The Consultative Committee for Space Data Systems

Report Concerning Space Data System Standards

SECURITY THREATS AGAINST SPACE MISSIONS

INFORMATIONAL REPORT

CCSDS 350.1-G-3

GREEN BOOK

February 2022

The Consultative Committee for Space Data Systems

Report Concerning Space Data System Standards

SECURITY THREATS AGAINST SPACE MISSIONS

INFORMATIONAL REPORT

CCSDS 350.1-G-3

GREEN BOOK

February 2022

AUTHORITY

Issue:	Informational Report, Issue 3
Date:	February 2022
Location:	Washington, DC, USA

This document has been approved for publication by the Management Council of the Consultative Committee for Space Data Systems (CCSDS) and reflects the consensus of technical panel experts from CCSDS Member Agencies. The procedure for review and authorization of CCSDS Reports is detailed in *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-4).

This document is published and maintained by:

CCSDS Secretariat
National Aeronautics and Space Administration
Washington, DC, USA
E-mail: secretariat@mailman.ccsds.org

FOREWORD

This document is a CCSDS Informational Report that describes the threats that could potentially be applied against space missions. It characterizes threats against various types of missions and examines their likelihood and the results of their having been carried out.

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This Report is therefore subject to CCSDS document management and change control procedures, which are defined in *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-4). Current versions of CCSDS documents are maintained at the CCSDS Web site:

http://www.ccsds.org/

Questions relating to the contents or status of this document should be sent to the CCSDS Secretariat at the e-mail address indicated on page i.

At time of publication, the active Member and Observer Agencies of the CCSDS were:

Member Agencies

- Agenzia Spaziale Italiana (ASI)/Italy.
- Canadian Space Agency (CSA)/Canada.
- Centre National d'Etudes Spatiales (CNES)/France.
- China National Space Administration (CNSA)/People's Republic of China.
- Deutsches Zentrum für Luft- und Raumfahrt (DLR)/Germany.
- European Space Agency (ESA)/Europe.
- Federal Space Agency (FSA)/Russian Federation.
- Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
- Japan Aerospace Exploration Agency (JAXA)/Japan.
- National Aeronautics and Space Administration (NASA)/USA.
- UK Space Agency/United Kingdom.

Observer Agencies

- Austrian Space Agency (ASA)/Austria.
- Belgian Federal Science Policy Office (BFSPO)/Belgium.
- Central Research Institute of Machine Building (TsNIIMash)/Russian Federation.
- China Satellite Launch and Tracking Control General, Beijing Institute of Tracking and Telecommunications Technology (CLTC/BITTT)/China.
- Chinese Academy of Sciences (CAS)/China.
- Chinese Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- Danish National Space Center (DNSC)/Denmark.
- Departamento de Ciência e Tecnologia Aeroespacial (DCTA)/Brazil.
- Electronics and Telecommunications Research Institute (ETRI)/Korea.
- European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
- European Telecommunications Satellite Organization (EUTELSAT)/Europe.
- Geo-Informatics and Space Technology Development Agency (GISTDA)/Thailand.
- Hellenic National Space Committee (HNSC)/Greece.
- Indian Space Research Organization (ISRO)/India.
- Institute of Space Research (IKI)/Russian Federation.
- KFKI Research Institute for Particle & Nuclear Physics (KFKI)/Hungary.
- Korea Aerospace Research Institute (KARI)/Korea.
- Ministry of Communications (MOC)/Israel.
- National Institute of Information and Communications Technology (NICT)/Japan.
- National Oceanic and Atmospheric Administration (NOAA)/USA.
- National Space Agency of the Republic of Kazakhstan (NSARK)/Kazakhstan.
- National Space Organization (NSPO)/Chinese Taipei.
- Naval Center for Space Technology (NCST)/USA.
- Scientific and Technological Research Council of Turkey (TUBITAK)/Turkey.
- South African National Space Agency (SANSA)/Republic of South Africa.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- Swiss Space Office (SSO)/Switzerland.
- United States Geological Survey (USGS)/USA.

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 350.1-G-1	Security Threats against Space Missions, Informational Report, Issue 1	October 2006	Original issue, superseded
CCSDS 350.1-G-2	Security Threats against Space Missions, Informational Report, Issue 2	December 2015	Issue 2, superseded
CCSDS 350.1-G-3	Security Threats against Space Missions, Informational Report, Issue 3	February 2022	Current issue

CONTENTS

CONTENTS (continued)

Section Page

Figure

Table

1 INTRODUCTION

1.1 PURPOSE

The purpose of this document is to provide mission planners with an overview of threat assessment as well as the common threats and threat sources that exist for various categories of civilian space missions. Security mechanisms to counter threats as well as threat mitigations and threat contingencies are introduced.

1.2 SCOPE

The target audience for this document is the mission planner. This document assumes that the mission planner has little or no background knowledge of threat assessment and threat identification. This document's scope is to provide mission planners with an initial overview of applicable threats to space missions. However, an in-depth description of a threat or risk assessment methodology is beyond the scope of this document. The mission planner is urged to obtain more detailed information from the responsible security authorities within his or her organization.

In terms of system applicability, the scope of this document encompasses the entire mission operations infrastructure as well as data dissemination infrastructures, that is, the entire space and ground segments. It considers not only the systems that directly operate the spacecraft, but also the supply chain acquisition process and the systems that are used to process the associated data and disseminate it to users.

1.3 APPLICABILITY

This Informational Report is applicable to mission planning for all CCSDS-compliant space missions. In the past, space missions using CCSDS Recommended Standards were typically thought of as '*civil*' and '*scientific*' missions that were not likely targets of malicious attackers. This is in contrast with military or National Security missions that would more likely be targeted and have traditionally been highly protected. However, in today's global environment of ubiquitous cyber threats, this view is no longer true as all missions must be deemed to be targets.

1.4 RATIONALE

Information and communication technologies have advanced rapidly, and world-wide connectivity is ubiquitous. This also applies to civilian space mission infrastructures. As a result, this opens missions to threats that would not have previously existed. At the same time, many space missions have become part of critical infrastructures such as navigation, weather, and disaster response activities. As a result, all space missions must consider mechanisms or employ policies to mitigate risks resulting from high-likelihood threats.

1.5 DOCUMENT STRUCTURE

This document is divided into five sections. Section 1 provides this introduction. Section 2 provides an overview discussing relevance and use of the document. Section 3 describes the threat sources and threat vectors. Section 4 discusses threat methodologies. Section 5 describes illustrative threats against seven classes of civil space missions and threat mitigations and contingencies.

1.6 REFERENCES

The following publications are referenced in this document. At the time of publication, the editions indicated were valid. All publications are subject to revision, and users of this document are encouraged to investigate the possibility of applying the most recent editions of the publications indicated below. The CCSDS Secretariat maintains a register of currently valid CCSDS publications.

[1] *Information Security Glossary of Terms*. Issue 2. Report Concerning Space Data System Standards (Magenta Book), CCSDS 350.8-M-2. Washington, D.C.: CCSDS, February 2020.

[2] *An Introduction to Information Security*. National Institute of Standards and Technology Special Publication 800-12 Revision 1. Gaithersburg, Maryland: NIST, June 2017.

[3] *Information Technology—Security Techniques—Information Security Risk Management*. International Standard, ISO/IEC 27005:2018. Geneva: ISO, 2018.

[4] *Information Processing Systems—Open Systems Interconnection—Basic Reference Model—Part 2: Security Architecture*. International Standard, ISO 7498-2:1989. Geneva: ISO, 1989.

[5] "Glossary of Terms." National Information Assurance Training and Education Center. http://niatec.info/Glossary.aspx.

[6] *Security Guide for Mission Planners*. Issue 2. Report Concerning Space Data System Standards (Green Book), CCSDS 350.7-G-2. Washington, D.C.: CCSDS, April 2019.

[7] *Guide for Conducting Risk Assessments*. Revision 1. National Institute of Standards and Technology Special Publication 800-30. Gaithersburg, Maryland: NIST, September 2012.

2 OVERVIEW

2.1 INTRODUCTION

This document provides an overview of threats, potential impacts of threats, and possible mechanisms to counter threats against space missions. The document also includes illustrative examples of threats against various classes of space missions. Detailed threat analyses should be carried out by mission planners in coordination with the responsible security authorities in order to understand and state their mission's security requirements.

With the increasing level of security awareness in the Information Technology (IT) community, civil and scientific missions must be security proactive and should not wait to act until after a security incident occurs. All possible threat sources and threats should be analyzed and understood (i.e., a threat assessment). Depending on the severity of the threats, the mission planner should consider implementing protection of assets and critical services so that they are less vulnerable to the identified threats. Once relevant threat sources and threats have been identified, the mission planner should execute a risk assessment with the help of security experts and in accordance with the risk assessment procedures of his or her organization. Risk assessment guidance is outside the scope of this document.

2.2 DEFINITION OF THE TERM 'THREAT'

The term 'threat' is central in this document and thus a common understanding is established here. While this document discusses threats against CCSDS missions, the terms 'threat' and 'risk' are often used interchangeably, which is incorrect.

ISO 27005 (reference [3]) defines 'threat' as 'A potential cause of an incident that may result in harm of systems and organization'.

ISO 7498-2 (reference [4]) defines 'threat' as 'A potential violation of security'.

CCSDS 350.8-M-2 (reference [1]) defines 'risk' as 'Possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability'.

A 'threat' is a function of a threat agent's capability and intent to do harm. 'Risk' is a function of the probability that an organization will be targeted and the harm that might be caused. We can distinguish the difference between threat and risk in mathematical terms:

– **Threat** = *Capability* × *Intent*;

– **Risk** = *Probability* × *Harm*.

This document will concentrate primarily on providing the reader with information on threat.

