Critical
software

Critical Software

TN04: Space systems threats and vulnerabilities

Cybersecurity For Space

CONTRACT REFERENCE: NOT APPLICABLE.

DATE: 2024-07-31
PROJECT CODE: CSEC4SPACE
DOC. REF.: CSW-2024-TNR-01468
STATUS: APPROVED
PAGES: 36
INFORMATION CLASSIFICATION: PUBLIC
VERSION: 1.0

DISCLAIMER -

The work described in this report was performed under the Master’s degree research titled “Cybersecurity for space domain”. Responsibility for the contents resides in the author or organization that prepared it.

PARTNERS:

Polytechnic
University of Coimbra

APPROVAL

VERSION	NAME	FUNCTION	SIGNATURE	DATE
1.0	Nuno Silva	Industry Supervisor		2024-07-31
1.0	João Carlos Cunha	Academic Supervisor		2024-07-31

AUTHORS AND CONTRIBUTORS

NAME	DESCRIPTION	DATE
Pedro Miguel Sousa	Author	2024-03-19
Nuno Silva	Reviewer	2024-05-30

COPYRIGHT

REVISION HISTORY

VERSION	DATE	DESCRIPTION	AUTHOR
0.1	2024-03-19	First revision of the technical note.	Pedro Sousa
1.0	2024-07-31	Updated document according to internal review comments. Document Approved for delivery.	Pedro Sousa

TABLE OF CONTENTS

TABLE OF TABLES

TABLE OF FIGURES

1. INTRODUCTION

In today's world, space systems play an integral role in many aspects of our daily lives. From predicting the weather using satellites to help us plan our trips, to navigating to new destinations using GPS technology, and even facilitating our communication and internet access, space systems are ubiquitous. These are just a few examples highlighting the diverse applications of space technology. Therefore, it's safe to say that space systems have become an indispensable part of our daily lives and impact a wide range of human activities.

However, space systems, like any other system, are vulnerable to both intentional and unintentional threats and vulnerabilities. These threats can have a range of effects, from disrupting operations and compromising data integrity to, in extreme cases, putting human lives at risk.

By identifying and addressing these threats and vulnerabilities, we can contribute to solving these issues and making space systems more secure.

1.1. OBJECTIVE

This technical note aims to present the threats and vulnerabilities faced by space systems. It draws insights from literature, earlier research in the space sector, and related domains. The results of a survey conducted among space sector specialists are also considered in the drafting of this technical note.

The goal of this note is to highlight the critical need for enhanced cybersecurity efforts within the space sector.

1.2. SCOPE

The technical note identifies and discusses various threats and vulnerabilities faced by space systems through a review of relevant literature, past research in the space sector, and insights from related security domains as well as from perception of space systems experts (survey results).

1.3. AUDIENCE

The audience of this technical note includes: Critical Software S.A., Coimbra Institute of Engineering, and Engineers/Researchers interested in the field of cybersecurity.

1.4. DEFINITIONS AND ACRONYMS

Table 1 presents the list of definitions used throughout this document.

NAME	DESCRIPTION
Availability	Ensuring timely and reliable access to and use of information.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Attack Vector	Attack vector is a path or means by which an attacker or hacker can gain access to a computer or network server to deliver a payload or malicious outcome.
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information

NAME	DESCRIPTION
	contained therein, to ensure its availability, integrity, authentication, and confidentiality.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Critical Infrastructure	Critical infrastructure refers to the systems, facilities and assets that are vital for the functioning of society and the economy.
Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
Threat	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.
Threat Actor	Threat actors, also known as cyberthreat actors or malicious actors, are individuals or groups that intentionally cause harm to digital devices or systems by exploiting vulnerabilities in computer systems, networks and software.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Reference Document	A document is considered a reference if it is referred but not applicable to this document. Reference documents are mainly used to provide further reading.

Table 1: Definitions

Table 2 presents the list of acronyms used throughout this document.

ACRONYM	DESCRIPTION
AI	Artificial Intelligence
ASAT	Anti-Satellite
BBC	British Broadcasting Corporation
CCSDS	Consultative Committee for Space Data Systems
CIA	Central Intelligence Agency
CISO	Chief Information Security Officer
COTS	Commercial Off-the-Shelf
C&C	Command and Control

ACRONYM	DESCRIPTION
DoS	Denial of Service
DNS	Domain Name System
EEPROM	Electrical Erasable Programmable-Read-Only Memory
ECC	Employing Error-Correcting Codes
FBI	Federal Bureau of Investigation
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
GEO	Geosynchronous Orbit
HTML	Hyper Text Markup Language
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IOM	Installation, Operation, Maintenance
IP	Internet Protocol
ISP	Internet Service Providers
IT	Information Technology
IBM	International Business Machines Corporation
MCU	Multiple Cell Upset
MBU	Multiple Bit Upset
ML	Machine Learning
MitM	Man-in-the-Middle
NIST	National Institute of Standards and Technology
PDF	Portable Document Format
SCA	Static Code Analysis
SRB	Solar Radio Burst
SEU	Single Event Upset
SEC	Securities and Exchange Commission
SRAM	Static Random-Access Memories

ACRONYM	DESCRIPTION
SATCOM	Satellite Communication
SQL	Structured Query Language
SSDL	Secure Software Development Lifecycle
SSN	Social Security Number
TV	Television
TCP	Transmission Control Protocol

Table 2: Acronyms

1.5. DOCUMENT STRUCTURE

Section 1 (Introduction) presents this document.

Section 2 (Threats) focuses on the variety of threats that the space sector faces.

Section 3 (Vulnerabilities) shows the vulnerabilities of the space sector that need to be addressed.

Annex A (Threats table) provides the list of identified space systems threats.

1.6. REFERENCE DOCUMENTS

Table 3 presents the list of reference documents.

REFERENCE DOCUMENT	DOCUMENT NUMBER
[RD-1] SpaceSecurity - What are the threats to space systems?	https://www.spacesecurity.info/en/what-are-the-threats-to-space-systems/, visited on 2024-03-07.
[RD-2] Hughes - Securing SATCOM: Modernizing Military Systems form Smarter Adversaries	https://www.hughes.com/resources/insights/satellite-broadband/securing-satcom-modernizing-military-systems-smarter, visited on 2024-03-08.
[RD-3] Safety4Sea - Vessels navigating in China report GPS spoofing incidents	https://safety4sea.com/vessels-navigating-in-china-report-gps-spoofing-incidents/, visited on 2024-03-08.
[RD-4] IEEE Xplore – Cyber-Space and Its Menaces	https://ieeexplore.ieee.org/document/8878848, visited on 2024-03-08.
[RD-5] Researchgate – Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight	(PDF) Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight (researchgate.net), visited on 2024-05-21.
[RD-6] Researchgate - Understanding and Investigating Adversary Threats and Countermeasures in the Context of Space Cybersecurity	(PDF) Understanding and Investigating Adversary Threats and Countermeasures in the Context of Space Cybersecurity (researchgate.net), visited on 2024-04-22.
[RD-7] Researchgate - Falco, Gregory. (2018). Cybersecurity Principles for Space Systems. Journal of Aerospace Information Systems	(PDF) Cybersecurity Principles for Space Systems (researchgate.net), visited on 2024-04-22.

REFERENCE DOCUMENT	DOCUMENT NUMBER
[RD-8] CCSDS - Security Threats Against Space Missions	https://public.ccsds.org/Pubs/350x1g3.pdf, visited on 2024-04-22.
[RD-9] IBM - Types of Cyberthreats	https://www.ibm.com/blog/types-of-cyberthreats/, visited on 2024-04-22.
[RD-10] IBM – What is a Threat Actor?	https://www.ibm.com/topics/threat-actor, visited on 2024-04-22.
[RD-11] Sentinelone – What is a Threat Actor?	What is a Threat Actor? - Types & Examples (sentinelone.com), visited on 2024-04-22.
[RD-12] Medium – Protecting Space Systems from Cyber Attack	https://medium.com/the-aerospace-corporation/protecting-space-systems-from-cyber-attack-3db773aff368, visited on 2024-04-22.
[RD-13] Cyberterrorism as a global threat: a review on repercussions and countermeasures	https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10803091/, visited on 2024-04-22.
[RD-14] The Times of Israel – Hamas hacks into Israeli TV	https://www.timesofisrael.com/hamas-hacks-israeli-tv-the-terror-will-never-end/, visited on 2024-04-22.
[RD-15] The Guardian – BBC fears Iranian cyber-attack over its Persian TV service	https://www.theguardian.com/media/2012/mar/14/bbc-fears-iran-cyber-attack-persian, visited on 2024-04-23.
[RD-16] Springer – How modernized and strengthened GPS signals enhance the system performance during solar radio burst	https://link.springer.com/article/10.1007/s10291-021-01091-5, visited on 2024-04-23.
[RD-17] Advancing Earth and Space Sciences – Solar Radio Burst Events on 6 September 2017 and Its impact on GNSS signal frequencies	https://agupubs.onlinelibrary.wiley.com/doi/full/10.1029/2019SW002198#swe20865-bib-0012, visited on 2024-04-23.
[RD-18] The Watchers – Solar Radio Bursts	https://watchers.news/2011/09/07/solar-radio-bursts/, visited on 2024-04-23.
[RD-19] Archive – GPS freaking out?	https://web.archive.org/web/20170925202637/https:/nrkbeta.no/2017/09/18/gps-freaking-out-maybe-youre-too-close-to-putin/, visited on 2024-04-23.
[RD-20] VICE – It´s Surprisingly Simple to Hack a Satellite	https://www.vice.com/en/article/bmjq5a/its-surprisingly-simple-to-hack-a-satellite, visited on 2024-04-23.
[RD-21] Resilient Navigation and Timing Foundation – GPS Jammer Delays Flights in France.	https://rntfnd.org/2017/09/15/gps-jammer-delays-flights-in-france/, visited on 2024-04-23.
[RD-22] Softwarelab – Spoofing Examples (2024): The 4 Worst Attacks of All Time	https://softwarelab.org/blog/spoofing-examples/#:~:text=Spoofing%20Examples%201%201.%20Operation%20Aurora%20%282009%29%3A%20A,%28Multiple%20Incidents%29%3A%20A%20String%20of%20Digital%20Thefts%20, visited on 2024-04-23.
[RD-23] Varonis – Malware Protection: Basics and Best Practices	https://www.varonis.com/blog/malware-protection, visited on 2024-04-23.
[RD-24] The Register – German Space Center Endures Cyberattack	https://www.theregister.com/2014/04/15/dlr_attacked_china_apt_trojans/, visited on 2024-04-23.
[RD-25] Kaspersky – Zero-Day exploits and Zero-Day attacks	https://www.kaspersky.com/resource-center/definitions/zero-day-exploit, visited on 2024-04-23.

