Instituto Superior
de Engenharia
Politécnico de Coimbra

DEPARTMENT OF SYSTEMS AND COMPUTER ENGINEERING

Cybersecurity for Space Applications

Internship Report to fulfill the Master's degree in Informatics Engineering
Specialization in Software Engineering

Author

Pedro Miguel Ferreira Sousa

Supervisor

João Cunha

Advisor in the organisation Critical Software S.A.

Nuno Pedro Silva

Coimbra, December, 2024

INSTITUTO POLITÉCNICO
DE COIMBRA

INSTITUTO SUPERIOR
DE ENGENHARIA
DE COIMBRA

ABSTRACT

Humanity, throughout history, has made significant progress in deepening our understanding of Space, both scientifically and technologically. For instance, we now communicate over vast distances thanks to satellites orbiting Earth, explore other celestial bodies by launching rovers, and even unravel the origins of the Universe using terrestrial and orbital telescopes to observe nearby and distant galaxies. It has become imperative to ensure the cybersecurity of space systems against cyber threats, protecting our way of life.

Since the Cold War era, space exploration was largely dominated by the United States and the former Soviet Union, which possessed the resources and expertise to develop and launch satellites, ensuring the utmost secrecy (security through obscurity) to guarantee safety. However, advancements in technology, especially computing and digitalization, have reduced the costs of satellite production, opening the doors of Space Exploration to new entities and increasing their vulnerability to cyberattacks. In recent years, cybersecurity has emerged as a significant concern in the space domain, impacting satellite control, mission objectives, asset integrity, and the security of communications.

Cybersecurity in space (both terrestrial and space segments) is a developing field, lacking established practices or with limited existing practices, technologies, methodologies, processes, tools, or standards, and remains vulnerable to cyberattacks such as jamming, spoofing, or social engineering attacks. Nonetheless, it has been gaining momentum due to increasing customer demands and the gradual incorporation of cybersecurity concerns into development standards. The European Space Agency, for example, is addressing cybersecurity in updates to its software space engineering standard ECSS-E-ST-40C and in software quality ECSS-Q-ST-80C.

This document details an integrated master's internship in the Space Area of Critical Software, focusing on the study of how to protect space systems against cyber threats. The internship involves researching threats specific to the Space domain and others similar (automotive, railway, and aviation), the state-of-the-art in cybersecurity, systems technologies, and proposing practices, technologies, methodologies, processes, tools, or even requirements for standards to improve the protection of space systems against threats and vulnerabilities.

Keywords: Cyberthreats; Space Cybersecurity; Space Infrastructure; Space System Security; Satellite Systems

RESUMO

A Humanidade, ao longo dos tempos, tem feito progressos significativos, no que respeita a um conhecimento mais apurado do Espaço, quer em termos científicos quer tecnológicos como por exemplo, comunicarmo-nos entre longas distâncias graças aos satélites em orbita do planeta Terra, exploração de outros corpos celestes através do lançamento de *rovers* ou até mesmo descobrir a origem do Universo usando telescópios terrestres e orbitais observando vizinhas e distantes galáxias. Torna-se, pois, determinante garantir a cibersegurança dos sistemas espaciais contra as ciberameaças, protegendo o nosso modo de vida.

Desde a era da Guerra Fria, a exploração espacial foi amplamente dominada pelos Estados Unidos e a antiga União Soviética que possuíam os recursos e "know-how" para desenvolver satélites e colocá-los em orbita, garantindo que todo esse processo fosse o mais secreto possível (segurança através da obscuridade), para garantir a segurança. No entanto, os avanços na tecnologia, especialmente na computação e digitalização, diminuíram os custos de produção dos satélites, abrindo as portas da Exploração Espacial a novas entidades, aumentando as suas vulnerabilidades a ataques cibernéticos, como consequência. Nos últimos anos, a cibersegurança surgiu como uma preocupação significativa no domínio espacial, impactando o controlo dos satélites, os objetivos da missão, a integridade dos ativos e a segurança das comunicações.

A cibersegurança no espaço (segmento terrestre e espacial) é um campo em desenvolvimento, carecendo do estabelecimento de práticas ou com práticas existentes limitadas, tecnologias, metodologias, processos, ferramentas ou normas, estando á mercê de ciberataques como *jamming*, *spoofing* ou ataques do tipo engenharia social. Não obstante, tem vindo a ganhar impulso devido às crescentes exigências dos clientes e à incorporação gradual de preocupações de cibersegurança nas normas de desenvolvimento. A Agência Espacial Europeia, por exemplo, está a abordar a cibersegurança nas atualizações da sua norma de engenharia espacial de software ECSS-E-ST-40C e também na qualidade do software ECSS-Q-ST-80C.

Este documento detalha um estágio de mestrado integrado na Área do Espaço da Critical Software, com foco no estudo de como proteger os sistemas espaciais contra as ciberameaças. O estágio envolve a pesquisa de ameaças específicas do domínio do Espaço e outros semelhantes (automóvel, ferrovia e aviação), o estado-da-arte em cibersegurança, tecnologias de sistemas e proposta de práticas, tecnologias, metodologias, processos, ferramentas ou mesmo requisitos de normas para melhorar a proteção dos sistemas espaciais contra ameaças e vulnerabilidades.

Palavras-chave: Ameaças cibernéticas; Cibersegurança Espacial; Infraestrutura Espacial; Segurança do Sistema Espacial; Sistemas de Satélite

ACKNOWLEDGMENT

I would like to express my deepest gratitude to Professor João Cunha, my academic supervisor, for his unwavering support, valuable guidance, and constructive feedback throughout this internship. His knowledge and experience were instrumental in my professional development and the success of this project.

I would also like to thank Nuno Silva, my supervisor at Critical Software S.A., for providing me with this unique opportunity for learning and growth within the SpaceForce Critical Software team. His leadership, mentorship, and trust in my abilities inspired me to overcome challenges and deliver high-quality results.

I am grateful to Critical Software S.A. and the Space Force team for welcoming and integrating me into a dynamic, innovative, and collaborative work environment. I thank all my colleagues for their camaraderie, support, and knowledge-sharing, which enriched my professional experience.

This internship has been a journey of learning and personal and professional development, which would not have been possible without everyone's support and collaboration.

Thank you.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

DEFINITIONS AND ACRONYMS

AI	Artificial Intelligence
AIP	Application Intelligence Platform
AJAX	Asynchronous JavaScript and XML
ANS	Air Navigation Services
API	Application Programming Interface
ARPANET	Advanced Research Projects Agency Network
ASH	Automated Security Helper
ASP	Active Server Pages
ASPM	Application Security Posture Management
ASST	Automated Software Security Toolkit
ASW	Amazon Web Services
ATM	Air Traffic Management
ATT	Attack
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.
ATV	Automated Transfer Vehicle
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. [1]
AUTOSAR	Automotive Open System Architecture
Availability	Ensuring timely and reliable access to and use of information. [2]
AVM	Application Vulnerability Mitigation
BBC	British Broadcasting Corporation
BSIMM	Building Security Maturity Model
BSP	Board Support Package

CAP	Composition Assurance Package
CCPA	California Consumer Privacy Act
CCRA	Common Criteria Recognition Arrangement
CCSDS	Consultative Committee for Space Data Systems
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CERT	Coordination Center of the Computer Emergency Response Team
CFML	ColdFusion Markup Language
CIA	Confidentiality, Integrity, Availability
CIP	Critical Infrastructure Protection
CISO	Chief Information Security Officer
CLC	CENELEC
CLI	Command Line Interface
CMITSE	Common Methodology for Information Technology Security Evaluation
CMS	Content Management System
CNE	Computer Network Exploitation
COBOL	Common Business Oriented Language
Code Smells	Traces in the code that indicates a deeper problem in the application or codebase.
COMP	Composite Product Package
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [3]
COTS	Commercial-of-the-shelf
CPI	Command Link Critical Program/Project Information
Critical Infrastructure	Critical infrastructure refers to the systems, facilities and assets that are vital for the functioning of society and the economy.
CSF	Cybersecurity Framework

CSMS	Comprehensive Cybersecurity Management System
CSW	Critical Software, S.A.
CTF	Capture the Flag
CUDA	Compute Unified Device Architecture
CUI	Control Unclassified Information
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, and confidentiality. [4]
DASIA	Data Systems in Aerospace
DAST	Dynamic Application Security Testing
DCS	Distributed Control System
DES	Data Encryption Standard
DOC	Document
DRD	Document Requirements Definition
DSL	Domain-specific Language
EAL	Evaluation Assurance Level
EASA	European Union Aviation Safety Agency
ECSS	European Cooperation for Space Standardization
EDR	Endpoint detection and response
ENVISAT	Environmental Satellite
EOS	Earth Observing System
ESA	European Space Agency
FAA	Federal Aviation Administration
FCA	Financial Conduct Authority
FCC	Federal Communications Commission
FHA	Functional Hazard Analysis
FIPS	Federal Information Processing Standard

FISMA	Federal Information Security Management
GCA	Global Cybersecurity Agenda
GDPR	General Data Protection Regulation
GEO	Geosynchronous Equatorial Orbit
GOTS	Government-off-the-shelf
GPS	Global Positioning System
HKTM	Housekeeping Telemetry
HSIA	Hardware-Software Interaction Analysis
HTML	Hyper Text Markup Language
I&C	Instrumentation and Control
IAC	Identification and Authentication Control
IACS	Industrial Automation and Control Systems
IAST	Interactive Application Security Testing
IBM	International Business Machine Corporation
IDE	Integrated Development Environment
IEC	International Electronic Commission
IEEE	The Institute of Electrical and Electronics Engineers
IIOT	Industrial Internet of Things
IMT	International Mobile Telecommunications
Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. [5]
ISA	International Standards on Auditing
ISBN	International Standard Book Number
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISVV	Independent Software Verification and Validation
ITU	International Telecommunication Union

JAXA	Japan Aerospace Exploration Agency
JSON	JavaScript Object Notation
JSP	Java Servlet Pages
LDAP	Lightweight Directory Access Protocol
LEO	Low Earth Orbit
MASTG	Mobile Application Security Testing Guide
MASVS	Application Security Verification Standard
MEO	Medium Earth Orbit
MISRA	Motor Industry Software Reliability Association
MOTS	Modified-off-the-shelf
MVC	Model, View, Controller
NASA	National Aeronautics and Space Administration
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NMAP	Network Map
NPR	NASA Procedural Requirements
NRB	Non-conformance Reporting Board
NTSP	NASA Technical Standards Program
NTSS	NASA Technical Standards System
OSI	Open Systems Interconnection
OSS	Open-Source Vulnerability Scanning
OT	Operational Technology
OWASP	Open Worldwide Application Security Project
PDCA	Plan-Do-Check-Act
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PNT	Position, Navigation and Timing

PPA	Protection Profile Assurance
RDF	Restricted Data Flow
REST	Representational State Transfer
SA	Standard Association
SAE	Society of Automotive Engineers
SAMM	Software Assurance Maturity Model
SAR	Security Assurance Requirement
SARIF	Static Analysis Results Interchange Format
SASDS	Security Architecture for Space Data System
SAST	Static Application Security Testing
SAT	Satellite
SBOM	Software Bill of Materials
SCA	Static Code Analysis
SCADA	Supervisory Control and Data Acquisition
SDL	Security Development Lifecycle
SEC	Securities and Exchange Commission
SEI	Software Engineering Institute
SIEM	Security information and event management
SOAR	Security orchestration, automation, and response
SOC	Security Operations Center
SPICE	Software Process Improvement and Capability Determination
SQL	Structured Query Language
SRTP	Security Risk Treatment Plan
SSA	System Safety Assessment
SSAR	Software Security Analysis Report
SSDLC	Secure Software Development Lifecycle
SSMP	Software Security Management Plan

SSPR	Space System Protection Requirement
STA	Security Target Assurance
STD	Standard
SUC	System Under Consideration
SwCA	Software Composition Analysis
TARA	Threat Analysis and Risk Assessment
Threat	A threat or cyberthreat is the possibility that a threat actor will impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals, by taking advantage of a space system's weakness, through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [6]
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.
TNR	Technical Note Report
TOE	Target of Evaluation
TRE	Timely Response to Events
TSF	Target of Evaluation Security Functionality
VMDR	Vulnerability Management, Detection and Response
Vulnerability	A weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability
WG	Working Group
XDR	Extend detection and response
XML	Extensible Markup Language
XSS	Cross-site Scripting
XXE	XML external entity injection
YAML	Yet Another Markup Language

1 INTRODUCTION

The increasing reliance on space systems for a wide range of applications, from weather forecasting to communication, has made their security paramount. While space exploration has been ongoing since the Cold War era, the rapid technological advancements, particularly in computing, have led to a surge in the number of satellites and constellations orbiting Earth. This proliferation, though beneficial in many ways, has also exposed these systems to an evolving landscape of cyber threats and vulnerabilities.

Historically, space systems relied on secrecy ("security through obscurity"), a practice that is no longer sufficient in today's interconnected world. The convergence of the physical and digital realms has made space systems susceptible to the same cyber risks that affect terrestrial critical infrastructures. This is further compounded by the rapid growth of the private space sector, where the focus on rapid development and cost-effectiveness may have inadvertently led to less emphasis on robust cybersecurity measures. Additionally, the presence of legacy systems, which are often difficult and expensive to upgrade, adds another layer of complexity to the security challenge.