2.3 THREAT AGENTS/SOURCES AND VULNERABILITIES

A threat agent (or threat source) can be human or non-human and can be intentional or unintentional. All threat agents attempt to do harm against a physical or logical resource/asset. In cases in which the resource has one or more vulnerabilities, they each may potentially be exploited by a threat agent, resulting in a compromise of system Confidentiality, Integrity, or Availability (C-I-A).

Loss of confidentiality will result in unauthorized disclosure of information. Loss of integrity can result in falsification of transactions as well as unauthorized modification or destruction of information. Loss of availability will result in a temporary or permanent loss of access to critical resources. Overall, the loss of C-I-A might result in harm to a Space Agency's operations, assets, or individuals. Figure 2-1 illustrates the interactions between C-I-A and the various aspects of the overall system.

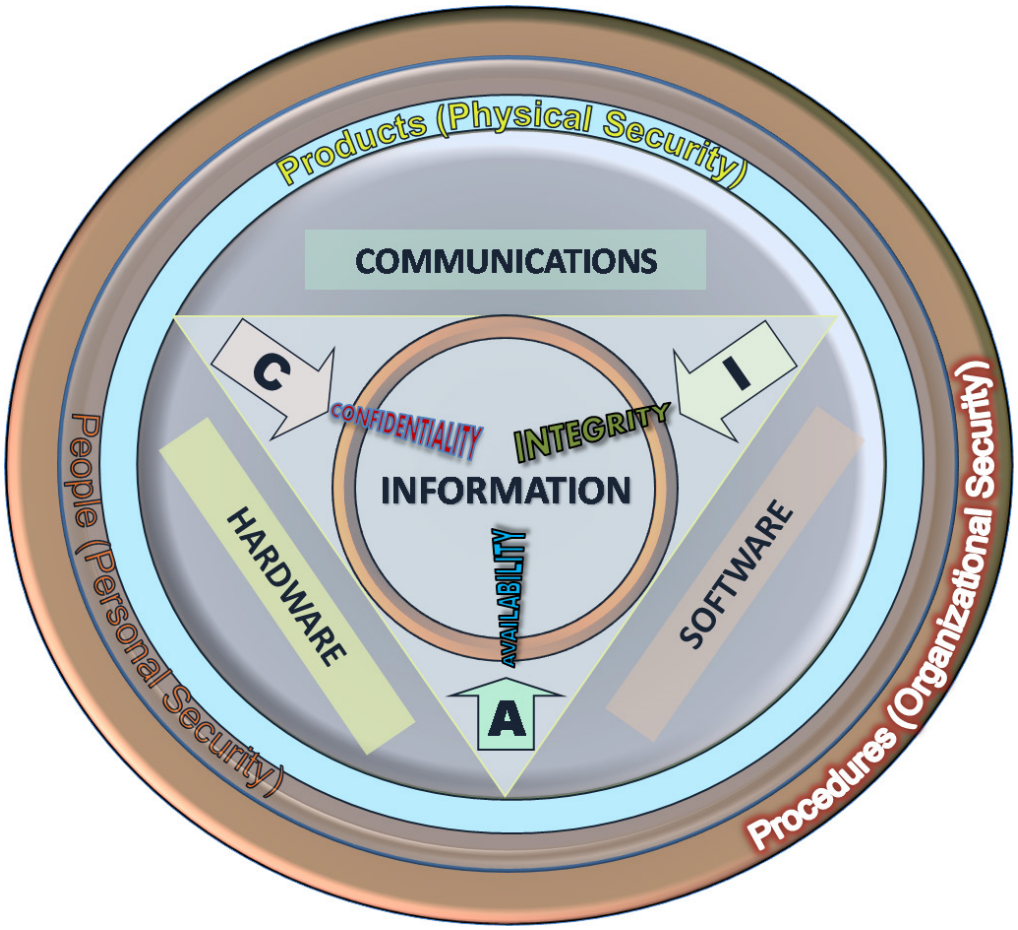

Figure 2-1: Confidentiality, Integrity, and Availability Interactions[1]

[1] John M. Kennedy; http://commons.wikipedia.org/wiki/File:CIAJMK1209.png; permission granted to copy, distribute, and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation.

A threat agent who aims to execute intentional attacks will take the time to study a resource or a system of resources to generate possible attack vectors that exploit a vulnerability. Security controls and mechanisms may be employed as countermeasures against threats. These countermeasures can reduce the likelihood of the threat being effective against a specific vulnerability.

Computer systems are typical targets of threats since they often suffer from a number of vulnerabilities. The National Institute of Standards and Technology's (NIST) Special Publication 800-12 (reference [2]) states,

> *If the system is vulnerable, threat sources can lead to threat events. A threat event is an incident or situation that could potentially cause undesirable consequences or impacts. An example of a threat source leading to a threat event is a hacker installing a keystroke monitor on an organizational system. The damage that threat events may cause on systems varies considerably. Some affect the confidentiality and integrity of the information stored in a system while others only affect the availability of the system*.

For example, a commercial entity may assume that there are threats against their infrastructure by virtue of their connection to the Internet. The threats are valid even if countermeasures are implemented. However, the system can reduce the likelihood of the threat agent's success and reduce the risk against their infrastructure by implementing security controls. The level of reduction in the risk will be based on the quality and suitability of the controls applied and the strength of the security functions inherent in the controls. Regular reassessment of the risks, the threats, and the controls is important and often overlooked.

2.4 ATTACKS AGAINST MISSIONS AND MISSION IMPACTS

Civilian space missions are supported by a large system of interconnected resources and assets both in space and on the ground (e.g., computer systems, communication devices, processors, etc.). Each of these entities is potentially vulnerable and could be exploited by a threat agent. A successful attack may impact a mission. Mission impacts can range from insignificant (e.g., software crash resulting in safe mode) to catastrophic (e.g., loss of mission). Successful attacks may result in a loss of mission C-I-A.

The relationship between threat agents and mission impacts is illustrated figure 2-2. A list of threats applicable to CCSDS mission infrastructures is presented and discussed in section 3.

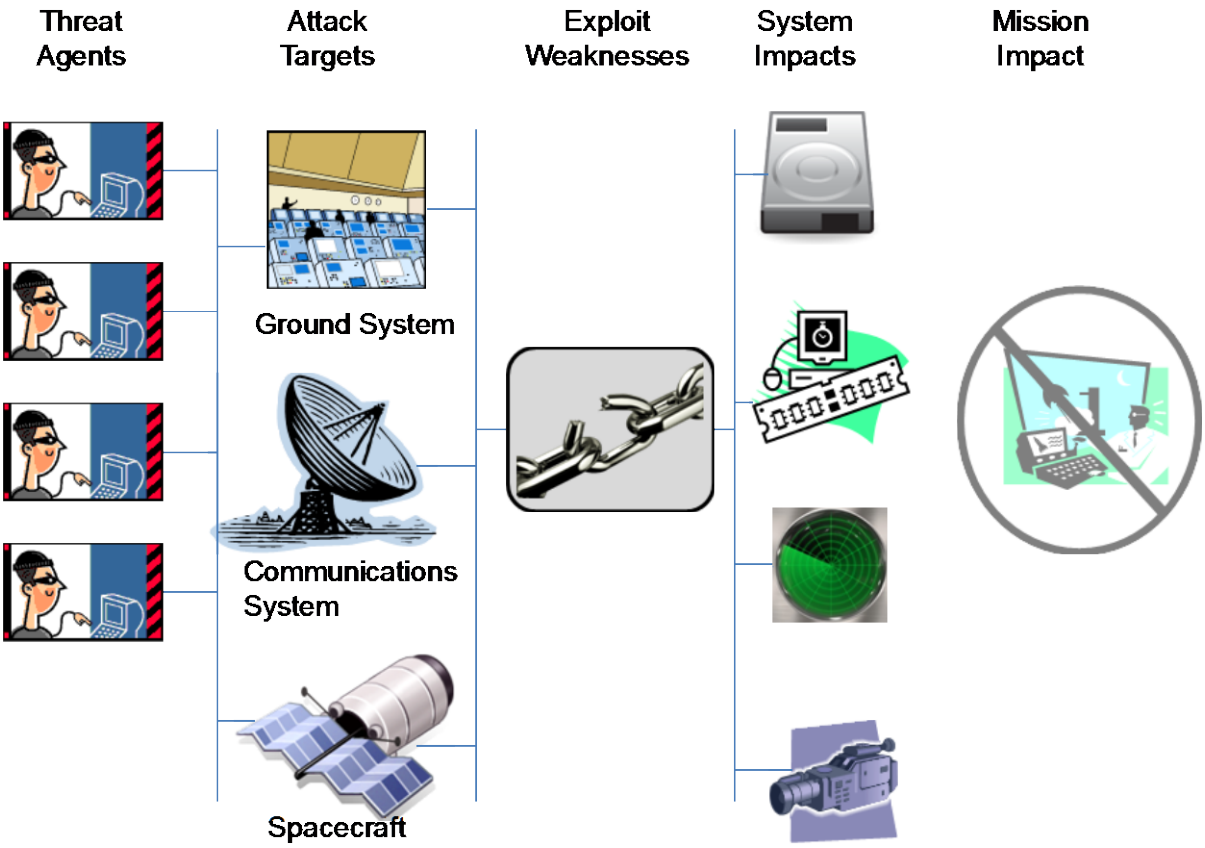

Figure 2-2: Threat Scenario

3 THREAT SOURCES AND THREATS APPLICABLE TO SPACE MISSIONS

3.1 OVERVIEW

This section introduces threats specific to space missions that should be considered when performing a threat assessment. These threats may come from a wide variety of sources. Figure 3-1 illustrates a generic threat model. The following subsections will provide a review of possible threat sources.