REFERENCE DOCUMENT	DOCUMENT NUMBER
[RD-26] OneLogin – 6 Types of Passwords Attacks and How to Stop Them	https://www.onelogin.com/learn/6-types-password-attacks, visited on 2024-04-23.
[RD-27] Expert insights – The Most Significant Password Breaches of 2021	https://expertinsights.com/insights/the-most-significant-password-breaches/, visited on 2024-04-23.
[RD-28] Mandiant – APT33 Targets Aerospace and Energy Sectors	https://www.mandiant.com/resources/blog/apt33-insights-into-iranian-cyber-espionage, visited on 2024-04-23.
[RD-29] Microsoft – Digital Defence Report 2023	https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023, visited on 2024-04-23.
[RD-30] ScienceDirect – Security Challenges When Space Merges with Cyberspace	https://www.sciencedirect.com/science/article/pii/S026596462300067X, visited on 2024-04-23.
[RD-31] World Economic Forum – 7 trends that could shape the future of cybersecurity in 2030	https://www.weforum.org/agenda/2023/03/trends-for-future-of-cybersecurity/, visited on 2024-04-23.
[RD-32] SatelliteToday – 10 Defining Moments in Cybersecurity and Satellite in 2023	https://interactive.satellitetoday.com/via/january-february-2024/10-defining-moments-in-cybersecurity-and-satellite-in-2023/, visited on 2024-04-23.
[RD-33] Report – Cybersecurity Survey	CSW-2024-TNR-03904, v. 1.0

Table 3: Reference documents

2. THREATS

A threat is the potential for a threat actor to exploit a vulnerability in a space system.

As mentioned in the introduction, space systems are ubiquitous, making them more susceptible to threats from various sources.

The recent influx of private companies into the space sector, such as Elon Musk's SpaceX and Jeff Bezos' Blue Origin, has contributed to this increased vulnerability. This rapid growth of new actors who may not have the same level of security experience compared to established players originate newer problems.

The origins of these new threats can be explained by four factors:

- **Diverse**: Increased international and commercial participation.
- **Disruptive**: The influx of new organizations entering the space sector and undertaking missions is reshaping the space landscape.
- **Unregulated**: Lack of established standards and legal frameworks.
- **Dangerous**: Dual-use commercial satellites are potential targets, and counterspace capabilities are growing.

Considering these four factors and the threats they create, we can categorize digital security threats to space systems into two main categories, as depicted in Figure 1 and some additional information to counter these threats can be found in Annex A. The two main categories are:

- **Electromagnetic**: Threats involving directed energy or electromagnetic interference targeting a space system.
- **Cyber**: Threats targeting the software, hardware, or communications infrastructure of a space system.

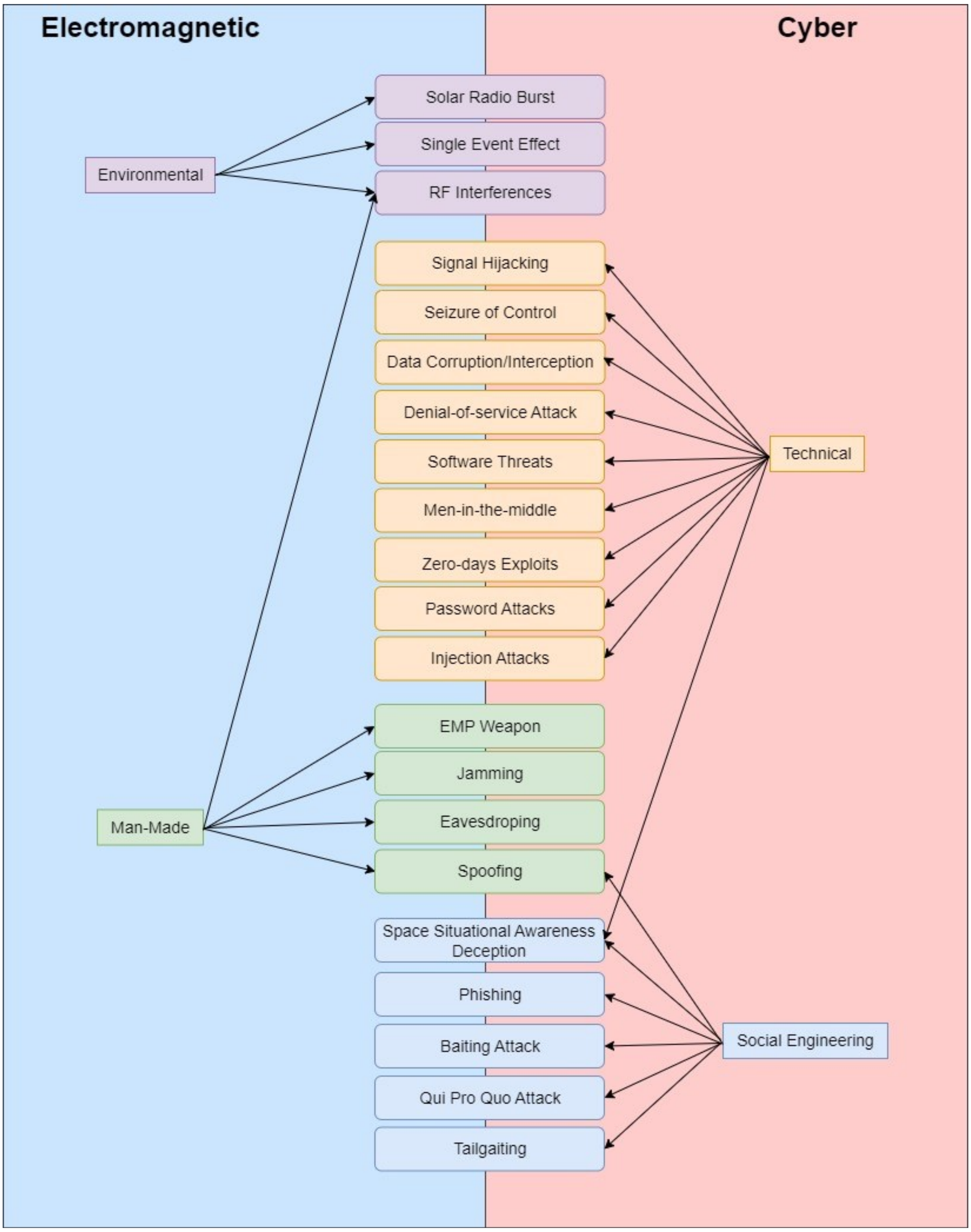

Figure 1: Digital Security Threats based on [RD-7]

Human actions, both intentional and unintentional, significantly contribute to cyber threats targeting space systems. When we focus on deliberate threats aimed at disrupting or damaging these systems, we encounter a diverse range of threat actors, each with distinct motives and objectives. Understanding the motivations and tactics employed by these actors is critical for stopping them in their tracks or even mitigating their potential impact.

Table 4 presents some of the most well-known perpetrators of cyberattacks, listing various threat actors with their respective motivations, skill levels, and tactics.

Threat Actor	Description	Motivation	Skill [RD-12]	Tactics
Amateur Hackers	Threat actors who target systems to test their cyber	•Personal motivations	Low	Pre-existing tools and techniques

Threat Actor	Description	Motivation	Skill [RD-12]	Tactics
	skills and mostly for their enjoyment.[RD-11]			
Cybercriminals	Individuals or groups that target computer systems for financial gain.[RD-10]	•Financial	Moderate	Ransomware and Phishing
Hacktivists	Threat actors that disrupt systems to promote political or social agendas: such as human rights violations and free speech.[RD-10]	•Ideological or Political	Moderate / High	Social engineering, hacking passwords, malware, logging keystrokes and DDoS
Insider Threats	There are two main categories of insider threats. Malicious insiders intentionally misuse their legitimate access to harm the organization's systems. Incautious insiders unintentionally cause data breaches due to carelessness.[RD-11]	•Personal motivations (promotions) •Corporate espionage •Financial	Low / High	Abuse of access privileges (malicious insiders)
Cyberterrorists	Cyberterrorists, funded by nations or non-governmental groups, aim to disrupt critical infrastructure, spread fear, and advance their causes/ideologies.[RD-11]	•Ideological or Political •Religion	High	Social engineering, DoS, malware, SQL injection, Man-in-the-Middle attacks, and Stuxnet-like attacks. [RD-13]
Nation-state Actors	Nation states and governments that attack or support other threat actors to target systems with the goal of spy or stealing sensitive data and cause disruption to another government´s critical infrastructure. [RD-11]	•State-cyber espionage •Technology Theft •Geo-Political	Very High	Cyber warfare

Table 4: Threat actors behind the attacks

Multiple methods exist for attacking digital systems, as detailed in the following sections. However, there are common steps most hackers follow. Figure 2 depicts this attack flow.