With cybersecurity being a rapidly growing field and cybercrime increasingly prevalent, vulnerabilities and exploitation opportunities are everywhere, and the space domain is no exception. Whether it is the command and control of satellites, the corruption of mission objectives, the destruction of expensive assets, spying on communications, or even cyberwarfare, the threats are significant. To address this, Critical Software proposed the internship titled "Cybersecurity for Space Applications" to investigate how to protect space systems against such threats.

Critical Software is a well-known software house that works in various domains, from automotive to space. It has collaborated with NASA in the past and currently has multiple projects with ESA.

This internship was conducted as part of the curricular unit "Project / Internship / Dissertation" in the Master's program in Informatics Engineering, specialization in Software Engineering, at the Coimbra Institute of Engineering (ISEC), in cooperation with Critical Software (CSW). ISEC is committed to creating, disseminating, and advancing culture, science, and technology, providing higher education for individuals pursuing careers in engineering, and actively contributing to regional development.

The following sections will present Critical Software in more detail, outline the main objectives of the internship, highlight internship contributions, and describe the structure of this document.

1.1 Critical Software

Critical Software is a renowned software house operating in diverse domains such as aerospace, automotive, defence and security, medical devices, e-commerce, energy, space, government, financial services, and telecommunications. With 26 years of experience delivering high-quality products, CSW is recognized for its excellence, evidenced by numerous quality certifications including ISO 27001, EN 9100, ISO 9001, CMMI-DEV ML5, and NATO AQAP 2110/2210. The company also boasts an impressive client satisfaction score of 8.95 out of 10 over the past 5 years (2019-2023), based on 309 projects.

Contributing to its ongoing success, the organization is continuously growing, with 10 offices across five countries (Portugal, United Kingdom, Germany, Brazil, Mozambique, and Angola) and a workforce exceeding 1,000 employees.

To effectively manage its workforce, Critical Software is structured into three divisions: Automotive, Railway, and Medical Devices (ARMS), Digital Engineering Services (DES), and Smart & Reliable Systems (SRS). Within each division, work is organized into platoons. This internship took place within the SRS division, specifically in the Space Force platoon. This platoon is responsible for all space projects and played a crucial role in the successful launch of Ariane 6.

1.2 Internship Objectives

The objectives of this internship are as follows:

1. **Collect and Analyse State-of-the-Art Data**: Gather comprehensive information on cybersecurity threats, vulnerabilities, and solutions from existing studies, papers, and industry sources, with a specific focus on the space sector.
2. **Engage with Key Stakeholders**: Establish contact with teams involved in space system and software development and validation. Distribute a targeted survey to relevant stakeholders to gather valuable insights and data.
3. **Propose Mitigations**: Develop proposals for processes, activities, and tools to address identified threats and vulnerabilities, incorporating studied best practices.
4. **Develop Recommendations and Standards**: Based on the collected data and analysis, formulate a list of recommendations (requirements) for the European Cooperation for Space Standardization (ECSS), with a specific focus on the space software engineering and product assurance standards (ECSS-E-ST-40C and ECSS-Q-ST-80C), as these are currently being reviewed and have elements of cybersecurity being added.
5. **Produce Scientific Publications**: Prepare and submit one or two scientific papers: one detailing the literature review, state-of-the-art, and threats/vulnerabilities study for space systems, and another outlining the

proposed solutions, standardization changes, and potential tools for development.

6. **Disseminate Findings**: Share a summary report with identified stakeholders, including key contacts at ESA, NASA, and other relevant industries, to foster collaboration and raise awareness of the research findings.

Based on these objectives, **four research questions** were proposed:

- **RQ-01**: What is the current state-of-the-art in space cybersecurity?
- **RQ-02**: What are the most relevant threats and vulnerabilities in cybersecurity applications for space systems?
- **RQ-03**: What mitigation strategies can be proposed to address identified threats and vulnerabilities?
- **RQ-04**: What improvements can be made to existing space standards to cover cybersecurity risks, threats, and vulnerabilities?

1.3 Work Methodology

The process used to complete the internship objectives can be broken down into the following steps (as shown in Figure 1):

Step 1: Literature Review

The first step was to conduct a thorough literature review and analyse scientific papers related to cybersecurity in the space sector. Chapter 2 will focus on the results of that analysis and present the state of the art.

Activities:

- Identify relevant literature and scientific papers.
- Compile a reference list of all the sources.
- Extract the relevant information from the selected literature.

Step 2: Threats and Vulnerabilities Identification

The second step involved identifying the main threats and vulnerabilities in the space sector. This included analysing the data gathered in the literature review and build a cybersecurity survey (Step 3) to capture the perspective of the specialist in the Space sector. Chapter 4 delves into the threats and vulnerabilities identified in more detailed.

Activities:

- Analyse the data gathered in the literature review and in cybersecurity survey.
- Identify the main threats and vulnerabilities in the space sector.
- Consider also standards, processes, tools, best practices, lessons learned, etc.
- Categorize the identified threats and vulnerabilities.

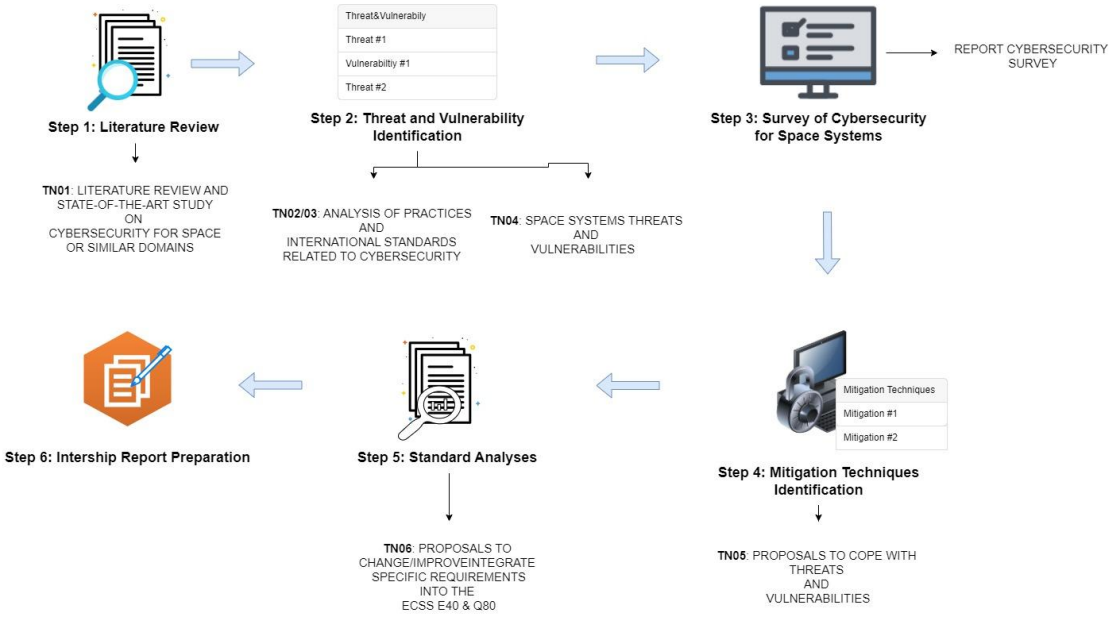


Figure 1: Work process

Step 3: Survey of Cybersecurity for Space Systems

The third step was conducted in parallel with step 2 and involved creating, sharing and collecting expert's inputs from a "Cybersecurity for Space Systems" survey. The collected survey data intended to confirm and complement the data gather in literature review (Steps 1 and 2) but in a closer and more practical way to the space systems domain.

Step 4: Mitigation Techniques Identification

The fourth step involves finding mitigation techniques and strategies to address the identified threats and vulnerabilities. This includes analysing the effectiveness of existing mitigation techniques, as well as the answers from the cybersecurity survey, and proposing innovative solutions to counter emerging threats. Chapter 5 presents the results of this step by providing several mitigations for threats and vulnerabilities.

Activities:

- Identify existing mitigation techniques and strategies.
- Consider also standards, processes, tools, best practices, lessons learned, etc.
- Analyse the effectiveness of existing mitigation techniques.
- Analyse the mitigation measures mentioned in the cybersecurity survey.
- Propose innovative solutions to counter emerging threats.

Step 5: Standard Analyses

The fifth step involves analysing ECSS E40 [7] and Q80 [8] standards to identify cybersecurity gaps and formulating cybersecurity requirements based on the

information gathered from the literature and the responses given by space engineers in the cybersecurity survey. Chapter 5 presents a table of proposed requirements to close the gaps identified in the analysis.

Activity:

- Conduct a comprehensive analysis of ECSS E40 and Q80 to identify existing cybersecurity gaps and potential areas for improvement.
- Utilize the information gathered from the literature review and cybersecurity survey responses to inform the analysis and identify specific cybersecurity requirements.
- Document the findings and recommendations in a detailed report, outlining the identified gaps, proposed solutions, and rationale for the proposed cybersecurity requirements.

Step 6: Internship Report Preparation

The final step involved compiling all technical notes (see Section 1.4) produced and organizing them into a document. The internship report is divided into separate sections to accommodate each technical note.

Activities:

- Compile the state-of-the-art, survey report, identified threats, vulnerabilities, and mitigation techniques and proposals to improve the ECSS standards into a document.
- Divide the document into separate sections for respective technical note.

1.4 Contributions

This internship has made contributions to the field of space sector cybersecurity. The following are some of the key outcomes:

Technical Notes

The internship resulted in a series of technical notes, establishing a centralized repository of cybersecurity knowledge that showcases the current state of cybersecurity in the space sector.

- **TN01 - State of the Art** [9]: Focus on the state-of-the-art of the cybersecurity in Space sector, mentioning the current landscape of the Space Systems and the cybersecurity related processes and tools.
- **TN02/03 - Analysis of Practices and International Standards** [10]: A focus on the analyses of cybersecurity standards, generic and sector-specific (Space, automotive, railway and aviation).

- **TN04 - Space System Threats and Vulnerabilities** [11]: A focus on Space Sector threats and vulnerabilities.
- **TN05 - Proposals to Cope with Threats and Vulnerabilities** [12]: Proposed Mitigation Strategies for Space System Threats and Vulnerabilities
- **TN06 - Proposal to Change/Improve/Integrate Specific Requirements into the ECSS E40 & Q80** [13]: Analyses of the European software space engineering standards to identify cybersecurity gaps and suggests specific requirements to improve the cybersecurity capabilities of space systems based on literature review and survey responses.
- **Survey Report** [14]: Report on analysis of expert responses on Space Sector Cybersecurity survey.

DASIA Conference

A comprehensive paper titled "Engineering and Assessing Cybersecurity for Space Systems" [15] was developed based on the cybersecurity survey findings. It was presented at the Eurospace DASIA 2024 conference in Croatia in May, the preeminent industrial conference in the domain of European space data. This paper provides valuable insights into the state of cybersecurity in the space sector, threats, vulnerabilities, and potential mitigation strategies. It can serve as a valuable resource for researchers, industry professionals, and policymakers.

European Commission Call

The internship's findings and recommendations have been used as support and experience material to the C-SARTIFY European proposal for the European Commission Call HORIZON-CL3-2024-CS-01. This proposal focuses on approaches and tools for security in software and hardware development and assessment, aiming to contribute to the advancement of space sector cybersecurity. Critical Software, S.A. is one of the stakeholders involved in this proposal.

1.5 Document Structure

The internship report comprises six sections and three annexes:

- **Section 1** (Introduction) introduces this document.
- **Section 2** presents the State-of-the-Art in cybersecurity for space and similar domains.
- **Section 3** presents the cybersecurity survey conducted and its results.
- **Section 4** presents space systems threats and vulnerabilities.
- **Section 5** proposes solutions to improve cybersecurity in space sector.
- **Section 6** provides the conclusions and recommendations for future work.

- **Annex A** presents the technical notes, survey report and DASIA paper produced in this internship and serve as supporting material for the internship final report.
- **Annex B** presents mitigation strategies for threat and vulnerabilities identified in literature and by the experts via survey.
- **Annex C** presents the survey questions and the LinkedIn message use to gather more participants**.**

2 CYBERSECURITY FOR SPACE OR SIMILAR DOMAINS: STATE-OF-THE-ART

Early space systems relied heavily on analogue technology, even onboard spacecrafts. These systems were primarily mechanical and lacked the extensive digital infrastructure that now permeates modern space assets. As a result, cybersecurity concerns were not a major focus in the early days of space exploration. Security for the technology launched into space relied on tightly controlled access to its documentation and the highly complexity of the systems themselves, the so called "security by obscurity".

As satellites shifted towards digital and software-driven systems, relying on "security by obscurity" became unfeasible. This transition offered numerous benefits like heightened productivity, faster execution of processes, and enhanced product quality. Yet, it also introduced notable vulnerabilities, given that these interconnected systems were now accessible via the internet, leaving them exposed to potential threats from the public. The lack of cybersecurity standards and regulations further exacerbated the security problems of space systems.