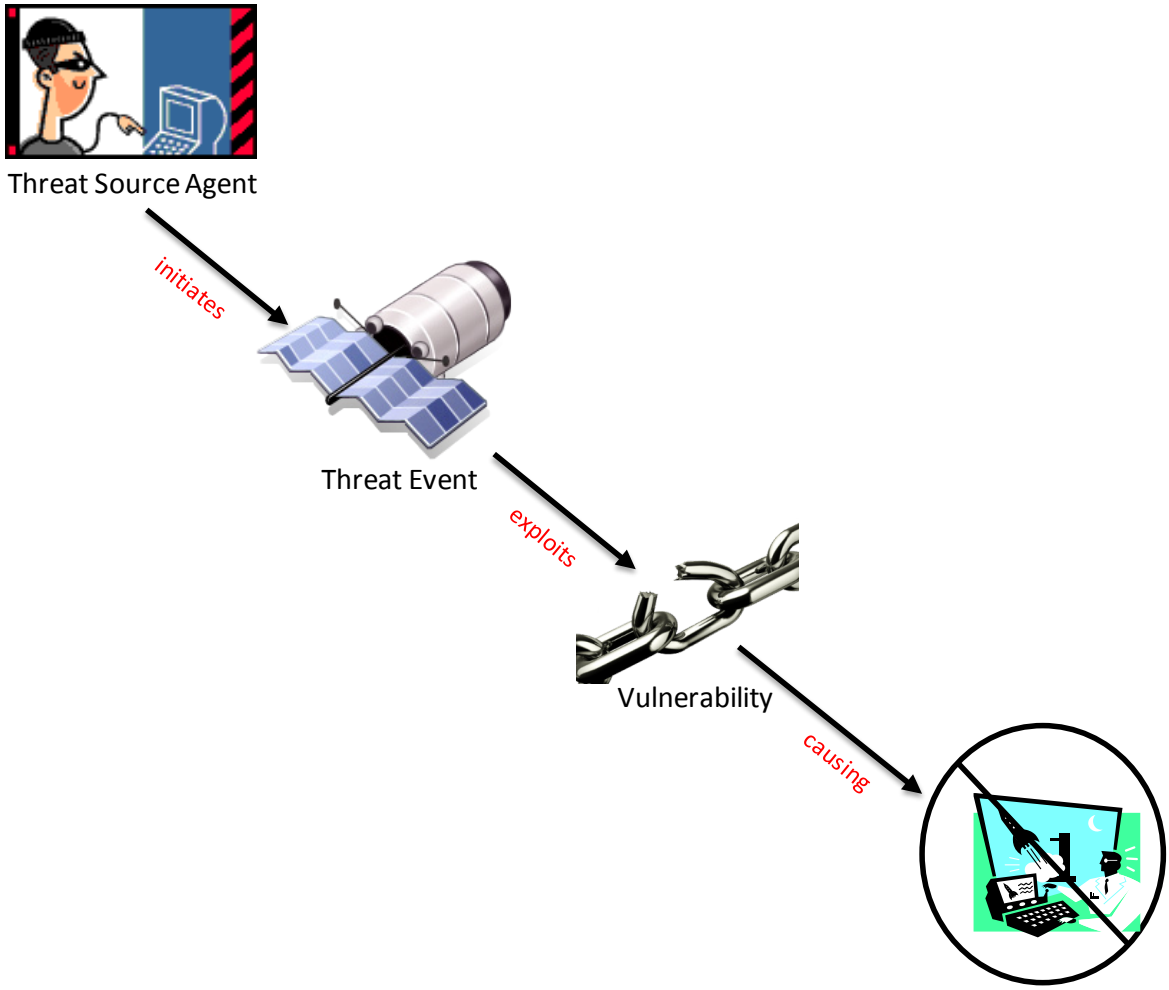

Figure 3-1: Threat Model

3.2 THREAT SOURCES APPLICABLE TO SPACE MISSIONS

There is a wide variety of possible threat sources against CCSDS missions. The following non-exhaustive list contains the most relevant threat sources for space missions:[2]

- Adversarial Sources:
  - terrorists and criminals;
  - foreign intelligence services;
  - subversives or political activists;
  - computer hackers;
  - commercial competitors;
- Insider Sources:
  - dishonest maintenance personnel;
  - dishonest systems personnel;
  - disgruntled staff members;
  - trusted business partners;
  - inadvertent actions of staff members;
  - rogue astronauts;
- Environmental Sources:
  - natural or man-made disasters;
  - pandemics;
  - space weather (e.g., solar flares);
  - space debris;
  - infrastructure failures/power outages;
- Structural Sources:
  - software failures;
  - hardware failures.

[2] An exhaustive list can be found in NIST Special Publication 800-30, appendix D (reference [7]).

3.3 TYPES OF THREATS

3.3.1 OVERVIEW

There are two types of threats: active and passive. These will be explained and discussed in the subsections below.

3.3.2 ACTIVE THREATS

An active threat requires a threat source, such as an Advanced Persistent Threat (APT) actor, to initiate a sequence of events that actively interferes with the system in an attempt to exploit a vulnerability.

Active threats include, but are not limited to, exploits such as:

- communications system jamming resulting in denial of service and loss of availability and data integrity;
- attempting access to an access-controlled system resulting in unauthorized access;
- replay of recorded authentic communications traffic at a later time with the hope that the authorized communications will provide data or some other system reaction;
- masquerading as an authorized entity in order to gain access;
- exploitation of software vulnerabilities (bugs/weaknesses);
- supply chain interruption or manipulation;
- unauthorized modification or corruption of data; and
- introduction of malicious software such as a virus, worm, Distributed Denial-Of-Service (DDOS) agent, keylogger, rootkit, or Trojan Horse.

Active threats may be carried out against spacecraft, ground systems, and communications systems.

3.3.3 PASSIVE THREATS

Passive threats do not require a threat source to actively attack or interfere with the operations of the target system(s).

Passive threats include but are not limited to exploits such as:

- tapping of communications links (wireline, RF, network) resulting in loss of confidentiality;
- traffic analysis to determine which entities are communicating with each other without the ability to access the communicated information.

3.4 COMMON THREATS APPLICABLE TO SPACE MISSIONS

3.4.1 OVERVIEW

There is a wide variety of possible threats against CCSDS missions. The following non-exhaustive list contains the most relevant threats for space missions.[3] Figure 3-2 provides an overview of the threats identified in subsequent sections and maps them to the elements of CCSDS space missions. A mission planner must be wary of what is trusted and must validate and re-validate that trust.

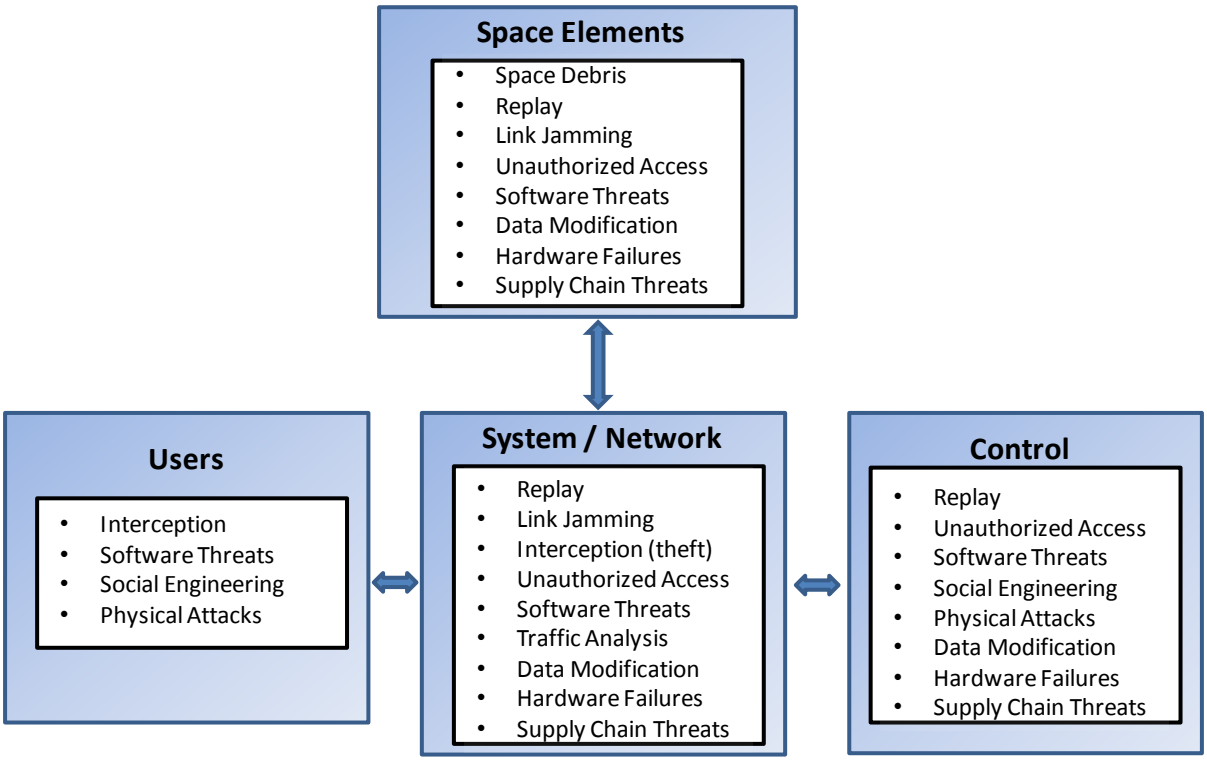

Figure 3-2: Potential Threats to CCSDS Space Missions

Figure 3-3 provides an illustrative mapping of threats to specific areas of a space mission's communications infrastructure.

[3] A more extensive list of example threat events can be found in NIST Special Publication 800-30, appendix E (reference [7]).

