

Report Concerning Space Data System Standards

**SECURITY THREATS
AGAINST SPACE
MISSIONS**

INFORMATIONAL REPORT

CCSDS 350.1-G-2

GREEN BOOK

December 2015

Report Concerning Space Data System Standards

**SECURITY THREATS
AGAINST SPACE
MISSIONS**

INFORMATIONAL REPORT

CCSDS 350.1-G-2

GREEN BOOK

December 2015

AUTHORITY

Issue:	Informational Report, Issue 2
Date:	December 2015
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 (BFSPPO)/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	Current issue

CONTENTS

<u>Section</u>	<u>Page</u>
1 INTRODUCTION.....	1-1
1.1 PURPOSE.....	1-1
1.2 SCOPE.....	1-1
1.3 APPLICABILITY.....	1-1
1.4 RATIONALE.....	1-1
1.5 DOCUMENT STRUCTURE	1-2
1.6 REFERENCES	1-2
2 OVERVIEW	2-1
2.1 INTRODUCTION	2-1
2.2 DEFINITION OF THE TERM ‘THREAT’	2-1
2.3 THREAT AGENTS/SOURCES AND VULNERABILITIES.....	2-2
2.4 ATTACKS AGAINST MISSIONS AND MISSION IMPACTS	2-3
3 THREAT SOURCES AND THREATS APPLICABLE TO SPACE MISSIONS... 3-1	
3.1 OVERVIEW	3-1
3.2 THREAT SOURCES APPLICABLE TO SPACE MISSIONS	3-1
3.3 TYPES OF THREATS	3-2
3.4 COMMON THREATS APPLICABLE TO SPACE MISSIONS	3-3
4 THREAT ASSESSMENT METHODOLOGY	4-1
4.1 GENERAL.....	4-1
4.2 METHODOLOGY OVERVIEW	4-1
4.3 ILLUSTRATIVE SPACE-DOMAIN SPECIFIC THREAT ASSESSMENT METHODOLOGY	4-3
4.4 THREAT ASSESSMENT AND MISSION PLANNING.....	4-3
5 THREATS AGAINST ILLUSTRATIVE MISSION TYPES.....	5-1
5.1 OVERVIEW	5-1
5.2 HUMAN SPACE FLIGHT.....	5-2
5.3 EARTH OBSERVATION SATELLITES.....	5-4
5.4 COMMUNICATIONS SATELLITES.....	5-5
5.5 SCIENCE MISSIONS	5-7
5.6 NAVIGATION SATELLITES.....	5-10
5.7 THREAT SUMMARY AND SECURITY MECHANISMS TO COUNTER THREATS	5-12

CONTENTS (continued)

<u>Section</u>	<u>Page</u>
ANNEX A ACRONYMS	A-1

Figure

2-1 Confidentiality, Integrity, and Availability Interactions.....	2-2
2-2 Threat Scenario	2-4
3-1 Threat Model.....	3-1
3-2 Potential Threats to CCSDS Space Missions	3-4
3-3 CCSDS Security Communications Threats	3-5
4-1 Risk Assessment Process	4-2
4-2 Space Mission Threat Assessment Process	4-3

Table

5-1 Manned Space Flight—Hypothetical International Space Station Threat Analysis.....	5-2
5-2 Earth Observation Satellite Threat Analysis.....	5-4
5-3 Communications Satellite Threat Analysis	5-6
5-4 Science Mission Threat Analysis.....	5-8
5-5 Navigation Satellite Threat Analysis	5-10
5-6 Threat Summary	5-12

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.

1.2 SCOPE

The scope of this document is twofold:

The target audience 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. An in-depth description of a threat or risk assessment methodology is beyond the scope of this document. A mission planner should obtain more detailed information from 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, i.e., the entire space and ground segments. It takes into account 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 associated and disseminate it to the 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, unlike military missions that would 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 considered to be targets.

1.4 RATIONALE

Information and communication technologies have advanced rapidly in recent years and connectivity has become ubiquitous. This also applies to civilian space mission infrastructures. As a result, this opens up many threats against missions that would not have previously existed. At the same time, civilian space missions have become part of critical infrastructures such as in navigation, weather, and disaster response activities. As a result, civil 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 six 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 1. Report Concerning Space Data System Standards (Green Book), CCSDS 350.8-G-1. Washington, D.C.: CCSDS, November 2012.
- [2] *Capability Maturity Model® Integration (CMMISM)*. Version 1.1. CMU-SEI-2002-TR-011. ESC-TR-2002-011. Pittsburgh, Pennsylvania: Carnegie Mellon University, 2002.
- [3] Willis H. Ware, ed. *Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security*. 1970. Rand Report R-609-1. Reissued, Santa Monica, California: The Rand Corp., 1979.
- [4] *An Introduction to Computer Security—The NIST Handbook*. National Institute of Standards and Technology Special Publication 800-12. Gaithersburg, Maryland: NIST, October 1995.
- [5] *Information Technology—Security Techniques—Information Security Risk Management*. International Standard, ISO/IEC 27005:2011. Geneva: ISO, 2011.
- [6] *Information Processing Systems—Open Systems Interconnection—Basic Reference Model—Part 2: Security Architecture*. International Standard, ISO 7498-2:1989. Geneva: ISO, 1989.
- [7] “Glossary of Terms.” National Information Assurance Training and Education Center. <http://niatec.info/Glossary.aspx>.
- [8] *Security Guide for Mission Planners*. Issue 1. Report Concerning Space Data System Standards (Green Book), CCSDS 350.7-G-1. Washington, D.C.: CCSDS, October 2011.
- [9] *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 presents an overview of threats against space missions, including illustrative examples of threats against various classes of 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 or misused.

ISO 27005 (reference [5]) defines 'threat' as 'A potential cause of an incident that may result in harm of systems and organization'.

ISO 7498-2 (reference [6]) defines 'threat' as 'A potential violation of security'.

CCSDS 350.8-G-1 (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 whereas 'risk' is a function of the probability that an organization will be targeted and the harm that might be caused. To further distinguish the difference:

- **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 case that the resource has one or more vulnerabilities, it can 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 will result in unauthorized modification or destruction of information. Loss of availability will result in a loss of access to critical resources. Overall, the loss of C-I-A might result in harm to an Agency's operations, assets, or individuals. Figure 2-1 illustrates the interactions between C-I-A and the various aspects of the overall system.