The process typically begins with a deep scan of the target system, focusing on either PCs or servers. The goal is to identify vulnerabilities and breaches that can be exploited for unauthorized access.

Once vulnerabilities are identified, the hacker infiltrates the system. This grants them the ability to manipulate the system or steal data, depending on their motives.

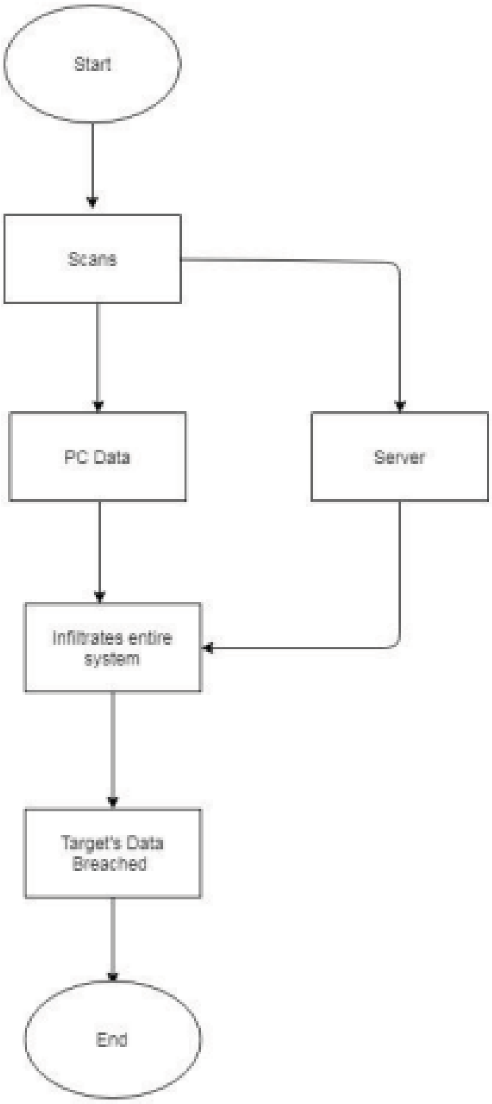

Figure 2: Cyberattack flowchart [RD-4]

During the digital era, the number of cyber incidents in space sector has increased exponentially, as shown in Figure 3. There has been a clear trend of increasing cyber-capabilities targeting space infrastructure, along with a rise in the number of actors capable of carrying out these attacks. Today, nearly 30 states have demonstrated some degree of cyber-offensive counterspace capabilities.

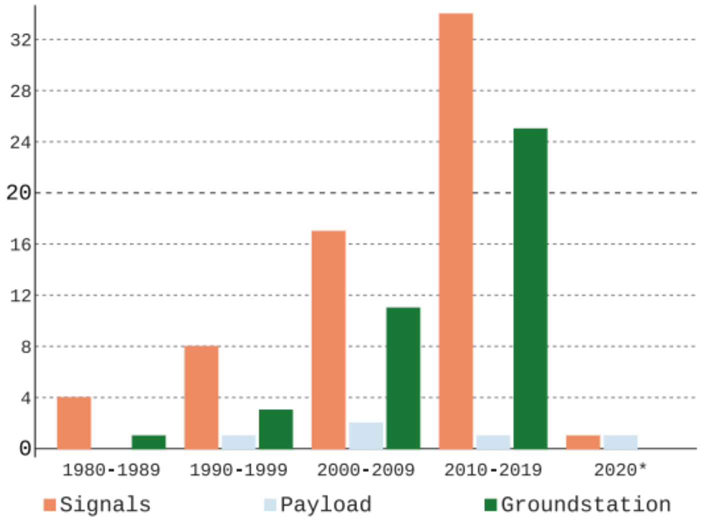

Figure 3: Target Segments by Decade [RD-5]

Cyberattacks on the space sector occur for multiple reasons. Figure 4 shows several motivations and type of attacks executed against space infrastructure.

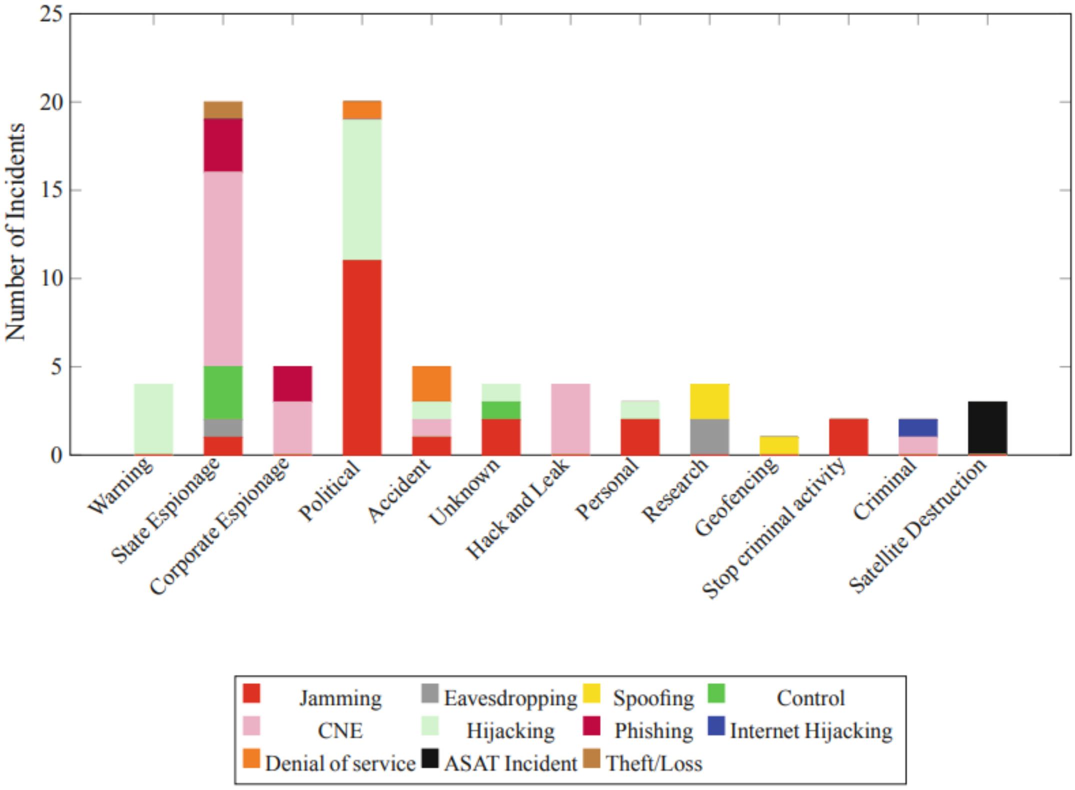

Figure 4: Motivation of Satellite Incidents [RD-5]

Each threat carries a degree of danger, depending on its effects on the affected systems. These effects can be reversible or irreversible. For example, a simple jamming attack is considered reversible because it disrupts communications for a short period. However, a kinetic or nuclear ASAT attack would result in the destruction of the satellite. Figure 5 depicts the range of effects caused by various threats.

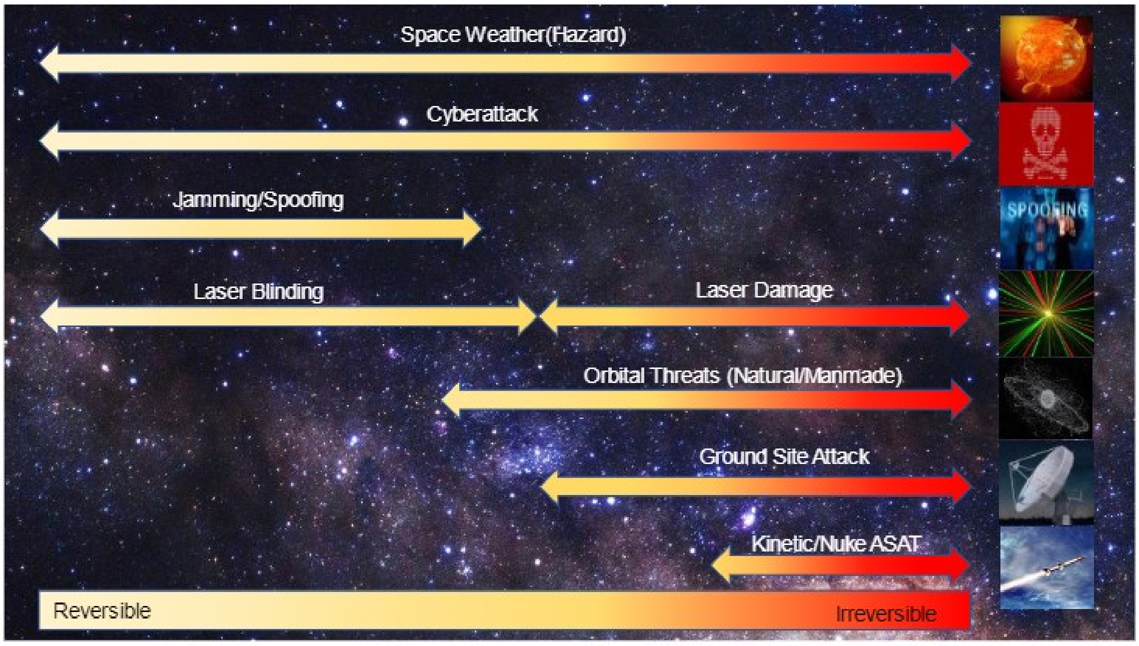

Figure 5: Range of effects cause by threats [RD-6]

2.1. Electromagnetic Threat

Electronic threats to space infrastructure encompass events that utilize the **electromagnetic spectrum** (waves or directed energy) to disrupt, damage, or disable critical digital assets. These threats can be categorized based on their origin, **Environmental** and **Man-made**.