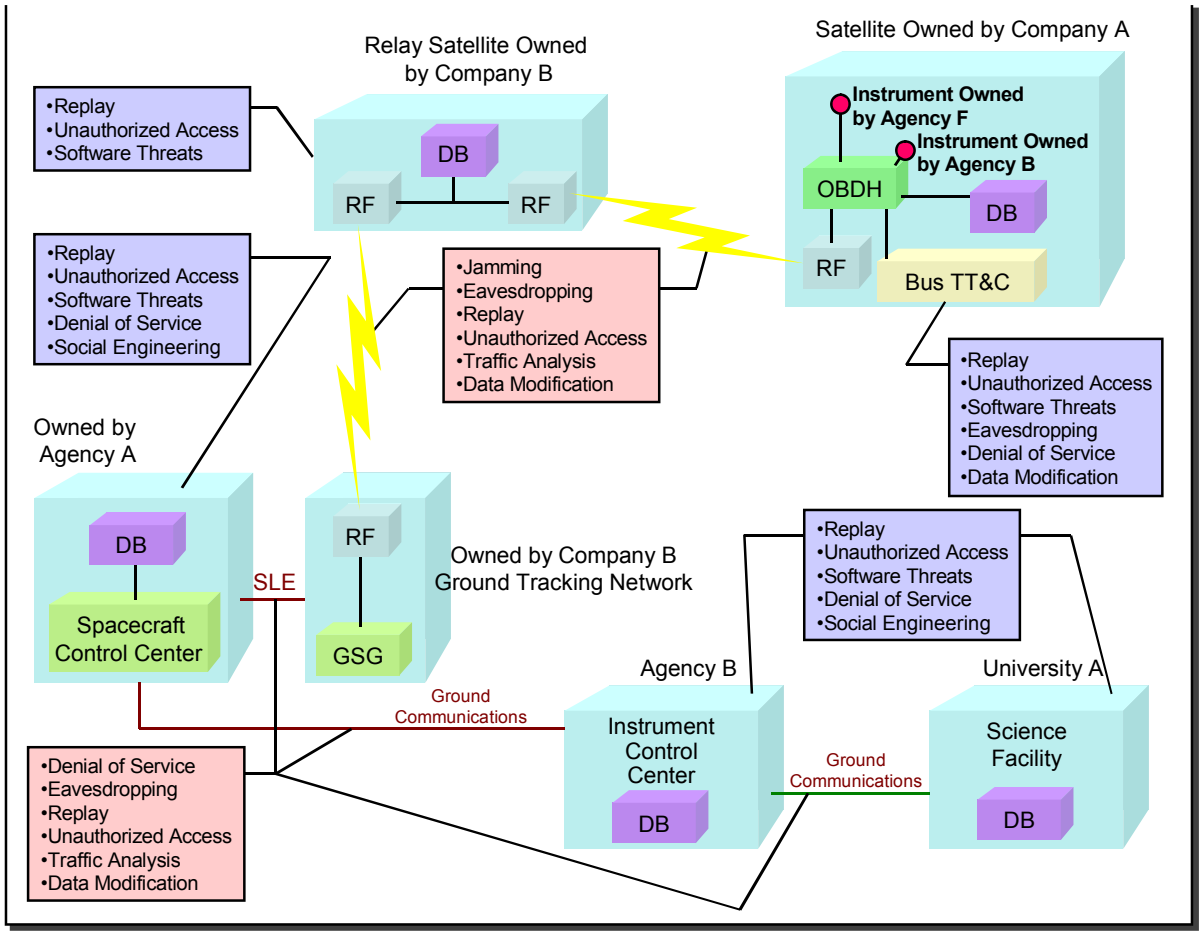

Figure 3-3: CCSDS Security Communications Threats

3.4.2 DATA MODIFICATION

Applicable to: Space Segment, Ground Segment, Space-Link Communication.

Description: Data Modification refers to the intentional or non-intentional alteration of data, whether being communicated or at rest. Data modification implies a breach of integrity. Data could be modified at its source, during transmission between ground and space systems, onboard a spacecraft, or at the ground system.

Possible Mission Impact: Modification might result from software failures, bugs or weaknesses, hardware failures, use of unauthorized software, counterfeit hardware or software, or active attempts to change/modify data to deny its use. A modified or corrupted spacecraft command could result in catastrophic loss if either no action occurred (e.g., command is discarded) or the wrong action was taken onboard a spacecraft. For example, if a navigation maneuver command was corrupted, the spacecraft might end up in an unusable orbit, miss an encounter with a comet/planet/asteroid, or be destroyed.

3.4.3 GROUND SYSTEM LOSS

Applicable to: Ground Segment.

Description: A successful exploitation of a vulnerability through a physical/cyber-attack might disable the ground facility and directly affect the operation of the mission and the services provided. An attack might also take physical control of the facility to take control of the spacecraft without technically attacking the facility's systems. Environmental factors might also result in the loss of a ground facility. Tornados, hurricanes, tsunamis, flooding, or other weather-related factors could result in physical damage to the facilities or the loss of electrical power to the ground station.

Possible Mission Impact: The loss of a ground system might result in the loss of data, loss of access to data in a timely manner, degradation or loss of spacecraft commanding, or loss of the entire mission.

3.4.4 INTERCEPTION OF DATA

Applicable to: Space Segment, Ground Segment, Space-Link Communication.

Description: Data transmitted to and received from spacecraft are sent over Radio Frequency (RF) communications links. All RF communications are subject to interception by listening to the specific allocated frequencies. However, RF used for spacecraft communication are potentially less susceptible to interception than common radio because of the large ground antennas and narrow beam widths used to communicate between the ground and space and, conversely, the low power and narrow beam widths used from space to ground. This is mission dependent since all missions are different.

As spacecraft evolve to use optical communications, data interception will become more difficult, but not impossible. A threat actor trying to intercept optical communication would have to be very close to the narrow optical beam width.

If ground system communications are operating over public networks (e.g., the Internet) they are susceptible to interception since the data is routed through many uncontrolled resources that could be tapped.

Possible Mission Impact: If the data is not encrypted, or is encrypted using weak algorithms or implementations, interception of data may result in the loss of data confidentiality and data privacy. In addition to those entities authorized for the data, non-authorized entities may also gain access. The interception of data could also result in masquerade or replay attacks.

3.4.5 JAMMING

Applicable to: Space Segment, Ground Segment, Space-Link Communication.

Description: Denial of communications to and from a spacecraft accomplished by interfering with the RF or optical signal. This can be achieved by injecting noise, transmitting on the same frequency from another source, Electromagnetic Pulse (EMP), high powered microwave, or overpowering the original source. Optical sensors could be blinded and solar arrays damaged by lasers.

Possible Mission Impact: The interference can result in link loss and loss of mission control. Spacecraft commanding, as well as the ability to receive science or engineering data from the spacecraft, could be blocked. In addition, authorized access to system resources can be impeded, possibly delaying time-critical operations on both the ground and in space.

3.4.6 DENIAL-OF-SERVICE

Applicable to: Space Segment, Ground Segment.

Description: Denial-of-service attacks could occur in several ways: consumption of resources (e.g., communication bandwidth, processor bandwidth, disk space, memory), disruption of system/network configurations (e.g., routing changes), disruption of state information (e.g., persistent network connection resets), disruption of network components (e.g., router or switch crashes), or obstruction/destruction of communications paths. High powered lasers could blind sensors or destroy solar cells. High powered microwaves could cause CPU restarts, disruption of electronics, or memory errors.

Possible Mission Impact: Denial-of-service attacks could prevent authorized access to resources, both in space and on the ground. Ground and space systems and their networks could be greatly affected by loss of system availability, which could result in an inability to control a mission or obtain data from a mission.

3.4.7 MASQUERADE

Applicable to: Space Segment, Ground Segment.

Description: Authentication of an entity's true identity is crucial for applying access control policies. When access control policies are enforced, selected entities can perform specific actions, while other entities may be denied. Access controls can be rendered useless if entities disguise their true identity or can masquerade as another entity. The lack of authentication can affect all space communications.

Possible Mission Impact: If an instrument operator masquerades as a spacecraft operator, incorrect spacecraft health and status actions might result in a loss of the mission. Likewise, if an external entity can masquerade as a spacecraft operator, unauthorized commands could be transmitted to the spacecraft resulting in damage, data loss, or loss of a mission.

3.4.8 REPLAY

Applicable to: Space Segment, Ground Segment, Space-Link Communication.

Description: Transmissions to or from a spacecraft or between ground system computers can be intercepted, recorded, and played back at a later time.

Possible Mission Impact: If the recorded data were a command set from the ground to the spacecraft and they are re-transmitted to their originally intended destination, they might be executed, potentially for a second time. If the replayed commands are not rejected, they could result in duplicate spacecraft operations, such as a maneuver or a spacecraft re-orientation with the result that a spacecraft is in an unintended orientation (e.g., tumbling, antenna pointed in the wrong direction, solar arrays pointed away from the sun, or the reset of critical onboard parameters).

3.4.9 SOFTWARE THREATS

Applicable to: Space Segment, Ground Segment.

Description: Users, system operators, and programmers often make mistakes that can result in security problems. Users or administrators can install unauthorized or unvetted software that might contain bugs, viruses, or spyware, which could result in system instability. System operators might misconfigure a system resulting in security weaknesses. Programmers may introduce logic or implementation errors that could result in system vulnerabilities, or instability/reliability. Weaknesses may be discovered after a mission is operational, which external threat agents might attempt to exploit to inject instructions, software, or configuration changes.

Possible Mission Impact: Software threats could result in loss of data and safety issues such as loss of spacecraft control, unauthorized spacecraft control, or loss of mission.

3.4.10 UNAUTHORIZED ACCESS

Applicable to: Space Segment, Ground Segment.

Description: Access control policies based on strong authentication provide a means by which only authorized entities are allowed to perform system actions, while all others are prohibited.

Possible Mission Impact: An access control breach would allow an unauthorized entity to take control of a ground system or a ground system network, shut down a ground system, upload unauthorized commands to a spacecraft, execute unauthorized commands aboard a crewed mission, obtain unauthorized data, contaminate archived data, or completely shut down a mission. If weak access controls are in place, unauthorized access might be obtained. Interception of data might result in unauthorized access because identities, identifiers, or passwords might be obtained. Social engineering could be employed to obtain identities, identifiers, passwords, or other technical details permitting unauthorized access.