This chapter delves into the existing literature on cybersecurity in space and related domains, examining the latest research, trends, and best practices to provide a comprehensive overview of the state-of-the-art in space sector cybersecurity required to complete the first objective of the internship as stated in Section 1.2.

2.1 State-of-the-art

The limited use, insufficient standards requirements or lack of industry-specific cybersecurity standards and regulations are major challenges to securing space systems. But some recent events, such the attack on ViaSat [16] by Russia, in the eve of the start of the war in Ukraine, were a wake-up call to all cybersecurity community and space sector.

The following subsections will introduce the main literature review, standard/frameworks and regulations used in various domains including the space industry.

2.1.1 Study of Existing Literature

This section introduces the existing literature use to gather information about cybersecurity in space applications.

1. **Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight, from Pavur, James; Martinovic, Ivan, 2022** [17]

In the face of rapid advancements in space technology, ensuring the security of space systems has become a paramount concern. This research delves into the critical aspects of satellite cybersecurity, examining the evolving landscape of the space industry, the historical neglect of space technology by the cybersecurity community, and the diverse threat models that pose risks to these vital systems.

2. **Cyber security in New Space, from Manulis, M; Bridges, P, C; Harrison, R; Sekar, V; Davis, A, 2020** [18]

The democratization of space has led to a surge in satellite deployments, offering essential services like communications, navigation, and Earth observation. However, this expansion has also increased the susceptibility of space systems to cyberattacks. This research delves into emerging security threats, challenges, and technological advancements shaping the space industry.

3. **Cybersecurity Principles for Space Systems, from Falco, Gregory, 2018** [19]

The space sector has experienced a surge in cyberattacks, targeting everything from communication satellites to ground control systems. This research examines the underlying causes of these vulnerabilities, including the complex supply chain, the use of commercial-off-the shelf software, and the lack of standardized security practices. By analysing high-profile cyberattacks and evaluating existing mitigation techniques, this study aims to identify critical gaps in the cybersecurity posture of the space sector and proposes a comprehensive framework for enhancing space system security.

4. **Cyber-space and its Menaces, from Sujeetha, R.; Das, Himanshu; Dhelawat, Tanish; Tanveer, Mohammad, 2019** [20]

Cybersecurity threats continue to evolve, posing significant risks to organizations of all sizes. From sophisticated ransomware attacks to data breaches that compromise sensitive information, the threat landscape is constantly changing. This research explores a variety of cyber threats, including SQL injection, phishing, and social engineering attacks. By understanding these threats, organizations can develop effective security strategies to protect their critical assets. This paper will discuss a range of preventive measures, such as implementing least privilege model of permissions, educating employees about cybersecurity best practices and more.

5. **Securing International Space Station Against Recent Cyber Threats, from Pazouki, Samaneh; Aydeger, Abdullah, 2023** [21]

The International Space Station (ISS) is a complex system that relies on a variety of interconnected subsystems. While the ISS has made significant strides in terms of security, it remains vulnerable to cyberattacks. This research aims to identify and model potential cyber threats to the ISS, with a particular focus on attacks targeting

the station's power system. By injecting false data into the power management system, adversaries could deplete batteries, overload circuits, and potentially cause a system-wide failure. Understanding these threats is essential for developing effective countermeasures and ensuring the continued operation of this critical asset.

6. **Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk assessment, from Elmarady, Ahmed; Rahouma, Kamel, 2021** [22]

Given the paramount importance of civil aviation safety, cybersecurity within the aviation sector cannot be ignored. As air navigation facilities transition from analogue to space-based digital systems, the urgency of cybersecurity has grown significantly. This research introduces cybersecurity risk assessment methodologies applicable to both traditional and contemporary critical infrastructures, encompassing ground-to-air communications, radio navigation aids, air surveillance, and comprehensive system-wide information management.

7. **Understanding and Mitigating Adversary Threats in Space Cybersecurity, from Thangavel, Kathiravan; Plotnek, Jordan; Gardi, Alessandro; Sabatini, Roberto, 2022** [23]

Satellite technologies support both civilian and military applications, providing critical services such as communications, navigation, and surveillance that impact economic, social, and environmental activities. This research focuses on cyber threats and vulnerabilities across the entire space architecture:

- Identifying applicable cyber threat mechanisms.
- Analysing threat actors.
- Assessing the implications for the commercial space sector.

8. **A Security Risk Taxonomy for Commercial Space Missions, from Falco, Gregory; Boschetti, Nicolò, 2021** [24]

This research focuses on the security risks and their associated incidents for the commercial space systems that can lead to mission failures. The authors propose a taxonomy of security risks based on an extensive database of 2000 space security incidents. This taxonomy consists of commercial space risk categories including physical (kinetic, non-kinetic), digital (electromagnetic, cyber), organizational (production, management) and regulatory (legal, political).

9. **Space Cybersecurity Lessons Learned from The ViaSat Cyberattack, from Boschetti, Nicolò; Gordon, Nathaniel; Falco, Gregory, 2022** [25]

The ViaSat satellite communication system used by the Ukrainian military suffered a cyberattack in the hours prior to the Russian invasion, compromising the entire Ukrainian intelligence infrastructure. This research explores how the attack occurred, presenting technical and organizational lessons demonstrated by the attack and its objectives within the conflict.

10. **Security challenges when space merges with cyberspace, from Varadharajan, Vijay; Suri, Neeraj, 2023** [26]

With the democratization of space, the threat landscape in the space sector has significantly increased, making it more attractive to threat actors. This research explores the current threat landscape of space infrastructures and security challenges, identifying key issues that need to be addressed in the formulation of cybersecurity solutions for space. Additionally, it provides recommendations for developing a policy framework for space security.

2.1.2 Standards and Frameworks

The space sector has neglected cybersecurity issues for too long, resulting in a lack of sector-specific cybersecurity focused standards. However, progress is being made to update current standards to address cybersecurity concerns. For example, the European Space Agency (ESA) is revising its ECSS standards, which are focused on the Space sector, specifically the space software engineering standard E40 [7] and product assurance Q80 [8]. Similarly, the United States has a long-standing focus on cybersecurity, particularly through NASA's Technical Standards Program (NTSP) [27].

Beyond national organizations, the Consultative Committee for Space Data Systems (CCSDS), comprising leading space communication experts from over 25 nations, is responsible for developing standards in space communication and data handling [28].

Recently, in 2023, the Institute of Electrical and Electronics Engineers (IEEE) established a dedicated working group specifically focused on the development of a space-based set of cybersecurity standards [29]. This group includes the participation of renowned American inventor and researcher in the field, Dr. Gregory Falco [30].

Since the revisions and creation of standards take a long time, to solve the gap some generic standards can be leveraged for the sector. These include the ISO 27000 family [31] from the International Organization for Standardization (ISO) [32] and standards from the National Institute of Standards and Technology (NIST) [33] in the United States. Table 1 presents a summarized version of examples of generic cybersecurity standards that can be applied to the Space sector, those can be explored in more detail in the technical note titled "Analysis of Practices and International Standards" listed in the Annex A.

Table 2 presents the actual space industry-specific standards developed by NASA, ECSS, and ISO, some of which have a specific focus on cybersecurity while others include references to it. These standards can be explored in more detail in the technical note titled "Analysis of Practices and International Standards" listed in the Annex A.

Table 1: Applicable Non-Space Cybersecurity Standards/Frameworks

Domain	Standard	Description
Cryptography	FIPS 140	The standard "Security Requirements for Cryptographic Modules" purpose is to outline the security criteria that must be met by a cryptographic module employed in a security system.
Security Categorization	FIPS 200	FIPS 200 outlines the minimum-security requirements for information and information systems.
Information Security	NIST SP 800-53	The purpose of the SP 800-53 is to enhance cybersecurity practices and protect sensitive information by providing a security and privacy controls for information systems and organizations.
Information Security	NIST SP 800-171	This standard concentrates on safeguarding information confidentiality shared between the federal government and its external service providers (e.g., financial, web, electronic mail, healthcare) as well as educational institutions such as colleges and universities, by the recommendation of security requirements.
Information security / Evaluation of IT security	ISO/IEC 15408	ISO/IEC 15408, commonly known as the Common Criteria (CC), is an international standard consisting of five parts, developed to provide a framework for evaluating and certifying the security features of information technology products.
Information security / Evaluation of IT security	ISO/IEC 18045	This standard is responsible to support the evaluation of the ISO/IEC 15408 series, by providing the minimum actions to be performed by an evaluator.
Automotive	ISO/IEC 21434	ISO/IEC 21434 provides a comprehensive set of requirements for cybersecurity risk management throughout the lifecycle of electrical and electronic (E/E) systems in road vehicles, including their components and interfaces, from the initial concept stage to decommissioning.
Information security	ISO/SAE 27000 family	The ISO/IEC 27000 family of standards is a set of international standards for information security management systems (ISMS).
Industrial automation and control systems	ISA/IEC 62443	Cybersecurity standard for industrial automation and control systems (IACS), provides a comprehensive set of requirements and guidance that can help organizations to protect their systems from cyberattacks.
Power plant I&C programmable digital systems	IEC 62645	This standard is used by the nuclear sector with the premise of establishing cybersecurity requirements needed to prevent and/or mitigate the impact of a cyber-attack against the digital Instrumentation and Control systems.

2.1.3 Regulations

In addition to the lack of industry-specific cybersecurity standards, regulatory frameworks are also lacking and pose a more significant challenge to overcome. Regulating the space sector presents difficulties due to the fragmented regulatory landscape, which can hinder swift and efficient regulation of companies. This complexity contrasts starkly with the rapid pace of technological innovation in the space industry, as evidenced by the assessment done in the U.S. Space Policy and Law [34]:

- **Outdated Regulatory Frameworks**: Existing policies are outdated and have not adapted to the changing commercial space landscape.

- **Need for Agile Licensing Process**: Current licensing processes are overly complex and need to be streamlined for greater agility.

Table 2: Space Industry Specific Standards dealing with or mentioning cybersecurity

Domain	Standard	Description
Space System Protection	NASA-STD-1006A	Establishes protection requirements across the agency, ensuring that all missions, programs and projects are resilient to cyber threats.
Space Software Assurance and Safety	NASA-STD-8739.8B	Defines requirements for implementing a systematic approach to independent assurance, safety, verification, and validation for software created, acquired, provided, used, or maintained by or for NASA.
Space Software Engineering	ECSS-E-ST-40C	Assists stakeholders in formulating their software requirements by leveraging the ECSS-E-ST-40C framework, which combines methods and requirements from other branches of ECSS.
Space System Software Product Assurance	ECSS-Q-ST-80C	Through the Q-80 standard, users leverage a set of software product assurance requirements for developing and maintaining the software component of firmware in space systems, including space, launch, and ground segments.
Security Architecture for Space Data Systems	ISO 20214	Security Architecture for Space Data Systems (SASDS), provides a high-level system engineering reference specifically tailored to securing space systems.

Overall, the space industry requires regulations that are adaptable, efficient, and foster innovation while ensuring safety and security. There is a need to strike a balance between encouraging a thriving commercial space economy and establishing robust regulatory frameworks.

Table 3 presents a list of some regulatory entities that regulate specific domains.

Table 3: Regulatory Entities from Other Domains

Domain	Name	Description
Telecommu-nications	Federal Communications Commission (FCC)	Regulates interstate and international telecommunications by providing licenses, establishing rules for broadcasters, fostering competition, and collaborates with industry and government agencies to develop best practices and guidelines for cybersecurity [35].
	International Telecommunication Union (ITU)	A specialized agency of the United Nations that coordinates global telecommunication regulations and policies. Global Cybersecurity Agenda is one of the contributions to cybersecurity, promoting international cooperation on cybersecurity and providing a framework for addressing global cybersecurity challenges [36].
Aviation	Federal Aviation Administration (FAA)	Oversees all aspects of civil aviation in the United States, including airworthiness certification, air traffic control, safety, and cybersecurity regulations. Such example is recently FAA proposed new rules to standardize its criteria for addressing cybersecurity threats for transport category airplanes, engines, and propellers [37].
	European Union Aviation Safety Agency (EASA)	Ensures a high level of uniform safety within civil aviation across the European Union. Its contribution to cybersecurity can be reflected by the Commission Delegated Regulation (EU) 2022/1645, provides rules for managing information security risks with a potential impact on aviation safety [38].

Domain	Name	Description
Finance	Securities and Exchange Commission (SEC)	Protects investors, maintains fair markets, and facilitates capital formation in the United States. While it doesn't directly set technical standards, it contributes to cybersecurity by implementing rules such as those requiring cybersecurity risk management and mandating that investment advisers and funds adopt and implement written cybersecurity policies and procedures [39].
	Financial Conduct Authority (FCA)	Regulates the financial services industry in the United Kingdom to protect consumers and promote financial stability. It also contributes to cybersecurity by regularly publishing guidance and reports on cybersecurity, providing best practices and expectations for firms [40].
Data Privacy	General Data Protection Regulation (GDPR)	Regulates how personal data is collected, used, and stored within the European Union.
	California Consumer Privacy Act (CCPA)	Grants California residents certain rights regarding the access, deletion, and sale of their personal information.