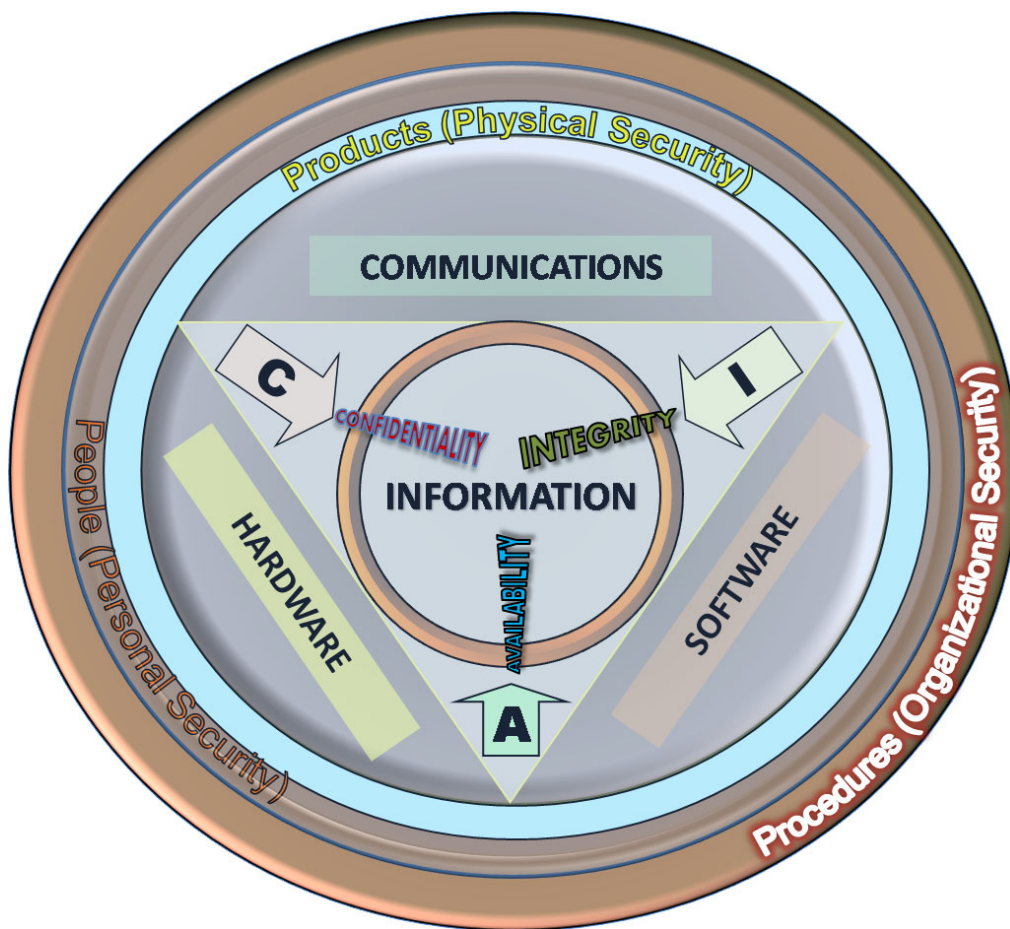


Figure 2-1: Confidentiality, Integrity, and Availability Interactions¹

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 [4]) states,

[C]omputer systems are vulnerable to many threats that can inflict various types of damage resulting in significant losses. This damage can range from errors harming database integrity to fires destroying entire computer centers. Losses can stem, for example, from the actions of supposedly trusted employees defrauding a system, from outside hackers, or from careless data entry clerks.

For example, a commercial entity assumes that there are possible threats against their infrastructure by virtue of their connection to the Internet. The threats are always applicable even if the system owners implement countermeasures. However, the system can reduce the likelihood of the threat agent's success and reduce the risk against their infrastructure by implementing security controls.

2.4 ATTACKS AGAINST MISSIONS AND MISSION IMPACTS

Civilian space mission 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 potentially has vulnerabilities that could be exploited by a threat agent. A successful attack may result in mission impact. Mission impacts can range from insignificant (such as software crash) to catastrophic (loss of mission). Successful attacks may result in a loss of mission confidentiality, integrity, or availability (C-I-A).

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

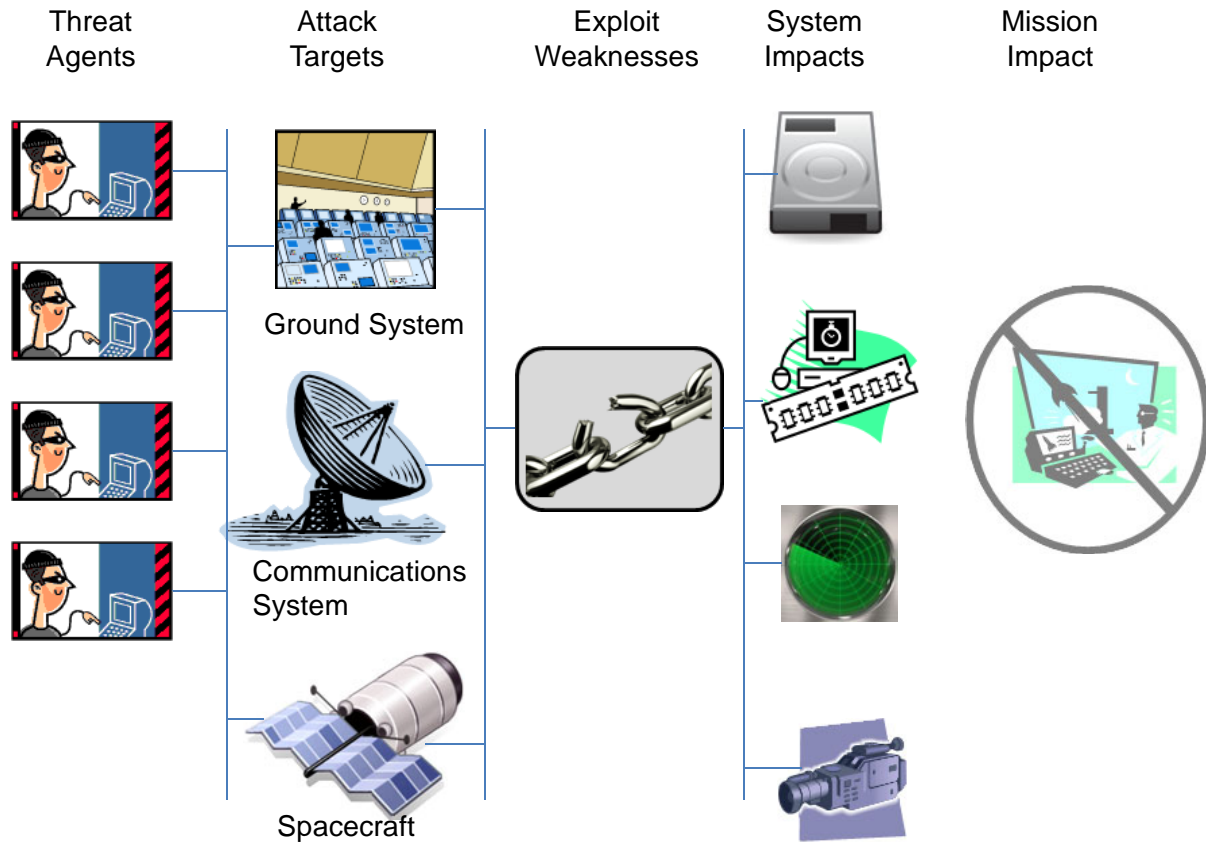


Figure 2-2: Threat Scenario

3 THREAT SOURCES AND THREATS APPLICABLE TO SPACE MISSIONS

3.1 OVERVIEW

This section introduces threats specific to space missions that should be taken into account during a threat assessment. These threats may come from a wide variety of sources. Figure 3-1 illustrates a generic threat model. However, before being able to identify threats, the following subsections will provide a review of possible threat sources.