3.4.11 TAINTED HARDWARE COMPONENTS

Applicable to: Space Segment, Ground Segment.

Description: Hardware, both ground and flight, might fail. Redundancy is used to ensure continuity of operation. However, hardware might be tainted because it could contain hidden, malicious capabilities. The hardware might not be produced by the claimed manufacturer and be counterfeit.

Possible Mission Impact: The mission may be seriously impacted by hardware that does not have all of the specified capabilities of the genuine hardware or software. The tainted hardware may lead to premature failure. The mission may be impacted by additional, hidden capabilities contained in the counterfeit hardware such as transmitting data to unauthorized and unintended destinations, intermittent system instability, damage to other system components, or other undesirable system effects that could lead to mission loss.

3.4.12 SUPPLY CHAIN THREATS

Applicable to: Space Segment, Ground Segment.

Description: Software and hardware originate from various sources. Some of the sources are domestic, and some are not. Some are vetted, trusted sources, whereas some are not. Chain-of-custody, even from vetted sources, is required to ensure that only genuine hardware and software, in full compliance with requirements and specifications, is delivered and integrated. Trust must be validated and re-validated as the supply chain may have access to sensitive materials that require protection.

Possible Mission Impact: Supply chain disruption could result in genuine parts being unavailable, thereby resulting in the potential use of counterfeit parts. If trust is not verified, counterfeit hardware or software could be delivered and used on a mission without anyone's knowledge. The hardware or software may contain malicious circuits or malicious code that could result in unintended mission consequences. The hardware or software might allow unauthorized access to the system or it might prohibit authorized access. It might send telemetry or observation data to an unauthorized entity. It might ignore authentic commands. Some of these scenarios could result in mission loss. Partners in the supply chain may expose or provide access to sensitive materials. Connected suppliers with security weaknesses could be compromised and used to launch attacks on Agencies, systems, and missions.

4 THREAT ASSESSMENT METHODOLOGY

4.1 GENERAL

In order to determine which security threats should be considered for a space mission, a threat assessment methodology should be followed.[4] In many cases, the threat assessment methodology is embedded in or part of an overall risk assessment methodology. As a result, an organization may follow a threat assessment methodology but not a separate specific risk assessment methodology. In the following subsections, a generic description of a typical threat assessment methodology is presented and then refined into a space-specific methodology.

4.2 METHODOLOGY OVERVIEW

As previously stated, a universally accepted threat assessment methodology does not exist, and organizations implement or use different (corporate, national, or international) methodologies. However, a generic approach to threat assessment can be identified and is common to most of these methodologies.

Figure 4-1 illustrates the NIST SP 800-30 Revision 1 (reference [7]) risk assessment process. The first activities executed in this process constitute preparation for the assessment and threat identification. While this report focuses only on the first threat assessment step, it is important to understand the entire relationship.

A threat assessment always begins with a system characterization. This involves the identification and valuation of assets and the understanding of the overall architecture of the system: its individual subsystems, its business function, and its interfaces. This general characterization is a prerequisite to executing a threat assessment. Additionally, general assumptions and limitations are defined. The second step requires the identification of threat sources and events, which is the main activity performed in a threat assessment. Depending on the system, a catalogue of threats may already exist or a new catalogue will have to be created. For space missions, this report contains a catalogue of space-mission-specific threat sources and events that can be used as input to a baseline by the mission planner (see sections 4.3 and 5). The third step is the identification of vulnerabilities that could be exploited by the identified threats. This step leads from the threat assessment into the primary portion of the risk assessment. Thus, the output of the threat assessment is the preliminary identification of risks.

There are several well-known and respected risk assessment methodologies commonly used by organizations that include threat assessment concepts:

- NIST SP 800-30: Guide for Conducting Risk Assessments (reference [7]);
- ISO 27005:2018 Information Security Risk Management (reference [3]).

[4] Agencies may have their own standard threat assessment methodology. There might also be national, governmental standards. Additionally, there are various public domain and commercial threat assessment methodologies that may be used.

The mission planner should consult with security experts or security accreditation organizations to identify the threat assessment methodology applicable to their respective organization. It is also highly recommended that a security expert consultancy is used while executing the threat assessment.

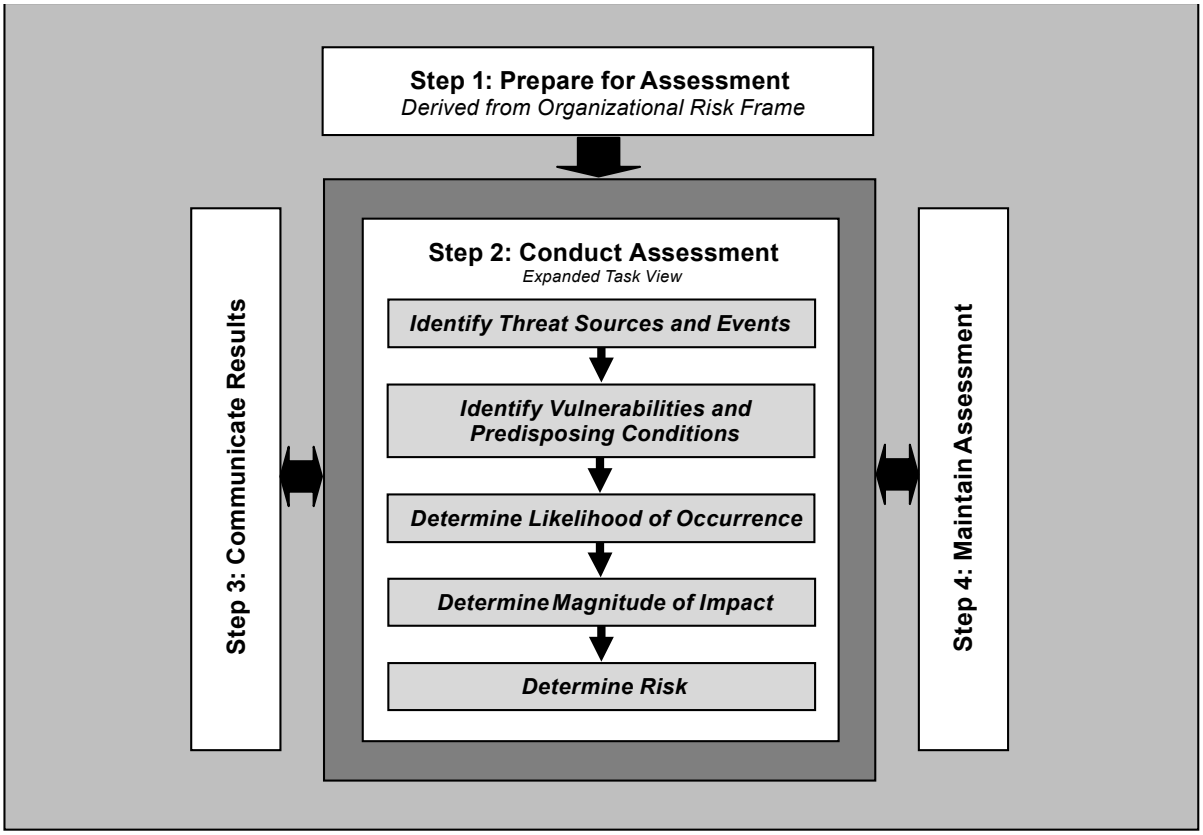

Figure 4-1: Risk Assessment Process[5]

[5] From reference [7].

4.3 ILLUSTRATIVE SPACE-DOMAIN SPECIFIC THREAT ASSESSMENT METHODOLOGY

For illustrative purposes, the generic threat assessment methodology introduced previously has been refined for use in space mission threat analyses. Figure 4-2 illustrates the threat analysis methodology.

