, from initial access to execution, persistence, privilege escalation, lateral movement, and data exfiltration. It breaks down each stage into techniques that adversaries use to achieve their objectives, such as phishing to gain initial access, leveraging misconfigurations for lateral movement, or using malware to steal sensitive data.

In space systems, ATT&CK is highly applicable to the ground segment, which typically includes mission control centers, data processing facilities, ground stations, and other terrestrial infrastructure responsible for communicating with and managing spacecraft. Since ground stations are often connected to more extensive enterprise networks, they face many of the same threats as traditional IT environments. Cyber adversaries targeting ground stations might exploit vulnerabilities in the network through phishing attacks, malware deployment, or privilege escalation techniques, allowing them to gain control of critical systems, manipulate spacecraft operations, or exfiltrate sensitive mission data.

ATT&CK's structure is helpful for threat modeling and defense planning within these ground segments. For instance, security teams can use ATT&CK to map out potential attack vectors and create a comprehensive view of how a sophisticated adversary might target ground infrastructure. It allows defenders to anticipate possible attack paths and focus on shoring up defenses in areas where the network may be vulnerable. By aligning detection, response, and mitigation strategies with the TTPs documented in ATT&CK, security teams can ensure their defenses are proactive and thorough, protecting mission-critical ground systems from compromise.

Additionally, ATT&CK helps organizations build resilience by identifying gaps in existing security controls and guiding the implementation of new safeguards. For example, ATT&CK might highlight the importance of multi-factor authentication (MFA) to prevent unauthorized access during phishing campaigns or emphasize the need for advanced monitoring and logging systems to detect lateral movement within a network. Ground stations, which play a crucial role in managing and controlling spacecraft, must be protected against such adversarial behaviors to ensure mission continuity and prevent cyber threats from impacting space operations. ATT&CK provides a structured methodology for achieving this, giving space system engineers and cybersecurity professionals a clear framework to understand and defend against adversaries.

2.3 SPACE-SHIELD FRAMEWORK

SPACE-SHIELD *{Space Attacks and Countermeasures Engineering Shield}*, developed by the European Space Agency (ESA), is a comprehensive model designed to protect space systems from cyber and counter-space threats. Recognizing that space systems face a unique and evolving set of risks, SPACE-SHIELD focuses not only on cyberattacks but also on other threats to space infrastructure, such as jamming, spoofing, and kinetic attacks. The framework is explicitly tailored for spaceborne assets like satellites, space stations, and spacecraft, which are increasingly targeted by sophisticated adversaries looking to disrupt or degrade their operations.

SPACE-SHIELD emphasizes the importance of hybrid defense tactics, combining cyber and physical security measures to address the full spectrum of threats that space systems may encounter. On the cyber side, the framework covers potential vulnerabilities in space systems, such as unauthorized access to command-and-control channels, data manipulation, and cyber intrusions that could interfere with a satellite's payload or operational systems. SPACE-SHIELD offers detailed strategies for mitigating these risks, including encryption of communication channels, strong authentication protocols, and onboard intrusion detection and prevention systems to identify and respond to unauthorized activities.

SPACE-SHIELD empowers space system engineers to design and operate more resilient space systems. The framework supports the development of security architectures that proactively protect against a wide range of adversarial tactics, ensuring that space assets can continue to function even under duress. SPACE-SHIELD also encourages continuous monitoring and threat detection, allowing operators to quickly identify and respond to emerging threats before they can cause significant damage, instilling a sense of preparedness and control.

Ultimately, SPACE-SHIELD provides an approach for protecting space infrastructure in an increasingly contested environment. As space systems become more integral to global communications, navigation, and national security, the need for comprehensive protection is not just urgent but a responsibility. By applying the defense tactics outlined in SPACE-SHIELD, space agencies, and operators can better defend their critical assets from both cyber intrusions and counterspace attacks, ensuring mission continuity and the long-term sustainability of space operations.

Mission Planners can apply the defense tactics outlined in SPACE-SHIELD so they can better defend their critical assets from both cyber intrusions and counterspace attacks, ensuring mission continuity and the long-term sustainability of space operations. As space systems become more integral to global communications, navigation, and national security, the need for comprehensive protection is not just urgent but a responsibility.

2.4 SPARTA FRAMEWORK

SPARTA *{Space Attack Research and Tactic Analysis}*, a specialized cybersecurity framework developed by The Aerospace Corporation, is uniquely tailored to address the vulnerabilities of space systems. Unlike traditional cybersecurity frameworks, SPARTA's focus is on space missions, specifically the threats that emerge in the distinct and demanding space environment. It offers a comprehensive analysis of adversarial TTPs that exploit weaknesses in space systems, particularly those in the link and space segments, which are fundamentally different from terrestrial networks.

SPARTA's framework maps out the attack surfaces associated with space assets such as satellites, spacecraft, and communication links, offering detailed insights into potential cyber threats. Spacecraft and satellites are critical infrastructure, performing functions like global communications, Earth observation, scientific research, and national defense. Because these systems operate in a hostile environment and are difficult to access physically, they present unique challenges for cybersecurity. SPARTA addresses these challenges by identifying the specific threats that spacecraft face, such as unauthorized command injections, data spoofing, sensor manipulation, and physical threats like signal jamming or ground station interference. The framework emphasizes protecting the spacecraft's onboard systems and the communication pathways (uplink and downlink) that transmit vital telemetry, command, and control data between the spacecraft and the ground station. While SPARTA provides a broad analysis of space system vulnerabilities, SPACE-SHIELD zeroes in on the specific threats faced by European space assets, ensuring that critical systems remain resilient against both cyber and physical threats.

SPARTA provides the space community with a practical understanding of how adversaries might exploit space system vulnerabilities, particularly through cyber means. For instance, adversaries could target the link segment, which involves communication between ground stations and spacecraft, by launching jamming or spoofing attacks to disrupt or manipulate these signals. The framework also highlights the risks to the space segment, where spacecraft systems could be compromised by cyber intrusions that impact their navigation, control, or payload operations. By cataloging these threats and offering detailed mitigation strategies, SPARTA equips space system engineers with the knowledge to design more resilient spacecraft architectures and communication systems, empowering them to effectively counter potential threats.

Moreover, SPARTA encourages a defense-in-depth approach, recognizing that space systems are part of a larger ecosystem that includes ground infrastructure and communications networks. The framework's threat models go beyond individual attack scenarios and provide broader guidance on

securing complex space missions. SPARTA empowers the space community to develop more robust defenses by identifying the most vulnerable space systems and offering actionable guidance for mitigating those risks. Through SPARTA, engineers gain a clearer picture of adversary behavior in space, enabling them to apply targeted countermeasures that ensure the continued safety and reliability of space assets in an increasingly contested domain.

The SPARTA framework has been designed with an intentional effort to map its techniques and countermeasures to those found within the SPACE-SHIELD framework, ensuring a cohesive and comprehensive approach to securing space systems. SPARTA aims to provide a robust, all-encompassing view of adversarial TTPs affecting space missions across a wide range of scenarios, including cyber and counter-space threats. By mapping SPARTA's techniques to corresponding mitigations and defensive strategies in SPACE-SHIELD, the frameworks create a more unified and interoperable defense model for the space community.

To complement this, SPARTA seeks to be more inclusive by covering a broader range of space cyber threats and defenses, ensuring that the space community at large, beyond just European interests, can benefit from its guidance. Cross-mapping SPARTA to SPACE-SHIELD helps create a consistent set of recommendations across frameworks, ensuring that the defensive measures applied are adaptable and reinforced. Cross-mapping ensures that wherever there is an identified risk in SPACE-SHIELD, SPARTA provides a corresponding or broader set of techniques and mitigations to address the threat effectively. By doing so, SPARTA aims to expand upon the specialized focus of SPACE-SHIELD and provide additional layers of defense, helping space system engineers and operators apply a more comprehensive security approach to their missions.

2.5 APPLICATION OF TTP FRAMEWORKS BY SEGMENT

2.5.1 GROUND SEGMENT

The ground segment of space systems, which includes mission control centers, ground stations, data processing facilities, and supporting infrastructure, is often the most exposed to cyber threats due to its direct connection to space assets and reliance on complex terrestrial networks. These ground systems are critical for controlling spacecraft, managing data flows, and ensuring the smooth operation of space missions. However, their integration with conventional IT networks and reliance on internet-connected infrastructure make them prime targets for cyber adversaries. Attackers often exploit human error, insecure network configurations, inadequate access controls, and poor segmentation within these ground systems to gain access to mission-critical assets.

ATT&CK maps out the specific tactics and techniques used by adversaries in different stages of an attack, providing detailed insights into how threat actors operate. This insight is particularly valuable in the ground segment, where attackers may use phishing to compromise user credentials, lateral movement to traverse networks undetected, privilege escalation to gain higher access levels, and data exfiltration to steal sensitive mission information. By understanding these adversarial behaviors, space system engineers can proactively design defenses that address the most likely points of entry and exploitation within ground infrastructure.

Ground stations face numerous vulnerabilities, ranging from unpatched software and outdated systems to improper network segmentation. These weaknesses can be exploited to gain unauthorized access to spacecraft control systems, allowing adversaries to manipulate satellite operations, disrupt communication links, or corrupt mission-critical data. Additionally, attackers can leverage lateral

movement techniques to expand their foothold within the ground network, compromising the ground station and potentially other connected assets.

To counter these threats, implementing ATT&CK-driven defenses provides a systematic approach to enhancing the security posture of ground systems. By mapping security controls and monitoring tools to specific ATT&CK techniques, space system engineers can better detect, prevent, and respond to potential threats. For example, network segmentation and micro-segmentation can be implemented to limit the ability of attackers to move laterally within the network, while multi-factor authentication and privilege management can help prevent unauthorized access to critical systems. Similarly, real-time monitoring and behavioral analytics, aligned with ATT&CK techniques, can detect unusual activity that may indicate an ongoing attack, allowing for rapid response and containment.

Mission Planners should leverage the ATT&CK framework to identify and mitigate vulnerabilities within the ground segment, space system engineers can create layered defenses that address the most pressing cyber threats to the ground segment.{2.5.1.1} This defense-in-depth approach not only helps to protect ground stations from external attacks but also strengthens the overall resilience of the space mission. As the ground segment serves as the gateway between terrestrial networks and space assets, securing this critical infrastructure is essential to safeguarding space systems from cyberattacks that could jeopardize mission success.

2.5.2 LINK SEGMENT

The link segment of space systems, which encompasses the communication pathways between ground stations and spacecraft, is a critical component that ensures the seamless exchange of telemetry, command, and control data. These communication links are the lifeline that connects mission control to space assets, enabling the execution of vital mission functions, ranging from orbital adjustments to data collection and transmission. However, the link segment is also highly vulnerable to a wide range of threats, including jamming, eavesdropping, message injection, and signal interference, which can disrupt mission operations or compromise the security of transmitted data.

The SPARTA and SPACE-SHIELD frameworks play a pivotal role in providing essential guidance for securing the link segment against these threats. SPARTA and SPACE-SHIELD frameworks can play complementary roles in securing the link segment. They both offer a robust defense-in-depth strategy that addresses both cyber and physical threats that encompasses both technical countermeasures and strategic defense tactics. They both focuses on the technical aspects of securing communication links, emphasizing the need for robust encryption protocols to safeguard the integrity and confidentiality of data as it traverses the link. They both also advocates for the use of redundancy in communication pathways, ensuring that alternative channels are available if primary links are disrupted by interference or physical attacks. This approach helps to ensure that space systems can maintain operational continuity even in the face of targeted attacks on their communication links.

In addition to encryption and redundancy, SPARTA and SPACE-SHIELD highlights the importance of securing command and control channels from message injection attacks, where an adversary might insert unauthorized or malicious commands into the communication stream. To counter this, the frameworks recommend rigorous authentication protocols and integrity checks, which help to verify the authenticity of commands and prevent tampering with transmitted data.

SPACE-SHIELD and SPARTA also outline strategies for implementing real-time monitoring systems to detect signal strength or pattern anomalies, allowing for rapid identification of potential attacks. By incorporating frequency hopping and spread spectrum technologies, these frameworks focus on

mitigating the impact of attacks, ensuring that communication links remain resilient even when under attack. These strategies are critical for maintaining secure and reliable communications, especially in contested environments where adversaries may actively seek to degrade or disrupt satellite operations.

Both frameworks emphasize the importance of proactive defense measures to protect the link segment. For example, eavesdropping, where adversaries intercept sensitive communication data, can be mitigated through advanced encryption techniques that ensure data remains confidential even if intercepted. Similarly, message injection attacks can be thwarted using secure cryptographic protocols that validate the integrity of commands and prevent unauthorized actors from influencing spacecraft operations. The urgency and necessity of these actions cannot be overstated.

Mission Planners should integrate SPARTA & SPACE-SHIELD into the link segment as links are critical to the success of space missions, securing this essential for ensuring mission integrity, safeguarding sensitive data, and maintaining continuous control over space assets {2.5.2.1}. Implementation of encryption, authentication, redundancy, and signal interference detection ensures that the communication links between ground stations and spacecraft are secure and reliable, even in the face of persistent attacks. As these links are critical to the success of space missions, securing the link segment is essential for ensuring mission integrity, safeguarding sensitive data, and maintaining continuous control over space assets.

2.5.3 SPACE SEGMENT

In the space segment, spacecraft and their subsystems are subject to a distinct and highly sophisticated array of threats beyond traditional cyber intrusions. These threats include cyberattacks, such as malware injections, unauthorized command execution, and exploitation of software vulnerabilities, but also signal jamming, eavesdropping, and advanced counter space tactics aimed at disabling, disrupting, or manipulating spacecraft operations. Adversaries may seek to interfere with satellite communications, tamper with onboard systems, or even hijack spacecraft controls, leading to potential mission failure or loss of critical assets. As spacecraft operate in remote and hostile environments, the security challenges are amplified by the lack of physical access for immediate remediation, the limited processing power available for security tools, and the extended mission durations that leave them vulnerable to long-term persistent threats.

The SPARTA and SPACE-SHIELD frameworks recognize the unique security challenges of the space segment and emphasize defense-in-depth strategies. Both frameworks advocate for a multilayered approach to security, ensuring that even if one defensive layer is breached, additional safeguards remain to protect mission-critical systems. One of the foundational defenses recommended by these frameworks is the implementation of encryption for both telemetry and telecommand links. Encryption plays a crucial role in securing the spacecraft's communication pathways, ensuring that the data transmitted between the spacecraft and ground stations remains confidential and protected from interception or manipulation by adversaries attempting to eavesdrop or inject malicious commands.

In addition to encryption, secure boot mechanisms are vital for safeguarding spacecraft from unauthorized software or firmware modifications. A secure boot ensures that only trusted and authenticated code can be executed during the spacecraft’s startup process, preventing attackers from introducing malicious code that could compromise onboard systems. Secure boot plays a crucial role in preventing unauthorized access to spacecraft controls, coupled with software hardening, which involves fortifying the spacecraft’s software against exploitation by reducing vulnerabilities and limiting the attack surface.