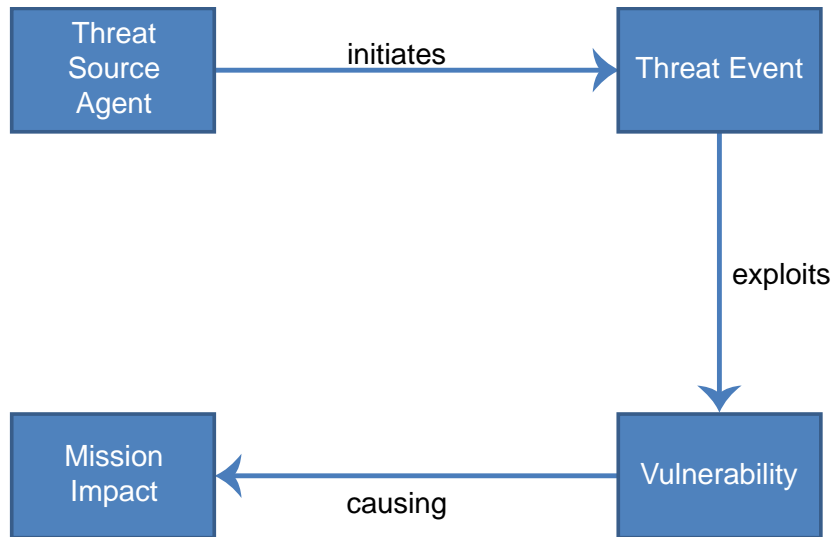


Figure 3-1: Threat Model

3.2 THREAT SOURCES APPLICABLE TO SPACE MISSIONS

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

- Adversarial
 - terrorists and criminals;
 - foreign intelligence services;
 - subversives or political activists;
 - computer hackers;
 - commercial competitors;

² An exhaustive list can be found in NIST Special Publication 800-30, appendix D (reference [9]).

- Insider
 - dishonest maintenance personnel;
 - dishonest systems personnel;
 - disgruntled staff members;
 - trusted business partners;
 - inadvertent actions of staff members;
- Environmental
 - natural or man-made disaster;
 - infrastructure failure / power outage
- Structural
 - software failures;
 - hardware failures;

3.3 TYPES OF THREATS

3.3.1 OVERVIEW

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

3.3.2 ACTIVE THREATS

An active threat requires a threat source to initiate a sequence of events and actively interfere with the system to 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 otherwise 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;
- the exploitation of software vulnerabilities (bugs);

- unauthorized modification or corruption of data; and
- 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 interfere with 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 actually being able to read the communicated information.

3.4 COMMON THREATS APPLICABLE TO SPACE MISSIONS

3.4.1 GENERAL

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.

³ An exhaustive list can be found in NIST Special Publication 800-30, appendix E (reference [9]).

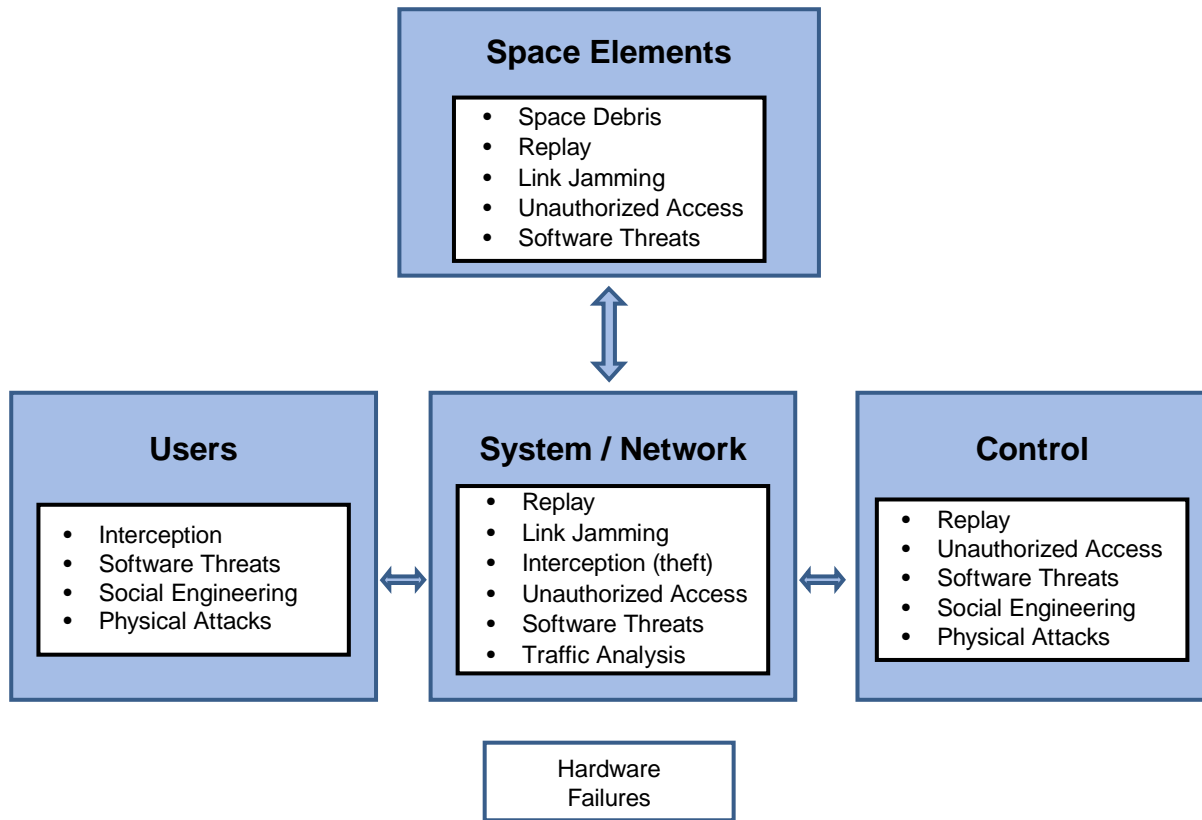


Figure 3-2: Potential Threats to CCSDS Space Missions

Figure 3-3 provides an illustrative mapping of threats to the specific parts of an example space mission's communications infrastructure.