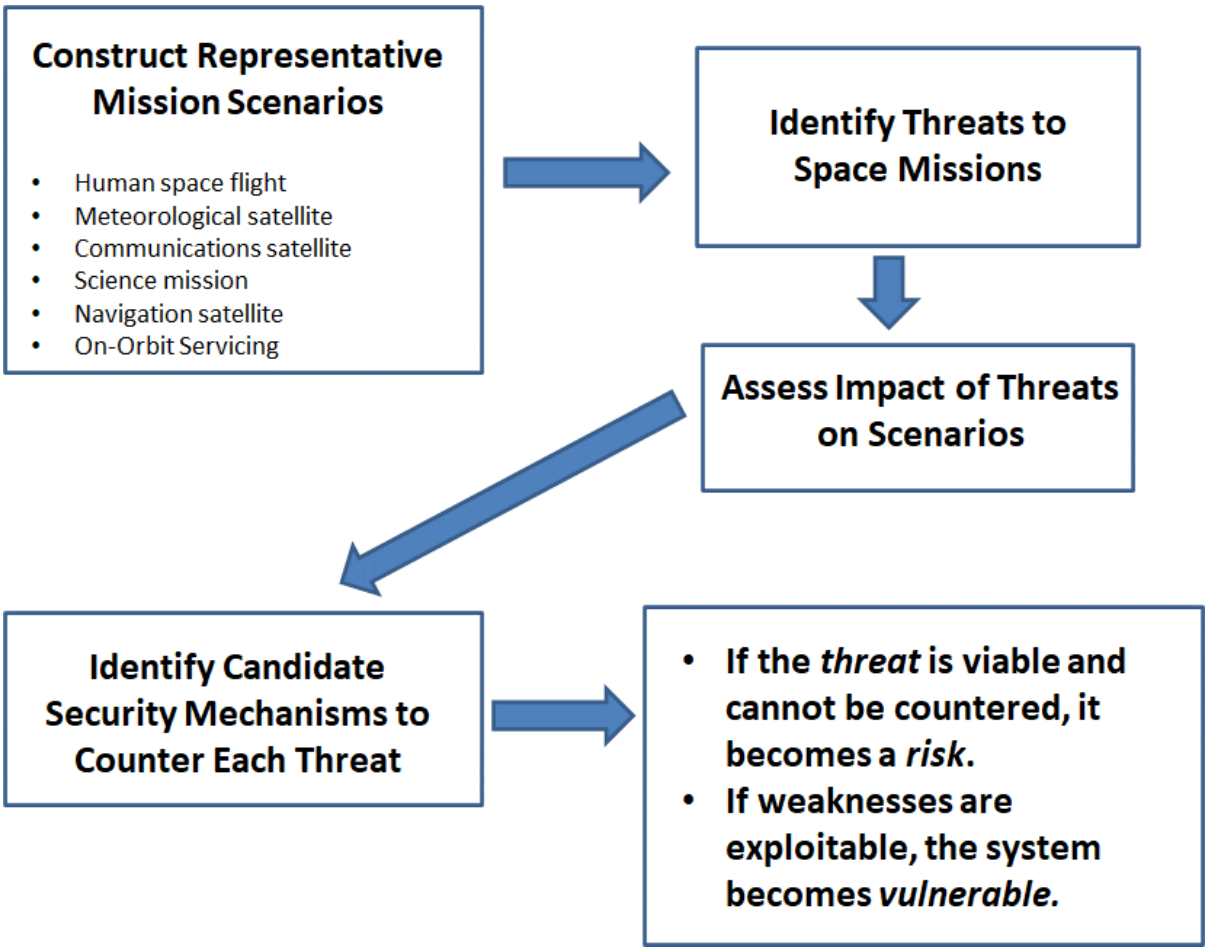

Figure 4-2: Space Mission Threat Assessment Process

4.4 THREAT ASSESSMENT AND MISSION PLANNING

As stated in the introduction, this document provides mission planners with a threat overview that can be used to help them understand their mission's specific security shortcomings as inputs to performing a threat assessment.[6]

[6] More specifics can be found in the CCSDS Security Guide for Missions Planners (reference [6]).

If one looks at the way a threat assessment should be conducted, it is very similar, if not identical to, a quality assurance process with the following steps:

- Mission start (design): recommendations resulting from the threat assessment and the risk analysis are produced;
- Implementation: standards (CCSDS and others), contingency and disaster recovery planning, and conformance testing are used;
- Operations: operating procedures, continuous contingency capability, and threat monitoring are applied.

A threat assessment begins by identifying the primary assets requiring protection, gathering data about relevant threats and impacts, and then analyzing the gathered information. Each asset or asset class being protected is assigned a *value*. Asset valuation should take into account the asset's intrinsic value as well as the near-term and long-term impacts if it is compromised. Sometimes assets can be assigned a monetary value. However, for some assets, a monetary value might prove to be impractical or impossible (e.g., when assessing impacts to safety, society, or reputation). In those cases, a determination must be made in assessing the value of the asset, system, and/or data (if it were to be lost or compromised). In some cases, a reputational impact might be assessed as a 'national disgrace'. In other cases, various impact types might be assessed as damaging to a national space program. In yet other cases, a system or data loss might be assessed as a situation of 'too bad — we'll get more data from another mission'.

Threats against the assets must be identified and analyzed to determine their likelihood of occurrence and their potential to inflict harm. If there is no (or very low) likelihood of the occurrence of a threat, then it is not a major concern. If there is a likelihood of occurrence, it should be rated either numerically (e.g., on a scale from 1 to 5) or, alternatively, as high, medium, or low.

A vulnerability analysis compares the outcome of the threat assessment against the functional mission systems. A valid threat is of no concern if there are no system vulnerabilities that it can exploit. For example, if there is a known Windows malware vulnerability, but all of the mission systems are UNIX, Linux, or VxWorks, then there is no concern, and no action needs to be taken.

If there are threats that are likely to occur, and there are system vulnerabilities that could be exploited by the threat, it must be determined if there is a way to counter the threat, either by technical means or policy. If neither is available, or if it is determined that the costs are too high to implement a response, then the residual risk must be documented and accepted by the mission authorities.

5 THREATS AGAINST ILLUSTRATIVE MISSION TYPES

5.1 OVERVIEW

The following subsections illustrate the threat assessment of various mission categories that may be of interest to civil space mission planners. This is not an exhaustive or detailed threat analysis. Rather, it is meant to provide a top-level description of the kinds of threats that are possible against these types of missions. The categories of missions that will be considered are:

- human space flight:
  - commercial,
  - Agency-sponsored;
- Earth observation (meteorological) satellites:
  - Low Earth Orbit (LEO),
  - Geosynchronous Earth Orbit (GEO);
- communications satellites:
  - LEO constellations,
  - MEO constellations,
  - GEO;
- science missions:
  - near Earth/Earth orbit,
  - lunar,
  - interplanetary/deep space;
- navigation satellites; and
- On-Orbit Servicing (OOS).

Additional mission sub-types, such as those with hosted payloads or fractionated/distributed spacecraft, may also exist. For example, a near-Earth science mission may have been built by one Agency but hosts payloads from other Agencies or commercial entities. Or a mission may be carried out via a constellation or swarm of spacecraft. These missions may potentially have increased threats because of the variety of payloads, additional communications links, and their varying implementation of security mechanisms.

However, for simplicity, this document discusses only the previously listed, top-level illustrative missions.

The categories denote missions in varying orbits, and the threats against each orbit type may be different. GEO missions, although at a higher altitude requiring high communications power levels and larger antennas, can potentially be more vulnerable than a low-Earth mission because they provide continuous visibility in their coverage area. LEO missions, on the other hand, provide limited view periods but can be reached with low power levels and small antennas.

A special case of LEO mission are communication constellations (e.g., *Iridium, Orbcomm, Globalstar, O3b, Starlink*). Whereas each individual LEO spacecraft provides only limited visibility, with a constellation, there are many spacecraft in orbit, providing almost continuous global coverage with satellite cross links creating a space network. Therefore the LEO communication constellation provides an adversary with more opportunity for attack than a single LEO mission.

More infrastructure, resulting in higher cost, is required to attack deep-space/interplanetary missions because of the larger antennas and greater power required to communicate with the spacecraft.

5.2 HUMAN SPACE FLIGHT

Human crewed space platforms such as the International Space Station (ISS), are examples of missions with international cross support and cooperation. Modules aboard the ISS have been built by different nations, and the ISS crews come from a variety of countries. As a result, the ISS is an international system-of-systems integrated to make a whole system but not necessarily supporting security mechanisms equally. Table 5-1 illustrates a possible threat analysis for the ISS. These threats, the impacts, and the security mechanisms to counter the threats are only *illustrative* and do not reflect what is actually being done on the International Space Station.

Table 5-1: Manned Space Flight—Hypothetical International Space Station Threat Analysis

Applicable Threats	Impacts	Probability (1 = Lowest, 5 = Highest)[7]	Security Mechanisms to Counter Threat
Data corruption	– Modification of information – System damage	2	– Data integrity schemes (hashing, check values, digital signatures) – Resilient hardware (e.g., SOS)
Ground facility physical attack	Loss of command, control, and data	2	Guards, gates, access controls, backup site(s)
Interception	Loss of sensitive data	3	Data encryption, spread spectrum
Jamming	– Loss of command and telemetry link – Loss of access to resources	2	– Multiple uplink paths – Spread spectrum
Denial-of-Service	– Loss of access to resources	3	– Firewalls – Routers – Switches – Intrusion Prevention Systems – Private, segregated networks – Encryption & authentication – ISP ‘edge’ support, mitigation
Masquerade	– Potential to disrupt operations (uplink) – Potential to receive false information (downlink)	3	– Strong authentication of uplinked commands and downlinked data – Access control scheme – Vetting of staff – No use of open networks
Replay	System damage (possible safety of life issues	1	Authenticated command counter, timestamp
Software threats	– Undesirable events – System damage – Enable other threats	2	– Acceptance testing – Independent Verification and Validation (IV&V) – Code walkthroughs – Automated code analysis – Run-time security monitoring – Auditing – Software partitioning (trusted computing base) – Supply chain confidence

[7] These probabilities (in this and all subsequent tables) are for *illustrative* purposes only. Mission planners should perform a threat analysis to determine actual probabilities for their specific missions.

Applicable Threats	Impacts	Probability (1 = Lowest, 5 = Highest)[7]	Security Mechanisms to Counter Threat
Unauthorized Access	– Disruption of operations – System damage (possible safety of life issues)	4	– Encryption of TT&C and mission data – Authentication/authorization of commands – Accountability of access – No use of open networks – Authentication tokens (e.g., smart card) – Auditing & accounting – Non-repudiation
Tainted Hardware Components	– Hidden, malicious capabilities – System instability – System damage – Undesirable system effects	3	– Supply chain confidence – Authenticity of hardware – Vetted hardware suppliers – Vetted hardware production – Analysis of hardware functionality
Supply Chain	– Delivery interruptions – Parts unavailability – Counterfeit parts – Counterfeit software	4	– Supply chain confidence – Vetted/trusted sources – Chain of custody evidence

5.3 EARTH OBSERVATION SATELLITES

Earth observation satellite systems illustrate missions that can either be scientific in nature or a critical asset (national or international such as a meteorological spacecraft). Over the years, these missions have become a necessary part of our climate observation and prediction infrastructure. Earth observation satellites may be in low Earth orbit, polar orbit, or geosynchronous orbit. Table 5-2 illustrates the possible threats against Earth Observation satellites.