Further strengthening spacecraft security, SPARTA and SPACE-SHIELD advocate for using intrusion detection and prevention systems (IDPS) specifically adapted for the space environment. These systems play a crucial role in real-time threat detection, continuously monitoring spacecraft operations and scanning for irregularities, unauthorized actions, or abnormal behavior that could indicate a cyber intrusion or system manipulation. For example, IDPS may detect deviations from expected operational parameters, such as sudden changes in spacecraft orientation or unexpected thruster activations, which could signal an attack on the spacecraft's attitude control system. By detecting these attacks in real-time, IDPS allows space operators to respond swiftly to potential threats, initiating corrective actions to mitigate the impact of an attack before it compromises the mission.

Redundancy and fault-tolerant architectures are also essential components of the defense-in-depth strategy recommended by SPARTA and SPACE-SHIELD. Redundancy ensures that critical subsystems, such as power, propulsion, and communications, have backup systems that can take over if the primary system is compromised or disabled. This resilience helps maintain spacecraft operations even under duress, preventing a single point of failure from leading to mission loss.

By combining these advanced security measures, such as encryption, secure boot, software hardening, IDPS, and redundancy, SPARTA and SPACE-SHIELD provide comprehensive frameworks for securing the space segment. These are a few example strategies that collectively ensure that spacecraft remain protected against various threats, from cyber intrusions to counterspace tactics, allowing for sustained and secure mission operations even in contested and high-risk environments. The frameworks have many more countermeasures mentioned, and they leverage threats to drive countermeasure selection. ***Mission Planners should integrate SPARTA and SPACE-SHIELD into the space segment, as the spaceborne components are central to mission execution, onboard autonomy, and data integrity {2.5.3.1}.*** Protecting the space segment is essential for ensuring the trusted operation of command and data handling, payload execution, and cross-subsystem communication. Implementation of secure boot, onboard anomaly detection, authentication of commands, data integrity validation, and isolation between subsystems helps ensure resilience against cyber threats that could degrade, disrupt, or destroy spacecraft functionality. The following sections will demonstrate an example of how to apply these frameworks.

2.6 THREAT MODELING WITH TTP FRAMEWORKS MODELING WITH TTP FRAMEWORKS

This section introduces the term and concept of threat modeling to provide essential context for its use throughout this document. Threat modeling is a structured process for identifying, analyzing, and prioritizing potential threats to a system. It enables mission planners, engineers, and cybersecurity professionals to understand how an adversary might exploit specific system elements and guides the development of mitigations aligned with real-world attack behaviors. In the space domain, threat modeling supports the design of more resilient architectures by exposing how attack chains could traverse the ground, link, and space segments. In this context, TTP techniques represent the behaviors an adversary may employ once system access is achieved or a vulnerability is exploited. Rather than focusing solely on who the threat actor is (e.g., an insider or nation-state), TTP frameworks emphasize what the adversary does. Techniques serve as the atomic unit of adversarial behavior, allowing teams to construct realistic attack scenarios, connect behaviors to vulnerable components, and derive targeted countermeasures and test cases. They effectively bridge the gap between abstract threat sources and concrete system weaknesses, enabling a more structured and actionable threat model.

TTP-based threat modeling differs from generic cybersecurity assessments by aligning risks with specific tactics, techniques, and procedures, whether observed (as in ATT&CK) or hypothesized (as in

SPARTA and SPACE-SHIELD). Instead of simply identifying vulnerabilities, this approach allows engineers to:

- Map mission-critical components and interfaces to likely adversary behaviors (e.g., Initial Access, Execution, Lateral Movement, Impact).
- Simulate multi-stage attack chains across ground, link, and space segments.
- Identify subsystems or data flows that are most exposed based on trust boundaries, architecture, or known design limitations.
- Select mitigations that directly address the techniques being modeled, improving precision in defensive design.

Each TTP framework offers a unique lens into the modeling process which also helps identify pivot points which are locations where an adversary could move laterally or escalate privileges between segments (e.g., from a compromised ground system to spacecraft command channels). Engineers can use this insight to break attack chains by applying security controls at high-leverage locations.

Ultimately, TTP-informed threat modeling shifts teams from reactive security postures to proactive defense engineering. It enables system designers to anticipate adversarial behaviors, validate protections against realistic threats, and trace security requirements back to known capabilities. This alignment also strengthens assurance arguments and supports downstream testing, simulation, and red/blue teaming exercises.

As the threat landscape for space systems grows increasingly contested, threat modeling with TTP frameworks becomes both a strategic planning tool and a tactical guide. It supports early identification of architectural weaknesses, reinforces security-by-design principles, and ensures traceability between threats, defenses, and validation efforts. Subsequent sections in this document reference threat modeling as a foundational activity in test planning, requirements derivation, red teaming, and compliance evaluation.

3 INTEGRATING TWO FRAMEWORKS (SPARTA AND ATT&CK)

It is evident that space missions often require an integrated approach that leverages multiple TTP frameworks to fully address the security challenges across all segments: ground, link, and space. In the examples provided, we saw how frameworks like MITRE ATT&CK® and SPARTA were applied to secure different parts of a satellite constellation and a deep-space mission, each addressing threats specific to its domain.

There are instances where it is necessary to combine two TTP frameworks to fully understand the end-to-end risks and attack chains present in complex space systems. As described in section **Error! R eference source not found.**, combining multiple frameworks allow for a more comprehensive analysis of attack vectors and the associated defensive strategies across interconnected systems.

This approach becomes particularly relevant when examining complete attack chains that may start with a ground system breach and extend to spacecraft manipulation through pivot points like communication links. By combining ATT&CK's focus on enterprise threats and SPARTA's emphasis on space-specific tactics, security teams can develop a holistic view of adversary behavior and better protect their systems from end-to-end threats. This integrated methodology enhances detection and mitigation efforts and ensures that all potential attack paths are accounted for, leading to more resilient and secure space missions. MITRE introduced this methodology in their Platform Independent Vectors of Techniques (PIVOT) paper.

The following section explores how this combined approach can be applied in practice, leveraging the strengths of both SPARTA and MITRE ATT&CK® to develop comprehensive attack chains that reflect the realities of interconnected space systems. This methodology allows for thorough risk analysis, testing, and countermeasure development, ensuring that space missions are equipped to withstand threats across multiple domains. ***Mission Planners should adopt an integrated methodology that combines frameworks (e.g., MITRE ATT&CK® and SPARTA) to analyze end-to-end attack chains across ground, link, and space segments, enabling threat identification, cross-domain mapping, and countermeasure testing to ensure resilient mission defenses {3.1}.***

3.1 A MULTI-DOMAIN ATTACK CHAIN METHODOLOGY

This integrated approach functions similarly to MITRE's PIVOT methodology, which connects threat tactics and techniques across domains to evaluate adversarial movement and system vulnerabilities. For space systems, a similar methodology should be applied to connect enterprise threat models like MITRE ATT&CK® to space-specific frameworks like SPARTA and SPACE-SHIELD. The focus of this methodology is to identify pivot points and interfaces where adversaries may move from terrestrial infrastructure into spacecraft systems.

To operationalize this method, the following process should be followed:

Step 1: Mission and System Decomposition:

- ***Mission architects should decompose the end-to-end mission architecture to identify critical assets in the ground, link, and space segments {3.1.1}.***
- ***Mission decomposition should include identification of key ground stations, communication relays, cross-links, and spacecraft subsystems such as command and data handling, attitude control, propulsion, and payload interfaces {3.1.2}.***
- ***Mission planners should document trust boundaries and identify where authentication, authorization, and encryption are applied or missing. {3.1.3}.***

Step 2: Identify Pivot Points:

- ***Mission architects should identify pivot points where an adversary could move laterally or vertically from one segment to another (e.g., from a compromised mission operations center to a command uplink) {3.1.4}.***
    - Examples of pivot points that to be assessed include protocol translators, RF interface demodulators, and time-synchronized command queues.
- ***Mission architects should model potential pivot points using threat-informed architecture diagrams or system dependency matrices. These matrices can help visualize how systems rely on one another across segments, revealing critical interfaces where added protections may be required {3.1.5}.***

Step 3: Map Attack Paths Across Segments:

- ***Mission architects should map threat actor behaviors using ATT&CK for enterprise and SPARTA for space-specific TTPs, connecting multi-segment attack chains {3.1.6}.*** This map of behaviors should support mission risk assessments by illustrating

how threat techniques can traverse technical boundaries and impact mission-critical functions.

  - A hybrid TTP map should illustrate how an adversary could progress through initial access (e.g., spear phishing on the ground), escalate privileges (e.g., lateral movement to C2 servers), and transition to the space segment (e.g., unauthorized command injection).

- ***Mission architects should use the map to identify which components are most exposed to adversarial behaviors and evaluate whether existing countermeasures/protections are sufficient {3.1.7}.***

  - The mapping is meant to facilitate the identification of security gaps across mission segments, particularly at integration points like data links, control paths, and command interfaces, where threat techniques may propagate if not properly mitigated. This process enables mission stakeholders to prioritize protections based on functional dependencies and potential mission impact.

Step 4: Simulate and Test Countermeasures:

- ***Engineers and cybersecurity analysts should simulate realistic attack scenarios informed by the mapped TTPs and identified pivot points to enhance test and evaluation coverage {3.1.8}.***

  - Traditional verification and validation efforts often focus on nominal behavior and functional correctness; however, the threat techniques identified through TTP frameworks offer critical insight into how adversaries may intentionally abuse or subvert system behavior. These techniques should be used to design threat-informed test cases that simulate adversarial actions across both ground and space segments.

- ***During the test planning phase, teams should augment standard test procedures with abuse cases that reflect how adversaries may exploit system interfaces, manipulate data flows, or misuse protocol behaviors especially across pivot points like uplinks, buses, or software interfaces {3.1.9}.***

  - For example, if a SPARTA technique involves signal injection or unauthorized command sequences via RF uplinks, test engineers should construct scenarios that emulate these conditions to validate the effectiveness of authentication, filtering, and anomaly detection mechanisms.

- ***TTP informed abuse scenarios should be executed during formal system integration testing, hardware-in-the-loop (HIL) environments, cyber ranges, or simulation-based campaigns, where feasible, to evaluate how well the system resists or recovers from such attacks {3.1.10}.***

  - Threat-informed testing not only uncovers vulnerabilities missed by traditional functional testing but also helps quantify the system's resilience under realistic adversarial conditions. The result is a more comprehensive security validation process that maps directly to known threat behaviors, mission risk, and protection effectiveness. The effectiveness of countermeasures / protection

techniques (e.g., secure boot, anomaly detection, encryption, interface hardening) will be evaluated based on these test scenarios.

- ***Results from TTP informed abuse scenarios and simulations should drive iterative design refinement and inform the early selection and tailoring of protection techniques and countermeasures {3.1.11}.***

    - By integrating threat-informed feedback into the engineering lifecycle, design teams can evaluate whether existing controls (e.g., authentication protocols, anomaly detection algorithms, redundancy mechanisms) are sufficient or require augmentation. Rather than waiting for operational anomalies or post-deployment incidents, early validation through adversary-driven testing enables proactive adjustments. This continuous feedback loop ensures that protection techniques are not just implemented but verified under the conditions they are meant to withstand, strengthening the overall system posture before deployment.

Step 5: Break the Attack Chain:

- ***Based on threat analysis and test results, mission architects should identify and prioritize protection opportunities at locations critical to mission assurance, including components that enable adversary escalation, impact mission success, or connect distinct trust domains {3.1.12}.***

    - These may include pivot points, critical software services, centralized control functions, or subsystems that aggregate or distribute commands and data.

- ***Mission architects deployment of defenses should be positioned to break the attack chain where adversaries can cause the most damage or gain the most leverage {3.1.13}.***

By connecting the dots between TTP frameworks (e.g. MITRE ATT&CK® and SPARTA), space system engineers can develop a comprehensive picture of how adversaries might exploit weaknesses across the ground and space segments. This multi-domain approach provides a clearer understanding of a cyberattacks full lifecycle, from the initial compromise of ground-based systems to the final manipulation of space assets.

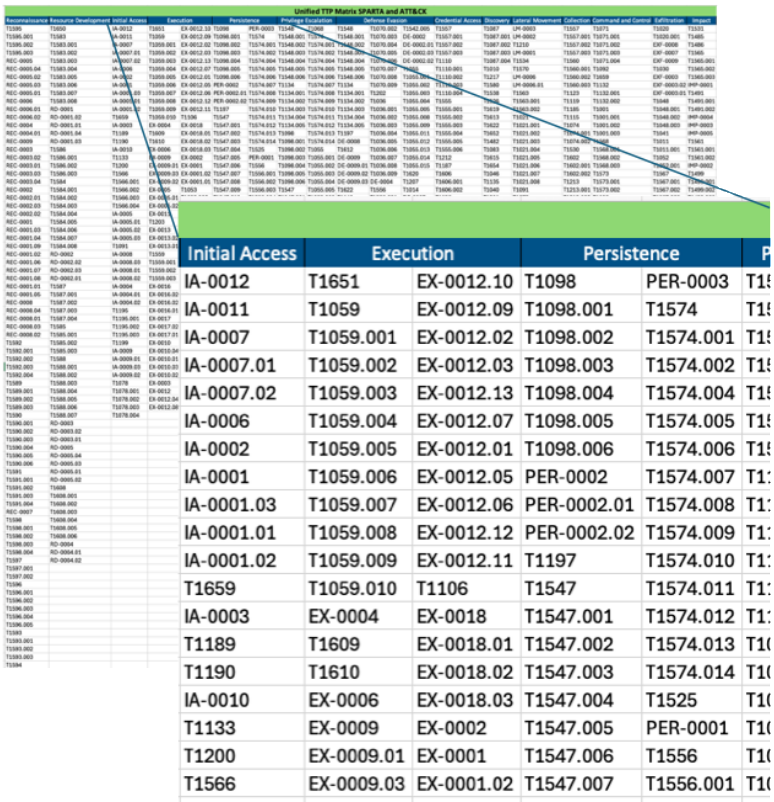
The value of this approach lies in its ability to ensure that security efforts are not siloed but integrated across the entire mission architecture. It allows for more robust risk analysis, highlighting vulnerabilities that may not be evident when focusing solely on a single domain. Moreover, the ability to test and validate various countermeasures against specific TTPs, both on the ground and in space, enables organizations to refine their defenses in a systematic and informed manner.

In essence, combining SPARTA and MITRE ATT&CK® creates a comprehensive attack chain framework that enhances the effectiveness of cybersecurity assessments for space systems. This integrated methodology offers a 'force multiplier effect ', a concept from military strategy that refers to a factor that significantly increases the effectiveness of a strategy or action. In the context of cybersecurity, this means that the methodology significantly improves the overall mission resilience by identifying critical attack paths and reinforcing defenses across interconnected ground and space domains.