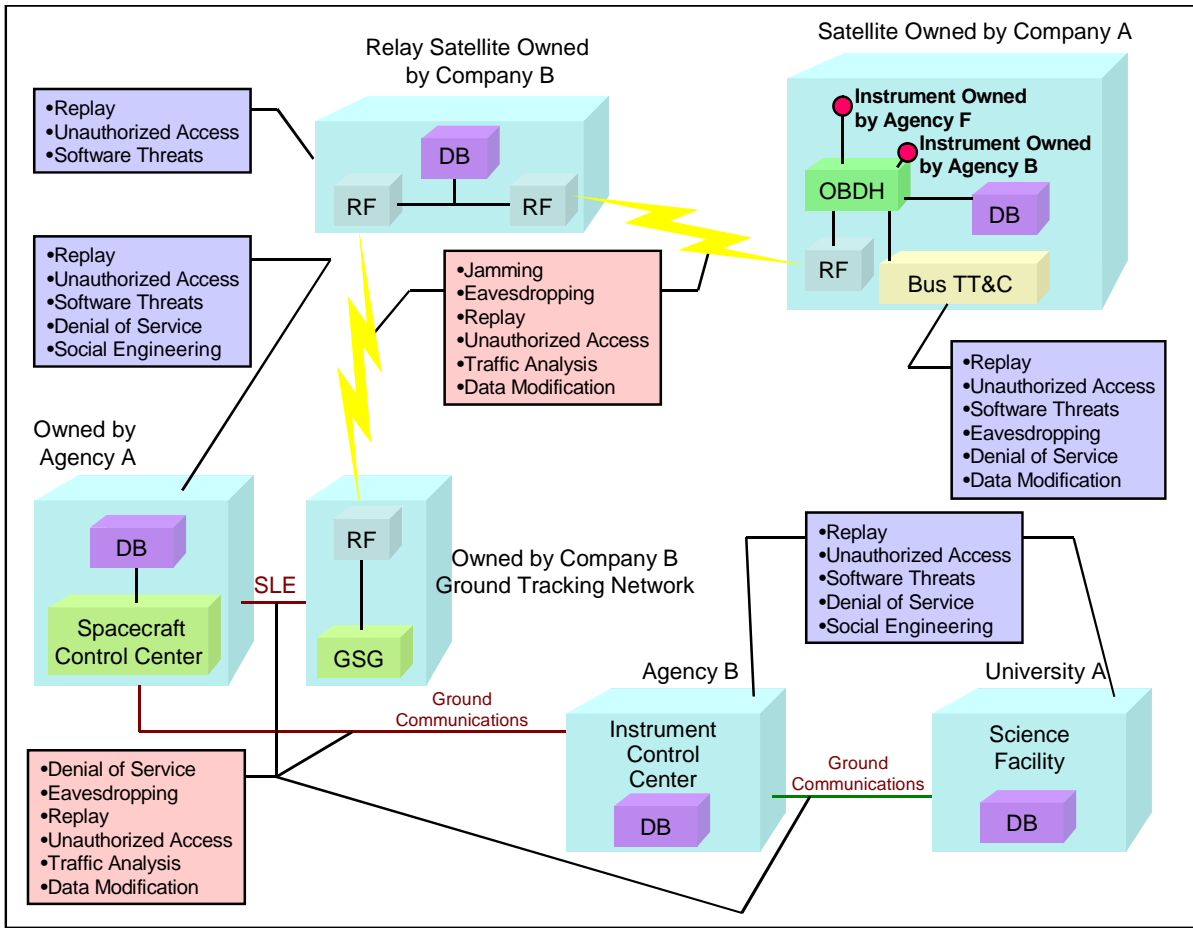


Figure 3-3: CCSDS Security Communications Threats

3.4.2 DATA CORRUPTION/ MODIFICATION

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

Description: Data Corruption/Modification refers to the intentional or non-intentional alteration of data, whether being communicated or at rest. Data corruption/modification always implies a breach of integrity. Data could be corrupted at its source, in transit to the ground system, or at the ground system. It could also be corrupted in transmission to/from or onboard a spacecraft.

Possible Mission Impact: Corruption might be a result of software failures or bugs, hardware failures, use of unauthorized software, or active attempts to change/modify data to deny its use. A 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 burn command were 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: The loss of a ground system might result in the loss of data, loss of access to data in a timely manner, or loss of the entire mission.

Possible Mission Impact: A successful exploitation of a vulnerability through a physical attack might disable the ground facility and directly affect the operation of the mission and the services provided. It might also aim to overtake the facility in order to take control of the spacecraft without technically attacking the systems. Environmental factors might also result in the loss of a ground facility. Tornados, hurricanes, tsunamis, or other weather related factors could result in physical damage to the facilities or the loss of electrical power to the ground station.

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. But this is mission dependent since all missions are different.

For example, GeoTransitory Orbit (GTO) and Geostationary Earth Orbit (GEO) would have a relatively large downlink beam width resulting in a much more easily intercepted signal. For a low-Earth orbiter, smaller dishes and power are needed, but because of short passes, tracking creates an obstacle for an interceptor. As spacecraft move towards optical communications, data interception will become more difficult, but not impossible. Someone 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 which could be tapped.

Possible Mission Impact: Interception of data may result in the loss of data confidentiality and data privacy if the data is not encrypted. 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 Communications

Description: Denial of communications to and from spacecraft could be accomplished by interfering with the RF signal. This can be done by injecting noise, by transmitting on the same frequency from another source, or by simply overpowering the original source. The interference can result in link loss and loss of mission control.

Possible Mission Impact: 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 blocked, 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 would prevent authorized access to resources. 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.

Possible Mission Impact: Ground 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 being enforced, certain entities are allowed to perform specific actions while other entities may be denied. However, the access controls can be rendered useless if entities can lie about their true identity or can assume the identity of another entity.

Possible Mission Impact: If an instrument operator masquerades as a spacecraft operator, incorrect spacecraft bus 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 Communications

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 acted upon, potentially for a second time. If the replayed commands are not rejected, they could result in a duplicate spacecraft operation such as a maneuver burn 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).

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 un-vetted software, which might contain bugs, viruses, spyware, or which might simply result in system instability. System operators might configure a system incorrectly resulting in security weaknesses. Programmers may introduce logic or implementation errors which could result in system vulnerabilities or instability. External threat agents might attempt to exploit a vulnerability to inject software or configuration changes.

Possible Mission Impact: Any such software could result in loss of data, loss of spacecraft control, unauthorized spacecraft control, or loss of mission.

3.4.10 UNAUTHORIZED ACCESS

Applicable to: Space Segment, Ground Segment

Description: Strong access control policies based on strong authentication provide a means by which only those entities that are authorized to perform actions are allowed to do so while all others are prevented. With no or weak access controls in place, the result might be unauthorized access to systems. Likewise, interception of data could also result in unauthorized access because identities and/or passwords might be obtained.

Possible Mission Impact: An access control breach would allow an unauthorized entity the ability to take control of a ground system or a ground system network, shut down a ground system, upload unauthorized commands to a spacecraft, obtain unauthorized data, contaminate archived data, or completely shut down a mission.

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. Because of that an organization may only 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 provided and then refined into a space-specific methodology.

4.2 METHODOLOGY OVERVIEW

As mentioned before, a general 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 shows the overall NIST SP 800-30 Revision 1 (reference [9]) risk assessment process. The first activities to be executed as part of this process constitute preparation for the assessment and the threat identification. While this Report is focusing only on this first threat assessment steps in the overall risk assessment process, it is important to understand the relationship.