2.2 Current Landscape of Space Systems

With digitization came the emergence of various protocols facilitating communication between network nodes. Each producer and operator of control systems had their own protocols, ensuring what they believed to be sufficiently secure. The lack of cybersecurity standards and regulations further exacerbated the lack of security of space systems.

The following sections explore space systems architecture as a critical infrastructure, the lack of imposing cybersecurity standards and regulations, complex supply chains, resource constraints, the use of Commercial Off-the-Shelf (COTS) technology, and the need for a specialized workforce and rigid penalties.

2.2.1 Space Architecture

The operations of every industry sector are underpinned, to varying degrees, by space systems. Whether it is telecommunications, navigation, weather forecasting, military endeavours, or other industries, their infrastructures are considered crucial to both society and the nation. Recognizing their significance, substantial investments in their cybersecurity are essential to prevent any potential disruptions.

Figure 2 depicts a simplified architecture of a space system. Each component within it is considered a potential target for an attack, and they are generally designed, manufactured, operated, and supported by different entities (supply chain vulnerabilities). The fact that sometimes each component has its own cybersecurity strategy means that not all threat intelligence is shared among the different interconnected components and therefore there is an increased risk that one of these components can impact the whole space system.

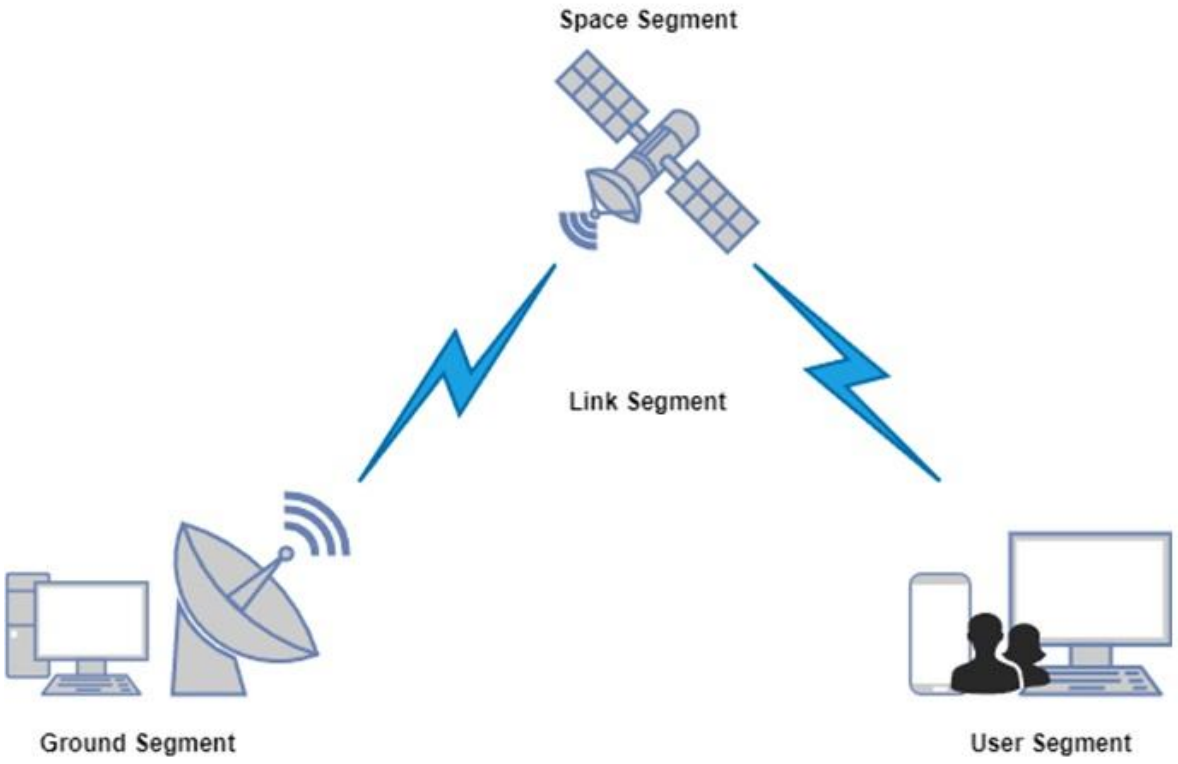


Figure 2: Common space system architecture

The Space Segment is the physical spacecraft itself, orbiting Earth or venturing further out. It houses the dedicated equipment for the mission's purpose, called the payload. This payload can range from scientific instruments like telescopes to communication antennas for relay satellites. Onboard computers process information, control the spacecraft's operations, and enable communication with the ground segment.

The Ground Segment encompasses all the infrastructure needed to communicate with and control the spacecraft. Ground stations act as communication hubs, exchanging data with the spacecraft through commands (telecommands) and receiving data transmissions (telemetries). Mission control centres monitor the spacecraft's health and location, analyse the received data, and send commands to control its operations. Launch facilities, where the spacecraft is prepared and launched into orbit, can also be considered part of this segment.

The Link Segment acts as a bridge between the ground and the space segment, and between the user and the space segments. It encompasses the methods used to transmit information between them, primarily relying on communication channels that utilize radio waves of specific frequencies. Factors like distance and data transmission rates influence the chosen frequencies. Tracking systems, often employing radar or optical telescopes, pinpoint the spacecraft's location and trajectory in orbit, allowing for accurate communication and mission planning.

The User Segment comprises the entities or individuals who ultimately benefit from the data or services provided by the space system. These users can include

universities or researchers studying climate change who utilize data from Earth observation satellites. Similarly, users can rely on GPS technology to receive precise location information and use satellites to communicate with others.

2.2.2 Critical Infrastructure of Space

The immense destructive potential of a cyberattack on Space Systems, such as the ability to wipe out an entire network of satellites, has become an appealing tactic for adversaries, especially during times of war. This was evident in the conflict between Russia and Ukraine, where there was a growing focus on developing and exploiting those capabilities.

Until recently, cybersecurity efforts for the space sector primarily focused on its infrastructure (ground segment), considered the most critical and vulnerable of all segments. However, it is crucial to consider all segments as critical infrastructure, especially the space segment, which has been more neglected. An attack on the space sector can have a snowball effect, disrupting or destroying critical infrastructure in other sectors, triggering severe negative economic and social impacts worldwide [41].

An attack on one critical infrastructure has impacts on other critical infrastructures. Currently the USA and Europe are considering designating space-based assets as a critical infrastructure. This is crucial because Space sector, not only interacts with individuals but mainly with business, military and other critical infrastructures [42] [43].

2.2.3 The Necessity of Strong Regulations and Standards Enforcement

It is recommended that a governing entity regulates the entire space industry to enforce higher standards for quality and security. This is the only way to prevent devastating consequences such as substantial financial losses, reputational damage, and even potential loss of life.

Consider the aviation industry, where the FAA in the United States and EASA in Europe regulate all aspects of civil aviation. This includes certifying repair shops, aircrews, and mechanics, while also ensuring organizational compliance with various standards, especially those related to cybersecurity and best practices. This comprehensive approach aims to protect aircraft, traffic control systems, and other critical infrastructures.

Without an entity enforcing compliance with standards, organizations in the space industry might adopt different cybersecurity strategies, based on their budget, expertise, and risk perception. This might lead to the existence of vulnerabilities across the entire ecosystem. Moreover, the lack of a common baseline for secure design and operation makes identifying and addressing vulnerabilities in space systems much more complex. Finally, the absence of dedicated space security standards can lead to the continued use of outdated security protocols and

technologies, leaving systems susceptible to known attacks and potentially disrupting critical services, causing widespread economic damage, and societal chaos.

2.2.4 Complex Supply Chain

The space system comprises multiple components, and the space program is structured with a multi-layer contract. Before reaching the hands of the customer, the lower tier companies (subcontractors) specialized in technology, manufacture their products, which are then sent to the prime contractor who is responsible to manage, ensuring the procurement and integrate all systems components. This complexity in the supply chain not only pertains to physical aspects but also encompasses cybersecurity considerations. For example, the European space industrial supply chain is made up of the big four (Airbus, Thales, Leonardo and Safran) and other smaller groups such as Kongsberg, Dassault, or RUAG. In total, the supply chain is comprised of more than 50000 people [44]. This situation carries a potential risk due to the involvement of multiple companies and individuals. Information about the components might be vulnerable to interception by hackers through methods such as phishing attacks or other cyber threats. By analysing these components and pinpointing their vulnerabilities, a hacker could potentially compromise all system upon integration of the component.

Figure 3 depicts the intricacies of the risk and cybersecurity responsibilities for a sample satellite project.

The reading of the Figure 3 is as follows: **company A** gives green light to develop a new satellite to the **company B (prime contractor),** responsible for the cybersecurity of the satellite. To acquire the necessary components **company B** subcontracts **companies C, D** and **E** who have their own responsibilities in cybersecurity. **Company B** assembles all the components and gives the final product to the client.

Then the client (**company A**) contracts another company (**company F**) to manage the operations of the satellite, who then assumes all the responsibilities about cybersecurity.

To put the satellite in space, **company F** contracts **company G** responsible for that purpose and as well the responsibility of cybersecurity during launch, but normally that responsibility is transferred to an insurance provider (**company H**).

When the satellite is in orbit and is ready to fulfil the mission purpose, the responsibility of cybersecurity for the operation shifts back to the **company F**.

Given a company's core focus on profitability, the client (**company A**) aims to optimize the satellite's utility. This involves maximizing bandwidth and processing capabilities for other companies like **I, J**, and **K**, who share responsibility for cybersecurity alongside their utilization of the satellite's services [19].

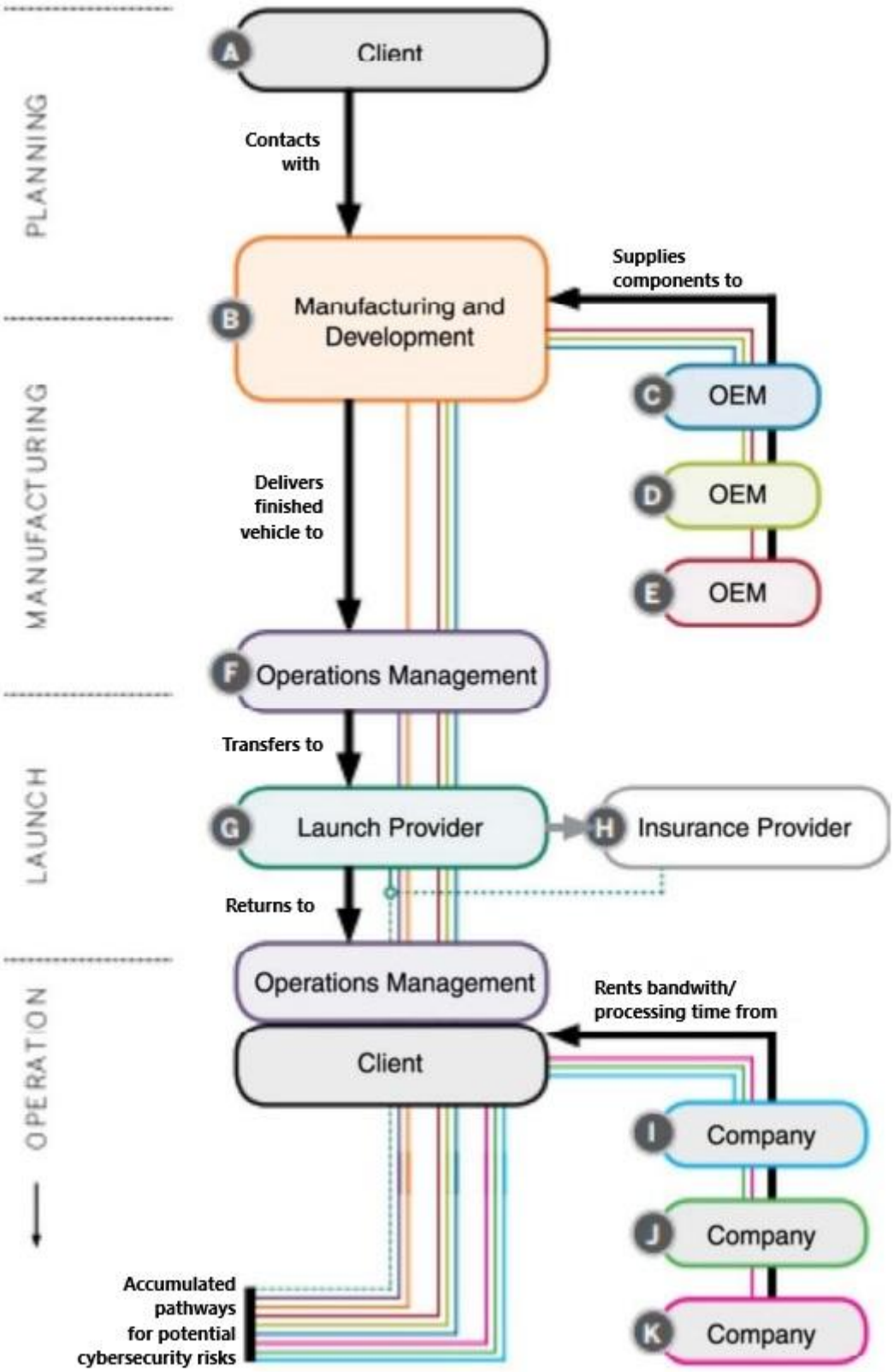


Figure 3: Cybersecurity responsibility landscape [19]

2.2.5 Resource Constraints

Securing satellites presents a unique challenge due to limited power, environment, memory, and other constraints. Demanding processing power for robust cybersecurity measures can significantly impact a satellite's ability to perform its mission and maintain its orbit. This includes unplanned manoeuvres to avoid debris or other satellites, which further strain the power budget.