Since SPARTA, SPACE-SHIELD, and MITRE ATT&CK® share common tactics across the top row of their frameworks but have domain-specific techniques beneath them, there is an opportunity to create a unified TTP matrix that consolidates all the techniques into a single view. This unified matrix would comprehensively visualize adversarial behaviors across the ground, link, and space segments, enabling security teams to map out how adversaries could pivot between domains using similar tactics but different techniques. This approach builds on the PIVOT concept, where threats originating in one domain, such as the ground segment, can move laterally to other domains, such as spacecraft, through key pivot points like communication links.

This unified TTP matrix provides organizations with a strategic advantage, allowing them to visualize the full attack chain across interconnected systems. It offers a clearer understanding of how tactics and techniques are leveraged across multiple domains, empowering security teams with valuable insights into which attack vectors are most frequently used or pose the most significant risk. By aggregating this data, security teams can prioritize defensive efforts in the most critical areas, identify potential gaps in their coverage, and ensure that their countermeasures are robust across the entire system.

This aggregated view significantly enhances risk analysis by allowing security teams to see all relevant techniques in one place. It empowers them to make more informed decisions about where to focus resources and improve defenses. Furthermore, by identifying high-risk tactics and techniques through the matrix, security professionals can tailor their testing, evaluation, and mitigation strategies, ensuring that all parts of the space system are adequately protected from cyber and counter-space threats. This unified approach improves visibility into adversarial behaviors and strengthens the overall resilience of space missions by addressing threats holistically across interconnected domains. Below is an example of a unified matrix using only ATT&CK and SPARTA, but you could add other frameworks like SPACE-SHIELD if desired.



Initial Access	Execution		Persistence		P
IA-0012	T1651	EX-0012.10	T1098	PER-0003	T1
IA-0011	T1059	EX-0012.09	T1098.001	T1574	T1
IA-0007	T1059.001	EX-0012.02	T1098.002	T1574.001	T1
IA-0007.01	T1059.002	EX-0012.03	T1098.003	T1574.002	T1
IA-0007.02	T1059.003	EX-0012.13	T1098.004	T1574.004	T1
IA-0006	T1059.004	EX-0012.07	T1098.005	T1574.005	T1
IA-0002	T1059.005	EX-0012.01	T1098.006	T1574.006	T1
IA-0001	T1059.006	EX-0012.05	PER-0002	T1574.007	T1
IA-0001.03	T1059.007	EX-0012.06	PER-0002.01	T1574.008	T1
IA-0001.01	T1059.008	EX-0012.12	PER-0002.02	T1574.009	T1
IA-0001.02	T1059.009	EX-0012.11	T1197	T1574.010	T1
T1659	T1059.010	T1106	T1547	T1574.011	T1
IA-0003	EX-0004	EX-0018	T1547.001	T1574.012	T1
T1189	T1609	EX-0018.01	T1547.002	T1574.013	T1
T1190	T1610	EX-0018.02	T1547.003	T1574.014	T1
IA-0010	EX-0006	EX-0018.03	T1547.004	T1525	T1
T1133	EX-0009	EX-0002	T1547.005	PER-0001	T1
T1200	EX-0009.01	EX-0001	T1547.006	T1556	T1
T1566	EX-0009.03	EX-0001.02	T1547.007	T1556.001	T1

Figure 3-1: Unified TTP Matrix (ATT&CK and SPARTA)

4 FRAMEWORK INTEGRATION FOR SECURE SPACE ENGINEERING

4.1 POLICY GUIDANCE

As space systems grow more complex and the cyber threat landscape evolves globally, policy makers must develop guidance rooted in threat-informed intelligence to secure military, governmental, and commercial space assets against sophisticated adversaries. TTP frameworks play a pivotal role in this process by providing a realistic and structured method for identifying risks to space systems. ***Policy makers should use TTP frameworks to identify, prioritize, and map cyber threats to appropriate mitigations and system-level requirements across all space system segments {4.1.1}.*** While TTPs themselves are valuable for understanding adversarial behavior, they primarily serve as a foundation for a larger risk assessment process that informs mitigations, security controls, and ultimately, requirements which are the true drivers of policy.

TTP frameworks enable policy makers to conduct more accurate risk assessments by cataloging adversarial TTPs that present real threats to space systems. These frameworks offer structured methods for understanding and mitigating threats, ensuring that cybersecurity policies like CNSSP 12 (U.S.), FISMA (U.S.), the NIST 800 series (U.S.), European Space Policy, the EU Cybersecurity Act, and ISO/IEC 27000 series are translated into effective protections across all segments of space systems: ground, link, and space. ***Risk assessments informed by TTP frameworks should be used to derive specific mitigations and security controls that are traceable to policy objectives and adversarial behaviors {4.1.2}.*** It is these requirements, derived from threat-informed analysis, that form the backbone of effective cybersecurity policy. Thus, TTPs are an intermediary step that offers a realistic method to pinpoint risks but are most valuable when they drive the creation of specific security controls and requirements that dictate how systems should be protected.

By using these TTP frameworks as an input, policy makers can ensure that their policies address the full range of adversarial behaviors specific to space missions. SPARTA, with its focus on space-specific TTPs, enables policy makers to identify and prioritize threats that are unique to the spaceborne environment then link these threats to specific mitigation strategies. This process helps inform the development of tailored requirements that align with policy objectives, ensuring that policies are both relevant and actionable for space missions. Policy makers should view TTP frameworks not just as threat catalogs, but as implementation tools. These frameworks make it possible to define mission-specific mitigations and protections in alignment with high-level policy goals. They also support ongoing assurance activities by enabling threat-informed assessments, audits, and design reviews.

4.1.1 INTEGRATING FRAMEWORKS WITH CNSSP 12, FISMA, NIST 800 SERIES, EUROPEAN SPACE POLICY, AND ISO 27000

While policy directives such as CNSSP 12, FISMA, the NIST 800 series, the EU Cybersecurity Act, and ISO/IEC 27000 establish critical cybersecurity goals, the challenge often lies in translating their abstract requirements into concrete technical actions. TTP frameworks provide a foundation to operationalize these policies by offering a structured, threat-informed knowledge base that maps known adversarial behaviors to mitigations, controls, and engineering-level protections.

Policy documents frequently reference the need to protect against threats, maintain availability, enforce access control, and ensure integrity yet they do not specify how these objectives should be implemented within a space mission context. TTP frameworks can help fill this gap by functioning as a shared lexicon and baseline reference. They enable system engineers, cyber professionals, and mission planners to

interpret policy requirements in light of real-world threats, linking them to specific techniques and mitigations that can be embedded into system architectures.

Mission planners should trace high-level policy directives and associated threat concerns to relevant TTP frameworks, and from there derive mitigations and engineering requirements, ensuring threat-informed implementation that aligns with policy intent {4.1.1.1} For example, mission planners should align NIST SP 800-53 or ISO 27000 series control implementations with TTP techniques to ensure relevance to space systems.

> Policy → Threat/Risk Reduction (from policy) → TTP → Mitigations → System Requirements

Policy directives like the Committee on National Security Systems Policy No. 12 (CNSSP 12), which mandates cybersecurity for National Security Space Systems, can be operationalized by mapping their requirements to threat techniques documented in SPARTA and ATT&CK. This threat-informed approach ensures that CNSSP 12-compliant policies are not just theoretically robust but also grounded in actual adversarial behaviors which provides specific, actionable guidance for protecting mission-critical space assets such as satellites, command links, and ground interfaces.

In Europe, the European Space Policy and the EU Cybersecurity Act emphasize the need for high levels of cybersecurity across the European Union's space assets. These TTP frameworks can provide the basis for threat-informed policies that meet the requirements of the EU Cybersecurity Certification Framework while ensuring that European space missions are secure against adversarial tactics targeting both ground and space infrastructure.

The Federal Information Security Management Act (FISMA) in the U.S. mandates federal agencies to implement robust information security programs. FISMA's emphasis on risk-based decision-making aligns well with the structured threat catalogs provided by SPARTA and ATT&CK. By integrating these frameworks into FISMA's risk management processes, policy makers can ensure that security programs are not only compliant but also reflective of real adversarial threats.

The NIST 800 series, particularly NIST SP 800-53, outlines the security controls necessary to protect federal systems. While these controls are broad, frameworks like SPARTA and ATT&CK offer detailed mappings that allow organizations to apply NIST controls in a threat-informed context. For instance, NIST SP 800-53 Control AC-6 (Least Privilege) can be directly mapped to ATT&CK techniques related to privilege escalation, providing clear guidance on how this control should be applied to space systems.

Similarly, the ISO/IEC 27000 series, which outlines internationally recognized standards for information security management systems, can be reinforced by SPARTA and ATT&CK. The frameworks allow for the customization of ISO 27000 controls to address specific threats in space missions, ensuring that space system operators comply with international standards while maintaining a high level of security against cyber threats.

A key challenge when adhering to policy is ensuring that high-level directives from policies such as CNSSP 12, FISMA, the NIST 800 series, European Space Policy, and ISO 27000 are effectively translated into practice. TTP frameworks can play a role in bridging this gap by providing a detailed taxonomy of threats and behaviors that can be mapped to specific security controls and operational procedures.

Using TTP frameworks to inform and support policies, ensures space agencies can remain proactive with their security measures and adaptable. Policy makers may want to go as far as updating policies

to encourage, or even mandate, the use of TTP frameworks to ensure consistent, threat-informed protection across all space segments, as the cybersecurity landscape for space systems continues to develop.

4.1.2 FUTURE POLICY DEVELOPMENT: BUILDING ADAPTIVE POLICIES

As space cybersecurity continues to evolve, policy development must remain flexible and adaptive to new threats. Threat-informed TTP frameworks provide an evolving foundation for updating policies to reflect the latest adversarial tactics. By embedding these frameworks into the policy development process, policy makers across the globe can ensure that their directives remain relevant, actionable, and effective as the threat landscape changes.

Policy makers should incorporate references to evolving TTP frameworks within cybersecurity policy to ensure that the implementation of controls remains aligned with current adversary behavior {4.1.2.1}. This approach reduces the risk of policy becoming outdated or ineffective due to the rapid evolution of cyber threats.

Where appropriate, policies may mandate the use of TTP frameworks as a baseline for risk assessment and mitigation planning across all space system segments {4.1.2.2}. Mandating their use ensures consistent, threat-informed protections that remain responsive to the dynamic space domain.

The responsibility not only falls on the policy makers, but ***mission planners should continuously assess policy relevance in light of emerging threats and evolving TTP data {4.1.2.3}.*** Doing so ensures that policy-driven security measures remain effective and proactive, rather than reactive, and that mission assurance objectives are not compromised by outdated guidance. ***Mission planners and system implementers should also establish a feedback loop to inform policy makers when operational insights or threat evolutions expose policy gaps or misalignments {4.1.2.4}.*** This feedback mechanism enables continuous policy refinement and ensures that high-level directives remain synchronized with on-the-ground realities and adversary behavior trends.

4.2 THREAT INFORMED ENGINEERING PRACTICES

To effectively integrate TTP frameworks into systems engineering, engineers should adopt a comprehensive, layered approach that addresses threats across all segments of space systems: ground, link, and space.

Engineering teams should leverage existing criticality analyses, often conducted as part of mission assurance or system design reviews, as the foundation for integrating TTP frameworks {4.2.1}. These crown jewel assessments, which identify mission-essential functions and systems across the ground, link, and space segments, provide a natural starting point for aligning cybersecurity protections with mission priorities. The functional decomposition approach involves breaking each segment into its essential functions and identifying the critical assets, often called “crown jewels”, vital to the mission’s success. For example, in the ground segment, mission control systems and data processing centers may be identified as critical assets, while in the link segment, the communication channels and encryption systems are considered paramount. The space segment’s critical assets could include the spacecraft’s attitude control systems, propulsion controls, and data storage.

Following criticality analysis, engineering teams should apply the appropriate TTP frameworks to conduct threat modeling against the mission critical components and functions {4.2.2}. The threat model involves using the relevant cybersecurity framework to identify potential adversarial TTPs that could be used against these critical assets. As mentioned in previous sections 1 and 3, for the ground segment, ATT&CK provides a detailed mapping of cyber threats such as unauthorized access, malware

execution, and data exfiltration. Meanwhile, SPARTA and SPACE-SHIELD frameworks are employed for the space and link segments to map threats such as signal jamming, data spoofing, or unauthorized command injection. The threat modeling phase helps engineers understand how adversaries might target specific functionalities within the system, identifying potential vulnerabilities and weak points that require mitigation. This threat modeling should not occur in isolation. ***Cross-functional teams should collaboratively assess attack vectors across segments to ensure a complete understanding of interdependencies {4.2.3}.***

The next step involves correlating the identified techniques or attacks with the appropriate defensive measures, which are also outlined within these frameworks. ***Engineers should prioritize threat-to-defense alignment by first identifying adversarial techniques from the frameworks, then selecting appropriate mitigations based on system-specific risk profiles {4.2.4}.*** For instance, if the threat model identifies jamming as a significant concern in the link segment, SPARTA or SPACE-SHIELD could guide the selection of countermeasures such as anti-jamming technologies or communication redundancy. Similarly, if the threat model highlights lateral movement as a risk in the ground segment, ATT&CK would help map defensive techniques like network segmentation or privilege access management.

To ensure coverage across all vectors, segment-specific teams should collaboratively align their defensive measures to ensure consistent implementation and eliminate seams in protection {4.2.5}. One key aspect of this integration is ensuring collaboration between teams responsible for different segments. Ground station teams should align their defenses using ATT&CK, while spacecraft teams focus on implementing SPARTA and SPACE-SHIELD measures to protect the satellite or spacecraft. By ensuring consistent security protocols and threat awareness across teams, space systems can be protected more effectively from end to end.

Mission planners and system engineers should use this structured, threat-informed engineering process, from criticality analysis to defense mapping, to develop tailored cybersecurity architectures that align protection measures with mission priorities {4.2.6}. Mission planners should incorporate outputs from this process into requirements traceability matrices, ensuring that each identified threat technique has a corresponding and verifiable mitigation or design control {4.2.7}. Below is a graphic of this process.