2.1.1. Environmental

These threats occur naturally due to phenomena like solar flares or geomagnetic storms. These events can induce electrical currents in spacecraft electronics and disrupt operations.

2.1.1.1. SOLAR RADIO BURST

Satellites orbiting Earth are exposed to harsh solar radiation due to the lack of protection from the Earth's atmosphere. This vulnerability makes them susceptible to natural hazards like solar radio bursts (SRBs), as depicted in Figure 6. SRBs can significantly impact satellites, especially those crucial for Global Navigation Satellite Systems (GNSS). Disruptions in GNSS performance can cause problems for users who rely heavily on these services.

Fortunately, techniques exist to mitigate the effects of SRBs. Some of these techniques are already in use, such as increasing the transmitted signal power at the L2 frequency and implementing new civilian codes, enhancing the stability and reliability of GNSS operations [RD-16].

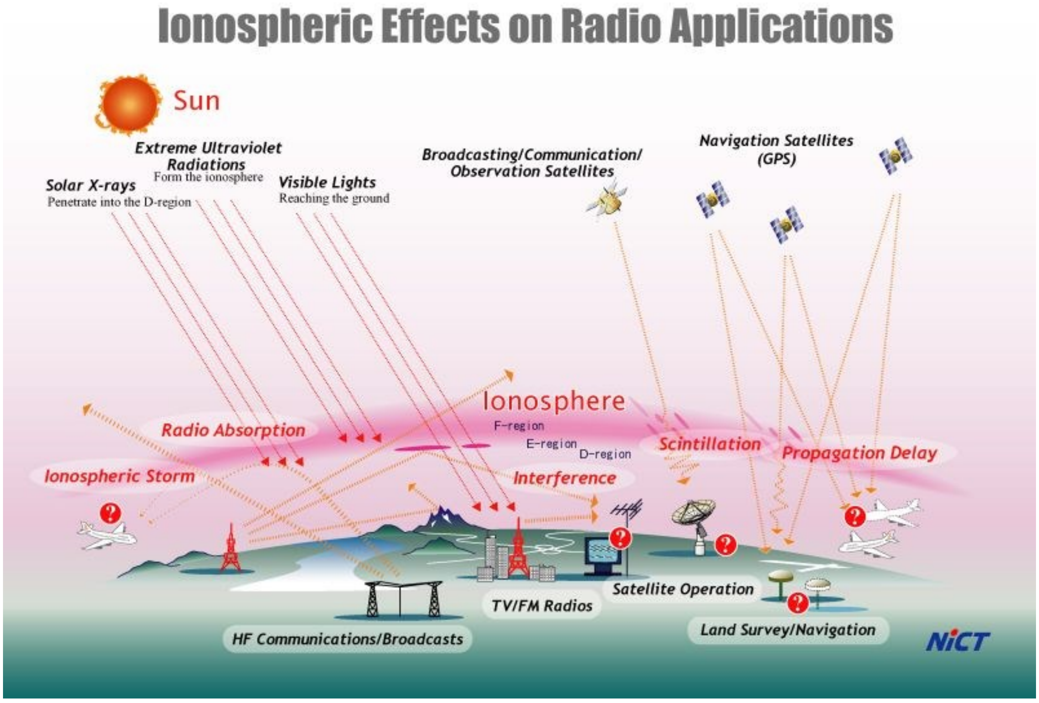

Figure 6: Solar radio burst effects on Space Infrastructure [RD-18]

On 6 September of 2017, the Sun expel X-class flares that cause a coronal mass ejection (auroras) on Earth and affecting the performance of GNSS signals [RD-17].

2.1.1.2. SINGLE EVENT EFFECTS

This threat arises from the deposition of charged particles within specific regions of a satellite or ground infrastructure. These charged particles can originate from cosmic events, or direct ionization and nuclear interactions within the components. The effects can range from catastrophic, leading to complete component destruction, to more subtle errors like bit flips in memory cells or registers.

Here are some of the catastrophic Single Events that can occur:

- **Burnout**: This is particularly dangerous when the space asset uses metal-oxide-semiconductor field-effect transistors, commonly found in multiplex bus architectures. High currents triggered by ionizing particles can cause these devices to overheat and fail permanently. This risk can be mitigated by using radiation-hardened semiconductors.
- **Functional Interrupt**: Like a Single Event Upset (SEU), this event causes unexpected loss of functionality or changes the state of a device. While a power-cycle may sometimes restore functionality, permanent damage is also possible.
- **Gate Rupture**: Here, the impact of ionizing particles damages the gate dielectric of a transistor, causing a breakdown of the insulator and a temperature increase. Assets utilizing non-volatile static random-access memories (SRAM) and electrically erasable programmable-read-only memories (EEPROMs) are particularly vulnerable.
- **Latchup**: This event creates a low-resistance path between the power supply and ground due to ionizing particles. This can lead to high currents, vaporized metals, fused wires, and melted silicon, resulting in permanent damage.

The non-catastrophic Single Events that cause less severe errors but can still disrupt operations are:

- **Multiple Bit Upset** (MBU): This event primarily affects memory components. Ionizing particles deposit enough energy to flip multiple bits within the same data word (a group of bits). Employing error-correcting codes (ECC) and arranging data bits non-contiguously in memory can mitigate this effect.

- **Multiple Cell Upset** (MCU): Here, ionizing particles cause multiple bits within an integrated circuit to flip state simultaneously. Increasing the spacing between transistors in an integrated circuit design can help mitigate this risk.
- **Transient Errors**: Ionizing particles can also induce temporary errors in a circuit's combinational logic. The likelihood of this event increases with faster operating speeds. Utilizing techniques like circuit redundancy and voting can help mitigate these transient errors.

2.1.2. Man-Made

These threats are deliberately carried out by malicious actors who employ techniques like jamming or spoofing of radio frequency (RF) signals.

2.1.2.1. JAMMING

Jamming interferes with RF communications by deliberately transmitting radio signals on the same frequency as the communication occurring between satellites or between satellites and ground stations. This causes temporary disruption to operations, making jamming a reversible attack, but non the less extremely dangerous because jamming critical navigation or communication signals could have severe consequences for national security or commercial activities.

Common targets for jamming technology include communication dishes, GPS receivers, and satellite phones. This is a primary threat because the technology needed to generate jamming signals is commercially available and inexpensive.

Figure 7 depicts two primary types of jamming that can disrupt satellite communications [RD-30]:

- **Uplink Jamming**: This type targets the satellite itself, disrupting services for all users within the satellite's reception area.
- **Downlink Jamming**: This type targets the ground station, causing localized disruptions to users receiving signals from the satellite.

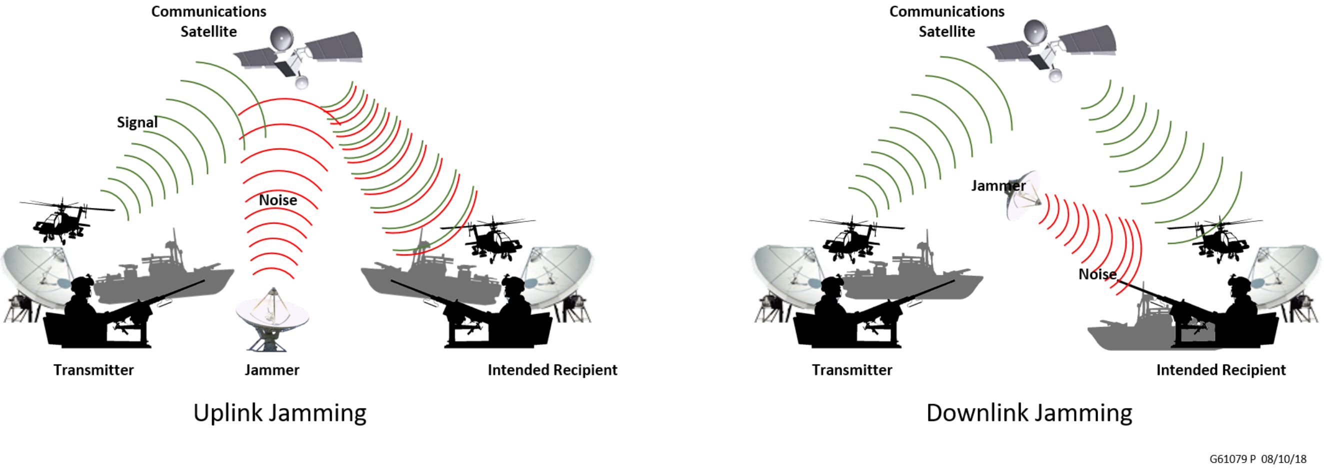

Figure 7: Jamming Threat [RD-2]

An unusual case of jamming occurred in 2017 at Nantes Airport in France. A driver left an operational GPS jammer in their parked car, which caused interference with aircraft tracking systems and cause delays in flights [RD-21].

2.1.2.2. SPOOFING

Spoofing is another electronic threat. It involves sending counterfeit signals that mimic legitimate signals with the intention of gaining unauthorized access to a system, network, or data. The location of the spoofing attempt determines its potential impact:

- **Uplink Spoofing**: If the spoofing occurs on the uplink (the signal sent from the ground to the satellite), it could allow the attacker to take control of the satellite.
- **Downlink Spoofing**: If the spoofing occurs on the downlink (the signal sent from the satellite to the ground), it could alter or corrupt the data being transmitted.