Satellite energy management prioritizes survivability, often directing power to critical components during emergencies. Consequently, many satellite communication protocols are designed to be lightweight, sacrificing some security features like stronger encryption algorithms, for faster transmission speeds and lower power consumption, as depicted in Figure 4. However, the optimal balance between performance and security depends on the specific mission objectives.

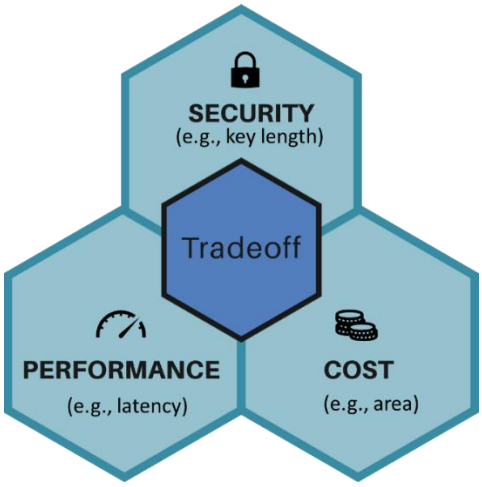


Figure 4: Trade-off between Security, Performance and Cost Dilemma [45]

Limited budgets within companies can significantly impact their cybersecurity posture. This often leads to the prioritization of certain measures over others, potentially leaving vulnerabilities unaddressed. Furthermore, resource constraints can complicate compliance with industry-specific regulations, such as budget limitations for training and technology investments, making it challenging for companies to navigate and adhere to these standards.

Addressing one of these challenges, NIST (National Institute of Standards and Technology) launched a lightweight cryptography competition in 2018 [45]. Aiming to address the needs of resource-constrained environments, the competition solicited submissions for new, more efficient cryptographic algorithms. With participation from 25 countries and over 50 submissions, the competition spurred significant innovation in this field.

The influx of innovative submissions has a wider impact than simply selecting a new standard. These advancements benefit not only resource-constrained environments like satellites and internet-of-things (IoT) devices, but also hold the potential to

improve the overall efficiency and security of cryptographic algorithms across the board.

2.2.6 Commercial-Off-The-Shelf Software and Cubesats

Throughout much of its history, only nations boasting robust financial resources and advanced technology could develop satellites equipped with intricate systems capable of implementing stringent security protocols. However, in the past decade, the space sector has witnessed a staggering total investment of 177.7 billion U.S. dollars distributed among 1,343 distinct companies. Predominantly, the United States and China stand as the primary contributors, accounting for 75% of this cumulative investment [46].

This substantial investment has facilitated the advancement of new technologies and the emergence of specialized technology companies, fostering the development of Commercial-off-the-Shelf (COTS) solutions within the space industry.

The commercial-off-the-shelf products brought with them some advantages mainly to the smaller companies in the sector, which are:

- Acquisition of COTS Software is cheaper.
- Easy implementation.
- Reviews of the product are online for everyone to see.

But also introduce some disadvantages in the form of security vulnerabilities:

- Several individuals contribute to the code behind open-source technology, raising the potential for the insertion of backdoors or vulnerabilities into the software.
- Scalability and security aspects are the responsibility of the COTS manufacturers.

COTS software sees the most use among CubeSats, type of miniature satellite measuring 10cm x 10cm x 10cm, due to their low construction cost and launch services, typically costing around 100,000 U.S dollars [47]. However, employing Commercial Off-The-Shelf (COTS) components in these small satellites could expand vulnerability points, posing risks to both military and commercial assets. As per the world´s largest database of nanosatellites [48], the last update facts as of May 31, 2024, 2396 CubeSats had been launched, with an anticipated launch of 2080 more by 2027.

2.2.7 Specialized Workforce and Rigid Penalties

Critical positions within a company, especially those related with information security, require qualified individuals. Certain entity like the Securities and Exchange Commission (SEC) have the objective to:

- Providing training on cybersecurity to ensure that personnel can effectively manage and safeguard sensitive information.
- Investigating whether companies comply with established cybersecurity standards and best practices.

The SolarWinds incident of 2020, where a Chief Information Security Officer (CISO) oversaw inadequate security measures and misled the public, led to the company becoming a target of a cyberattack, resulting in a breach of their servers. [41]. This highlights the importance of both thorough personnel training and strong accountability.

To ensure effective information security, there should be a combined approach: **robust training programs** alongside **substantial consequences** for those who fail to fulfil their cybersecurity responsibilities.

2.3 Current Cybersecurity Related Processes and Tools

Cybersecurity is critical for guaranteeing the protection of systems, networks, and data. Organizations employ various strategies to identify, prevent, and respond to cyber threats. The following subsections explore some of the essential tools that form the backbone of a robust cybersecurity posture, from firewalls and encryption to cutting-edge threat detection systems.

2.3.1 Processes

Cybersecurity related processes are essential steps and practices that cybersecurity analysts implement to protect systems, networks, and data from cyber threats. Processes help prevent and defend against unauthorized access, attacks, and breaches. They follow a set of stages that are intertwined with each other [49]:

- **Identify the Assets** – identify the assets that need to be protected against cyber threats.
- **Protect the Assets** – implement measures to safeguard the previously identified assets. On the technical side, cybersecurity analysts will recommend appropriate VPNs, encryption algorithms, and anti-malware solutions, among others. On the organizational side, employee awareness training should be employed.
- **Monitor System** – with the protection means implemented on the assets, a proactive attitude must be taken to monitor and test the system to see if there are vulnerabilities that can be favour to hackers.
- **Respond to Incidents** – despite the best efforts to protect systems, a cybersecurity incident response plan is essential in case of a breach. It

contains a series of actions to be implemented to mitigate the effects of the cyber-attack.

- **Recovery** – in the worst-case scenario of sensitive information leaks or operational disruptions, having backups and a recovery plan in place is crucial.

Table 4 presents some examples the space industry uses in protecting their projects.

Table 4: Cybersecurity Processes

Processes	Description	Examples
Risk Management	Manage the risk of a given threat by determining the probability (vulnerability **vs** threat intent **vs** threat capability) of a cyber-attack target the three principles of cybersecurity. The next step is to calculate the technical, economic, and social impact of each attack and design a strategy to reduce the risk to an acceptable level, based on a cost-benefit analysis or feasibility assessment [23]	NIST Cybersecurity Framework Risk Management Framework ISO/IEC 27001
Access Management	Focuses on controlling a monitoring access to data, resources, and systems within an organization through a series of key steps [50]: **Authentication** – verifying the identity of a user, through a username and password or more modern methods like biometrics or multi-factor authentication. **Authorization** – a given resource or information a user is authorized to access, based by role, permissions, and access levels. **Access Control** – management of granting or denying access to a given resource or information considering the user´s authorization. There are three mechanism and include control lists, role-based and attribute-based access controls. **User Management** – creating or deleting user accounts and modifying by managing attributes such roles, permissions, and access level. Policies for password management also take place in the user management. **Preventing Unauthorized Access** – preventing access to sensitive resources or information by implementing multi-factor authentication, physical security measures, monitoring user access, and conduct analysis.	IBM Identity and Access Management Microsoft Identity and Access Management CyberArk Certified Delivery Engineer

Processes	Description	Examples
Incident Response	Organizations develop a plan that utilizes tools and procedures to detect and respond effectively to cyberattacks, minimizing or preventing their impact. These plans usually include the following [51]: Roles and responsibilities of each member of the security team. Software, hardware, and other security tools install across the organization. Plan for restoring critical affected systems and data in the eventuality of a disruption attack. Roadmap that guides organizations through effectively identifying, containing, eradicating, and recovering from a cyberattack. Transparency communication to all contributors and customers of the company in case of an attack. Document the attack and how it came to be, to a later date do an analysis and correct the vulnerabilities.	Security information and event management (SIEM) Security orchestration, automation, and response (SOAR) Endpoint detection and response (EDR) Extend detection and response (XDR)
Encryption	By using mathematical techniques, we can transform data to make it unreadable to the naked eye. Only those who possess the key can decrypt and understand it. There are two main types of cryptographic keys [52]: **symmetric** and **asymmetric**. Symmetric keys use the same key for both encryption and decryption, offering better performance but posing a higher risk if compromised. Asymmetric keys utilize two separate keys: a public key for encryption, which can be widely distributed, and a private key for decryption, which is kept secret by authorized individuals.	Data Encryption Standard (DES) Advanced Encryption Standard (AES) International Data Encryption Algorithm (IDEA) Rivest–Shamir–Adleman (RSA) Elliptic curve cryptography (ECC)
Vulnerability Management	Ongoing process that helps organizations identify, assess, prioritize, and remediate vulnerabilities in their systems, networks, and applications, reducing organization´s overall risk exposure. It follows a set of phases: **Discovery** – identify vulnerabilities in your asset inventory. **Prioritization of assets** – prioritization of the assets by its criticality in the organization view. **Assessment** – identify and prioritize the risk that need to be address first. **Reporting** – Develop a security plan and report knows vulnerabilities. **Remediation** – solve the vulnerabilities that are more concern to the organization. **Verification and monitoring** – regular audits to ensure the threats are eliminated.	Microsoft Defender Vulnerability Management Tenable Nessus Rapid7 InsightVM Qualys VMDR

2.3.2 Security Requirements Analysis

Security requirements analysis plays a crucial role in safeguarding information and systems from cyber threats. Therefore, developing well-defined security requirements in the project design phase is imperative. This systematic process identifies, documents, and refines the security needs of a system or organization. The first step involves identifying and classifying systems to assess what kind of threats and vulnerabilities they may have. With this list of threats, a risk assessment is then conducted to evaluate the likelihood and potential impact of each threat, identifying the most concerning ones.

Based on the identified threats and risks, specific security requirements are established. Commonly used standards that focus on cybersecurity can be leveraged, such as IEC 62443 [53].

Consider IEC 62443-3-3, which is described in more detail in the technical note titled "Analysis of Practices and International Standards" listed in the Annex A. This standard outlines seven foundational requirements, each containing several specific security requirements, depicted in Table 5.

Table 5: IEC 62443-3-3 Foundational and Security Requirements

Foundational Requirement	Security Requirements
Identification and Authentication Control	Human user identification and authentication
	Software process and device identification and authentication
	Account management.
Use Control	Authorization enforcement
	Wireless use control
	Use control for portable and mobile devices
System Integrity	Communication integrity
	Malicious code protection
	Security functionality verification.
Data Confidentiality	Information confidentiality
	Information persistence
	Use of cryptographic
Restricted Data Flow	Network segmentation
	Zone boundary protection
	General purpose person-to-person communication restrictions
Timely Response to Events	Audit log accessibility
Resource Availability	Denial of service protection
	Resource management
	Control system backup

2.3.3 Security Validation/Testing

Security validation/testing is a systematic process of evaluating the effectiveness of security controls in a system or organization. It serves as a form of proactive defence, testing the security of a system to identify weaknesses before attackers exploit them. This allows for the implementation of appropriate security controls to address these vulnerabilities.

The IEC 62443-4-1 part includes a section that focuses on documenting the outcomes of all security testing. This documentation helps verify if the security requirements are being met, ensuring the product is effectively maintained throughout its real-world use. Table 6 shows the security verification and validation testing that the IEC 62443-4-1 demands.

Table 6: IEC 62443-4-1 Security verification and validation testing

Security Verification and Validation Testing	Examples
Security Requirements Testing	Functional testing of security requirements
	Performance and scalability testing
	Boundary/edge condition, stress and malformed or unexpected input test
Threat Mitigation Testing	Create and execute mitigation plans
	Create and execute plans for attempting to thwart each mitigation
Vulnerability Testing	Attack surface analysis
	Black box known vulnerability scanning
	Dynamic runtime resource management testing
Penetration Testing	Password cracking
	Privilege escalation
	Exploiting software vulnerabilities
Independence of Testers	Security consulting firms
	Freelance security researchers
	Internal audit teams with dedicated security expertise

In the automotive industry, cybersecurity homologation assessment using the Automotive SPICE tool became mandatory in July 2022 [54]. To verify and validate cybersecurity requirements, the industry began conducting threat modelling to identify critical interfaces, data, and asset groups.

Following threat modelling, a Threat Analysis and Risk Assessment (TARA), as detailed in ISO 21434 [55], is performed to measure threat and impact levels. This allows for the calculation of the security level (threat + impact) and the definition of cybersecurity goals.

These security goals are then broken down into system requirements, critical functions, and software data requirements. To validate the identified requirements, penetration testing teams utilize a structured test strategy based on attack patterns derived from the MITRE framework [56].

2.3.4 Security Qualification/Certification

Security qualification and certification are two critical processes that help organizations build trust and confidence in the security posture of their systems and software.

Security Qualification involves rigorous testing and evaluation of a system or software product against a set of predetermined security requirements in areas like access control, encryption, data integrity, and vulnerability management.