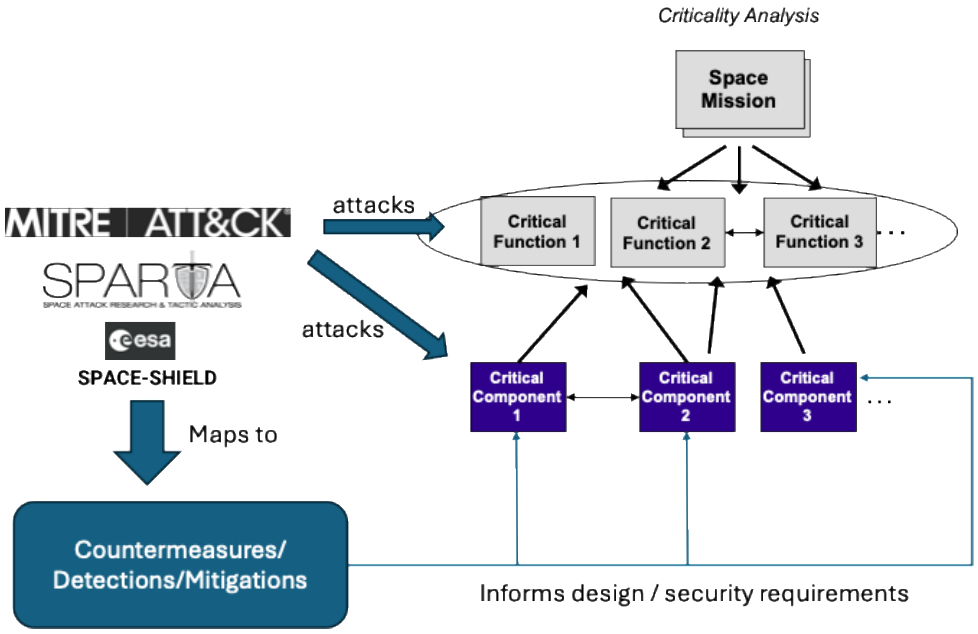


Figure 4-1: Informing Design Based on TTPs

4.2.1 OPERATIONALIZING SECURE-BY-DESIGN WITH TTP FRAMEWORKS

Engineers should adopt a secure-by-design approach that incorporates threat-informed insights from the earliest stages of system development, rather than relying on reactive controls applied late in the lifecycle {4.2.1.1}. This methodology is particularly critical for "new space" missions where rapid development cycles and high mission diversity create both opportunity and risk. ***New space programs and commercial entrants in particular should leverage decades of security research and lessons learned across aerospace and adjacent industries to rapidly mature their security while avoiding legacy technical debt. Engineering teams should align secure-by-design objectives with TTP-based threat modeling outputs to ensure protections are functionally relevant, risk-aligned, and segment-specific from the outset to avoid costly post-deployment mitigation {4.2.1.2}. Where feasible, teams should adopt a layered defense strategy that applies multiple protection techniques to mitigate single-point failure from any one control/defense {4.2.1.3}.***

This design paradigm is consistent with established secure-by-design best practices published by NIST 800-160 (Vols. 1 and 2), Cybersecurity and Infrastructure Security Agency (CISA)'s Secure-by-Design guidance, and UK's National Cyber Security Centre, all of which promote embedding cybersecurity throughout the engineering lifecycle. Despite its value, secure-by-design guidance often lacks concrete implementation techniques specific to the space domain.

Mission planners and systems engineers often struggle to determine the appropriate level of abstraction, depth of protections, and scope of application when implementing secure-by-design across diverse space missions. TTP frameworks provide the missing implementation layer by enabling system architects to tie protection techniques directly to adversarial behaviors, mission functionality, and technical elements. ***Engineers should leverage TTP frameworks because they support traceability from threat identification through requirement derivation and validation, enabling security controls to be tested and verified against specific threat behaviors {4.2.1.4}.***

As a result, this combined approach not only builds resilience into the space system but also provides a standardized, threat-informed methodology that scales across commercial, civil, and national security space missions. ***System engineers should ensure that secure-by-design controls derived from TTP frameworks are allocated to specific segments and subsystems during early architectural trade studies, rather than deferred to implementation phases {4.2.1.5}.***

4.2.1.1 Example Application on Space Segment

This section will provide a more robust explanation of how to apply one of these frameworks, SPARTA, for an applicable segment, the space segment. The same process could be applied using a different framework on a different segment, but this is meant to be an exemplar. Developing more secure spacecraft subsystems or components involves several key steps, including functional decomposition, threat modeling, vulnerability mapping, and translating these into specific, actionable security requirements. This approach ensures that spacecraft systems are resilient against potential cyberattacks and other threats that could compromise mission-critical operations, such as the loss of spacecraft control. The below is merely an example

Step 1: Establishing a Modular Security Reference Spacecraft Architecture

The process begins with developing a modular security reference architecture for the spacecraft, breaking down the system into core components and functions. This architecture serves as a baseline decomposition, capturing essential functions such as communication, propulsion, power management, and attitude control along with their components, like antennas, sensors, actuators, and control systems. Each functional area is broken down into standardized security building blocks, designed to be reused across different missions. These building blocks offer a

foundational security framework, ensuring mission-critical assets are well-understood and can be customized to fit the specific needs and constraints of each mission. By establishing this reference architecture, each mission can identify the building blocks required based on unique security requirements, such as assurance levels, mission objectives, and operational environments.

Step 2: Threat Modeling Using Applicable Frameworks

After establishing the modular security reference architecture, each mission tailors the architecture to its specific context and requirements. Using SPARTA threat modeling is applied to each subsystem by mapping the tailored security building blocks to relevant threats and adversarial techniques. For instance, the SPARTA framework may reveal risks like command injection or sensor manipulation within tailored control system blocks. This threat modeling process ensures that all relevant attack vectors are considered and that selected security building blocks align with the unique mission profile, providing an adaptable yet robust security foundation tailored to each mission's operational demands.

Step 3: Mapping Threats to Countermeasures

After identifying the threats using the frameworks, engineers proceed to map these threats to specific countermeasures or secure design principles. Since each mission tailors the reference architecture to its unique context, this step involves adapting pre-defined mappings within the frameworks to the tailored components. SPARTA comes with many of these already pre-mapped within the toolset (e.g., NIST 800-53, NIST 800-160, ISO 27001). This step involves determining the appropriate defensive techniques that correspond to the identified attack vectors. For example, if threat modeling reveals vulnerabilities in the spacecraft's communication system, such as susceptibility to command spoofing, countermeasures like encryption, authentication, and integrity checks can be implemented to mitigate these risks. Similarly, threats to control systems might be countered by employing redundancy, intrusion detection and prevention, or privilege-based access controls. By aligning tailored threats with adaptable countermeasures, directly correlating threats with countermeasures, engineers ensure that the security architecture is robust and comprehensive.

Step 4: Developing "Shall Statements" for Design Requirements

The final step should, but not always, involve translating these countermeasures into formal security requirements through "shall statements" that inform spacecraft design. These statements are based on the tailored architecture and provide specific, actionable directives that guide engineers in implementing security across the mission-specific building blocks. These statements are specific, actionable directives that guide engineers in implementing security throughout the system. Each requirement is directly traced to the threats identified during the threat modeling phase and aims to prevent or mitigate those threats through countermeasures. For example, a requirement to protect against unauthorized command injection might state, "The communication subsystem shall implement end-to-end authenticated encryption to prevent unauthorized access to control signals." Similarly, a requirement for the attitude control subsystem could be, "The attitude control subsystem shall include integrity checks to detect unauthorized manipulation of sensor data." These statements ensure that security is embedded into the design of each spacecraft component, customized to meet mission-specific needs and thereby mitigating the identified threats and protecting mission-critical operations. SPARTA comes prepopulated with hundreds of "shall statements" already linked to countermeasures.

Other frameworks do not have that level of detail, but SPARTA can provide sample requirements for adoption to help implement the countermeasure and mitigate the techniques.

4.2.2 IMPORTANCE OF TAILORING REQUIREMENTS TO THE SYSTEM

Security implementations must be tailored to the specific components and functions of space systems is critical to ensuring that the right protections are in place. For example, a vulnerability like improper authentication may manifest differently in the communication subsystem compared to the attitude control subsystem. While the communication system may require multi-factor authentication to protect access to control signals and prevent unauthorized commands, the attitude control system may focus on privilege-based access restrictions and the integrity of sensor data to prevent adversaries from manipulating the spacecraft's orientation. The corresponding "shall statements" for these systems would therefore vary based on the context of the subsystem, ensuring that security measures are applied to address the unique risks associated with each part of the spacecraft. ***Mission planners should ensure that security requirements are tailored to the unique functions and threat exposures of each subsystem, aligning protection techniques with the specific role and vulnerabilities of each component {4.2.2.1}.***

As space systems become more integrated and threat-aware, it is essential that acquisition professionals embed cybersecurity into procurement from the outset, not as an afterthought. Acquisition personnel involved in procuring space systems, components, or mission support services should ensure that all contracts, statements of work, and acquisition policies include security requirements driven by threat-informed TTP frameworks.

Mission planners, including acquisition teams, should ensure that contractual system-level security requirements are derived from known threat techniques and explicitly linked to mission-specific failure modes to guarantee alignment with operational risk {4.2.2.2}. This ensures that contractual language aligns with operational realities rather than generic cybersecurity boilerplate, "thou shall follow security policy XYZ". For instance, if the threat model highlights the risk of command spoofing in a communication subsystem, the acquisition team should include a requirement for cryptographic command authentication in the procurement documents. If the threat is lateral movement across a spacecraft bus, requirements should be included for segmentation, privilege management, or traffic filtering.

To support this, ***mission planners should collaborate with acquisition professionals and system engineers to develop tailored cybersecurity requirements early in the acquisition lifecycle, ideally during request for proposal (RFP) development {4.2.2.3}. Contracting officers should then require vendors to demonstrate traceability between implemented mitigations and the threat techniques they address, and this traceability should be reviewed as part of contract deliverables such as cybersecurity test plans, design documents, or system security engineering artifacts {4.2.2.4}.***

Following this approach ensures that security measures are not only tailored to the unique characteristics of each subsystem but are also grounded in current threat intelligence and mission risk. By requiring traceability between threat techniques, protection mechanisms, and mission-specific failure modes, acquisition practices become a proactive instrument in delivering resilient space systems. This methodology strengthens overall mission assurance by reducing the risk of security gaps, ensuring that spacecraft subsystems are equipped to withstand a wide range of cyber and counterspace threats. Furthermore, integrating threat-informed security requirements early in the acquisition lifecycle, particularly during RFP development, enables both engineering and procurement teams to embed

protection into system design from the outset, rather than relying on late-stage mitigations that are often costlier and less effective.

4.2.3 EXTENDING FRAMEWORKS FOR TEST AND EVALUATION

TTP frameworks provide a structured, threat-informed foundation for developing and executing security Test and Evaluation (T&E) campaigns across the space mission lifecycle. Rather than relying on static test procedures or ad hoc security testing, these frameworks offer an extensive, curated knowledge base of real-world adversarial techniques, enabling test teams to systematically assess how a system behaves under abuse conditions, not just nominal use. ***Mission planners and test engineers should adopt TTP frameworks as the baseline structure for designing, executing, and evaluating cybersecurity test and evaluation campaigns across the space system lifecycle {4.2.3.1}.***

Space system engineers, test engineers, and cybersecurity professionals can leverage these frameworks to simulate realistic attacks, generate abuse cases, and validate the system's response and defenses against known threats. This approach transforms T&E into a proactive mechanism for discovering weaknesses before launch, enabling course corrections early in the development lifecycle.

TTP frameworks excel at scenario-based testing. They enable mission-relevant threat emulation, supporting tabletop exercises, cyber ranges, hardware-in-the-loop (HIL) simulation, and red team assessments. For example, SPARTA can be used to map specific spacecraft subsystems, such as C&DH, ADCS, or propulsion, and simulate techniques like command injection, replay attacks, or bus flooding. ***Mission Planners should ensure TTP techniques are used as test stimuli to validate how systems respond under stress and determine whether detection, prevention, or recovery mechanisms are properly configured {4.2.3.2}.***

Rather than relying solely on functional test plans, teams should augment their test suites with threat-informed abuse cases. These include deliberately malformed commands, spoofed telemetry, protocol fuzzing, replayed ground commands, or flooding legitimate interfaces each mapped to a known techniques in SPARTA or ATT&CK. ***Test engineers should explicitly include abuse cases derived from and mapped to known TTPs in their cybersecurity verification plans to uncover failure modes that may not emerge during traditional functional testing {4.2.3.3}.***

To support this, threat mapping and system decomposition should feed into test scenario development. This ensures that each high-priority adversarial technique has a corresponding test case or validation activity. For example, if lateral movement is identified as a risk in the ground segment, then test cases should evaluate whether existing segmentation or privilege enforcement mitigates this behavior. ***Engineers should trace each TTP to the specific countermeasure it is intended to validate, enabling measurable security assurance and closing the gap between controls and real-world threats {4.2.3.4}.***

To ensure relevance across the architecture, segment-specific testing strategies must be adopted. Each segment, ground, link, and space, presents unique threat surfaces and failure modes that require tailored adversary emulation and validation activities. ***Test engineers should tailor TTP-driven test scenarios to the specific threat profiles and architectural features of each space system segment {4.2.3.5}.***

For ground segment systems, existing ATT&CK-based tooling such as Atomic Red Team, AttackIQ, or Scythe can automate the execution of cyberattack simulations. These platforms execute well-defined TTPs (e.g., credential dumping, phishing payload delivery, or privilege escalation) to test the system's ability to detect and block malicious behaviors. ***Engineers should integrate TTP-based test harnesses, automation frameworks, and adversary emulation tools during integration testing to quantify detection coverage, evaluate resilience, and improve system hardening {4.2.3.6}.*** These testing

frameworks help teams systematically evaluate their security controls, determine how well they perform against known TTPs, and identify areas for improvement. This capability allows for testing the resilience of the ground segments highly efficiently, reducing the time and resources needed to conduct thorough testing and ultimately strengthening the defenses of mission-critical infrastructure.

On the space segment, threat-informed testing should use high-fidelity spacecraft environments, such as hardware-in-the-loop (HIL), digital twin, or simulation frameworks, to evaluate whether defensive mechanisms are effective against threat techniques (i.e., from SPARTA). For example, techniques like command link intrusion and sensor data manipulation should be emulated by injecting unauthorized commands, spoofing telemetry values, or corrupting sensor data. These tests assess the performance of command authentication schemes, anomaly detection logic, watchdog timer response, and interface whitelisting. Below is an exemplar of a three-step methodology using SPARTA on the space segment:

1. **Select High-Priority Techniques Using Mission Impact and Likelihood:** Engineering teams would decompose the mission to understand which subsystems and functions, if compromised, would lead to mission failure or loss of trust. Using SPARTA's threat taxonomy, which is already mapped to spacecraft components, analysts would prioritize techniques that could result in effects like denial of service, misdirection, or loss of telemetry. This prioritization enables test objective development that reflects realistic, mission-critical scenarios.

2. **Develop Threat-Informed Test Procedures:** Once high-impact TTPs are identified, test teams should build procedures to emulate these attacks using techniques like:

    a. Injecting malicious binaries into flight software

    b. Sending unauthorized telecommands that mimic attacker objectives

    c. Exploiting misconfigured protocols or insufficient authentication mechanisms

    These procedures should be executed in hardware-in-the-loop (HIL), FlatSat, or software-defined spacecraft models to evaluate actual system behavior under adversarial conditions .