An example of an RF signal spoofing attack is called **"meaconing**" [RD-1]. This involves broadcasting a copy of the signal that is either out of time or with corrupt data, depicted in Figure 8. This can be done even if the signal is encrypted. This distinction highlights the seriousness of spoofing, as it can potentially lead to the complete compromise of a satellite or the manipulation of critical information.

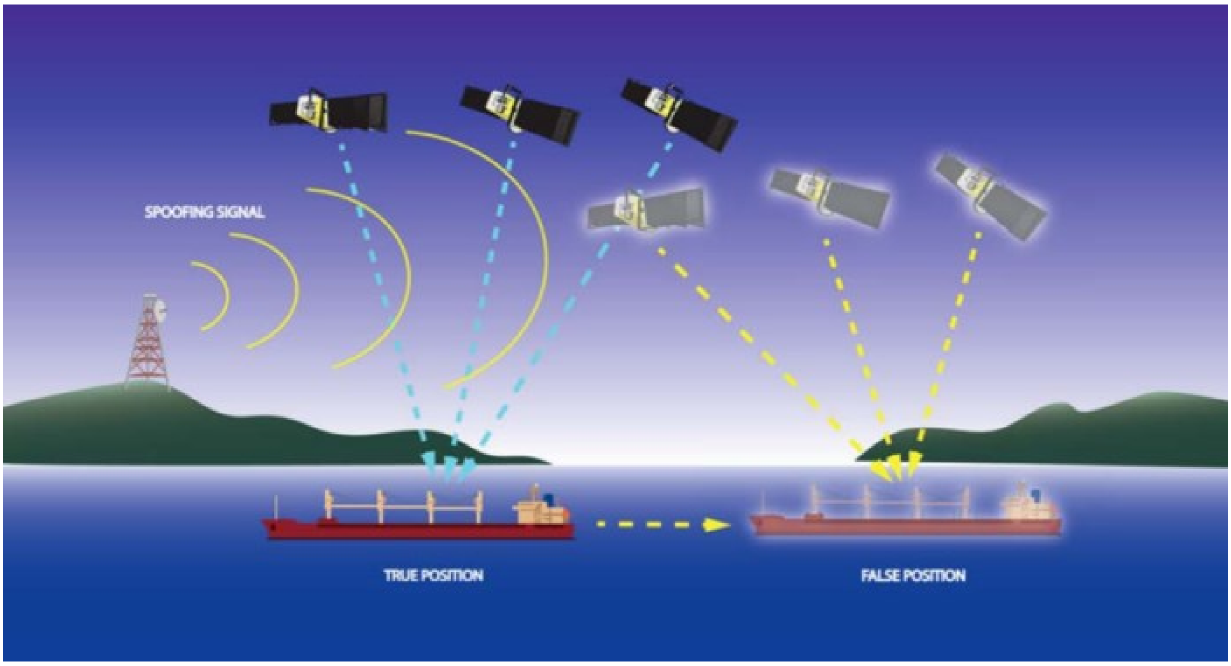

Figure 8: Spoofing threat [RD-3]

In 2017, ships on the Black Sea experienced an anomaly in their maritime navigation systems. The systems reported incorrect locations, placing the vessels near Gelendzhik Airport. This incident is a suspected case of GPS spoofing, allegedly perpetrated by Russia [RD-19].

2.1.2.3. EAVESDROPPING

Another electronic threat to consider is **eavesdropping**. This involves intercepting signals from satellites or other sources for monitoring purposes. This activity, often referred to as signals intelligence, is a technique used by security agencies like the FBI and CIA. Signals intelligence can be further divided into two categories: communications intelligence and electronic intelligence. The key difference lies in the type of signal intercepted. Communications intelligence focuses on voice communications, while electronic intelligence focuses on other radio signals.

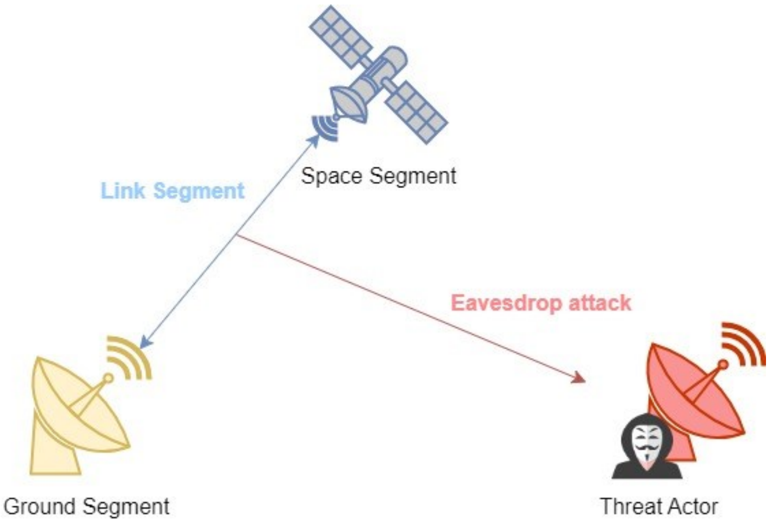

Figure 9: Eavesdrop attack on satellite communications

In 2015, during a Chaos Communication Camp held in Germany, researchers demonstrated a potential vulnerability in the Iridium satellite communications constellation. They were able to analyse and decode signals, potentially allowing access to readable information within Iridium pager traffic [RD-20].

2.2. Cyber

This type of threat does not require significant resources but necessitates a prominent level of knowledge about the target system.

For that reason, the perpetrators of these attacks can be individuals or groups, with or without state support, making the cyber threat one of the most challenging threats to trace due to the difficulty of identifying the attacker's origin.

We can categorize cyber threats into two main groups: **technical** and **social engineering**.

2.2.1. Technical

Taking advantage of technical vulnerabilities in software to gain unauthorized access to systems and data, potentially causing disruption or damage. This category of threats encompasses various methods, presenting in the following subsections.

2.2.1.1. SIGNAL HIJACKING

Consists in an unauthorized takeover of a transmission channel to cause disruption or to spread malicious content. Put in a space system perspective, the threat actor could do a spectrum analysis to search if a given transponder has free communication slots. In case of existing unuse communication slots, it can leverage it and interfere with the normal data stream causing a denial-of-service. This threat does not have a very steep learning curve and do not need significant resources to execute.

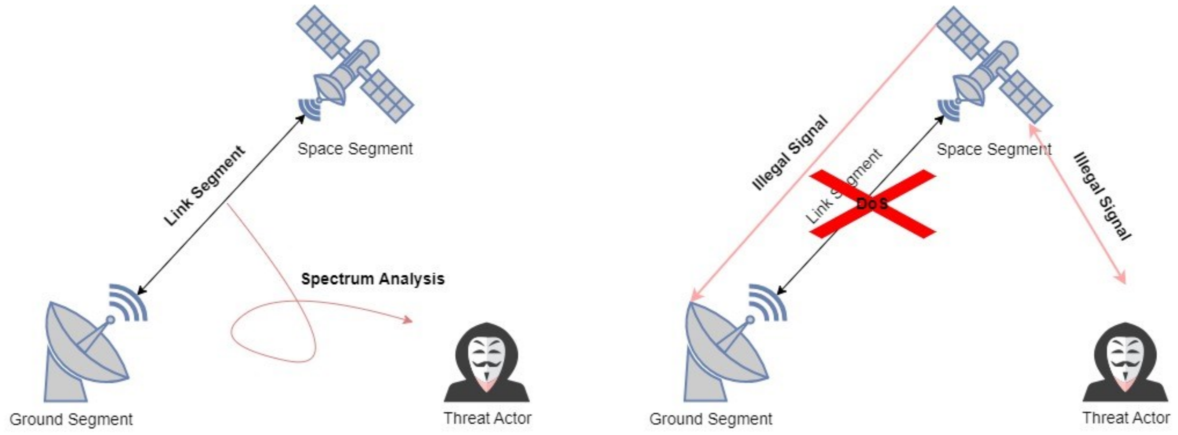

Figure 10: Spectrum analysis and Signal hijacking

The following is a real-world example of signal hijacking. In 2016, the Palestinian Islamic movement Hamas interrupted the Israeli Channel Two broadcast with an illegal signal. This caused viewers' TV screens to be filled with images and messages inciting terrorism [RD-14].

2.2.1.2. DATA CORRUPTION AND INTERCEPTION

While spoofing a satellite's communication is challenging, it can be achieved by intercepting or corrupting radio frequency signals. This becomes a critical issue if the Command and Control (C&C) link lacks robust encryption, that offers the threat actors an open door to the entire satellite´s communication system [RD-7]. In such a scenario, attackers could introduce software/hardware failures, bugs, or alter data. A simple corrupt command can lead to a catastrophic loss of the satellite or potentially hijack the satellite's communication system and cause severe financial and reputational arm to the targeted companies.

2.2.1.3. DENIAL-OF-SERVICE ATTACK

This attack method, known as a Denial-of-Service (DoS) attack, aims to disrupt a system's operations by overloading it with data. Hackers often leverage botnets, networks of compromised computers infected with malware. These botnets then bombard the target system with malicious traffic, overwhelming its capacity to handle legitimate requests. This can disrupt control operations and data transfer between the ground and space segments, potentially leading to a loss of critical assets.