Security Certification builds upon security qualification. A software product successfully undergoes a qualification process and is awarded a formal certification by a recognized certification body. This certification signifies that the product meets a specific set of security criteria and demonstrates a level of assurance regarding its security posture.

There are different assessment approaches to evaluate the maturity of secure development, for example:

- Software Assurance Maturity Model (SAMM)
- Building Security In Maturity Model (BSIMM)
- Common Criteria (CC)

2.3.4.1 Software Assurance Maturity Model (SAMM)

One way to qualify and certify software is by using the Software Assurance Maturity Model (SAMM) [57], developed by OWASP. SAMM's main purpose is to provide an effective and measurable analysis of an organization's secure development lifecycle (SDL) and to recommend improvements.

SAMM is an open framework, risk-driven, and constantly evolving. It helps organizations formulate and implement strategies for improving their software security posture [57].

Figure 5 illustrates the areas covered by the framework.

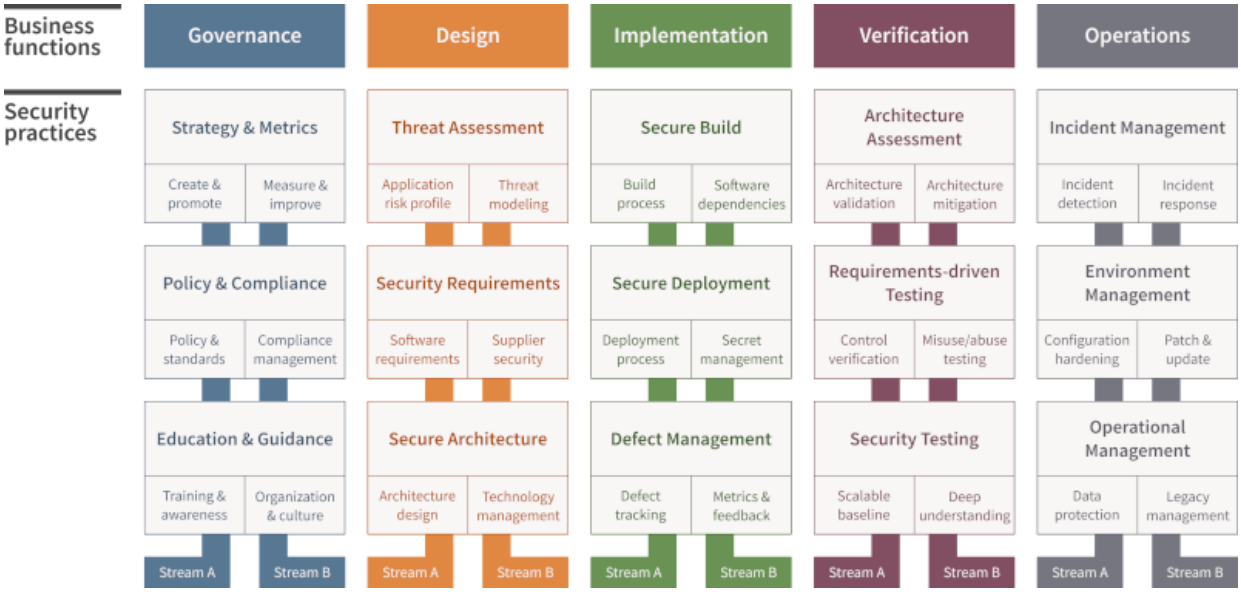


Figure 5: OWASP SAMM v2 model [57]

2.3.4.2 Building Security In Maturity Model (BSIMM)

Gaining an external perspective on a company's security posture is crucial. The Building Security In Maturity Model (BSIMM) from Synopsys can be a valuable tool in this regard.

BSIMM analyses and benchmarks software security programs across various industries. It does this by comparing a company's security needs against established best practices in software security programs. This analysis helps identifying strengths and weaknesses, enabling the company to prioritize improvements and evolve its security posture.

Ultimately, BSIMM facilitates building trust with stakeholders by allowing to share a clear picture of the company's security posture.

Additionally, BSIMM helps organizations identify the most effective security practices to achieve a strong security posture, considering available resources, time, and budget [58].

2.3.4.3 Common Criteria (CC)

The third and final example of security qualification/certification is the Common Criteria for Information Technology Security Evaluation (CC). The CC is an internationally recognized framework for evaluating the security of Information Technology (IT) products [59].

It has two companion documents:

- Common Methodology for Information Technology Security Evaluation (CMITSE) [60]: This document is divided into five parts, covering the introduction and general models, security functional requirements, security

assurance requirements, a framework for specifying evaluation methods and activities, and predefined packages of security requirements.

- Common Criteria Recognition Arrangement (CCRA) [61]: This arrangement outlines four objectives that are shared by its signatories.
    - **Maintain high evaluations standards**: Ensure IT product and protection profile evaluations are rigorous, consistent, and instil confidence in their security.
    - **Increase availability of secure products**: Promote the development of and availability of thoroughly evaluated IT products with robust security features.
    - **Eliminate Duplicate Evaluations**: Prevent redundant evaluations by establishing a globally recognized framework.
    - **Enhance efficiency and cost effectiveness**: Continuously improve the evaluation and certification process to be more efficient and cost effective for all stakeholders.

2.3.5 Tools

Organizations heavily rely on information technology, necessitating proactive measures to safeguard their confidential data. Cybersecurity tools play a vital role by continuously monitoring computer systems and networks, helping companies and individuals maintain data privacy and security.

Depending on the threats, cybersecurity tools can be tailored to counter them. Figure 6 depicts examples of cybersecurity tools.

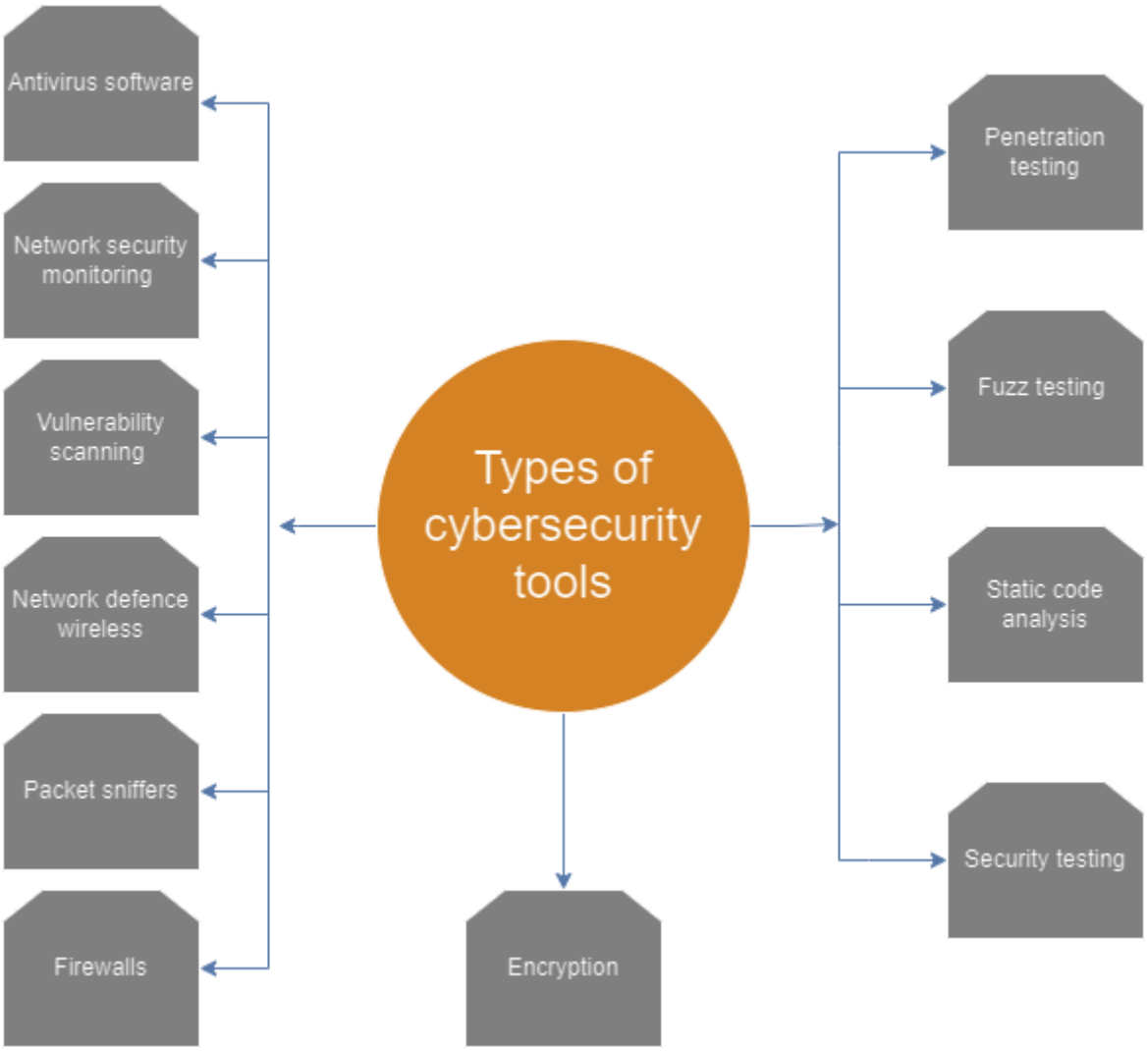


Figure 6: Types of cybersecurity tools adapted from [62]

Table 7 provides different types of tools [62].

Table 7: Cybersecurity tools

Tool	Description	Examples
Network security monitoring	Identify external threats by detecting and preventing attacks. Use in organizational level + ground segment.	Cisco Stealthwatch Darktrace Suricata
Vulnerability scanning	Identify weaknesses in software and hardware components. Use in organizational level + ground segment.	Splunk OpenVAS Acunetix
Network defence wireless-tools	Protect data while maintaining the network´s usability and integrity. Use in organizational level + ground segment.	KisMAC OpenWIPS Cisco ISE

Tool	Description	Examples
Encryption	Scramble data to ensure confidentiality during transmission or storage. Use in organizational level + ground and space segment.	Advanced Encryption Standard FIPS 140 - Security Requirements for Cryptographic Modules [63] Rivest-Shamir-Adleman
Firewalls	Control incoming and outgoing traffic, acting as a barrier between trusted and untrusted networks. Use in organizational level + ground segment.	Fortinet Fortigate CiscoASA Palo Alto Networks Firewall
Packet sniffers	Applications that analyse the network and gather data to be analyse by technicians. Use in organizational level + ground segment.	Wireshark tcpdump Fiddler
Antivirus software	Monitor, block and remove any malicious software that compromises the computer functionality. Use in organizational level + ground segment.	Windows Defender Bitdefender Norton
Penetration testing	Detect vulnerabilities by staging an attack to their systems. Use in organizational level + ground and space segment.	Kali Linux Metasploit
Fuzz testing	Software testing to uncover implementation bugs by injecting "trash" input and analyse the reaction. Use in organizational level + ground and space segment.	PortSwigger Burp Suite Professional OWASP WSFuzzer Synopsys Defensics
Static code analysis	Analysis the source code to identify potential issues, bad practices and vulnerabilities. Use in organizational level + ground and space segment.	Astrée OWASP WSFuzzer MISRA
Security testing	Comprise with performance tools, simulated attacks, buffer overflow, DoS testing and equivalence class partitioning test. Use in organizational level + ground and space segment.	Kali Linux Metasploit

2.4 Conclusion

The space sector, once a relatively isolated domain, has become increasingly intertwined with global critical infrastructures. The growing complexity of space systems, coupled with the rise of cyber threats, necessitates a robust and comprehensive approach to cybersecurity. While significant advancements have been made in recent years, challenges persist, including the need to create and reenforce space-based standards with cybersecurity elements, standardized regulations, addressing supply chain vulnerabilities, mitigating resource constraints, and ensuring a skilled workforce.

To effectively address these challenges, a multi-faceted strategy is required. This includes:

- **Stronger International Cooperation**: Fostering collaboration among nations to develop and enforce common cybersecurity standards.
- **Enhanced Cybersecurity Regulations**: Implementing stringent regulations and compliance frameworks to ensure the security of space systems.
- **Increased Investment in Research and Development**: Supporting innovation in cybersecurity technologies to address emerging threats and vulnerabilities.
- **Building a Skilled Workforce**: Developing and retaining a highly skilled cybersecurity workforce to safeguard space assets.
- **Continuous Monitoring and Threat Intelligence**: Implementing robust monitoring and threat intelligence systems to detect and respond to cyberattacks promptly.

By adopting these measures, the space sector can mitigate risks, protect critical infrastructures, and ensure the continued advancement of space exploration and innovation.

3 CYBERSECURITY SURVEY

As part of the second objective of the internship (objective 2 - Engage with Key Stakeholders), a cybersecurity survey was conducted with the goal of gathering data from space engineers' perspectives on the vulnerabilities, threats, and potential mitigation strategies faced by space systems. To achieve this, space engineers from various agencies were contacted and asked to participate in the survey.

This chapter explores the process of creating the cybersecurity survey and its results, which contribute to another of the internship's objectives (objective 5 - Produce Scientific Publications), the development of a scientific paper.