3. **Evaluate Actual Impact in Mission Context:** The final step would be an impact assessment to determine whether the simulated attack produces consequences such as telemetry falsification, degraded maneuverability, communication blackout, or other mission-degrading effects. Mission planners and evaluators would then classify impacts using categories like Deception, Disruption, Denial, Degradation, Destruction, or Theft (the "6 D's" model), enabling clear articulation of cybersecurity risk to the spacecraft and mission. These observed impacts should be documented and mapped to mission-level consequences to support risk acceptance decisions and inform system refinements.

Regardless of which segment is under test, ***engineers should define pass/fail criteria based on whether the system appropriately detects, blocks, or mitigates the simulated threat behaviors {4.2.3.7}.*** Also, when feasible, test scenarios should also include adversarial persistence across multiple vectors (e.g., exploiting both command and telemetry channels) or segment to evaluate the system's resilience under compound threat conditions. Each iteration of testing improves the system's posture by revealing gaps in countermeasures and enables continuous refinement of security requirements. ***Mission Planners/System Engineers should refine mitigations based on failed TTP-based test outcomes, ensuring system protections are not only defined but proven through empirical evidence {4.2.3.8}.***

Beyond control validation, these frameworks provide risk quantification. By mapping TTPs to mission impacts and performing failure mode assessments, mission planners can identify which threat vectors are most likely to disrupt or degrade mission objectives. ***Mission assurance teams should use TTP-based results to inform mission risk scoring and prioritize future investment in protection enhancements {4.2.3.9}.***

Finally, the standardized taxonomy and traceability of TTP frameworks make them ideal for supporting test repeatability, requirement validation, and stakeholder communication. ***Test documentation should include a threat-to-requirement-to-test-case mapping matrix that aligns each TTP with corresponding mitigations and test outcomes {4.2.3.10}. This traceability should be maintained across lifecycle artifacts, including test reports, security assessments, and system accreditation documentation {4.2.3.11}.*** When integrated across lifecycle phases, TTP-based T&E provides defensible evidence for risk acceptance, security control effectiveness, and mission survivability under cyber-contested conditions. ***Mission planners should archive TTP-based test results and use them to guide future spacecraft designs, enabling engineering teams to inherit proven countermeasures and avoid repeating past vulnerabilities {4.2.3.12}.***

4.2.3.1 Extending Frameworks for Tabletop Exercises

Tabletop exercises are structured, discussion-based simulations that allow organizations to evaluate their readiness to respond to cyber and counterspace threats in a controlled, low-risk environment. These exercises do not simulate technical execution, but instead focus on decision-making, process validation, cross-team coordination, and escalation paths under pressure. In tabletop exercises, teams walk through hypothetical cyberattack scenarios to evaluate how well they can detect, respond to, and recover from incidents. For space missions, where response options are constrained and attack timelines may be short, the ability to rehearse these scenarios in advance is mission critical.

As described in section 2, TTP frameworks provide the structure, specificity, and realism needed to design tabletop exercises that move beyond generic incident walkthroughs. Rather than inventing hypothetical threats, mission planners can use curated threat techniques from SPARTA and MITRE ATT&CK® to construct exercises that reflect actual adversarial behavior, enabling more targeted evaluations of response plans. ***Mission planners should use TTP frameworks to anchor tabletop exercises in real-world adversarial techniques, ensuring that scenario design aligns with mission-specific threats and subsystem vulnerabilities {4.2.3.1.1}.*** This ensures that the exercise tests not only general crisis management, but also how well the organization can detect, attribute, and respond to specific attacks on space system elements such as uplinks, onboard processors, or mission-critical software.

For example, a table-top exercise might simulate an attack where adversaries attempt to gain access to a spacecraft's command and control systems via a compromised ground station. Using TTP frameworks, the exercise can incorporate specific techniques like phishing, privilege escalation, and lateral movement (from ATT&CK) leading up to the space-focused attack, where adversaries attempt to exploit communication protocols or inject malicious commands (SPARTA). This level of detail ensures that the exercise reflects realistic attack chains, providing valuable insights into how the organization might fare in an actual attack. These scenario chains can expose weaknesses in both cyber hygiene and incident coordination across domains. ***Cybersecurity and mission operations personnel should jointly participate in tabletop exercises to evaluate how decisions at each phase of the attack chain influence system availability, mission assurance, and recovery timelines. {4.2.3.1.2}***

To maximize learning value, these exercises should include:

- Mapping each step of the scenario to the appropriate framework techniques (i.e., SPARTA for space or ATT&CK for ground)
- Predefined triggers for detection, response, and escalation discussions
- Discussion prompts for assessing telemetry gaps or operational blind spots
- Role assignments for operations, cyber, comms, and leadership teams
- Injects simulating adversary persistence or secondary impacts

Tabletop teams should document which TTPs were successfully mitigated, which failed prevention/detection, and which required escalation to system owners or incident response staff. This mapping should feed into a post-exercise gap analysis. {4.2.3.1.3}

Ultimately, tabletop exercises using TTP frameworks enable mission planners to validate their readiness not just to "respond to an incident," but to respond to the types of incidents most likely to target their specific systems and architectures. They support strategic readiness, informed investment, and help identify whether roles and responsibilities are well understood across cyber, mission, and operator communities.

4.2.3.2 Extending Frameworks for Red Teaming/Penetration Testing

Red teaming, also often referred to as penetration testing, involves the authorized simulation of adversarial behavior to test the robustness of security controls, operational defenses, and mission assurance processes. Unlike tabletop exercises, which focus on process and coordination, red teaming actively challenges system defenses through technical execution, probing both cyber and physical pathways. For space systems, red teaming is an essential tool for uncovering real-world vulnerabilities that may not be evident in design documentation or functional testing.

TTP frameworks such as MITRE ATT&CK® for enterprise/ground systems and SPARTA for spacecraft and link-layer threats provide red teams with structured libraries of adversary behaviors, enabling realistic and mission-relevant threat emulation. These frameworks eliminate guesswork by supplying tested techniques that map directly to known threat actors, providing the foundation for building high-fidelity attack chains.

Red teams should use TTP frameworks to construct full-spectrum attack paths across the ground, link, and space segments focusing on seams where adversaries may pivot between subsystems or domains {4.2.3.2.1}.

For example, a red team might use:

- ATT&CK would provide techniques to execute like phishing, malware delivery, credential dumping, and lateral movement in the ground segment
- SPARTA would provide techniques to execute unauthorized commanding, telemetry spoofing, or memory corruption targeting onboard subsystems

By chaining these techniques, red teams can test both defense-in-depth strategies and segmentation assumptions, revealing whether attacks against one segment can cascade to mission-impacting consequences in another.

Mission stakeholders should scope red team engagements to validate whether layered defenses and anomaly detection systems effectively detect or delay realistic threats derived from TTP frameworks, rather than relying solely on checklist compliance. {4.2.3.2.2}

TTP-based red teaming enables:

- Tailored threat chaining to test specific mission architectures (e.g., cross-segment exploitation)
- Proof-of-concept validation of suspected vulnerabilities or insecure interfaces
- Generation of Indicators of Compromise (IOCs) for tuning detection systems
- Post-exercise forensics to assess defender awareness, detection timelines, and missed telemetry

Red team exercises should not only aim to gain access or disrupt operations but to document the full path of exploitation and compare outcomes against mission objectives. Whether the adversary was able to disable watchdog timers, inject malicious commands, or cause misconfiguration of communications systems, each result should be evaluated in terms of operational impact, including degraded performance, mission abort conditions, loss of trust, or unacceptable data manipulation enabling planners to determine residual risk and update protection strategies. ***Mission planners and cybersecurity engineers should use red team results to calibrate residual risk levels and refine architectural protections (e.g., access controls, fault isolation strategies). {4.2.3.2.3}***

These exercises also serve a critical secondary purpose: training and maturing blue teams which are the defenders responsible for detecting, responding to, and recovering from cyber and counterspace threats. In many space missions, blue team personnel may be highly skilled in operations or engineering but lack hands-on experience with adversarial tactics. TTP-informed red teaming exercises provide a low-risk but high-fidelity training environment where defenders can observe and react to realistic attack patterns that are otherwise absent in nominal operations.

By emulating novel or low-observable techniques, such as subtle manipulation of telemetry, time-delayed command injection, or cross-domain lateral movement, these exercises sharpen the defenders' ability to recognize weak signals of compromise, validate anomaly detection rules, and tune alert thresholds. They also test the operational handoffs between security operations analysts, mission controllers, and flight software engineers, identifying breakdowns in communication or delays in response. ***Mission planners should incorporate red team exercises and outputs into blue team training cycles, using observed detection failures, delayed responses, or missed IOCs as direct input to enhance procedures, playbooks, and alerting logic {4.2.3.2.4}. Cybersecurity leads should develop post-exercise debriefs and replay sessions to walk blue teams through red team techniques, highlighting gaps in observability, misinterpretation of telemetry, or delays in escalating suspicious activity {4.2.3.2.5}.*** This threat-informed feedback loop ensures that red teaming doesn't just reveal system weaknesses, it also strengthens the human layer of defense, ensuring that operational personnel are equipped to defend missions in real time.

To close the loop on corrections to the system, red team activity must be followed by root cause analysis and remediation tracking, ideally integrated into system security engineering baselines. Threat techniques used during red teaming that fall outside the current detection or response capabilities should be cataloged as coverage gaps and prioritized for mitigation. ***Organizations conducting red team activities should maintain successful attack to technique mappings and ensure that each successful compromise is linked to a failed countermeasure/control, a missed detection rule, or a gap in policy coverage. These insights should be used to inform updates to system design, detection tools, and operational procedures{4.2.3.2.6}.*** Ultimately, TTP-driven red teaming transitions organizations from compliance-based testing to threat-informed resilience engineering enabling faster detection, coordinated response, and hardened architectures purpose-built to resist adversary behaviors.

4.2.4 EXTENDING FRAMEWORKS FOR COMPLIANCE & STANDARDS DEVELOPMENT (NIST, ISO, ETC.)

TTP frameworks can be extended beyond engineering and operations to support compliance verification, control implementation, and the development of space-specific security standards. They help organizations map adversarial behaviors to existing baselines like NIST SP 800-53, ISO/IEC 27001, and Consultative Committee for Space Data Systems (CCSDS) recommendations ensuring that implemented controls are both compliant and threat informed.

Standards bodies such as the CCSDS, the European Cooperation for Space Standardization (ECSS), and the Institute of Electrical and Electronics Engineers (IEEE) can use TTP frameworks to inform updates to legacy standards or define new protections aligned with evolving cyber and counterspace threats. ***Standards development organizations should incorporate TTP-based mappings into their requirements and/or threat catalogs to ensure coverage of both traditional and emerging adversary behaviors across space system segments. {4.2.4.1}***

TTP frameworks offer a structured way to trace real-world adversarial techniques (e.g., privilege escalation, bus denial, or data corruption) back to baseline control requirements like NIST AC-6 (Least Privilege) or ISO A.9.2 (User Access Management). This improves fidelity in requirement interpretation and strengthens the justification for implementing specific mitigations. ***Compliance professionals and security control owners should document traceability from required controls to the TTPs they mitigate to ensure threat-relevant justification for each control selection. {4.2.4.2}***

For example, a spacecraft operator might use TTP frameworks to ensure that access control mechanisms intended to meet NIST or ISO directives are also effective against threat techniques like credential dumping or unauthorized command injection. ***System engineers should validate that their control implementations not only meet regulatory text but also map to adversarial techniques most likely to impact mission assurance {4.2.4.3}.***

Additionally, TTP-informed testing (as discussed in Section 4.2.3) can be used to demonstrate control effectiveness during compliance audits. For instance, executing ATT&CK or SPARTA techniques in a controlled test environment can validate that the cryptographic protections required under ISO 27001 Section A.10 are operationally resilient to real-world threats. ***Test teams and assessors should use TTP-driven test cases to validate the effectiveness of compliance controls during audits, Plan of Action and Milestones closures, and security authorizations. {4.2.4.4}***

This integration of threat-informed intelligence into compliance activities reduces the risk of implementing "checklist security" that satisfies oversight but fails under attack. It also provides a feedback loop: if controls consistently fail to mitigate mapped TTPs in simulation or red team exercises, then those failures should be used to update control guidance and compliance scoring. ***Mission planners developing space mission requirements or seeking certification should require that compliance artifacts include mappings between controls, mitigations, and adversarial behaviors derived from TTP frameworks. {4.2.4.5}***

4.2.4.1 Standards Development: Driving Updates and New Standards

Standards bodies such as the CCSDS, the IEEE, and the ECSS can, and should, leverage TTP frameworks to inform updates to existing standards and create new cybersecurity guidelines designed to address the unique and evolving threats facing space systems. They reflect the latest intelligence on how real-world actors compromise spacecraft, ground stations, and communications links. This makes them a valuable resource for standards development organizations seeking to codify protections that are

not just theoretical but grounded in observed attack vectors. ***Standards development organizations (SDOs) should incorporate TTP-derived adversary techniques and countermeasures as input into the creation or revision of standards to ensure alignment with realistic threat models and to drive security-by-design principles across the space domain {4.2.4.1.1}.*** This ensures that emerging techniques such as command link replay, telemetry spoofing, or payload tampering are addressed explicitly, rather than generically.

Standards efforts should use TTP-to-control mappings to identify gaps in current baseline protections and prioritize updates to standards that address real-world vulnerabilities {4.2.4.1.2}. For instance, if current standards do not address bus-level segmentation, but SPARTA identifies lateral movement across communication buses as a common or high-risk technique, that gap should be closed in the next revision cycle.

Integration of TTP frameworks into standards development ensures feedback loops between field activity (e.g., testing, red teaming, failure events) and policy. As new adversary behaviors are discovered or simulated, they would be added to TTP frameworks which then could trigger updates to related standards. This provides a dynamic evolution model for standards and one that adapts with the threat landscape instead of lagging behind it.

4.2.4.2 Pre-Mapped Compliance and Its Role in Standards Evolution

As previously discussed in Section 4.2.1.1, both the SPARTA and MITRE ATT&CK® frameworks provide pre-established mappings to regulatory standards such as NIST SP 800-53 and ISO/IEC 27001. These pre-validated associations serve as authoritative reference points for aligning adversarial TTPs with control families from widely accepted cybersecurity frameworks. This capability enables organizations to integrate threat-informed risk management directly into their design and compliance efforts.