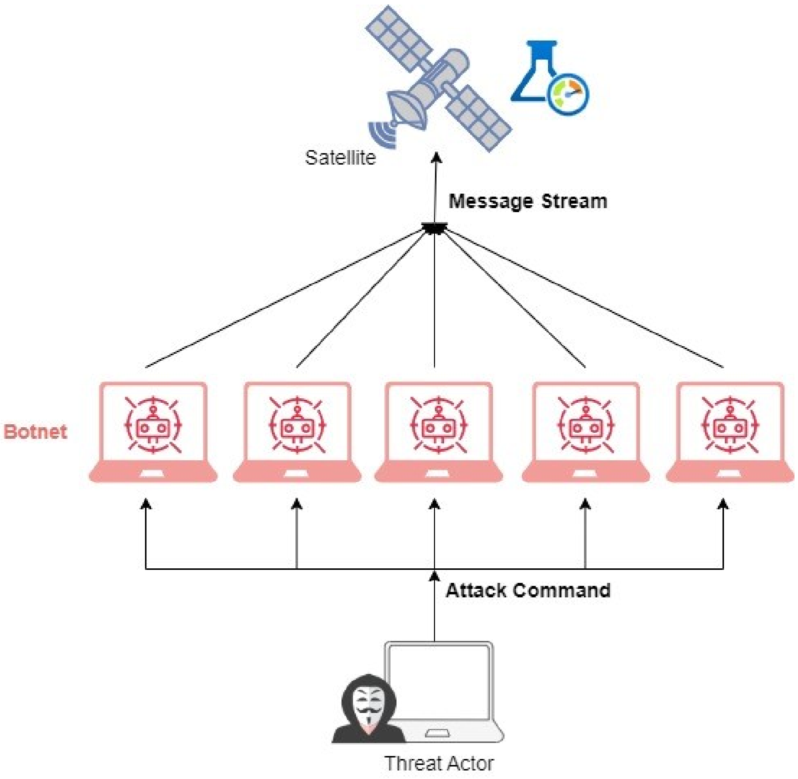

Figure 11: Denial-of-Service attack (botnet)

On March 2, 2012, BBC Persia's satellite feed and phone lines were targeted in a denial-of-service (DoS) attack. The BBC witnessed a sudden and massive spike in viewership for its Persian TV service, overwhelming their online systems in London. Hacktivists in Iran were suspected to be behind the attack, which involved flooding the BBC's systems with a large volume of requests, making it difficult for legitimate users to access services [RD-15].

2.2.1.4. WEB SPOOFING

Now in the domain of the network, spoofing is a deceptive practice where cybercriminals gain access to the system by using a false identity. The most common types of spoofing are:

- Email Spoofing
- IP Spoofing
- Website Spoofing

This can be accomplished using stolen user credentials or a false IP address. After the attacker successfully gains access as a legitimate user or host, elevation of privileges or abuse using authorization can begin.

In 2017, Brazilian banks fell victim to DNS spoofing attacks. These attacks redirected users from legitimate bank websites to fraudulent ones, potentially allowing attackers to steal sensitive data [RD-22]. Similar tactics can be employed in the space sector. Attacks could target ground segments to steal data or, in a more audacious scenario, even attempt to seize control of a satellite.

2.2.1.5. SOFTWARE THREATS

Designed to take control of internal organizational information systems, identify sensitive information, exfiltrate the information back to adversary, and conceal these actions software threats like **malware** can be a nightmare to the space systems.

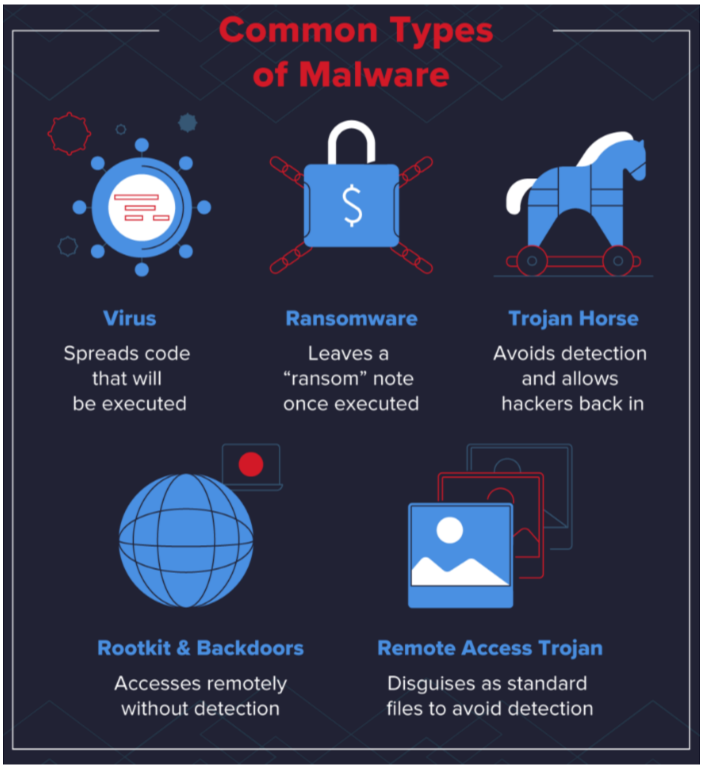
Common Types of Malware
Virus
Spreads code that will be executed
Ransomware
Leaves a "ransom" note once executed
Trojan Horse
Avoids detection and allows hackers back in
Rootkit & Backdoors
Accesses remotely without detection
Remote Access Trojan
Disguises as standard files to avoid detection

Figure 12: Types of Malware [RD-23]

In 2014, the German space research centre in Cologne was compromised by a malware attack targeting researchers' machines working on armament and rocket technologies. The malware included Trojans designed to self-destruct upon detection, while others remained dormant for potential later activation [RD-24].

2.2.1.6. MAN IN THE MIDDLE

A man-in-the-middle attack is a cyberattack where a threat actor inserts themselves into a communication channel between two parties. The attacker's goal is to eavesdrop on the conversation and potentially steal data [RD-9]. These attacks can be difficult to detect nowadays because of the use of AI. While AI can be used to create realistic voice and text for social engineering purposes, there are still methods to protect against these attacks, like use of cryptography before transmitting data and use of hashed message authentication to prevent alteration of data.

2.2.1.7. ZERO-DAYS EXPLOITS

This type of threat involves a zero-day exploit, where a malicious actor discovers a software vulnerability before the developers and leverages it to disrupt or harm systems that rely on that software [RD-9].

Zero-day exploits are particularly concerning for open-source software because its open nature can make vulnerabilities easier to find. However, with the increasing use of commercial off-the-shelf (COTS) software in the space sector, this threat becomes relevant there as well.

Fortunately, there are techniques to mitigate this threat:

- **Vulnerability Databases**: Using resources like the National Institute of Standards and Technology (NIST) National Vulnerability Database allows for quicker identification and patching of known vulnerabilities.
- **Machine Learning for Anomaly Detection**: Machine learning can analyze past exploit data to set up a baseline for normal system behavior. Deviations from this baseline might indicate a potential zero-day attack.

During the COVID-19 pandemic lockdown, the use of video conferencing platforms like Zoom surged. Unfortunately, Zoom fell victim to a zero-day exploit. This exploit allowed attackers to remotely access a user's computer if they were running an older version of the Windows operating system [RD-25].

Imagine a scenario where the target was an administrator for a space sector company. If their computer were compromised, the attacker could gain access to sensitive files or even manipulate commands sent to satellites.

This example highlights the potential dangers of zero-day exploits and the importance of proactive security measures.

2.2.1.8. PASSWORD ATTACKS

Passwords function as the first line of defense, protecting data access from unauthorized individuals. Over time, password creation has become more stringent. Now, passwords often require a minimum length, a combination of uppercase and lowercase letters, numbers, and special characters.

Despite these advancements, password attacks are still one of the most common causes of data breaches. In 2020 alone, over 80% of data breaches involved compromised credentials [RD-26].

Hackers employ various methods to crack passwords. Here are some of the most common:

- **Phishing**: Deceptive emails or messages designed to trick users into revealing their passwords or clicking malicious links.
- **Man-in-the-Middle** (MitM): Attackers insert themselves into a communication channel to intercept data, including passwords.
- **Brute-Force Attack**: Automated software rapidly tries millions of username and password combinations to gain access to an account. This method is most effective against weak passwords.
- **Dictionary Attack**: Hackers use a list of frequently used words and phrases, such as birthdays, pet names, or song titles, to guess passwords.
- **Credential Stuffing**: Hackers exploit previously leaked username and password combinations from other data breaches, hoping users have not changed their credentials across different platforms.
- **Keyloggers**: Malicious software that records every keystroke a user types, including passwords.

The 2021 SolarWinds supply chain attack serves as a stark reminder of the importance of strong password practices. In this incident, attackers are believed to have gained access through a weak password used by an intern. This weak password was reportedly publicly accessible due to a misconfigured GitHub repository [RD-27].

2.2.1.9. INJECTION ATTACKS

Injection attacks are a common and powerful threat, targeting vulnerabilities in web applications, databases, and other systems that rely on user input. These attacks work by crafting malicious code disguised as legitimate data, which then gets injected into the system's processing pipeline. Once inside, the attacker's code can wreak havoc, such as:

- **Stealing sensitive data**: Usernames, passwords, financial information, or other confidential data can be stolen off by the injected code.
- **Taking control of systems**: Injected code can manipulate ground system's core functionalities, potentially allowing attackers to gain unauthorized access or even complete control.
- **Disrupting operations**: Malicious code can cause systems to crash, malfunction, or become unavailable, hindering normal operations.

These attacks are particularly dangerous because they often exploit harmless user inputs, like login credentials, search queries, or form submissions.