Table 5-2: Earth Observation Satellite Threat Analysis

Applicable Threats	Impacts	Probability (1 = Lowest, 5 = Highest)[8]	Security Mechanisms to Counter Threat
Data Corruption	– Modification of information – System damage	4	– Data integrity schemes (hashing, check values, digital signatures) – Resilient hardware (e.g., SOS)
Ground facility physical attack	Loss of command, control, and data	2	– Guards, gates, facility design, access controls, backup site(s)
Interception	– Loss of sensitive data – Theft of commercial data	3 (LEO) 3 (GEO)	Protection of archive & distribution systems via encryption
Jamming	– Loss of command and/or telemetry link – Loss of access to resources – Commercial impact	3 (LEO) 2 (GEO)	– Multiple uplink paths – Multiple downlink paths – Spread spectrum
Denial-of-Service	– Loss of access to resources	3	– Firewalls – Routers – Switches – Intrusion Prevention Systems – Private, segregated networks – Encryption & authentication – ISP ‘edge’ support, mitigation
Masquerade	– Potential to disrupt operations (uplink) – Potential to receive false information (downlink)	2	– Strong authentication of uplinked commands and downlinked data – Access control scheme – Vetting of staff – No use of open networks
Replay	– System damage (possible safety of life issues	1	– Authenticated command counter, timestamp

[8] These probabilities are for *illustrative* purposes only and will change for specific missions. Mission planners should perform a threat analysis to determine actual probabilities for their specific missions.

Applicable Threats	Impacts	Probability (1 = Lowest, 5 = Highest)[8]	Security Mechanisms to Counter Threat
Software threats	– Undesirable events – System damage – Enable other threats	2	– Acceptance testing – IV&V – Code walkthroughs – Automated code analysis – Run-time security monitoring – Auditing – Software partitioning (trusted computing base) – Supply chain confidence
Unauthorized Access	– Theft of commercial data – Disruption of operations – System damage	3	– Encryption of TT&C and mission data – Authentication/authorization of commands – Accountability of access – Access control in control and dissemination systems – No use of open networks – Authentication tokens (e.g., smart card) – Auditing & accounting – Non-repudiation
Tainted Hardware Components	– Hidden, malicious capabilities – System instability – System damage – Undesirable system effects	3	– Supply chain confidence – Authenticity of hardware – Vetted hardware suppliers – Vetted hardware production – Analysis of hardware functionality
Supply Chain	– Delivery interruptions – Parts unavailability – Counterfeit parts – Counterfeit software	4	– Supply chain confidence – Vetted/trusted sources – Chain of custody evidence

5.4 COMMUNICATIONS SATELLITES

Geosynchronous Earth orbit communications satellites have become one of the most ever-present parts of the international communications infrastructure. These satellites are relied upon to relay voice, video, data, paging, etc., all over the world. Outages of these satellites would wreak havoc with the international communications systems, as is best witnessed by the major concerns during periods of high sun-spot activity.

Constellations of communications satellites in low Earth orbit with cross links, such as *Iridium*, *Globalstar*, *and Starlink*, are operating, with additional constellations in progress. LEO constellations reduce the communications latency experienced with GEO satellites while still providing extensive Earth coverage previously only available from GEOs. However, the reduced threat to LEO satellites, as previously discussed, no longer holds true because of the on-orbit routed network created by the satellite constellation. While a single LEO satellite is visible for a short amount of time, each satellite in the constellation acts as a relay to its neighbor spacecraft, resulting in increased threats against the entire constellation. A threat analysis of generic communications satellite systems is illustrated in table 5-3.

Table 5-3: Communications Satellite Threat Analysis

Applicable Threats	Impacts	Probability (1 = Lowest, 5 = Highest)[9]	Security Mechanisms to Counter Threat
Data corruption	– Modification of information – System damage	4 (GEO) 2 (LEO)	Data integrity schemes (hashing, check values, digital signatures)
Ground facility physical attack	Loss of command, control, and data	2	Guards, gates, facility design, access controls
Interception	– Loss of sensitive data – Theft of commercial data	4 (GEO) 2 (LEO)	Protection of traffic (potentially user responsibility)
Jamming	– Loss of TT&C and/or traffic circuits – Commercial impact – Loss of access to resources – Possible safety impact	3 (GEO) 3 (LEO)	– Multiple uplink and downlink paths – Multiple access points – Spread spectrum – Spacecraft autonomy
Denial-of-Service	– Loss of access to resources	3	– Firewalls – Routers – Switches – Intrusion Prevention Systems – Private, segregated networks – Encryption & authentication – ISP ‘edge’ support, mitigation
Masquerade	– Potential to disrupt operations (uplink) – Potential to receive false information (downlink)	2	– Strong authentication of uplinked commands and downlinked data – Access control scheme – Vetting of staff – No use of open networks
Replay	– System damage (possible safety of life issues)	1	– Authenticated message counter, timestamp
Software threats	– Undesirable events – System damage – Enable other events	2	– Acceptance testing – IV&V – Code walkthroughs – Automated code analysis – Run-time security monitoring – Auditing – Software partitioning (trusted computing base) – Supply chain confidence
Unauthorized Access	– Disruption of operations – System damage	2	– Encryption of TT&C data – Authentication/authorization of commands – Auditing & accounting – Non-repudiation

[9] These probabilities are for *illustrative* purposes only and will change for specific missions. Mission planners should perform a threat analysis to determine actual probabilities for their specific missions.

Applicable Threats	Impacts	Probability (1 = Lowest, 5 = Highest)[9]	Security Mechanisms to Counter Threat
Tainted Hardware Components	– Hidden, malicious capabilities – System instability – System damage – Undesirable system effects	3	– Supply chain confidence – Authenticity of hardware – Vetted hardware suppliers – Vetted hardware production – Analysis of hardware functionality
Supply Chain	– Delivery interruptions – Parts unavailability – Counterfeit parts – Counterfeit software	4	– Supply chain confidence – Vetted/trusted sources – Chain of custody evidence

5.5 SCIENCE MISSIONS

Science missions constitute a class of missions that are not typically considered operational or part of a national (or international) infrastructure. In as much as this is the case, while the threats against such categories of missions are essentially the same as for other missions, the resulting risks are decreased compared to those in which life or infrastructure may be disrupted. For science missions, while money was spent to build the system and gather the information, for the most part, only the monetary investment and the data collection will be lost. Science missions tend to fall into three subclasses:

– near-Earth/Earth orbit;

– lunar;

– interplanetary/deep space.

Near-Earth and Earth orbit missions are similar to other LEO, Medium Earth Orbit (MEO), and GEO missions, but because they are not part of an ‘operational infrastructure’, the resulting risks are diminished.

Lunar missions and interplanetary/deep-space missions are similar to one another. However, they take on multiple threat characteristics depending on whether they are in Earth orbit prior to their cruise phase, in cruise, or in some cases, in a sling-shot trajectory in which they leave Earth orbit and go into cruise but come back to near-Earth for a sling-shot effect to a more distant encounter.

While in Earth orbit or near Earth, these missions are just like other LEO, MEO, and GEO missions. However, their threat characteristics change with time as they move in and out of Earth orbit.

When they finally leave Earth orbit, more power is required to communicate with them than Earth orbit spacecraft, they have a non-orbit cruise phase while in transit from the Earth to their target destination(s), and they will have limited viewing from the Earth once in orbit or when landed at their respective destination(s). However, where these missions differ is in the amount of power and the size of the Earth station antennas required for communication.

Interplanetary/deep-space missions require significantly more power and larger dishes for reliable communications than do lunar missions. Likewise, interplanetary/deep-space missions suffer from much longer communications latency than do lunar missions. As a result, for interplanetary missions, the increased power and the large size of the antenna dishes provide immunity from 'casual' attack, although not from hostile 'nation-state' attacks.

What must be remembered is that both lunar and interplanetary missions must also consider the threats faced by Earth orbit and near-Earth missions because they are in those orbits early in their chronology.

A threat analysis for international science category missions is illustrated in table 5-4.

Table 5-4: Science Mission Threat Analysis

Applicable Threats	Impacts	Probability (1 = Lowest, 5 = Highest)[10]	Security Mechanisms to Counter Threat
Data corruption	– Modification of information – System damage	3	– Data integrity schemes (hashing, check values, digital signatures)
Ground facility physical attack	Loss of command, control, and data	2	Guards, gates, facility design,access control
Interception	Loss of sensitive data	1 (deep-space) 3 (lunar) 3 (Earth)	– Data encryption – Spread spectrum
Jamming	– Loss of TT&C and/or traffic circuits – Commercial impact – Loss of access to resources – Possible safety impact	1 (deep-space) 2 (lunar) 3 (Earth)	– Multiple uplink and downlink paths – Multiple access points – Spread spectrum
Denial-of-Service	– Loss of access to resources	3	– Firewalls – Routers – Switches – Intrusion Prevention Systems – Private, segregated networks – Encryption & authentication – ISP ‘edge’ support, mitigation
Masquerade	– Potential to disrupt operations (uplink) – Potential to receive false information (downlink)	2	– Strong authentication of uplinked commands and downlinked data – Access control scheme – Vetting of staff – No use of open networks
Replay	– System damage	1	– Authenticated message counter, timestamp
Software threats	– Undesirable events – System damage	2	– Acceptance testing – IV&V – Code walkthroughs – Automated code analysis – Run-time security monitoring – Auditing – Software partitioning (trusted computing base) – Supply chain confidence

[10] These probabilities are for *illustrative* purposes only and will change for specific missions. Mission planners should perform a threat analysis to determine actual probabilities for their specific missions.

Applicable Threats	Impacts	Probability (1 = Lowest, 5 = Highest)[10]	Security Mechanisms to Counter Threat
Unauthorized Access	– Disruption of operations – System damage – Potential loss of mission	3	– Authentication/authorization of commands – Access control in control center – Access control in cross support network – Accountability of access – No use of open networks – Auditing & accounting – Non-repudiation
Tainted Hardware Components	– Hidden, malicious capabilities – System instability – System damage – Undesirable system effects	3	– Supply chain confidence – Authenticity of hardware – Vetted hardware suppliers – Vetted hardware production – Analysis of hardware functionality
Supply Chain	– Delivery interruptions – Parts unavailability – Counterfeit parts – Counterfeit software	4	– Supply chain confidence – Vetted/trusted sources – Chain of custody evidence

5.6 NAVIGATION SATELLITES

Navigation satellites, such as the Global Positioning System (GPS), Glonass, BeiDou, and Galileo, are irreplaceable for enterprises such as airlines, maritime, trucking, and the military. Similarly, navigation satellites are in private use for automobile navigation systems, cellular telephones for navigation and emergency locating, and via hand-held units in hunting, exploring, and hiking. Like communications satellites, the loss of navigation satellite systems would result in the loss of investment dollars. There would also be a high potential for the loss of life, safety, and infrastructure. A threat analysis of this mission category is illustrated in table 5-5.