Utilizing these pre-built mappings can significantly reduce the burden on engineers, assessors, and compliance officers by accelerating the identification of applicable controls and enabling traceability between real-world threat behaviors and control objectives. For instance, the ATT&CK knowledge base is mappable to NIST 800-53's control catalog, supporting continuous monitoring, threat modeling, and control verification activities across the system lifecycle. ***System engineers should leverage these mappings to ensure that security engineering and compliance assurance remain current with the evolving threat landscape {4.2.4.2.1}.***

TTP-to-control mappings can assist standards bodies and regulatory authorities in harmonizing global security expectations, fostering interoperability and mutual trust between international partners in both commercial and government space missions. However, these mappings must not be treated as prescriptive or exhaustive. While they provide authoritative alignment between TTPs and controls, they do not account for system-specific context, mission risk tolerance, or architectural nuance. ***System engineers are encouraged to interpret these mappings as informative guidance rather than rigid mandates, validating applicability within the scope of their own operational environment and tailoring implementation to meet mission-specific objectives {4.2.4.2.2}.***

4.2.4.2.1 Example Application – Leveraging SPARTA for Compliance with NIST 800-53 on Spacecraft

The SPARTA framework provides a structured, threat-informed method to help space systems achieve cybersecurity compliance, particularly with control catalogs such as NIST SP 800-53. By mapping adversarial techniques and countermeasures to specific security controls, SPARTA allows space system engineers to build compliance strategies that are rooted in real-world attack scenarios.

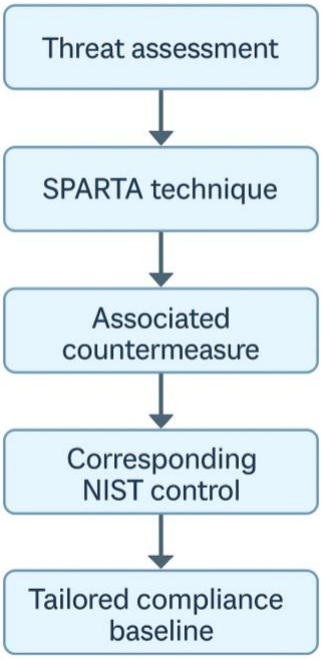


Figure 4-2: Relationship Flow to Controls

In the context of space missions, traditional baselines like NIST 800-53 define security controls that apply across all information systems. However, these controls are intentionally broad and not always specific to the technical or operational realities of space environments. By integrating SPARTA, organizations can assess specific risks to the space segment, including vulnerabilities in spacecraft subsystems and communication links, and identify the corresponding NIST controls that need implementation. This approach helps bridge the gap between generic security guidance and the unique challenges of space environments, ensuring that controls are mission-relevant and effective.

The methodology defined in TOR-2023-02161 Rev A - Space Segment Cybersecurity Profile demonstrates this alignment. The process begins with a threat-based assessment, using SPARTA techniques to identify TTPs most relevant to the mission profile. These techniques are then mapped to appropriate NIST controls, enabling a tailored compliance approach that remains aligned with baseline security expectations.

For example, the encryption of telemetry and telecommand links, identified within SPARTA as a critical countermeasure, maps directly to cryptographic controls such as SC-12 through SC-13 in NIST 800-53. Likewise, SPARTA's emphasis on secure boot and onboard intrusion detection can be mapped to controls such as SI-7 (Software, Firmware, and Information Integrity) and AU-6 (Audit Review, Analysis, and Reporting).

SPARTA's pre-mapped control relationships may be used as a starting point but must be reviewed in the context of each spacecraft's unique mission, architecture, and operational constraints. By utilizing these established mappings, organizations can save time and resources, ensuring that their cybersecurity efforts are both efficient and comprehensive. However, it is important to recognize that these mappings are not definitive solutions, but they are informative references that guide the security and compliance process. Organizations must tailor these mappings to their specific operational contexts, ensuring that the applied controls are effective for their unique missions and risk environments. Implementers are encouraged to conduct an internal validation of control applicability using the SPARTA mappings, rather than relying on them as prescriptive sources.

This dual alignment of threat-based rigor and standards-based compliance supports a more resilient spacecraft design, ensuring the cybersecurity architecture remains grounded in both regulatory expectations and adversarial realities.

5 TRACKING TTPS IN SPACE SYSTEMS: THE ROLE OF TTP FRAMEWORKS FOR THREAT INTELLIGENCE AND DETECTION

TTP frameworks serve a critical role in tracking adversary behavior across the space system lifecycle. By codifying threat actor tactics, techniques, and procedures, these frameworks provide a structured foundation for cyber threat intelligence (CTI), detection engineering, and threat attribution. This section explores how TTP-driven models support the development of indicators, mapping of threat activity, and integration with STIX for actionable intelligence sharing in the space domain.

5.1 CYBER THREAT INTELLIGENCE OVERVIEW AND IMPORTANCE FOR SPACE SYSTEMS

Cyber Threat Intelligence (CTI) involves the collection, analysis, and contextualization of information about potential or active cyber threats to support informed decision-making. For space systems where spacecraft, constellations, and supporting infrastructure are tightly coupled with national security, economic continuity, and critical services CTI is a foundational component of proactive defense.

The application of CTI to space systems faces unique challenges that are not present in traditional IT domains. Unlike enterprise networks, which benefit from decades of threat reporting and intelligence sharing, the space and link segments operate with far less visibility. Many spaceborne systems rely on bespoke hardware, proprietary software, and isolated architectures, often disconnected from terrestrial detection infrastructures. As a result, intelligence sharing across space sector organizations remains limited due to mission sensitivity and classification boundaries. ***Mission planners should work with appropriate cybersecurity personnel to develop internal CTI programs that are specifically tailored to space operations and informed by the unique mission, adversaries, and system architecture {5.1.1}. Where possible, space system operators are should contribute to sector-wide threat intelligence initiatives (e.g., through ISACs or information-sharing agreements), particularly to expand collective awareness of spaceborne threats {5.1.2}.***

While frameworks like MITRE ATT&CK® have established a strong foundation for understanding cyber threats in ground-based environments, their application to space missions is limited. In response, space-centric TTP frameworks such as SPARTA and SPACE-SHIELD have emerged to address this gap. These frameworks catalog space-specific adversarial behaviors and are evolving to capture

techniques targeting orbital assets, command links, navigation, and telemetry paths. ***Operators and mission assurance teams should incorporate space-focused TTP frameworks into their threat modeling and intelligence operations (i.e., collection and dissemination) to ensure alignment with emerging threat behaviors {5.1.3}.***

A persistent challenge is the scarcity of historical data on adversarial behaviors in space environments. This lack of visibility limits the predictive power of threat models and hinders the development of behavioral baselines. Moreover, the absence of persistent monitoring, especially in the link and onboard spacecraft segments, means that many threats may go undetected or unreported. To mitigate intelligence gaps, ***systems engineers should establish mission-specific telemetry collection strategies that prioritize security-relevant observables {5.1.4}.*** Emerging spaceborne threat behaviors may not align with previously observed terrestrial patterns, making them harder to detect using traditional methods. As such, CTI for space must be both adaptable, mission-aware, and capable of anticipating novel threat vectors while grounded in realistic spacecraft operations.

5.1.1 TTP FRAMEWORKS FOR DETECTIONS

Detection in cybersecurity is the process of identifying malicious activity, anomalous behavior, or unauthorized system access within a network or space system. It is a foundational capability for maintaining a defensive cybersecurity posture, enabling defenders to respond promptly and ideally before adversarial actions result in mission degradation or data compromise. Effective detection relies on correlating behavioral patterns, known Indicators of Compromise (IOCs), and deviations from established baselines for behavioral norms.

This is where CTI becomes indispensable. CTI provides enriched context about threat actors, including their likely objectives, known capabilities, and documented TTPs. When CTI is integrated into detection workflows, it enhances the ability to recognize adversarial behaviors such as unauthorized command execution, exploitation of onboard services, or link-layer interference. It enables mission teams to anticipate threat behaviors, implement targeted detections, and reduce time to response. TTP frameworks support detection efforts by providing a shared structure for tagging, correlating, and interpreting adversarial activity. This makes it possible not only to identify intrusions, but also to understand them in context thereby improving coordination and response.

TTP frameworks strengthen detection strategies by offering a standardized taxonomy for expressing adversary behavior. These frameworks organize known tactics and techniques by attack phase, affected assets, and observable actions making them well-suited for tagging, correlating, and investigating threat activity. ***Space system defenders should integrate TTP-informed CTI into their detection architecture to improve situational awareness and shorten the time between threat manifestation and mitigation {5.1.1.1}. Detection rules and alerting logic should reference TTP identifiers wherever feasible, enabling consistent tracking, reporting, and correlation of adversarial behaviors across missions and systems {5.1.1.2}.***

For example, network events can be enriched by tagging them using SPARTA or ATT&CK technique IDs, allowing automated systems and analysts to associate observed activity with known threat patterns. This shared lexicon supports not only internal detection efforts but also intelligence sharing across agencies, mission partners, and commercial operators.

5.2 A UNIFIED THREAT INTELLIGENCE MODEL FOR SPACE SYSTEMS

Despite the challenges outlined in previous sections, TTP frameworks provide value for enhancing threat intelligence sharing across space and ground segments. The use of TTP frameworks standardizes

how threats are categorized and tracked, allowing for a common language to facilitate interoperability across organizations and agencies. Such shared understanding facilitates information sharing and collaborative detection and response, which are crucial in the space industry given its global and interconnected nature. ***Organizations involved in space system operations and information sharing should adopt a common domain relevant TTP frameworks to ensure consistency and fidelity in threat reporting and collaboration {5.2.1}.***

Information sharing organizations, such as the Space Information Sharing and Analysis Center (ISAC), play a pivotal role by centralizing threat intelligence and disseminating critical information to space agencies, satellite operators, and defense contractors. Shared frameworks allow contributors to better understand adversary behaviors and coordinate responses to emerging threats. ***Contributors to and developers of threat-sharing platforms should use framework-aligned TTP identifiers when submitting reports or analysis, to promote normalization and cross-organizational correlation {5.2.2}.***

For example, the ATT&CK framework's success in mapping out ground-based TTPs allows ground station operators to anticipate potential attack vectors and take preemptive action. Similarly, SPARTA and SPACE-SHIELD can document space-specific techniques, providing a reference point for analyzing threats to communication links and spacecraft.

5.2.1 LEVERAGING RECOMMENDED PRACTICES FOR TTP MAPPING IN CTI

Accurate and consistent mapping of TTPs is foundational to high-quality CTI. Mapping observed or suspected adversary activity to known TTPs helps structure incident reporting, improve detection fidelity, and enable intelligence sharing across organizational and mission boundaries. While originally developed for enterprise networks, TTP mapping methodologies as those codified by DHS CISA for the MITRE ATT&CK® framework are increasingly applicable to the space domain.

In space systems, where telemetry anomalies or link disruptions may indicate sophisticated threat activity, mapping those observations to SPARTA or SPACE-SHIELD techniques allows CTI teams to identify commonalities with known threat behaviors (i.e., trending analysis). This process supports enriched analysis, facilitates cross-organizational intelligence fusion, and enables defenders to communicate risk in a standardized, interoperable format. ***Space-focused CTI programs should incorporate TTP mapping practices to ensure consistency in threat analysis, improve information exchange, and support community-wide situational awareness {5.2.1.1}. In general, space cybersecurity engineers should adopt methodologies proven in terrestrial IT environments, adapting them to address the distinct characteristics of ground, link, and space segments {5.2.1.2}***. For example, mapping anomalous satellite behavior to corresponding SPARTA techniques enables analysts to better understand how attacks are executed. These mappings can then drive defensive strategies such as refining intrusion detection algorithms, strengthening encryption implementations, or introducing redundancy in communication architectures. ***Threat intelligence outputs should inform the development of detection rules and response actions based on mapped TTPs and associated observables {5.2.1.3}***.

When mapping CTI and TTPs, CTI analysts should contextualize mapped TTPs to understand their relevance to operational objectives and mission impact. This includes identifying how a given TTP could affect system availability, data integrity, or control of the asset. Such contextualization enhances threat reports by translating technical behavior into mission-relevant risk. This is likely an extension to the TTP mappings, but it helps become more actionable when the report also notes that the activity targeted a critical attitude control component. This linkage gives decision-makers and partner organizations better insight into adversary intent and system-level consequences. ***Threat intelligence***

products should include context on how mapped TTPs relate to mission impact, to improve relevance and downstream utility for recipients {5.2.1.4}.

As previously discussed in the PIVOT paper, another recommended practices is cross-framework mapping by establishing links between techniques across frameworks such as ATT&CK, SPARTA, and SPACE-SHIELD. This practice is especially important for space systems, where ground-side compromises often precede or enable attacks on space assets. For example, a credential theft technique observed on a ground station (mapped via ATT&CK) may directly enable uplink spoofing or command injection attacks on a satellite (mapped via SPARTA). Cross-mapping these actions enables analysts to track campaign progression across domains and communicate end-to-end attack paths to other stakeholders. ***Organizations producing threat intelligence should support cross-framework mapping to reflect multi-domain attack chains and enable correlation between terrestrial and spaceborne TTPs {5.2.1.5}.***

5.2.2 VALUE OF USING STIX 2.1 FOR SHARING CYBER THREAT INTELLIGENCE (CTI) IN SPACE SYSTEMS

Effective cybersecurity policy in the space domain depends on timely, structured, and standardized information sharing. While TTP frameworks like SPARTA, SPACE-SHIELD, and ATT&CK offer a shared taxonomy for describing adversarial behavior, they require an implementation mechanism to enable operational coordination and automation. That role is fulfilled by Structured Threat Information Expression (STIX) 2.1, a machine-readable standard designed for exchanging cyber threat intelligence across tools and global organizations.

Policy makers must recognize the importance of STIX as both a technical enabler and a policy accelerant. By encouraging, or even mandating, its use in directives, memoranda, and standards, governing bodies can ensure that threat intelligence flows efficiently between commercial entities, government agencies, and international partners. This becomes essential as missions increasingly involve multinational constellations, shared infrastructure, and collaborative operations. ***Cybersecurity policies and mission security baselines should require or incentivize the use of STIX 2.1 for cyber threat intelligence exchange to enable interoperability and reduce friction in multilateral sharing environments {5.2.2.1}.***

Organizations such as the Space ISAC, ENISA, and mission-specific security working groups can serve as aggregation and distribution hubs, helping normalize and disseminate STIX-based CTI across the space ecosystem.

As space systems face increasing cyber and counterspace threats, the ability to rapidly share structured CTI is becoming mission critical. STIX 2.1 enables this by encoding threat data, including TTPs, indicators, attack patterns, and relationships, in a format that supports automation, correlation, and real-time decision support.

For space systems, which often operate in siloed, proprietary, or high-assurance environments, adopting STIX-based sharing enables:

- Reduced manual processing of alerts and intelligence
- Faster detection of shared adversary behaviors across missions
- Cross-platform integration with Security Information and Event Management (SIEM), Threat Intelligence Platforms (TIPs), and incident response tools
- Enhanced situational awareness across space, link, and ground segments

Tool vendors and space operators of space systems should adopt STIX 2.1 as the baseline format for sharing and consuming cyber threat intelligence to facilitate automation, consistency, and speed of response {5.2.2.2}.