3.1 Survey Preparation Process

As the survey aimed to capture feedback from space engineers on cyber threats, vulnerabilities, and mitigation strategies, the questions were crafted around these three key aspects. It was crucial to ensure the questions were carefully constructed, highly specific, and easy to answer. This is because survey participation can be limited (due to respondents' availability), and the objective was to encourage serious and thoughtful responses.

A first version of the survey was created using Microsoft Excel. This version consisted of seven questions:

1. List up to 5 of the most common or severe vulnerabilities that you believe affect space or ground systems (or embedded real-time systems). (Consider SW development, V&V, Acceptance, Installation, Updates and Operations related vulnerabilities).
2. List up to 5 cybersecurity threats that you consider relevant for space or ground systems (or embedded real-time systems). (Consider SW development, V&V, Acceptance, Installation, Updates and Operations threats).
3. Identify up to 5 Technical Mitigations that are applied or could be applied to prevent cybersecurity problems in space or ground systems.
4. Identify up to 5 Processual mitigations that are applied or could be applied to prevent cybersecurity problems in space or ground systems.
5. List the standards or cybersecurity resources used to ensure compliance and security of space or ground systems.
6. Select the segment of space systems that do you think are most vulnerable to cybersecurity threats (Ground/User, Space, Link/Signal).
7. Any other cybersecurity concerns/trends that you see in the short/middle term (up to 10 years from now) for safety-critical embedded systems, particularly space systems.

Each question was accompanied by a rationale to facilitate understanding for the respondents. The questions addressed the following topics:

- Identification of up to five cyber threats.
- Identification of up to five vulnerabilities.
- Identification of both technical and procedural mitigation strategies.
- Standards and other cybersecurity resources used.
- Selection of the space segment most vulnerable to cyberattacks.
- Anticipated future cybersecurity concerns and trends affecting the space sector.

To assess the survey's structure and completion time, a pilot test was conducted internally at Critical Software. Initial feedback regarding the survey structure was positive. The time to complete the survey was approximately 30 minutes, as expected. However, some confusion arose concerning the rationale for questions 3 and 4, which focused on technical and procedural mitigations. Respondents had difficulty distinguishing between the two concepts. To address the confusion around technical and procedural mitigations (questions 3 and 4), the survey was revised by improving the rationale and providing examples for both questions.

To enhance accessibility and user experience, the survey was migrated from Microsoft Excel to Microsoft Forms. This transition made the survey more visually appealing and easier to complete.

A targeted list of potential participants was created, consisting primarily of European space engineers. This approach leveraged Critical Software's collaboration history with the European Space Agency (ESA) and helped contacting individuals from ESA to take part. Additionally, the survey was sent to participants from NASA JPL, JAXA and Brazil, for example.

To broaden participation further, the survey link was made publicly available on LinkedIn for anyone interested in responding. The publication made on LinkedIn can be seen in Annex C.2.

3.2 Overview of Results

The survey received a total of 21 responses from space engineers over a period of 5 months, between February 1, 2024, and June 1, 2024. The originally planned closing date was extended due to a lower-than-anticipated response rate. The average time to complete the survey was 21 minutes.

A variety of responses were provided for each question, with the number of different answers ranging from 19 for standards and resources to 39 for technical mitigations.

- **Perceptions of Vulnerabilities and Threats**: Engineers named a diverse range of potential vulnerabilities (35) and threats (33) to space systems.

- **Mitigation Strategies**: Respondents offered a broad spectrum of technical mitigation strategies (39) and processual mitigation strategies (31) to address identified vulnerabilities and threats.
- **Most Vulnerable Segment**: The ground segment was perceived as the most vulnerable to cyberattacks, with 20 respondents selecting it. Link and space segments received 2 and 12 votes, respectively.
- **Future Cybersecurity Concerns**: Engineers expressed various concerns and predicted trends about future cybersecurity challenges in the space sector, with 19 different responses provided.

3.3 Vulnerabilities

The 35 vulnerabilities that the experts found are listed in Table 8, arranged from the most to the least commonly stated. The Common Weakness Enumeration (CWE) [64] which is a community-developed list of common software and hardware weaknesses, served as the basis for classifying each vulnerability. It is crucial to remember that not all classifications will reach total agreement. Consequently, these categories must be regarded as an initial effort to arrange the vulnerabilities according to a common taxonomy.

The use of "several" in the "Category" column indicates that there are more than three categorizations. To maintain table clarity, the category "several" is used.

Finally, the use of "NVD-CWE-Other" is use when there is no correct category in CWE that represent the answer.

Table 8: Vulnerabilities identified

#	Answers	Response Frequency	Category
1	**Access control vulnerabilities**: this may lead to unauthorized access to sensitive information. e.g. (1) during system development or during S/C (Spacecraft) flight operations. (2) neglect the design of ground-on-board protocol to prevent unauthorized access. (3) missing authentication in the Ground Operation System, in which untrained people can access the facilities, command functions in satellite, and access sensitive data.	38 %	CWE-287 - Improper Authentication

#	Answers	Response Frequency	Category
2	**V&V vulnerabilities - most of testing is done blindly based on traces to requirements and not based on a proper testing strategy.** e.g. (1) cover extra situations, performance, stress, volume, security situations, combinations, not necessarily stated in the requirements. (2) Test campaigns not sufficiently covering requirements and beyond, out of bounds and unspecified cases. (3) Insufficient / incomplete testing activities (not only having interfaces, code coverage or requirements coverage-based tests, but ensure security-based tests and coverage of all possibilities) (4) Prioritizing speed over thoroughness in the validation process can lead to incomplete testing. (5) do not test conditions that prevent the on-board system to receive erroneous TCs. (6) non reporting of abnormal situations during testing.	33 %	Several
3	**Communication link encryption/protection vulnerabilities**	29 %	CWE-311 - Missing Encryption of Sensitive Data CWE-327 - Use of a Broken or Risky Cryptographic Algorithm CWE-326 - Inadequate Encryption Strength
4	**Open-source software/libraries/Operating Systems/COTS vulnerabilities**	29 %	CWE-1395 - Dependency on Vulnerable Third-Party Component CWE-1357 - Reliance on Insufficiently Trustworthy Component
5	**Software design not protected against fuzzed inputs**	19 %	CWE-20 - Improper Input Validation
6	**Reuse of software/system not thoroughly tested or trusted wrongly.** e.g. (1) lead to strange problems such crashes, hangs, buffer overflow.	19 %	Several
7	**Use of tools that are not mature enough for software development, testing.** e.g. (1) static code analysis tool	19 %	Several
8	**Software bugs with security impacts.** e.g. (1) bugs in code that lead the system to execute commands (in ground station) and/or telecommands (on-board of satellite) that open access to malicious attacks. (2) Hidden backdoors in application deployment	19 %	CWE-94: Improper Control of Generation of Code ('Code Injection')

#	Answers	Response Frequency	Category
9	**Lack of basic security services in the space segment.** e.g. (1) lack of basic authentication and access control, lack of any form of partitioning or segmentation of functions	19 %	CWE-276: Incorrect Default Permissions
10	**Using of weak/sloppy development process.** e.g. (1) Agile methodologies should be forbidden, analysis, requirements, design, implementation, testing	14 %	NVD-CWE-Other
11	**Read and write operations in memory.** e.g. (1) stack overflow	14 %	CWE-657 - Violation of Secure Design Principles
12	**Insufficient safety and security analysis done in the initial phases** (prior to requirements baseline) **e.g.** (1) **poor requirements** (2) **Lack of security assessment and analysis** to derive requirements	14 %	CWE-119 - Improper Restriction of Operations within the Bounds of a Memory Buffer
13	**Overly complex software/system. e.g.** (1) **Bad design**, when people do not do design and instead generate it from code that might be flawed.	14 %	CWE-657 - Violation of Secure Design Principles
14	Software updates: **S/C systems allow software updates during its lifetime**. This way, **hackers might inject malicious code** that can lead to the system failure, to spy flight data, or even to affect/destroy other missions.	14 %	Several
15	**Software development environments not protected** enough (allowing to get access to key Software artifacts)	10 %	Several
16	**Debug ports not protected** (e.g. Access to the target memories through debug ports)	10 %	Several
17	**Ignore code smells and other code rules violations** provided by commercial static analysis tools.	10 %	CWE-284: Improper Access Control
18	**Updates and Operations phase- lack of tests to verify the stability of a modification and impact on the rest of the system/components/functions,** which will lead to patches and updates that might cause problems in the future (side problems not easily identifiable during installation); **lack of operator training due to incomplete user/operation manual** (for example not referring to the limitations of the system + security problems/precautions)	10 %	CWE-710: Improper Adherence to Coding Standards

#	Answers	Response Frequency	Category
19	**Acceptance - No security acceptance plan exists,** usually acceptance is based on a subset of the tests, and tests, as we all know are not necessarily covering security and odd situations (this also represents a contractual limitation because the subcontractor needs to have specific scope defined and will hide contractually behind that while affecting security, yes, this is also a vulnerability, contracts represent a vulnerability because they will "lead" to only do what is written...) (2) accepting based on already provided test results by the supplier, instead of going deep into an acceptance set of activities (audit, documentation scrutiny, independent assessment/V&V, and specific tests for security situations)	10 %	Several
20	**Installation -** incorrect or modified versions installed, virus on installation machines, informal patches installed, lack of verification of the installed system… (2) incomplete configurations during uploading on-board software, telecommand lists, or during storing payload data in cloud storage banks. (3) leaving undesired installations or configurations, lack of installation logs and records	10 %	NVD-CWE-Other
21	**Documentation, Code, Electronic ICDs and database contents** are **shared** between official entities with resource to **unusual communication means or through 3rd party providers** (e.g.: email, SharePoint, FTP).	5 %	CWE-922 - Insecure Storage of Sensitive Information
22	**Possibility to inject failures** (e.g. (1) supply chain attacks)	5 %	CWE-754 - Improper Check for Unusual or Exceptional Conditions
23	Not secure **boundary parameters**	5 %	CWE-754 - Improper Check for Unusual or Exceptional Conditions
24	**Hardware devices access poorly protected or no protected at all.**	5 %	CWE-287 - Improper Authentication
25	**Weak passwords policies**	5 %	CWE-287 - Improper Authentication
26	**Use of outdated languages, tools and libraries.**	5 %	NVD-CWE-Other
27	**High turnover of contractors** - opportunities for attacks of social engineering	5 %	NVD-CWE-Other

#	Answers	Response Frequency	Category
28	**Bad design**, when people do not do design and instead generate it from code that might be flawed.	5 %	CWE-94 - Improper Control of Generation of Code CWE-657 - Violation of Secure Design Principles
29	**Updates and Operations -** open ports or interfaces, giving too much functionality for the operator (in operations manuals)	5 %	CWE-284: Improper Access Control
30	**Use dynamic memory in space systems.**	5 %	Several
31	**Deserialization of untrusted data**	5 %	CWE-345 - Insufficient Verification of Data Authenticity CWE-913 - Improper Control of Dynamically Managed Code Resources
32	**Integer overflow of wraparound**	5 %	CWE-682 - Incorrect Calculation
33	**Improper/insufficient monitoring of the ground and space segments for anomalies and attacks.**	5 %	CWE-223: Omission of Security-relevant Information
34	**Lack of training/awareness in cybersecurity subjects** (for management, development/technical, and installation, maintenance, and operations).	5 %	NVD-CWE-Other
35	**Poor management of the exchanged data** between ground and space segments. (1) **Limit the amount** of telecommands received in batch.	5 %	CWE-269: Improper Privilege Management

The experts' Top 5 most often cited vulnerabilities were:

- **Access control vulnerabilities:** These vulnerabilities exploit weaknesses in the mechanisms that control access to systems and data.
- **Verification and validation (V&V) vulnerabilities:** These vulnerabilities stem from flaws in the processes used to ensure that systems meet their intended requirements.
- **Communication link encryption/protection vulnerabilities:** These vulnerabilities compromise the encryption or protection mechanisms safeguarding communication links between space and ground segments.
- **Open-source software/libraries/operating systems/COTS (Commercial-Off-The-Shelf) vulnerabilities:** These vulnerabilities reside within software components obtained from external sources, including open-source libraries, operating systems, and COTS products.
- A set of 5 vulnerabilities tied in 5th place: **Software design not protected against fuzzed inputs, Reuse of software/system not thoroughly tested or trusted wrongly, Use of tools that are not mature enough for software development, testing, Software bugs with security impacts, Lack of basic security services in the space segment.**

Beyond the top five vulnerabilities, the survey identified other noteworthy issues that deserve further exploration.

One critical concern raised by the experts (Item 34) is the need for a strong cybersecurity culture across not just the space sector, but also in other critical sectors. This can be achieved through training programs that raise awareness of cybersecurity best practices and empower personnel to act as the first line of defence against cyberattacks.

The survey also suggests a potential vulnerability associated with using agile methodologies for critical systems (Item 10). Experts raised concerns about the evolving nature of requirements in agile development, which could introduce vulnerabilities if not carefully managed.