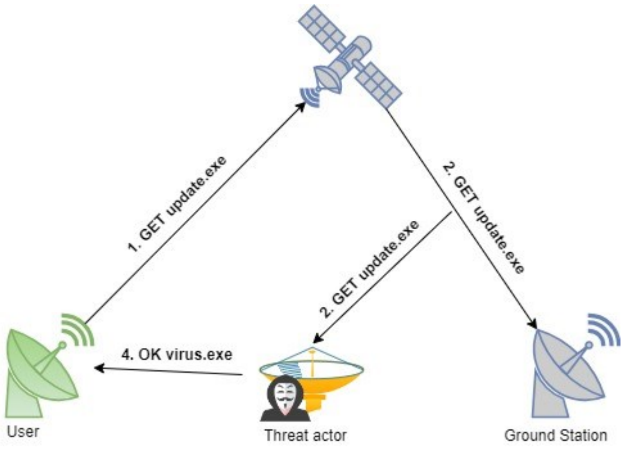

Figure 13: Example of an Injection attack

In 2007, a Russian government-affiliated group called Turla used satellite internet signals to exfiltrate data from malware infections in countries ranging from the United States to the former Eastern Bloc. By using a ground antenna, Turla could detect IP addresses of satellite internet users and initiate TCP/IP connections with minimal traceability [RD-7].

2.2.1.10. OTHERS TECHNICAL THREATS

The following technical threats were identified through the cybersecurity survey titled "Survey on Cybersecurity Challenges and Solutions for Space Systems" [RD-33], conducted among space sector specialists. A summary of these threats is presented in Table 5:

Threat	Example
Source Code Tampering	Tampering with source code/binary to introduce accidental or malicious code that could either prevent correct operation or allow unauthorized parties to interact with the software.
Spacecraft configuration modification	Modifying spacecraft configuration to turn equipment on or off, disable a camera at a critical moment, change the spacecraft's direction, target incorrectly (ClearSpace-1), alter FDIR configurations, or remove detection mechanisms.
Bad design	When design is neglected, and instead, code is generated that may be flawed.
Speed up development / pressure	Prioritizing speed over thoroughness in design, code analysis, and testing can leave vulnerabilities in the final product.
Lack of certification of space systems	Unlike industries like aviation (FAA) and railways (TUV), space systems lack comprehensive certification processes that include cybersecurity aspects.
Lack of vulnerability / threat analysis	Failure to perform software vulnerability or threat analysis before finalizing system and software requirements, which these analyses should actively contribute to.
Exploit development tools	Exploiting known vulnerabilities in commonly used development tools like compilers or debuggers to inject malicious code into space system software during the build process.
Unmitigated errata	Failing to patch a known vulnerability in a satellite's operating system, leaving it exposed to potential attacks.

Table 5:Threats identify by the specialists

2.2.2. Social Engineering

These attacks exploit psychological vulnerabilities and aim to manipulate and deceive victims into taking actions that compromise systems. This can involve disabling security features or unknowingly providing their login credentials. These following subsections show some examples of attacks using social engineering.

2.2.2.1. PHISHING/SPEAR PHISHING ATTACK

Threat actors engage in phishing attacks by forging communications that appear to originate from a legitimate or trustworthy source. Their goal is to trick users into revealing sensitive information like usernames, passwords, or Social Security Numbers (SSNs). These attacks commonly occur via email, instant messaging, or similar channels and often direct users to fraudulent websites that mimic legitimate ones. Once users enter their information on these fake sites, it's stolen by the attackers.

In 2017, a suspected Iranian group known as APT33 targeted organizations headquartered in the United States, Saudi Arabia, and South Korea. These organizations spanned the military and commercial sectors of the aviation industry, as well as the petrochemical production segment of the energy sector.

APT33 employed spear phishing emails that incorporated recruitment lures. These emails contained malicious HTML application files. Unbeknownst to the recipients, these files harboured embedded code that automatically downloaded a custom APT33 backdoor onto their systems [RD-28].

2.2.2.2. BAITING ATTACK

Threat actor’s places removable media (e.g., flash drives) containing malware in locations external to organizational physical perimeters but where employees are likely to find the media (e.g., facilities parking lots, exhibits at conferences attended by employees) and use it on organizational information systems.

2.2.2.3. QUID PRO QUO ATTACK

Threat actors may leverage quid pro quo attacks by impersonating IT support staff. These attackers exploit a user's trust by offering to perform helpful services, such as software installation or system updates. However, in exchange for this supposed assistance, they seek to obtain a user's login credentials or other sensitive data. Often, these attackers’ prey on the victim's potential panic or lack of technical knowledge, posing as the solution to a non-existent or exaggerated problem.

2.2.2.4. TAILGATING

Threat actors may employ a technique called "tailgating" to gain unauthorized access to secure facilities. Tailgating involves following authorized individuals closely behind them as they enter a secure location, bypassing physical security checks.

2.2.2.5. WEB SPOOFING

Threat actors can create duplicates of legitimate websites, known as phishing sites. When users visit these counterfeit sites, they may unknowingly enter their private information, such as login credentials or other sensitive details, which are then collected by the attackers behind the scheme.

3. Vulnerabilities

A vulnerability is a flaw or weakness in the design, implementation, or operation and management of an asset that could be exploited by a threat.

The following sections explore some of the main vulnerabilities that pose a significant risk to space systems.

3.1. Human Factor

The **human factor** is a significant vulnerability in space systems and other critical infrastructure across various industries. Human error, both intentional and unintentional, can play a role in cyberattacks. This includes actions taken by individuals, wittingly or unwittingly, on behalf of malicious actors, as well as neglecting essential security measures like patching, misconfiguring systems or open a suspicious link or using an untrusted external storage device.

3.2. Development Life Cycle

From the outset of any space mission project, careful selection of a secure software development life cycle (SSDL) is critical. This choice should be guided by the specific mission requirements of the satellite. The Software Security Development Lifecycle (SSDL) provides a framework that integrates security considerations throughout every stage of the software development process. This "security by design" approach ensures that developers prioritize security concerns from the project's inception.

Choosing an inappropriate SSDL can have disastrous long-term consequences for both the mission and the organization. For projects designed for extended lifespans, technological advancements on Earth will inevitably occur. Software built with an outdated SSDL will struggle to keep pace, creating vulnerabilities that attackers can exploit.

3.3. Supply Chain

The global nature of the space industry's supply chain presents a significant cybersecurity challenge for space agencies. Satellites and other critical systems often consist of numerous components manufactured by diverse companies across the globe. Unfortunately, these companies may operate under varying regulations with inconsistent enforcement regarding cybersecurity protocols. This inconsistency introduces potential vulnerabilities that malicious actors could exploit. For example, attackers might insert hardware or software backdoors, tamper with firmware/code, or exploit weaknesses in components at a later stage.

Recent high-profile software supply chain attacks, such as SolarWinds, Log4j, Codecov, and Kaseya, highlight the severity of this threat. According to the 2023 Microsoft Digital Defence Report, these incidents impacted over 490 million customers and exposed over 100,000 malicious open-source packages. Microsoft's analysis identified ransomware, phishing, and malware as the primary supply chain threats.

While the report highlights social engineering attacks as a concern within the supply chain, it's crucial that companies and their suppliers must work together to strengthen their defences. Investing in education and awareness training for employees across the supply chain is paramount in mitigating these risks [RD-29].

3.4. Commercial-Off-The-Shelf

The rapid growth of the small satellite sector brings with it an increased vulnerability to cyberattacks. This trend is driven by several factors: significantly reduced construction costs due to cheaper **Commercial-Off-The-Shelf** (COTS) hardware and open-source software, alongside new initiatives like **Ground Stations-as-a-Service**. Consequently, the likelihood of cyberattacks targeting these systems becomes significant.

The attack surface of both the space and ground segments has grown and will continue to do so. The two primary areas of concern are the ground infrastructure and the **open-source software** used in **COTS hardware** on satellites. The ground segment presents a more accessible target due to its internet connectivity and human operation, making it more susceptible to social engineering attacks.

3.5. Legacy Technology

Reliance on legacy technology, such as satellites in geosynchronous orbit (GEO) with missions around 25 years, creates persistent vulnerabilities. Upgrading these systems presents a challenge due to the extensive testing required to ensure compatibility with newer equipment and avoid disrupting the functionality of other systems.

Many operational satellites still utilize legacy technologies. For instance, some may rely on older generation processors that lack robust security features, making them susceptible to cyberattacks. Additionally, some systems may have hardcoded security credentials or employ insecure communication protocols, further increasing vulnerabilities [RD-30].

3.6. Training and Cybersecurity Culture

The cybersecurity landscape is rapidly evolving, and organizations in the space sector, like any others, face significant consequences for failing to prioritize it. Neglecting to implement a strong cybersecurity training program and foster a security culture within their organizations can have dire repercussions, as show as follows:

- **Increased Legal and Regulatory Scrutiny**: The Securities and Exchange Commission (SEC) is tightening its grip on cybersecurity compliance. As evidenced by the SolarWinds case, where the CISO faced legal ramifications for a weak security program and misleading information, organizations with inadequate cybersecurity measures can be held liable and face heavy penalties [RD-32].
- **Reputational Damage**: Unlike Viasat, companies that choose to conceal security vulnerabilities risk public backlash and a loss of trust from investors, partners, and customers. Transparency and acknowledging shortcomings, like Viasat's approach, can be a positive step towards rebuilding trust [RD-32].
- **Operational Disruptions and Financial Losses**: Without proper training and a strong cybersecurity culture, organizations are more susceptible to cyberattacks. These attacks can lead to data breaches, operational disruptions, compromised systems, and significant financial losses.

3.7. Technological Evolution

The relentless pace of technological advancement presents a double-edged sword for cybersecurity. New technologies offer solutions to current problems, but they also create new vulnerabilities for attackers to exploit. The space sector, with its critical role in supporting modern society across various industries and individual lives, needs to be at the forefront of cybersecurity efforts.