While STIX 2.1 offers a robust schema for threat intelligence sharing, many current COTS and open-source implementations are optimized for enterprise IT and not spaceborne platforms. As a result, existing observables may not fully capture telemetry patterns, control commands, or link-layer anomalies unique to space missions. To address this, space cybersecurity professionals must begin decomposing space-specific TTPs, as defined in SPARTA and SPACE-SHIELD, into STIX-compliant indicators and observables.

STIX's true value lies in its ability to structure relationships between attackers, campaigns, tools, infrastructure, and victim assets. For space missions, where attack chains may begin with credential theft on the ground and culminate in manipulation of a space asset, STIX enables cross-segment and cross-agency tracking of adversary behavior. Encoding these relationships facilitates:

- Threat actor profiling and campaign tracking
- Multi-segment correlation across space, link, and ground
- Attack chain modeling and pivot detection
- Predictive analytics and behavior-based defense

STIX also allows for machine-to-machine exchange across diverse tools and partners, reducing the need for manual reformatting. This is especially vital in international or coalition operations, where semantic and structural consistency is required to maintain synchronized defense postures.

5.2.3 OVERCOMING GAPS IN EXISTING STIX STANDARDS FOR SPACE SYSTEMS

One of the primary challenges facing the adoption of STIX 2.1 in the space domain is the limited support for space-specific observables and telemetry behaviors. While STIX was designed with flexibility in mind, many COTS tools and schemas are optimized for enterprise IT environments leaving gaps in the ability to model and detect adversarial behavior targeting spacecraft, satellite constellations, and RF links. This poses a challenge for space systems, which exhibit domain-specific behaviors, protocols, and telemetry patterns not yet captured in many existing STIX implementations.

Examples of these space-specific gaps include:

- Observables tied to spacecraft subsystem behavior (e.g., anomalous attitude adjustments or resets)
- Telemetry anomalies unique to attitude control, propulsion, or payload subsystems
- Standard command counters within the flight software
- Command uplink patterns and validation anomalies
- Satellite-to-satellite link manipulation or spoofing attempts
- RF-based injection, replay, or disruption across S-band, X-band, and proprietary links

Despite these limitations, the space cybersecurity community has already begun bridging this gap. The SPARTA framework, for instance, includes nearly 200 Indicators of Behavior (IOBs) crafted with STIX 2.1 syntax and designed to be ingested by OpenCTI-compatible platforms. These IOBs represent behavior-driven detections that are already tailored to the unique threat landscape of spaceborne systems and are readily available to CTI producers and consumers. ***Space system stakeholders should leverage***

existing STIX-compatible IOBs, such as those provided in the SPARTA framework, as a baseline for standardizing space-relevant observables across missions {5.2.3.1}.

The challenges and gaps are not insurmountable as indicated in SPARTA's initial publication of IOBs. Since, STIX 2.1 allows for custom object extensions, and the space cybersecurity community is well-positioned to define, validate, and propose these enhancements collaboratively. Organizations such as the Space ISAC, international space agencies, and standards bodies like CCSDS or OASIS should jointly lead efforts to formalize these extensions, ensuring broad compatibility and tool support. This work should then rolled into the STIX standard; therefore, ***the STIX standards body should extend existing STIX object definitions or leverage custom extensions to represent space-specific observables and indicators {5.2.3.2}.*** These definitions should prioritize clarity, interoperability, and ease of implementation within existing TIPs and SIEMs. Addressing this gap will enhance the resilience of the broader space ecosystem by allowing operators to detect novel TTPs, share them rapidly, and build reusable defense content that protects global space infrastructure.

6 OTHER CHALLENGES AND CONSIDERATIONS

6.1 CHALLENGES IN APPLYING FRAMEWORKS TO SPACE SYSTEMS

While TTP frameworks can provide robust guidance for securing space systems, applying them effectively can be challenging. Space systems differ significantly from traditional IT systems, requiring adaptations to the frameworks to account for the unique characteristics of the space environment.

One key challenge is the constrained resources available onboard spacecraft. Unlike ground-based systems, which can afford to run complex security monitoring and detection systems, spacecraft often have limited processing power, memory, and energy. Limited resources mean that security measures must be carefully designed to balance protection with resource usage.

Another challenge is the long lifecycle of space missions. Spacecraft often operate for years or even decades without direct physical access, making applying software updates or patching vulnerabilities challenging. Security measures must therefore be forward-looking and robust enough to withstand evolving threats over the mission's duration.

One of the largest challenges in applying cybersecurity to space systems is the need for more mature, space-proven countermeasures on the space segment. In contrast to traditional IT systems, where many of the mitigations and detections recommended by the ATT&CK framework are well-established and commercially available, the space domain needs a long history or inventory of countermeasure implementations. Many of the theoretical protections outlined by these frameworks remain at low Technology Readiness Levels (TRLs) when deployed in the harsh and unique space environment.

For example, COTS intrusion detection systems, widely available and used in enterprise IT environments, are virtually nonexistent for spacecraft. Space systems have specific challenges, such as extreme radiation, extended mission lifecycles, and limited processing power, that make it challenging to adapt conventional IT security tools. While IDS are standard components in IT networks, spacecraft often lack the infrastructure to support real-time threat detection due to bandwidth constraints, limited computational resources, and the absence of well-developed space-grade IDS solutions. The development of IDS technology that is both effective and can operate in a low resource (e.g. compute and memory) remains in its infancy, contributing to a significant gap in spacecraft cybersecurity.

Similarly, secure boot mechanisms, designed to ensure that only authenticated software can run on a system, are commonly implemented in terrestrial computing systems but face significant challenges in space. While secure boot is a critical countermeasure to prevent unauthorized or malicious software from executing, spacecraft require secure boot solutions that are effective and radiation-hardened to withstand the environmental hazards of space. Currently, limited secure boot capabilities are available to meet the stringent requirements of space missions. Engineers must contend with long development cycles and the challenge of balancing security features with the spacecraft's limited processing capacity and resistance to space-specific risks like radiation and extreme temperatures.

Additionally, many of the proposed countermeasures outlined in frameworks such as SPARTA and SPACE-SHIELD are theoretically sound but need more TRL for space applications. These frameworks provide critical guidance on protecting spacecraft from cyber and physical threats, yet their recommendations often involve countermeasures that have not been fully tested or validated in space environments. For instance, while intrusion detection and system redundancy are valuable defense strategies, implementing these techniques in spacecraft subsystems where every extra line of code or piece of hardware impacts power consumption and system stability remains a significant hurdle. The lack of space-hardened technologies means that many of the recommended mitigations may be challenging to operationalize for current and future missions. Many of these countermeasures are based on tried-and-true security principles widely accepted by the cybersecurity community, but their TRLs for space applications have yet to mature despite their proven effectiveness in other domains.

The absence of a mature inventory of space-specific countermeasures also means that engineers and mission planners must often rely on custom-built security solutions that require extensive testing and validation before deployment. The need to rely on custom solutions could lead to longer development timelines and increased costs, limiting the ability to rapidly adopt and implement new security measures in space systems. Furthermore, the lack of proven solutions increases the risk of failure during space missions, as untested countermeasures may not function as expected in the space environment, potentially compromising mission success.

While TTP frameworks offer a robust foundation for space system cybersecurity, their effectiveness could be hindered by the immaturity of many countermeasures in space environments. Intrusion detection and prevention systems and secure boot are just examples of countermeasures that lack maturity in the space industry, highlighting the ongoing challenge of developing space-grade security solutions that can meet the unique demands of space environments. Overcoming these obstacles will require continued research, testing, and innovation investment to raise the TRLs of these countermeasures, ensuring they can be reliably deployed in space missions and protecting spacecraft from an ever-evolving threat landscape.

In addition to technical constraints, there are also cultural and operational integration challenges. Most traditional space engineering teams are unfamiliar with TTP-based design thinking, and many development workflows are still siloed between safety, mission assurance, and cybersecurity teams. While TTP frameworks provide clear mappings between threats and countermeasures, applying them in a meaningful way often requires a level of cybersecurity fluency and threat modeling capability that may not yet exist within many spacecraft development organizations.

Furthermore, not all missions interpret TTPs the same way. The risk posed by a spoofed command, for example, might be mission-ending for a human-rated vehicle but tolerable for a non-critical Earth observation CubeSat. This underscores the need for mission context-aware tailoring of information within TTP frameworks which is something that is currently left as an exercise for each program rather than standardized or guided centrally.

6.2 THE NEED TO BALANCE RISK AND IMPLEMENT EMERGING COUNTERMEASURES

While TTP frameworks offer guidance for defending space systems, their adoption is sometimes met with hesitation, particularly due to concerns around the maturity of recommended countermeasures. It is true that some mitigations currently lack high TRLs in space environments. However, this reality must not deter the community from adopting these frameworks or exploring novel defenses. ***Mission Planners and engineers should not reject TTP frameworks or countermeasures simply because their TRLs are low; rather, they should treat them as starting points for progress and experimentation {6.2.1}***.

TTP frameworks are not static tools, but they are living resources that expose emerging threats, document adversary behaviors, and propose countermeasures that may not yet exist in a flight-qualified form. That is a feature, not a bug. In fact, by identifying theoretical threats or proposing aspirational defenses, TTP frameworks help push the community toward new forms of resilience and threat modeling not constrained by legacy mindsets. TTP frameworks should be embraced not only for what is immediately deployable, but for how they challenge conventional assumptions and expand the design space for cybersecurity.

In the past, the space domain focused primarily on physical risks like radiation, launch failure, orbital debris and protecting the command link with encryption. Cyber threats were rarely considered. That can no longer be the case. Even if a particular adversarial technique seems highly sophisticated or hasn't yet been observed in the wild, waiting for perfect evidence before planning defenses only ensures that those threats will succeed unchallenged.

By leaning forward, experimenting with lightweight intrusion detection, exploring ways to adapt secure boot, or prototyping behavioral anomaly detectors, engineers not only protect missions, but contribute to the broader TRL maturation of space-grade cybersecurity. ***Space system teams should treat early-stage countermeasures as dual-purpose: protective mechanisms and accelerants for future readiness {6.2.2}***.

Additionally, the value of these frameworks is not limited to their list of mitigations. Their true strength lies in:

- The structure they provide for threat modeling
- Their role in surfacing edge-case or complex attack chains
- Their ability to foster shared vocabulary and intelligence exchange

In many cases, the greatest benefit may come not from implementing a countermeasure immediately, but from the shift in perspective the framework introduces. A well-articulated threat scenario, even if not yet observed, may spark new subsystem-level design thinking or guide future anomaly detection requirements. ***Mission planners should adopt TTP frameworks to shape mindset and architecture, even when full implementation of mitigations is deferred {6.2.3}.***

Cybersecurity in space cannot afford to be purely reactive. Adoption of TTP frameworks, even imperfectly, signals a commitment to resilience, to innovation, and to collective progress. Rather than rejecting emerging ideas because they are early-stage or untested, space cybersecurity must be

characterized by strategic risk-taking, creative problem solving, and threat-informed design evolution. The threat won't wait so neither should your defenses.

6.3 "NEW SPACE" & FUTURE DEVELOPMENTS IN SPACE CYBERSECURITY

The rapid growth of the commercial space sector, often referred to as New Space, has introduced a wave of innovative, fast-moving companies into orbit. Unlike traditional space exploration and defense, which were predominantly driven by government and large aerospace contractors, New Space embraces a more dynamic, market-driven approach. These organizations embrace agile development cycles, reduced launch costs, and rapid iteration in hardware and software design. However, they also face a sobering reality: while launch is cheaper and development is faster, the threat landscape is more sophisticated and unforgiving than ever before.

Early space programs operated in relative cyber isolation. Today's missions must account for adversaries capable of a multitude of attack techniques like jamming, spoofing, intercepting, and executing code on the space segment. Unlike traditional space primes with decades of institutional knowledge, many New Space players are entering this contested domain without a deep foundation in cybersecurity engineering for spaceborne assets. This is where threat-informed TTP frameworks offer transformative value, especially the space and link specific frameworks SPARTA and SPACE-SHIELD. TTP frameworks enable New Space actors to stand on the shoulders of giants by applying decades of hard-earned threat intelligence and defense strategies from space and terrestrial domains.

By adopting these frameworks early, New Space companies can bootstrap their security practices with proven methodologies. Rather than building bespoke threat models from scratch, teams can immediately do some of the following:

- Map adversarial behaviors to spacecraft components,
- Leverage existing countermeasures tailored for space systems,
- Use established nomenclature for sharing and analyzing incidents,
- And align their architecture with compliance and resilience baselines.

This will enable efficiency and with tighter timelines, smaller budgets, and leaner engineering teams, New Space firms cannot afford to treat cybersecurity as a bolt-on feature. Frameworks like SPARTA compress the learning curve, enabling startups to integrate detection logic, hardening techniques, and access controls from the earliest design phases.

In essence, New Space represents an era where space exploration and operations are increasingly democratized, with a vibrant, competitive marketplace driving new solutions. By adopting recommended practices and robust cybersecurity frameworks, New Space companies are better positioned to innovate securely, protecting both their missions and the broader interests of the space industry.

7 CONCLUSIONS

The ATT&CK, SPARTA, and SPACE-SHIELD frameworks provide invaluable guidance for securing space systems across all three segments: ground, link, and space. While each framework has its unique focus, ATT&CK on enterprise and ground systems, SPARTA on space-specific threats, and SPACE-SHIELD on hybrid cyber/counter-space threats, their integration equips space system engineers and cybersecurity professionals with a comprehensive toolkit for building resilient space architectures.

Throughout this paper, real-world scenarios and example applications have shown how these frameworks can support threat-informed design, enhance detection and response, and align security practices with mission assurance objectives**.** As the space domain continues to evolve, collaboration between the space and cybersecurity communities remains essential**.** Continued engagement across industry, government, and academia will shape the future of secure space operations, driving innovation in both defensive technologies and operational best practices.

As threats evolve, so too must the strategies and tools used to defend space assets. The insights and recommend practices outlined in this document highlight the importance of structured, threat-informed approaches to achieving security across the space enterprise. By fostering a shared understanding of threats and defenses, these TTP frameworks can support a more secure and sustainable future for the space domain.

ANNEX A

SUMMARY OF RECOMMENDATIONS

This table provides and extraction of every recommendation from the paper into a single table.