A threat assessment always starts with the characterization of the system. This includes the identification and valuation of assets, and understanding of the overall architecture of the system as well as its individual subsystems, its business function, and its interfaces. This general characterization is a prerequisite to executing a threat assessment. In this step also general assumptions and limitations are defined. The second step is then 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 taken as a baseline by the mission planer (see 4.3 and section 5). The third step is then the identification of vulnerabilities that could be exploited by the identified threats. This step already leads from the threat assessment into the main part of the risk assessment. Thus, the output of the threat assessment is the preliminary identification of risks.

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

The following is a selection of common risk assessment methodologies used by various organizations. They include as well threat assessment concepts:

- NIST SP 800-30: Guide for Conducting Risk Assessments (reference [9]);
- ISO 27005:2011 Information Security Risk Management (reference [5]).

The mission planer should consult with a security expert to identify the threat assessment methodology applicable for his organization. It is also highly recommended to make use of security expert consultancy while executing the threat assessment.

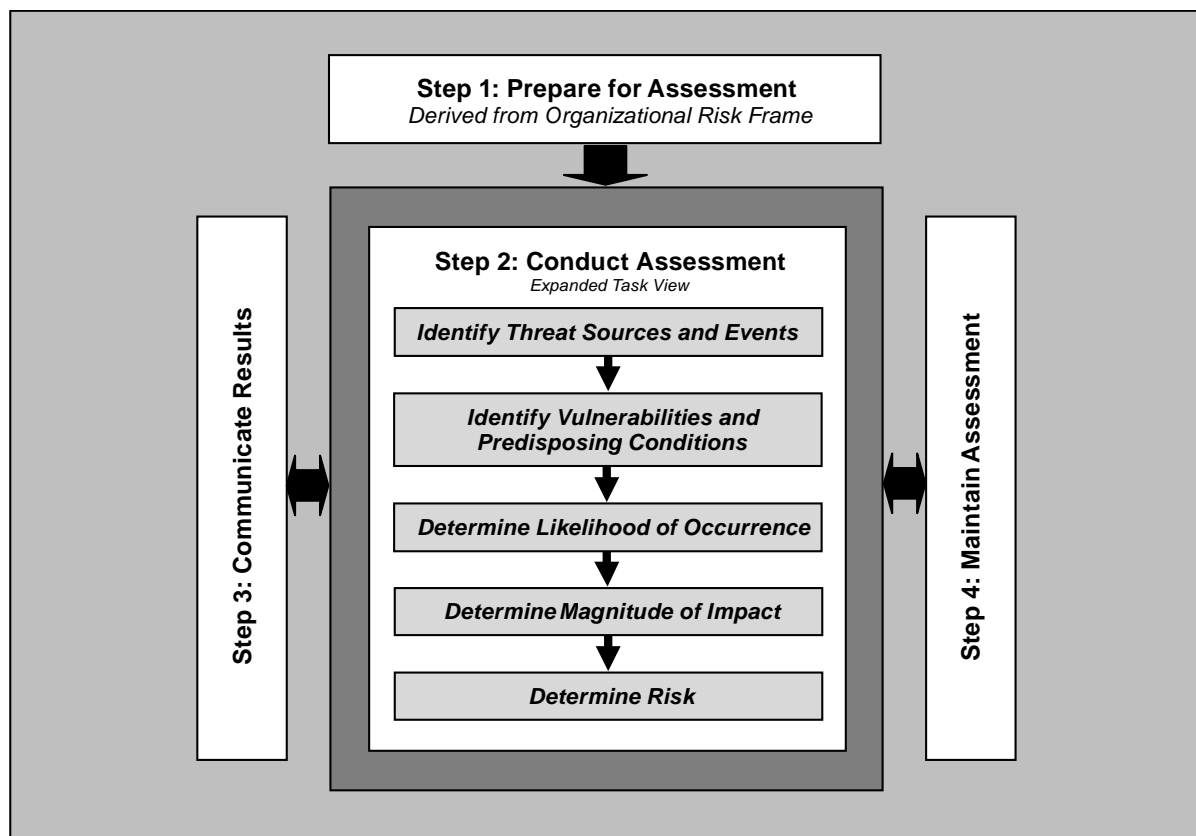


Figure 4-1: Risk Assessment Process⁵

⁵ From reference [9].

4.3 ILLUSTRATIVE SPACE-DOMAIN SPECIFIC THREAT ASSESSMENT METHODOLOGY

For illustrative purposes, the generic threat assessment methodology introduced above has been refined for use in space mission threat analyses. It is illustrated in figure 4-2.