Here are some key trends, tensions, and trade-offs that will shape the future of cybersecurity as a whole [RD-31]:

- **Widening Cybersecurity Access**: We need to shift the cybersecurity mindset from defending fortresses to building resilience and recovery capabilities. Introducing cybersecurity education at younger ages, such as elementary school, will be a significant step towards fostering cyber awareness.
- **Endangered Online Trust**: Advancements in Artificial Intelligence (AI) and Machine Learning (ML) make it increasingly difficult to distinguish between humans and machines. This raises concerns about cyberattacks exploiting this technology to compromise information integrity. Consequently, this might lead to a shift away from online activities, potentially pushing some people back towards rudimentary technologies like analogue devices.
- **Digital Sovereignty vs. Open Internet**: Governments are increasingly seeking greater control over their online spaces, potentially leading to the creation of localized or regional internets with their own rules and regulations. Currently, the internet is relatively interconnected, allowing for the free flow of information and data across borders.

3.8. Static Code Analysis Tools

Without them, developers may unknowingly introduce vulnerabilities into software that SCA tools would have flagged immediately. Attackers can then exploit these vulnerabilities to gain unauthorized access, steal data, or disrupt operations.

3.9. Security Analysis (Threats and Vulnerabilities)

This step focuses on identifying and understanding potential threats and vulnerabilities within a system. It's crucial for organizations, particularly those in the space sector, to conduct thorough security analyses. Threat modelling, vulnerability scanning, and other proactive security measures help to mitigate risks and protect critical infrastructure.

Failing to conduct a proper security analysis essentially invites threat actors to exploit previously unidentified vulnerabilities, jeopardizing the systems that govern the satellite. This risk can arise from simply reusing existing technologies or tools in a new project.

Reused technology, like systems and tools, can become a security Achilles' heel for a project. The assumption that something has already been thoroughly tested can lead to neglecting further security assessments. However, before incorporating any tool (compilers, auto-code generator, configurator generations, V&V tools, simulators) into a project, it's paramount to conduct a comprehensive security evaluation to identify any vulnerabilities that could compromise its intended functionality. Consider a simulator: if it harbours a vulnerability, it could produce simulation results that deviate significantly from real-world project execution.

3.10. Security Requirements

Regulations and standards in cybersecurity play a crucial role in ensuring that products and systems follow an approved methodology and basic requirements that enhances their security against potential threats. The absence of such regulatory security requirements and standards creates significant challenges for organizations, particularly in the space sector. Without a common baseline, different organizations may adopt varying security practices, leading to uneven levels of protection across the industry. This inconsistency creates vulnerabilities that attackers can exploit. Additionally, even if an organization chooses security requirements for a project, they might be insufficient to combat the ever-evolving ingenuity of threat actors.

Following established standards like IEC 62443 represents a significant step forward. This comprehensive standard provides a framework for building highly secure software from the very beginning, adhering to the "defence-in-depth" strategy, by providing basic security requirements and industry best practices.

3.11. Security Design

Security design is a fundamental principle in cybersecurity. It focuses on incorporating security measures throughout the entire development lifecycle of a system. Neglecting this crucial step has serious consequences, leading to increased vulnerability to attacks.

Poorly designed systems are much more susceptible to cyberattacks. Weaknesses become entry points for threat actors, allowing them to exploit vulnerabilities and gain unauthorized access. One example is the use of weak encryption algorithms. This can easily lead to data breaches, compromising sensitive information, and system disruptions that hinder operations.

3.12. Security Implementation

Once security requirements are defined and the secure design is complete, it's time to translate theory into practice. This involves applying security controls to safeguard systems, data, and assets from cyber threats.

However, poor implementation can leave your organization vulnerable to attacks, like data breaches, disruption and downtime and damage to the reputation.

During this crucial phase, adhering to secure coding guidelines and code standards is essential. This helps mitigate unnecessary risks by promoting secure coding practices and minimizing the introduction of vulnerabilities. Additionally, utilizing Static Code Analysis (SCA) tools is highly recommended. These tools scan your code for known security weaknesses and bad coding practices, further strengthening your security posture.

3.13. Security Testing

With security controls implemented, the next critical step is to actively search for vulnerabilities in systems, applications, and networks. This process, like a security audit, aims to identify weaknesses before attackers can exploit them. Skipping this crucial phase can have severe consequences, some exemplified below:

- **Skipping Testing**: The notion of saving money by skipping security testing is a false economy and irresponsible. It's like neglecting to maintain your car's brakes – a potential disaster waiting to happen.
- **Lack of security testing**: Conducting security testing but not doing it thoroughly, such as omitting penetration testing (pen testing), provides a false sense of security. Pen testing simulates real-world attacker behaviour to identify vulnerabilities in systems.
- **Incomplete testing**: Gaps in the testing process can leave some areas of the system untested and vulnerable. This can be caused by incompetence or prioritizing speed over thoroughness.

3.14. Installation/Operation/Maintenance

Installation, Operation, and Maintenance (IOM) are three fundamental phases in the lifecycle of any system, from simple software applications to complex machinery or infrastructure. These phases ensure a system is set up properly, used effectively, and maintained for optimal performance throughout its lifespan.

The installation process begins when a system is ready for delivery to the client. It involves physically installing hardware components, configuring software applications, and integrating the system seamlessly with existing infrastructure. This ensures the system functions correctly within the client's environment. Once installed, the system enters the operation phase. This is where users interact with the software to complete tasks and achieve their goals. During this phase, it's crucial to have proper maintenance procedures in place. Regular maintenance helps prevent problems, ensures smooth operation, and extends the system's lifespan.

Comprehensive manuals are essential for all three IOM phases. These manuals, which can include user manuals, installation guides, and maintenance instructions, provide users and developers with the knowledge and steps necessary to successfully install, operate, and maintain the system. Proper training based on these manuals is equally important. Without it, users may struggle to set up and use the system correctly, leading to inefficiencies, wasted time, and even security vulnerabilities. Untrained users are more susceptible to phishing attacks, clicking on malicious links, or unintentionally sharing sensitive information.

Two critical security aspects can significantly impact a system's vulnerability: a lack of standard incident response and the absence of security patches. Without a defined incident response plan, organizations are likely to respond chaotically to cyberattacks. This can lead to delayed responses, extended downtime, and potentially greater damage from the security incident. Furthermore, failing to apply security patches leaves systems exposed to known exploits that attackers can easily leverage. These vulnerabilities can have serious consequences for the organization's security posture.

3.15. OTHER VULNERABILITIES

The following vulnerabilities were identified through the cybersecurity survey titled "Survey on Cybersecurity Challenges and Solutions for Space Systems" [RD-33], conducted among space sector specialists. A summary of these vulnerabilities is presented in Table 6:

Vulnerability	Example
Software bugs with security impacts	Bugs in code that lead the system to execute commands (in the ground station) and/or telecommands (onboard the satellite), opening access to malicious attacks. Hidden backdoors in application deployment.
Using of weak development process	The use of agile methodologies should be avoided in critical projects.
Read and write operations in memory	Poor memory management may cause stack overflow.
Overly complex software/system.	Poor design, resulting from neglecting proper design practices and generating code from potentially flawed sources.
Software update	Spacecraft systems allowing software updates during their lifetime could enable hackers to inject malicious code, leading to system failure, spying on flight data, or even impacting/destroying other missions.
Weak software development protection	Lack of or inadequate security in the software development environment could allow malicious actors to access key software artifacts.
Debug ports not protected	Access to target memories through unprotected debug ports.
Bad code practices	Ignoring code smells and other code rule violations identified by commercial static analysis tools.
Lack of security acceptance plan	Acceptance plans are often based on a subset of tests that may not cover security or unusual situations. Contracts can also be a vulnerability, as subcontractors might prioritize scope over security, creating gaps.
Weak secure information and deliverables flow	Documentation, code, electronic ICDs, and database contents are shared between entities using insecure communication means or through third-party providers (e.g., email, SharePoint, FTP).
Weak secure boundary parameter	Failure to define and enforce strict access controls between different components or systems within a space infrastructure, allowing unauthorized access and potential lateral movement of attackers.
Weak password policies	Using easily guessable passwords or not enforcing regular password changes can give attackers a simple entry point into space systems.
High turnover of contractors	Frequent changes in the workforce increase the risk of social engineering attacks.
Use of dynamic memory	Dynamic memory use is prohibited in space projects due to the harsh space environment, where radiation can cause bit flips, endangering the entire spacecraft.
Deserialization of untrusted data	Accepting and processing serialized data from untrusted sources without proper validation can lead to remote code execution vulnerabilities.

Vulnerability	Example
Integer overflow of wraparound	A calculation that produces a result outside the range of values an integer can represent can lead to unexpected behaviour or security vulnerabilities in space system software.
Improper monitoring in ground and space segment	Inadequate monitoring of network traffic, system logs, and security events can delay the detection of cyberattacks and allow them to cause significant damage before being addressed.
Poor management of the exchange data	Insufficient encryption or authentication of data transmitted between ground stations and spacecraft can expose sensitive information to interception or tampering.

Table 6: Vulnerabilities identify by the specialists

ANNEXES

ANNEX A. THREATS TABLE

Table 7 depicts examples of security mechanisms and mitigations used against a specific number of threats relevant for space systems as documented in [RD-8]. Mitigations for the complete list of threats presented in Section 2 will be derived and presented in a future technical note (Technical Note 05).

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 •Behaviour •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 •Continuous threat monitoring, continuous risk management •Run-time security monitoring •Auditing Software partitioning (trusted computing base) Supply chain confidence	•Secure software development methodologies	•Develop multiple, independent implementations from the same specification for higher assurance platforms

Threats	Security Mechanisms to Counter Threat	Threat Mitigations	Threat Contingencies
Unauthorized Access	•Encryption of TT&C and mission data •Authentication/authorization of commands •No use of open networks •Access control in control centre •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

Table 7: Threats and Mitigations [RD-8]

Critical software

We are CMMI Maturity Level 5 rated.

For a list of our certifications & standards
visit our website.

www.criticalsoftware.com