Table 5-5: Navigation Satellite Threat Analysis

Applicable Threats	Impacts	Probability (1 = Lowest, 5 = Highest)[11]	Security Mechanisms to Counter Threat
Data Corruption	– Modification of information – System damage	3	– Data integrity schemes (hashing, check values, digital signatures) – Encryption of timing data
Ground facility physical attack	Loss of command, control, and data	3	Guards, gates, facility design, access control, backup sites(s)
Interception	Loss of sensitive data	1	– Data encryption – Spread Spectrum
Jamming	– Loss of TT&C and/or traffic circuits – Commercial impact – Loss of access to resources – Possible safety impact	3	– Multiple uplink and downlink paths – Multiple access points – Frequency hopping – Spread spectrum
Denial-of-Service	– Loss of access to resources	3	– Firewalls – Routers – Switches – Intrusion Prevention Systems – Private, segregated networks – Encryption & authentication – ISP ‘edge’ support, mitigation
Masquerade	Potential to disrupt operations	2	– Strong authentication – Access control scheme – Vetting of staff – No use of open networks
Replay	System damage	1	Authenticated message counter

[11] These probabilities are for *illustrative* purposes only and will change for specific missions. Mission planners should perform a threat analysis to determine actual probabilities for their specific missions.

Applicable Threats	Impacts	Probability (1 = Lowest, 5 = Highest)[11]	Security Mechanisms to Counter Threat
Software threats	– Undesirable events – System damage	2	– Acceptance testing – IV&V – Code walkthroughs – Automated code analysis – Run-time security monitoring – Auditing – Software partitioning (trusted computing base) – Supply chain confidence
Unauthorized Access	– Disruption of operations – System damage – Potential loss of mission	3	– Authentication/authorization of commands – Access control in control center – Access control in cross support network – Accountability of access – No use of open networks – Auditing & accounting – Non-repudiation
Tainted Hardware Components	– Hidden, malicious capabilities – System instability – System damage – Undesirable system effects	3	– Supply chain confidence – Authenticity of hardware – Vetted hardware suppliers – Vetted hardware production – Analysis of hardware functionality
Supply Chain	– Delivery interruptions – Parts unavailability – Counterfeit parts – Counterfeit software	4	– Supply chain confidence – Vetted/trusted sources – Chain of custody evidence

5.7 ON-ORBIT SERVICING MISSIONS

OOS mission Servicer Spacecraft have unique capabilities and responsibilities for approaching and modifying other spacecraft. Loss of control of the servicer spacecraft before approaching a Client Space Object (CSO) could result in a loss to the servicer organization and loss of the service to the CSO. Loss of control of the servicer spacecraft or CSO while they are in close proximity or mated/docked could potentially result in those same losses for both servicer and client organizations, as well as loss of both spacecraft. The unique capability of servicing spacecraft to conduct rendezvous and proximity operations and to interact with other spacecraft creates a significant risk that must be considered.

Table 5-6: On-Orbit Servicing Mission Threat Analysis

Applicable Threats	Impacts	Probability (1 = Lowest, 5 = Highest)[12]	Security Mechanisms to Counter Threat
Data Corruption	– Modification of information – System damage	3	Data integrity schemes (hashing, check values, digital signatures)
Ground facility physical attack	Loss of command, control, and data	3	Guards, gates, facility design, access control, backup sites(s)
Interception	Loss of sensitive data	1	– Data encryption – Spread Spectrum
Jamming	– Loss of TT&C and/or traffic circuits – Commercial impact – Loss of access to resources – Possible safety impact	3	– Multiple uplink and downlink paths – Multiple access points – Frequency hopping – Spread spectrum
Denial-of-Service	– Loss of access to resources	3	– Firewalls – Routers – Switches – Intrusion Prevention Systems – Private, segregated networks – Encryption & authentication – ISP ‘edge’ support, mitigation
Masquerade	– Potential to disrupt operations	2	– Strong authentication – Access control scheme – Vetting of staff – No use of open networks –
Replay	System damage	1	Authenticated message counter
Software threats	– Undesirable events – System damage	2	– Acceptance testing – IV&V – Code walkthroughs – Automated code analysis – Run-time security monitoring – Auditing – Software partitioning (trusted computing base) – Supply chain confidence

[12] These probabilities are for illustrative purposes only and will change for specific missions.

Applicable Threats	Impacts	Probability (1 = Lowest, 5 = Highest)[12]	Security Mechanisms to Counter Threat
Unauthorized Access	– Disruption of operations – System damage – Potential loss of mission – Damage to a third-party spacecraft. – Damage to servicer spacecraft or client spacecraft – Political fallout and industry mistrust – Disclosure of Sensitive Information	3	– Authentication/authorization of commands – Access controls; flight, flight-to-ground and on-ground – Access controls using data and service segregation, and least privilege principles – Auditing & accounting – Vetting of staff – No use of open networks – Non-repudiation
Tainted Hardware Components	– Hidden, malicious capabilities – System instability – System damage – Undesirable system effects	3	– Supply chain confidence – Authenticity of hardware – Vetted hardware suppliers – Vetted hardware production – Analysis of hardware functionality
Supply Chain	– Delivery interruptions – Parts unavailability – Counterfeit parts – Counterfeit software	4	– Supply chain confidence – Vetted/trusted sources – Chain of custody evidence

5.8 THREAT SUMMARY AND SECURITY MECHANISMS TO COUNTER THREATS

Table 5-7: Threat Summary

Applicable Threats	Security Mechanisms to Counter Threat	Threat Mitigations	Threat Contingencies
Data corruption	– Data integrity schemes (hashing, check values, digital signatures) – Resilient hardware	– Secure data backups	– Verify integrity of backups
Ground facility physical attack	– Guards – Gates – Facility design – Access control	– Alternate/backup ground facilities	– Failover or hot-standby to alternate site
Interception	– Protection of traffic via encryption, frequency hopping, spread spectrum – Protection of archive & distribution systems via encryption	– Use secure transmission	– Use hardened transmission facilities
Jamming	– Multiple uplink/downlink paths – Multiple access points – Frequency hopping, spread spectrum	– Legislation – Monitoring – Interdiction – Reporting	– Have alternate frequencies or transmission facilities available
Denial-of-Service	– Firewalls – Routers – Switches – Intrusion Prevention Systems – Private, segregated networks – Encryption & authentication – ISP ‘edge’ support, mitigation	– Access control lists – Rate limiting – ‘expect’ scripting – Service screening	– Safe Mode – Fault detection and isolation –
Masquerade	– Strong authentication – Access control scheme – Vetting of staff – No use of open networks	– Strong authentication – Session tokens – Behavior – Timestamps	– Intrusion Detection Systems – Intrusion Prevention Systems
Replay	– Data integrity schemes (e.g., authenticated command counter, timestamps)	– Sequence numbers – One-time passwords – Session tokens (nonces) – Timestamps – Challenge-response	– Intrusion Detection Systems – Intrusion Prevention Systems
Software Threats	– Acceptance testing – System evaluation (e.g., IV&V, code analysis) – COTS product use	– Secure software development methodologies	– Develop multiple, independent implementations from the same

Applicable Threats	Security Mechanisms to Counter Threat	Threat Mitigations	Threat Contingencies
	– Continuous threat monitoring, continuous risk management – Run-time security monitoring – Auditing – Software partitioning (trusted computing base) – Supply chain confidence		specification for higher assurance platforms
Unauthorized Access	– Encryption of TT&C and mission data – Authentication/authorization of commands – No use of open networks – Access control in control center – Access control in cross support network – Access control in control and dissemination systems – Accountability of access – Multiple access paths – Auditing & accounting – Non-repudiation – Authentication tokens (e.g., smart cards) – Access controls; flight, flight-to-ground, on-ground – Access controls using data and service segregation and least privilege principals – Vetting of staff	– Strong authentication – Session tokens (nonces) – One-time passwords – Multi-factor authentication	– Intrusion Detection Systems – Intrusion Prevention Systems
Tainted Hardware Components	– Supply chain confidence – Authenticity of hardware – Vetted hardware suppliers – Vetted hardware production – Analysis of hardware functionality – Multi-vendor hardware components	– Diverse hardware purchasing – Blind buy purchasing – Random IV&V testing	– Resource utilization monitoring – Intrusion detection – Intrusion prevention – Vetted back-up hardware stocks
Supply Chain	– Supply chain confidence – Vetted/trusted sources – Chain of custody evidence	– Multiple, vetted sources (non-reliance on a single source) – Strong chain of custody documentation	– Accumulation of parts enabling emergency reaction

ANNEX A

ABBREVIATIONS AND ACRONYMS

APT	Advanced Persistent Threat
CCSDS	Consultative Committee for Space Data Systems
C-I-A	confidentiality, integrity, availability
COTS	commercial-off-the-shelf
CSO	client space object
DDOS	distributed denial-of-service
GEO	geosynchronous Earth orbit
GPS	Global Positioning System
GTO	geotransitory orbit
ISS	International Space Station
IT	information technology
IV&V	Independent Verification and Validation
LEO	low Earth orbit
MEO	medium Earth orbit
OOS	on-orbit servicing
RF	radio frequency
SOS	silicon-on-sapphire
TT&C	tracking, telemetry, and command