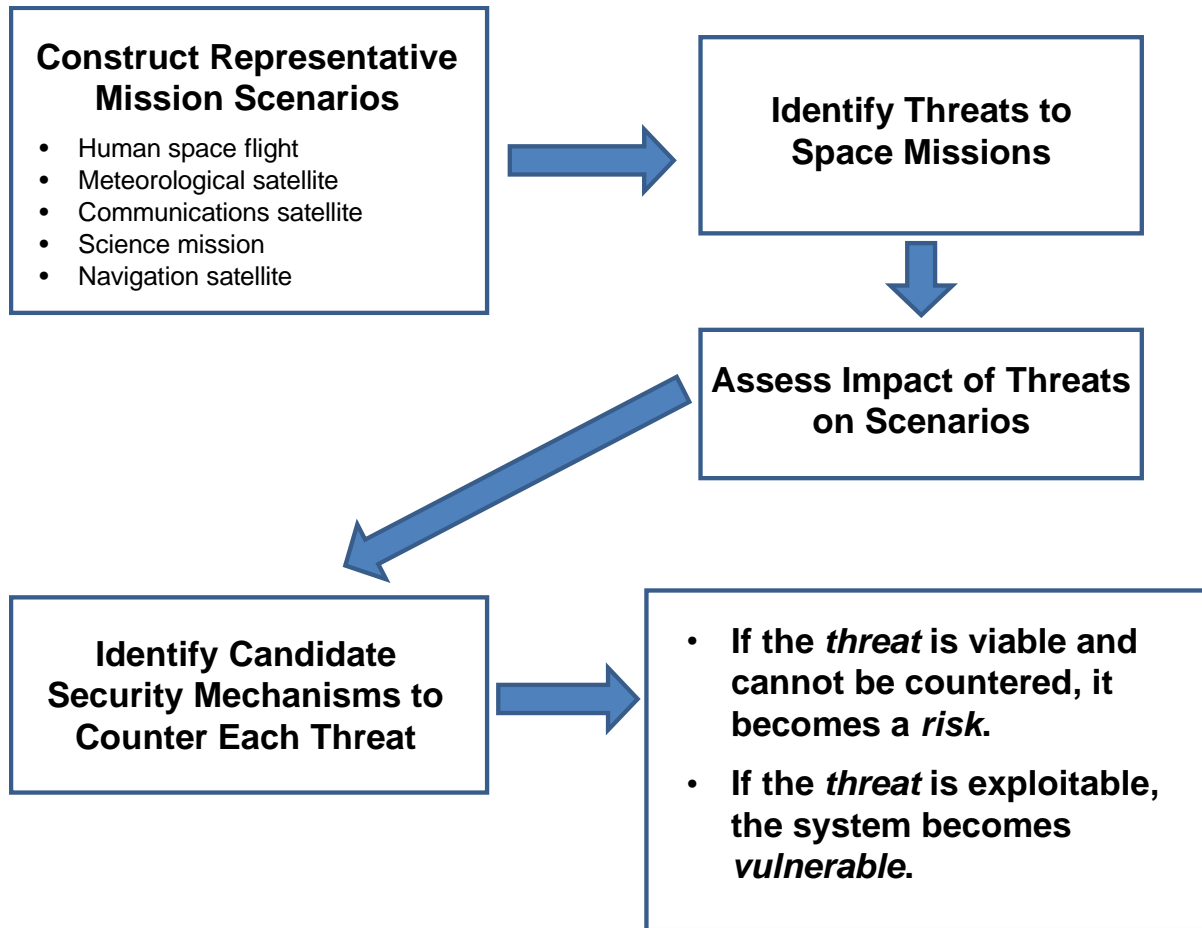


Figure 4-2: Space Mission Threat Assessment Process

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 short-comings as inputs to performing a threat assessment.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:

⁶ More specifics can be found in the CCSDS Security Guide for Missions Planners (reference [8]).

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

A threat assessment begins with gathering data about the threatened areas and analyzing the information. The assets being protected must be assigned a value. Such an asset valuation should take into account the asset's intrinsic value as well as the near and long-term impacts if it is compromised. Some assets can be assigned a monetary value. For some, assigning a monetary value might prove to be impractical or impossible. In those cases, a determination must be made to assess the value of the system and/or the data if it were to be lost. In some cases, the loss might be assessed as a 'national disgrace'. In some cases, it might be assessed as damaging to a national space program. In yet other cases, it might be assessed as a 'too bad—we'll get more data from another mission' occurrence.

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 of high concern. If there is a likelihood of occurrence, it should be rated either numerically (e.g., on a scale from 1 to 5) or as high, medium, or low.

A vulnerability analysis compares the outcome of the threat assessment against the mission systems. A valid threat is not of concern if there are no system vulnerabilities that it can exploit. For example, if there is a damaging Windows virus threat in the wild but all systems involved in the mission are based on 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 counter, 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. By no means is this 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 discussed are:

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

Other sub-types of missions 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 an Agency but hosts payloads from various other Agencies or commercial entities. Or a mission may be carried out by 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 more communications power, can 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 is the communication constellation (e.g., *Iridium*, *Orbcomm*, *Globalstar*). Whereas each individual LEO spacecraft provides only limited visibility, 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 does a single LEO mission.

More infrastructure (resulting in higher cost) is required to attack deep-space/interplanetary missions than Earth/near-Earth orbit missions because of the larger antennas and higher power required to communicate with the spacecraft.

5.2 HUMAN SPACE FLIGHT

Human crewed space platforms (e.g., International Space Station (ISS)) are good 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	<ul style="list-style-type: none"> – Modification of information – System damage 	2	<ul style="list-style-type: none"> – 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	<ul style="list-style-type: none"> – Loss of command and telemetry link – Loss of access to resources 	2	<ul style="list-style-type: none"> – Multiple uplink paths – Spread spectrum

⁷ These probabilities (in this and all subsequent tables) are for illustrative purposes only and will change for specific missions.

CCSDS REPORT CONCERNING SECURITY THREATS AGAINST SPACE MISSIONS

Applicable Threats	Impacts	Probability (1= Lowest, 5= Highest)⁷	Security Mechanisms to Counter Threat
Denial-of-Service	<ul style="list-style-type: none"> - Loss of access to resources 	3	<ul style="list-style-type: none"> - Firewalls - Routers - Switches - Intrusion Prevention Systems - Private, segregated networks - Encryption & authentication - ISP 'edge' support
Masquerade	<ul style="list-style-type: none"> - Potential to disrupt operations (uplink) - Potential to receive false information (downlink) 	3	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - Undesirable events - System damage - Enable other threats 	2	<ul style="list-style-type: none"> - Acceptance testing - Independent Verification and Validation (IVV) - Code walkthroughs - Automated code analysis - Run-time security monitoring - Auditing - Software partitioning (trusted computing base) - Supply chain confidence
Unauthorized Access	<ul style="list-style-type: none"> - Disruption of operations - System damage (possible safety of life issues) 	4	<ul style="list-style-type: none"> - Encryption of TT&C and mission data - Authentication of commands - No use of open networks - Authentication tokens (e.g., smart card) - Auditing
Tainted Hardware Components	<ul style="list-style-type: none"> - Hidden, malicious capabilities - System instability - System damage - Undesirable system effects 	3	<ul style="list-style-type: none"> - Supply chain confidence - Authenticity of hardware - Vetted hardware suppliers - Vetted hardware production - Analysis of hardware functionality

5.3 EARTH OBSERVATION SATELLITES

Earth observation satellite systems illustrate a type of mission that can be either 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 or in geosynchronous Earth orbit. Table 5-2 illustrates the possible threats against meteorological 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	<ul style="list-style-type: none"> – Modification of information – System damage 	4	<ul style="list-style-type: none"> – Data integrity schemes (hashing, check values, digital signatures) – Resilient hardware (e.g., SOS)
Ground facility physical attack	Loss of command, control, and data	2	<ul style="list-style-type: none"> – Guards, gates, access controls, backup site(s)
Interception	<ul style="list-style-type: none"> – Loss of sensitive data – Theft of commercial data 	3 (LEO) 3 (GEO)	Protection of archive & distribution systems via encryption
Jamming	<ul style="list-style-type: none"> – Loss of command and/or telemetry link – Loss of access to resources – Commercial impact 	2 (LEO) 2 (GEO)	<ul style="list-style-type: none"> – Multiple uplink paths – Multiple downlink paths – Spread spectrum
Denial-of-Service	<ul style="list-style-type: none"> – Loss of access to resources 	3	<ul style="list-style-type: none"> – Firewalls – Routers – Switches – Intrusion Prevention Systems – Private, segregated networks – Encryption & authentication – ISP 'edge' support
Masquerade	<ul style="list-style-type: none"> – Potential to disrupt operations (uplink) – Potential to receive false information (downlink) 	2	<ul style="list-style-type: none"> – Strong authentication of uplinked commands and downlinked data – Access control scheme – Vetting of staff – No use of open networks
Replay	<ul style="list-style-type: none"> – System damage (possible safety of life issues) 	1	<ul style="list-style-type: none"> – Authenticated command counter, timestamp

⁸ These probabilities are for illustrative purposes only and will change for specific missions.