Recommendation	Section #
Mission Planners should integrate these TTP frameworks into their cybersecurity methodologies to proactively identify the potential threats across all phases of attack chains, enabling a robust defense throughout the entire lifecycle.	2.1.1
Mission Planners should leverage the ATT&CK framework to identify and mitigate vulnerabilities within the ground segment, space system engineers can create layered defenses that address the most pressing cyber threats to the ground segment.	2.5.1.1
Mission Planners should integrate SPARTA & SPACE-SHIELD into the link segment as links are critical to the success of space missions, securing this essential for ensuring mission integrity, safeguarding sensitive data, and maintaining continuous control over space assets.	2.5.2.1
Mission Planners should integrate SPARTA and SPACE-SHIELD into the space segment, as the spaceborne components are central to mission execution, onboard autonomy, and data integrity.	2.5.3.1
Mission Planners should adopt an integrated methodology that combines frameworks (e.g., MITRE ATT&CK® and SPARTA) to analyze end-to-end attack chains across ground, link, and space segments, enabling threat identification, cross-domain mapping, and countermeasure testing to ensure resilient mission defenses	3.1
Mission architects should decompose the end-to-end mission architecture to identify critical assets in the ground, link, and space segments	3.1.1
Mission decomposition should include identification of key ground stations, communication relays, cross-links, and spacecraft subsystems such as command and data handling, attitude control, propulsion, and payload interfaces	3.1.2
Mission planners should document trust boundaries and identify where authentication, authorization, and encryption are applied or missing.	3.1.3
Mission architects should identify pivot points where an adversary could move laterally or vertically from one segment to another (e.g., from a compromised mission operations center to a command uplink)	3.1.4
Mission architects should model potential pivot points using threat-informed architecture diagrams or system dependency matrices. These matrices can help visualize how systems rely on one another across segments, revealing critical interfaces where added protections may be required	3.1.5
Mission architects should map threat actor behaviors using ATT&CK for enterprise and SPARTA for space-specific TTPs, connecting multi-segment attack chains	3.1.6
Mission architects should use the map to identify which components are most exposed to adversarial behaviors and evaluate whether existing countermeasures/protections are sufficient	3.1.7
Engineers and cybersecurity analysts should simulate realistic attack scenarios informed by the mapped TTPs and identified pivot points to enhance test and evaluation coverage	3.1.8
During the test planning phase, teams should augment standard test procedures with abuse cases that reflect how adversaries may exploit system interfaces, manipulate data flows, or misuse protocol behaviors especially across pivot points like uplinks, buses, or software interfaces	3.1.9

TTP informed abuse scenarios should be executed during formal system integration testing, hardware-in-the-loop (HIL) environments, cyber ranges, or simulation-based campaigns, where feasible, to evaluate how well the system resists or recovers from such attacks	3.1.10
Results from TTP informed abuse scenarios and simulations should drive iterative design refinement and inform the early selection and tailoring of protection techniques and countermeasures	3.1.11
Based on threat analysis and test results, mission architects should identify and prioritize protection opportunities at locations critical to mission assurance, including components that enable adversary escalation, impact mission success, or connect distinct trust domains	3.1.12
Mission architects deployment of defenses should be positioned to break the attack chain where adversaries can cause the most damage or gain the most leverage	3.1.13
Policy makers should use TTP frameworks to identify, prioritize, and map cyber threats to appropriate mitigations and system-level requirements across all space system segments	4.1.1
Risk assessments informed by TTP frameworks should be used to derive specific mitigations and security controls that are traceable to policy objectives and adversarial behaviors	4.1.2
Mission planners should trace high-level policy directives and associated threat concerns to relevant TTP frameworks, and from there derive mitigations and engineering requirements, ensuring threat-informed implementation that aligns with policy intent	4.1.1.1
Policy makers should incorporate references to evolving TTP frameworks within cybersecurity policy to ensure that the implementation of controls remains aligned with current adversary behavior	4.1.2.1
Where appropriate, policies may mandate the use of TTP frameworks as a baseline for risk assessment and mitigation planning across all space system segments	4.1.2.2
mission planners should continuously assess policy relevance in light of emerging threats and evolving TTP data	4.1.2.3
Mission planners and system implementers should also establish a feedback loop to inform policy makers when operational insights or threat evolutions expose policy gaps or misalignments	4.1.2.4
Engineering teams should leverage existing criticality analyses, often conducted as part of mission assurance or system design reviews, as the foundation for integrating TTP frameworks	4.2.1
Following criticality analysis, engineering teams should apply the appropriate TTP frameworks to conduct threat modeling against the mission critical components and functions	4.2.2
Cross-functional teams should collaboratively assess attack vectors across segments to ensure a complete understanding of interdependencies	4.2.3
Engineers should prioritize threat-to-defense alignment by first identifying adversarial techniques from the frameworks, then selecting appropriate mitigations based on system-specific risk profiles	4.2.4
To ensure coverage across all vectors, segment-specific teams should collaboratively align their defensive measures to ensure consistent implementation and eliminate seams in protection	4.2.5
Mission planners and system engineers should use this structured, threat-informed engineering process, from criticality analysis to defense mapping, to develop tailored cybersecurity architectures that align protection measures with mission priorities	4.2.6
Mission planners should incorporate outputs from this process into requirements traceability matrices, ensuring that each identified threat technique has a corresponding and verifiable mitigation or design control	4.2.7
Engineers should adopt a secure-by-design approach that incorporates threat-informed insights from the earliest stages of system development, rather than relying on reactive controls applied late in the lifecycle	4.2.1.1

New space programs and commercial entrants in particular should leverage decades of security research and lessons learned across aerospace and adjacent industries to rapidly mature their security while avoiding legacy technical debt. Engineering teams should align secure-by-design objectives with TTP-based threat modeling outputs to ensure protections are functionally relevant, risk-aligned, and segment-specific from the outset to avoid costly post-deployment mitigation	4.2.1.2
Where feasible, teams should adopt a layered defense strategy that applies multiple protection techniques to mitigate single-point failure from any one control/defense	4.2.1.3
Engineers should leverage TTP frameworks because they support traceability from threat identification through requirement derivation and validation, enabling security controls to be tested and verified against specific threat behaviors	4.2.1.4
System engineers should ensure that secure-by-design controls derived from TTP frameworks are allocated to specific segments and subsystems during early architectural trade studies, rather than deferred to implementation phases	4.2.1.5
Mission planners should ensure that security requirements are tailored to the unique functions and threat exposures of each subsystem, aligning protection techniques with the specific role and vulnerabilities of each component	4.2.2.1
Mission planners, including acquisition teams, should ensure that contractual system-level security requirements are derived from known threat techniques and explicitly linked to mission-specific failure modes to guarantee alignment with operational risk	4.2.2.2
mission planners should collaborate with acquisition professionals and system engineers to develop tailored cybersecurity requirements early in the acquisition lifecycle, ideally during request for proposal (RFP) development	4.2.2.3
Contracting officers should then require vendors to demonstrate traceability between implemented mitigations and the threat techniques they address, and this traceability should be reviewed as part of contract deliverables such as cybersecurity test plans, design documents, or system security engineering artifacts	4.2.2.4
Mission planners and test engineers should adopt TTP frameworks as the baseline structure for designing, executing, and evaluating cybersecurity test and evaluation campaigns across the space system lifecycle	4.2.3.1
Mission Planners should ensure TTP techniques are used as test stimuli to validate how systems respond under stress and determine whether detection, prevention, or recovery mechanisms are properly configured	4.2.3.2
Test engineers should explicitly include abuse cases derived from and mapped to known TTPs in their cybersecurity verification plans to uncover failure modes that may not emerge during traditional functional testing	4.2.3.3
Engineers should trace each TTP to the specific countermeasure it is intended to validate, enabling measurable security assurance and closing the gap between controls and real-world threats	4.2.3.4
Test engineers should tailor TTP-driven test scenarios to the specific threat profiles and architectural features of each space system segment	4.2.3.5
Engineers should integrate TTP-based test harnesses, automation frameworks, and adversary emulation tools during integration testing to quantify detection coverage, evaluate resilience, and improve system hardening	4.2.3.6
engineers should define pass/fail criteria based on whether the system appropriately detects, blocks, or mitigates the simulated threat behaviors	4.2.3.7
Mission Planners/System Engineers should refine mitigations based on failed TTP-based test outcomes, ensuring system protections are not only defined but proven through empirical evidence	4.2.3.8

Mission assurance teams should use TTP-based results to inform mission risk scoring and prioritize future investment in protection enhancements	4.2.3.9
Test documentation should include a threat-to-requirement-to-test-case mapping matrix that aligns each TTP with corresponding mitigations and test outcomes	4.2.3.10
This traceability should be maintained across lifecycle artifacts, including test reports, security assessments, and system accreditation documentation	4.2.3.11
Mission planners should archive TTP-based test results and use them to guide future spacecraft designs, enabling engineering teams to inherit proven countermeasures and avoid repeating past vulnerabilities	4.2.3.12
Mission planners should use TTP frameworks to anchor tabletop exercises in real-world adversarial techniques, ensuring that scenario design aligns with mission-specific threats and subsystem vulnerabilities	4.2.3.1.1
Cybersecurity and mission operations personnel should jointly participate in tabletop exercises to evaluate how decisions at each phase of the attack chain influence system availability, mission assurance, and recovery timelines.	4.2.3.1.2
Tabletop teams should document which TTPs were successfully mitigated, which failed prevention/detection, and which required escalation to system owners or incident response staff. This mapping should feed into a post-exercise gap analysis.	4.2.3.1.3
Red teams should use TTP frameworks to construct full-spectrum attack paths across the ground, link, and space segments focusing on seams where adversaries may pivot between subsystems or domains	4.2.3.2.1
Mission stakeholders should scope red team engagements to validate whether layered defenses and anomaly detection systems effectively detect or delay realistic threats derived from TTP frameworks, rather than relying solely on checklist compliance.	4.2.3.2.2
Mission planners and cybersecurity engineers should use red team results to calibrate residual risk levels and refine architectural protections (e.g., access controls, fault isolation strategies).	4.2.3.2.3
Mission planners should incorporate red team exercises and outputs into blue team training cycles, using observed detection failures, delayed responses, or missed IOCs as direct input to enhance procedures, playbooks, and alerting logic	4.2.3.2.4
Cybersecurity leads should develop post-exercise debriefs and replay sessions to walk blue teams through red team techniques, highlighting gaps in observability, misinterpretation of telemetry, or delays in escalating suspicious activity	4.2.3.2.5
Organizations conducting red team activities should maintain successful attack to technique mappings and ensure that each successful compromise is linked to a failed countermeasure/control, a missed detection rule, or a gap in policy coverage. These insights should be used to inform updates to system design, detection tools, and operational procedures	4.2.3.2.6
Standards development organizations should incorporate TTP-based mappings into their requirements and/or threat catalogs to ensure coverage of both traditional and emerging adversary behaviors across space system segments.	4.2.4.1
Compliance professionals and security control owners should document traceability from required controls to the TTPs they mitigate to ensure threat-relevant justification for each control selection.	4.2.4.2
System engineers should validate that their control implementations not only meet regulatory text but also map to adversarial techniques most likely to impact mission assurance	4.2.4.3
Test teams and assessors should use TTP-driven test cases to validate the effectiveness of compliance controls during audits, Plan of Action and Milestones closures, and security authorizations.	4.2.4.4

Mission planners developing space mission requirements or seeking certification should require that compliance artifacts include mappings between controls, mitigations, and adversarial behaviors derived from TTP frameworks.	4.2.4.5
Standards development organizations (SDOs) should incorporate TTP-derived adversary techniques and countermeasures as input into the creation or revision of standards to ensure alignment with realistic threat models and to drive security-by-design principles across the space domain	4.2.4.1.1
Standards efforts should use TTP-to-control mappings to identify gaps in current baseline protections and prioritize updates to standards that address real-world vulnerabilities	4.2.4.1.2
System engineers should leverage these mappings to ensure that security engineering and compliance assurance remain current with the evolving threat landscape	4.2.4.2.1
System engineers are encouraged to interpret these mappings as informative guidance rather than rigid mandates, validating applicability within the scope of their own operational environment and tailoring implementation to meet mission-specific objectives	4.2.4.2.2
Mission planners should work with appropriate cybersecurity personnel to develop internal CTI programs that are specifically tailored to space operations and informed by the unique mission, adversaries, and system architecture	5.1.1
Where possible, space system operators are should contribute to sector-wide threat intelligence initiatives (e.g., through ISACs or information-sharing agreements), particularly to expand collective awareness of spaceborne threats	5.1.2
Operators and mission assurance teams should incorporate space-focused TTP frameworks into their threat modeling and intelligence operations (i.e., collection and dissemination) to ensure alignment with emerging threat behaviors	5.1.3
systems engineers should establish mission-specific telemetry collection strategies that prioritize security-relevant observables	5.1.4
Space system defenders should integrate TTP-informed CTI into their detection architecture to improve situational awareness and shorten the time between threat manifestation and mitigation	5.1.1.1
Detection rules and alerting logic should reference TTP identifiers wherever feasible, enabling consistent tracking, reporting, and correlation of adversarial behaviors across missions and systems	5.1.1.2
Organizations involved in space system operations and information sharing should adopt a common domain relevant TTP frameworks to ensure consistency and fidelity in threat reporting and collaboration	5.2.1
Contributors to and developers of threat-sharing platforms should use framework-aligned TTP identifiers when submitting reports or analysis, to promote normalization and cross-organizational correlation	5.2.2
Space-focused CTI programs should incorporate TTP mapping practices to ensure consistency in threat analysis, improve information exchange, and support community-wide situational awareness	5.2.1.1
In general, space cybersecurity engineers should adopt methodologies proven in terrestrial IT environments, adapting them to address the distinct characteristics of ground, link, and space segments	5.2.1.2
Threat intelligence outputs should inform the development of detection rules and response actions based on mapped TTPs and associated observables	5.2.1.3
Threat intelligence products should include context on how mapped TTPs relate to mission impact, to improve relevance and downstream utility for recipients	5.2.1.4
Organizations producing threat intelligence should support cross-framework mapping to reflect multi-domain attack chains and enable correlation between terrestrial and spaceborne TTPs	5.2.1.5

Cybersecurity policies and mission security baselines should require or incentivize the use of STIX 2.1 for cyber threat intelligence exchange to enable interoperability and reduce friction in multilateral sharing environments	5.2.2.1
Tool vendors and space operators of space systems should adopt STIX 2.1 as the baseline format for sharing and consuming cyber threat intelligence to facilitate automation, consistency, and speed of response	5.2.2.2
Space system stakeholders should leverage existing STIX-compatible IOBs, such as those provided in the SPARTA framework, as a baseline for standardizing space-relevant observables across missions	5.2.3.1
the STIX standards body should extend existing STIX object definitions or leverage custom extensions to represent space-specific observables and indicators	5.2.3.2
Mission Planners and engineers should not reject TTP frameworks or countermeasures simply because their TRLs are low; rather, they should treat them as starting points for progress and experimentation	6.2.1
Space system teams should treat early-stage countermeasures as dual-purpose: protective mechanisms and accelerants for future readiness	6.2.2
Mission planners should adopt TTP frameworks to shape mindset and architecture, even when full implementation of mitigations is deferred	6.2.3