Applicable Threats	Impacts	Probability (1=Lowest, 5=Highest) ⁸	Security Mechanisms to Counter Threat
Software threats	<ul style="list-style-type: none"> - Undesirable events - System damage - Enable other threats 	2	<ul style="list-style-type: none"> - Acceptance testing - Independent verification and validation (IVV) - Code walkthroughs - Automated code analysis - Run-time security monitoring - Auditing - Software partitioning (trusted computing base) - Supply chain confidence
Unauthorized Access	<ul style="list-style-type: none"> - Theft of commercial data - Disruption of operations - System damage 	3	<ul style="list-style-type: none"> - Encryption of TT&C and mission data - Authentication of commands - Access control in control and dissemination systems - No use of open networks - Authentication tokens (e.g., smart card) - Auditing
Tainted Hardware Components	<ul style="list-style-type: none"> - Hidden, malicious capabilities - System instability - System damage - Undesirable system effects 	3	<ul style="list-style-type: none"> - Supply chain confidence - Authenticity of hardware - Vetted hardware suppliers - Vetted hardware production - Analysis of hardware functionality

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*, are operating. The 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 discussed previously, no longer holds true because of the on-orbit routed network created by the satellite constellation. While a single LEO satellite is still only 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	<ul style="list-style-type: none"> - 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, access controls
Interception	<ul style="list-style-type: none"> - Loss of sensitive data - Theft of commercial data 	4 (GEO) 2 (LEO)	Protection of traffic (potentially user responsibility)
Jamming	<ul style="list-style-type: none"> - Loss of TT&C and/or traffic circuits - Commercial impact - Loss of access to resources - Possible safety impact 	3 (GEO) 3 (LEO)	<ul style="list-style-type: none"> - Multiple uplink and downlink paths - Multiple access points - Spread spectrum - Spacecraft autonomy
Denial-of-Service	<ul style="list-style-type: none"> - Loss of access to resources 	3	<ul style="list-style-type: none"> - Firewalls - Routers - Switches - Intrusion Prevention Systems - Private, segregated networks - Encryption & authentication - ISP 'edge' support
Masquerade	<ul style="list-style-type: none"> - Potential to disrupt operations (uplink) - Potential to receive false information (downlink) 	2	<ul style="list-style-type: none"> - Strong authentication of uplinked commands and downlinked data - Access control scheme - Vetting of staff - No use of open networks
Replay	<ul style="list-style-type: none"> - System damage (possible safety of life issues) 	1	<ul style="list-style-type: none"> - Authenticated message counter, timestamp
Software threats	<ul style="list-style-type: none"> - Undesirable events - System damage - Enable other events 	2	<ul style="list-style-type: none"> - Acceptance testing - Independent verification and validation (IVV) - Code walkthroughs - Automated code analysis - Run-time security monitoring - Auditing - Software partitioning (trusted computing base) - Supply chain confidence
Unauthorized Access	<ul style="list-style-type: none"> - Disruption of operations - System damage 	2	<ul style="list-style-type: none"> - Encryption of TT&C data - Authentication of commands - Auditing
Tainted Hardware Components	<ul style="list-style-type: none"> - Hidden, malicious capabilities - System instability - System damage - Undesirable system effects 	3	<ul style="list-style-type: none"> - Supply chain confidence - Authenticity of hardware - Vetted hardware suppliers - Vetted hardware production - Analysis of hardware functionality

⁹ These probabilities are for illustrative purposes only and will change for specific missions.

5.5 SCIENCE MISSIONS

Science missions are a class of missions which are typically not considered operational or part of a national (or international) asset 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 much less than against those where life or infrastructure may be disrupted. In the case of science missions, while money was spent to gather the information, 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 before beginning their cruise phase, in cruise, or in some cases, in a sling-shot trajectory where they leave Earth orbit, go into a 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 the other LEO, MEO, and GEO missions. However, their threat characteristics change with time since they will move in and out of Earth orbit.

When they finally leave Earth orbit, they both require more power to communicate with than Earth orbit spacecraft, they both have a non-orbit cruise phase while in transit from the Earth to their target destination(s), and they both 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 large 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 with their longer round-trip communications, the increased power and the size of the dishes required provide immunity from ‘casual’ attack, although not from hostile ‘nation-state’ attacks.

But what must be remembered is that both lunar and interplanetary missions also must take into account the threats faced by Earth orbit and near-Earth missions because they often find themselves in those orbits early in their lives.

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	<ul style="list-style-type: none"> – Modification of information – System damage 	3	<ul style="list-style-type: none"> – Data integrity schemes (hashing, check values, digital signatures)
Ground facility physical attack	Loss of command, control, and data	2	Guards, gates, access control
Interception	Loss of sensitive data	1 (deep-space) 3 (lunar) 3 (Earth)	<ul style="list-style-type: none"> – Data encryption – Spread spectrum
Jamming	<ul style="list-style-type: none"> – 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)	<ul style="list-style-type: none"> – Multiple uplink and downlink paths – Multiple access points – Spread spectrum
Denial-of-Service	<ul style="list-style-type: none"> – Loss of access to resources 	3	<ul style="list-style-type: none"> – Firewalls – Routers – Switches – Intrusion Prevention Systems – Private, segregated networks – Encryption & authentication – ISP 'edge' support
Masquerade	<ul style="list-style-type: none"> – Potential to disrupt operations (uplink) – Potential to receive false information (downlink) 	2	<ul style="list-style-type: none"> – Strong authentication of uplinked commands and downlinked data – Access control scheme – Vetting of staff – No use of open networks
Replay	<ul style="list-style-type: none"> – System damage 	1	<ul style="list-style-type: none"> – Authenticated message counter, timestamp
Software threats	<ul style="list-style-type: none"> – Undesirable events – System damage 	2	<ul style="list-style-type: none"> – Acceptance testing – Independent verification and validation (IVV) – Code walkthroughs – Automated code analysis – Run-time security monitoring – Auditing – Software partitioning (trusted computing base) – Supply chain confidence
Unauthorized Access	<ul style="list-style-type: none"> – Disruption of operations – System damage – Potential loss of mission 	3	<ul style="list-style-type: none"> – Authentication of commands – Access control in control center – Access control in cross support network – No use of open networks – Auditing

¹⁰ These probabilities are for illustrative purposes only and will change for specific missions.

CCSDS REPORT CONCERNING SECURITY THREATS AGAINST SPACE MISSIONS

Applicable Threats	Impacts	Probability (1=Lowest, 5=Highest) ¹⁰	Security Mechanisms to Counter Threat
Tainted Hardware Components	<ul style="list-style-type: none"> - Hidden, malicious capabilities - System instability - System damage - Undesirable system effects 	3	<ul style="list-style-type: none"> - Supply chain confidence - Authenticity of hardware - Vetted hardware suppliers - Vetted hardware production - Analysis of hardware functionality

5.6 NAVIGATION SATELLITES

Navigation satellites such as the Global Positioning System (GPS) are irreplaceable for enterprises such as airlines, maritime, trucking, and the military. Similarly, navigation satellites are being used for private use in automobile navigation systems, cellular telephones for emergency locating, and via hand-held units in hunting, exploring, and hiking. Like communications satellites, the loss of navigation satellite systems would result not only in loss of investment dollars; there would also be the high potential for the loss of life, safety, and infrastructure. A threat analysis of such a 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	<ul style="list-style-type: none"> – 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, access control, backup sites(s)
Interception	Loss of sensitive data	1	<ul style="list-style-type: none"> – Data encryption – Spread Spectrum
Jamming	<ul style="list-style-type: none"> – Loss of TT&C and/or traffic circuits – Commercial impact – Loss of access to resources – Possible safety impact 	3	<ul style="list-style-type: none"> – Multiple uplink and downlink paths – Multiple access points – Frequency hopping – Spread spectrum
Denial-of-Service	<ul style="list-style-type: none"> – Loss of access to resources 	3	<ul style="list-style-type: none"> – Firewalls – Routers – Switches – Intrusion Prevention Systems – Private, segregated networks – Encryption & authentication – ISP 'edge' support
Masquerade	Potential to disrupt operations	2	<ul style="list-style-type: none"> – 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.

CCSDS REPORT CONCERNING SECURITY THREATS AGAINST SPACE MISSIONS

Applicable Threats	Impacts	Probability (1=Lowest, 5=Highest) ¹¹	Security Mechanisms to Counter Threat
Software threats	<ul style="list-style-type: none"> - Undesirable events - System damage 	2	<ul style="list-style-type: none"> - Acceptance testing - Independent verification and validation (IVV) - Code walkthroughs - Automated code analysis - Run-time security monitoring - Auditing - Software partitioning (trusted computing base) - Supply chain confidence
Unauthorized Access	<ul style="list-style-type: none"> - Disruption of operations - System damage - Potential loss of mission 	3	<ul style="list-style-type: none"> - Authentication of commands - Access control in control center - Access control in cross support network - No use of open networks - Auditing
Tainted Hardware Components	<ul style="list-style-type: none"> - Hidden, malicious capabilities - System instability - System damage - Undesirable system effects 	3	<ul style="list-style-type: none"> - Supply chain confidence - Authenticity of hardware - Vetted hardware suppliers - Vetted hardware production - Analysis of hardware functionality

5.7 THREAT SUMMARY AND SECURITY MECHANISMS TO COUNTER THREATS

Table 5-6: Threat Summary

Applicable Threats	Security Mechanisms to Counter Threat	Threat Mitigations	Threat Contingencies
Data corruption	<ul style="list-style-type: none"> - Data integrity schemes (hashing, check values, digital signatures) - Resilient hardware 	<ul style="list-style-type: none"> - Secure data backups 	<ul style="list-style-type: none"> - Verify integrity of backups
Ground facility physical attack	<ul style="list-style-type: none"> - Guards - Gates - Access control 	<ul style="list-style-type: none"> - Alternate ground facilities 	<ul style="list-style-type: none"> - Failover or hot-standby to alternate site
Interception	<ul style="list-style-type: none"> - Protection of traffic via encryption, frequency hopping, spread spectrum - Protection of archive & distribution systems via encryption 	<ul style="list-style-type: none"> - Use secure transmission 	<ul style="list-style-type: none"> - Use hardened transmission facilities
Jamming	<ul style="list-style-type: none"> - Multiple uplink paths - Multiple access points - Frequency hopping, spread spectrum 	<ul style="list-style-type: none"> - Legislation - Monitoring - Interdiction - Reporting 	<ul style="list-style-type: none"> - Have alternate frequencies or transmission facilities available
Denial-of-Service	<ul style="list-style-type: none"> - Loss of access to resources 	<ul style="list-style-type: none"> - Access control lists - Rate limiting - 'expect' scripting - Service screening 	<ul style="list-style-type: none"> - Firewalls - Routers - Switches - Intrusion Prevention Systems - Private, segregated networks - Encryption & authentication - ISP 'edge' support
Masquerade	<ul style="list-style-type: none"> - Strong authentication - Access control scheme - Vetting of staff - No use of open networks 	<ul style="list-style-type: none"> - Strong authentication - Session tokens - Behavior - Timestamps 	<ul style="list-style-type: none"> - Intrusion Detection Systems - Intrusion Prevention Systems
Replay	<ul style="list-style-type: none"> - Data integrity schemes (e.g., authenticated command counter, timestamps) 	<ul style="list-style-type: none"> - Sequence numbers - One-time passwords - Session tokens (nonces) - Timestamps - Challenge-response 	<ul style="list-style-type: none"> - Intrusion Detection Systems - Intrusion Prevention Systems
Software Threats	<ul style="list-style-type: none"> - Acceptance testing - System evaluation (e.g., IVV, code 	<ul style="list-style-type: none"> - Secure software development methodologies 	<ul style="list-style-type: none"> - Develop multiple, independent implementations from

CCSDS REPORT CONCERNING SECURITY THREATS AGAINST SPACE MISSIONS

Applicable Threats	Security Mechanisms to Counter Threat	Threat Mitigations	Threat Contingencies
	<ul style="list-style-type: none"> analysis) – COTS product use – Continuous threat Monitoring, continuous risk management – Run-time security monitoring – Auditing – Software partitioning (trusted computing base) – Supply chain confidence 		<p>the same specification for higher assurance platforms</p>
Unauthorized Access	<ul style="list-style-type: none"> – Encryption of TT&C and mission data – Authentication 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 – Multiple access paths – Auditing 	<ul style="list-style-type: none"> – Strong authentication – Session tokens (nonces) – One-time passwords – Multi-factor authentication 	<ul style="list-style-type: none"> – Intrusion Detection Systems – Intrusion Prevention Systems
Tainted Hardware Components	<ul style="list-style-type: none"> – Supply chain confidence – Authenticity of hardware – Vetted hardware suppliers – Vetted hardware production – Analysis of hardware functionality – Multi-vendor hardware components 	<ul style="list-style-type: none"> – Diverse hardware purchasing – Blind buy purchasing – Random IVV testing 	<ul style="list-style-type: none"> – Resource utilization monitoring – Intrusion detection – Intrusion prevention – Vetted back-up hardware stocks

ANNEX A

ABBREVIATIONS AND ACRONYMS

CCSDS	Consultative Committee for Space Data Systems
C-I-A	confidentiality, integrity, availability
CMMI	Capability Maturity Model Integration
COTS	commercial-off-the-shelf
DB	database
DDOS	distributed denial-of-service
GEO	geosynchronous Earth orbit
GPS	Global Positioning System
GSG	ground-segment gateway
GTO	geotransitory orbit
ISS	International Space Station
IT	information technology
IVV	independent verification and validation
LEO	low Earth orbit
MEO	medium Earth orbit
OBDH	onboard data handling
RF	radio frequency
SOS	silicon-on-sapphire
TT&C	tracking, telemetry, and command