Finally, the importance of clear and comprehensive user and installation manuals was highlighted (Items 18 & 20). Poorly written documentation can lead to misconfigurations and improper use, potentially creating openings for malicious actors to exploit vulnerabilities within the system. These points emphasize the need for a holistic approach to cybersecurity that goes beyond simply identifying and patching technical flaws.

3.4 Threats

Table 9 presents the 33 threats identified by the experts, sorted from the most frequently mentioned to the least frequent. The categorization of each threat was based on the taxonomy proposed by Gregory Falco and Nicolò Boschetti [24].

Table 9: Threats identified

#	Answers	Response Frequency %	Category
1	**Jamming of** communications channel/Satellite.	43 %	Electromagnetic - Man-Made
2	**Malware and ransomware**	24 %	Cyber - Technical
3	**Distributed Denial of Service** (DDOS)	24 %	Cyber - Technical
4	**The middle-man threats** in ground operations of space asset (e.g. bad configuration management on the flight parameters of Ariane 5 took the satellite into wrong orbit which caused the use of fuel to correct the orbit with the consequent reduction in satellite lifetime).	19 %	Cyber - Technical
5	**Data being stolen on ground stations** (e.g. USB ports used to steal data and introduce virus/trojans).	19 %	Cyber - Technical
6	**Space weather/solar storms**	14 %	Electromagnetic - Environmental
7	Hacking into space networks (**eavesdropping**) seems to be quite impossible, but in here one could divide the security problem between the uplink (sending telecommands (TC)) and the downlink (receiving telemetry (TM)). For the uplink, it will be difficult to bypass the encryption units normally onboard, besides the need to have a tracking ground station and other physical problems, but satellite orbits are public, and you can build your own tracking Ground Station. For the downlink you can always try to decode the information received from the spacecraft specifically if it is not encrypted.	14 %	Electromagnetic - Man-Made
8	**Insider attacks. e.g.** (1) Attacking the development/validation environment with the objective of introducing undetected vulnerabilities/bugs. (2) Software patch to exclude commandability from correct ground station.	14 %	Cyber - Technical
9	**Spoofing. e.g.** (1) Sending malicious TCs/TMs to/from spacecraft/ground segment. (2) Third parties sending commands to satellite.	14 %	Cyber - Technical

#	Answers	Response Frequency %	Category
10	**Tampering with source code/ binary to introduce accidental or malicious code** that could either prevent the correct operation or could allow unauthorized parties to interact with the SW.	10 %	Cyber - Technical
11	**Supply chain attacks**	10 %	Organizational - Management
12	Network vulnerabilities are also a threat since most of the space systems collect data that ends up somewhere on earth for further processing. The data is quite important and expensive and should not be lost or hijacked. **Cloud security and other types of security measures could be under threat.**	5 %	Cyber - Technical
13	**Change the S/C configuration** (e.g., switch on or off equipment, switch a camera off in a moment when it should shoot a specific target, change S/C direction, grab the wrong target (ClearSpace-1), change FDIR configurations, removing detection mechanism)	5 %	Cyber - Technical
14	**Hijacking** S/C (AOCS operations) and change its direction.	5 %	Cyber - Technical
15	**Identity theft**	5 %	Cyber - Social Engineering
16	**Bad design**, when people do not do design and instead generate it from code that might be flawed	5 %	Cyber - Technical
17	**Speed up development / pressure** - not doing things properly like design, code analysis, testing, will always leave issues in the final product	5 %	Organizational - Management
18	**Lack of certification of space system**s (not that FAA certification or TUV for railways are perfect, but they try)	5 %	Regulatory - Legal
19	**No Software vulnerabilities analysis / Threats analysis** is performed before closing the system and software requirements that they should actively contribute too (like a FMEA for cybersecurity)	5 %	Cyber - Technical
20	**Malicious states agents**	5 %	Organizational - Production
21	Keyboards, especially wireless keyboards may be **logging keystrokes** and transmitting them, similar for screens.	5 %	Cyber - Technical
22	**Stealing of IP** (working from home)	5 %	Cyber - Technical

#	Answers	Response Frequency %	Category
23	**Stealing of encryption keys**	5 %	Cyber - Technical
24	**Electromagnetic Pulse**	5 %	Electromagnetic - Man-Made
25	**Blinding sensors by Lasers**	5 %	Physical - non-kinetic
26	**ASAT testing**	5 %	Physical - Kinetic
27	**Electronic warfare in the outer space.**	5 %	Electromagnetic - Man-Made
28	**Exploiting development tools**	5 %	Cyber - Technical
29	**Unmitigated errata**	5 %	Cyber - Technical
30	**Electronic attacks against space-based services at the transmission site, the satellite, and the user' s equipment.**	5 %	Electromagnetic - Man-Made
31	**Physical attacks against actual launchers, satellites, and spacecrafts.**	5 %	Physical - Kinetic

The distribution of threats across the many categories that space engineers found is shown in Figure 7. When compared to other categories, the "Cyber-Technical" category is the most relevant, according to the data analysis. This focus probably results from the fact that cyber-technical attacks specifically target weaknesses in space assets' hardware, software, and communication systems. This demonstrates how urgently space systems-specific cybersecurity rules are needed.

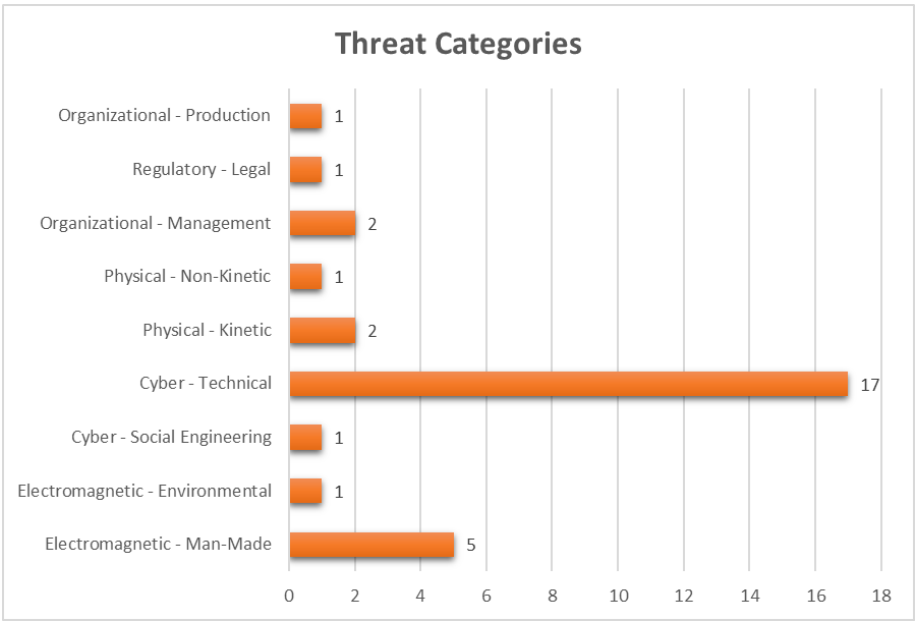


Figure 7: Identified Threats per category

The experts Top 5 most often cited threats are:

- **Jamming of communication channels/satellites**: This threat involves disrupting communication between space and ground systems.
- **Malware and ransomware**: These are malicious software programs that can damage, encrypt, or steal data from space or ground systems.
- **Distributed Denial-of-Service (DDoS) attacks**: These attacks overwhelm systems with traffic, making them unavailable to legitimate users.
- **Man-in-the-middle attacks during ground operations**: This threat involves attackers intercepting or modifying communication between ground stations and space assets (especially if they understand the protocol).
- **Data theft from ground stations**: This threat involves unauthorized access and exfiltration of sensitive data from ground stations.

Although the most frequently cited issues were represented by the top five weaknesses, the poll also revealed other intriguing threats.

The push to expedite development processes is one such issue (Item 17). Efficiency is ideal, but skipping important processes like security testing might have negative effects. Development that is rushed can result in security flaws that could cause expensive mission failures. This can further compromise overall security by contributing to systems that are poorly built (Item 16).

It is interesting to note that supply chain attacks were mentioned comparatively infrequently in the survey results. Given the intrinsic complexity of the supply chain for the space industry, which involves many components going through several phases prior to satellite manufacturing, this is a little surprising.

3.5 Technical Mitigations

Table 10 presents the 39 technical mitigations identified by the experts, sorted from the most frequently mentioned to the least frequent. The categorization of each mitigation technique was based on the five functions of the NIST Cybersecurity Framework [65]:

- **Identify**: focuses on understanding the systems, assets, data, and threats that an organization needs to protect. It involves activities like asset discovery and inventory, data classification, and identification of potential vulnerabilities.
- **Protect**: implementing safeguards to deter, prevent, or mitigate the impact of cyberattacks. Common protective measures include secure configurations, data encryption, access controls, and network segmentation.

- **Detect**: activities that help identify and report security incidents in a timely manner. It encompasses security monitoring, anomaly detection, log analysis, and intrusion detection systems.
- **Respond**: procedures for acting in response to a security incident. It includes activities like containment, eradication, remediation, and recovery.
- **Recover**: focuses on restoring systems and data to a functional state after a security incident. It involves activities like data backup and restoration, disaster recovery planning, and business continuity exercises.

Table 10: Technical mitigations identified

#	Answers	Response Frequency %	Category
1	Advanced **encryption** in the communication link and data storage.	52 %	Protect
2	**Extensive code analysis** (static analysis with cybersecurity rules)	24 %	Protect
3	**Intrusion detection mechanisms** and tools (1) Monitoring and anomaly detection (2) **Robust FDIR configuration** that could detect and recover from injected failures	19 %	Detect
4	**Proper authentication methods and access control**	14 %	Protect
5	**CRCs for all data transmission.** e.g. (1) In transmissions that involve sending information in multiple TCs/TMs, implement a Checksum that applies to all the data transmitted as a whole (e.g., checksum for a file that was transmitted in multiple TCs/TMs).	14 %	Protect
6	**Secure-by-design approach** (e.g. zero trust solutions)	14 %	Protect
7	**Protect routing and distribute controls**, considering Inter-Satellite Links (ISLs) routing. e.g. (1) **Give an ID to every entity in the system** and **validate** that the communication is being performed between allowed entities.	10 %	Protect
8	**Firewall**	10 %	Protect
9	**Strong password policies**	10 %	Protect
10	**Penetration testing** (e.g. Explicit penetration testing of exposed systems and interfaces)	10 %	Protect
11	**Zero code smells and zero warnings objective** (as measured by static analysis tools)	10 %	Protect

#	Answers	Response Frequency %	Category
12	**Secure Protocols to protect attacks during uploads and downloads.** (1) **Handshake protocols** between ground and satellite.	10 %	Protect
13	**Telecommands acceptance is subject to validation** by either SW or HW, which reduces or eliminates most attempts of commanding by unauthorized parties.	5 %	Detect
14	**Periodically change the CRC/checksum/cryptography algorithms** being used.	5 %	Protect
15	**Use of certified tools** (Software development processes can look for SW vulnerabilities within the code being developed, using static analysis tools and other type of SW assisted tools with proper certifications)**.**	5 %	Identify
16	**Usage of secure hardware**	5 %	Identify
17	**Protection of software development environments**	5 %	Protect
18	**Authentication on software patch**	5 %	Protect
19	**Protect debug port** accessed	5 %	Protect
20	**Defensive programming** of the embedded software	5 %	Protect
21	**Extensive V&V** of the embedded device **against fuzz inputs**	5 %	Protect
22	**Enforce patch management**	5 %	Protect
23	**HW tokens for key storage**	5 %	Protect
24	**Plan and strategy to ensure the security best practices,** for example by having technical activities to ensure OWASP top 25 are assessed	5 %	Protect
25	**Specific security assessment of the design/code** (for example with tools such as Absint's Astrée) and fixing of the deviations (soon in the process and not only at the end) - report also the results of these analysis to the customer	5 %	Protect
26	**Built-in or self-tests** to **ensure application and data integrity**	5 %	Detect
27	**Better languages and libraries.**	5 %	Identify

#	Answers	Response Frequency %	Category
28	**Network segmentation**, protecting ground assets.	5 %	Protect
29	**Availability insurance** under extreme conditions.	5 %	Protect
30	**Accept telecommands** and download telemetry **only when flying above certain regions.**	5 %	Protect
31	**Radio transmitters operate in different frequencies.**	5 %	Protect
32	**Avoid equipment from foreign sources (untrusted sources)**, especially in key components: networks, keyboards, screens, storage.	5 %	Identify
33	Use **cryptographic keys** instead of passwords.	5 %	Protect
34	**Advanced interference mitigation, e.g. with filters**	5 %	Respond
35	**Use security zones in the architecture and prevent data flows**	5 %	Protect
36	**Perform input validation**	5 %	Detect
37	**Integrity checks for all data, configurations, inputs to the system**	5 %	Detect
38	**Regular updates for ground systems**	5 %	Protect
39	**Redundance in ground systems to avoid operation disruption**	5 %	Protect

Based on the NIST Cybersecurity Framework, Figure 8 shows how cybersecurity mitigations are distributed across different categories. With 29 comments, the "Protect" category is the most popular, followed by "Detect" with 5 mentions. According to this research, there should be a lot of focus on putting preventative measures in place to protect against cyberattacks, but it is also critical to have systems in place to recognize them when they do happen.

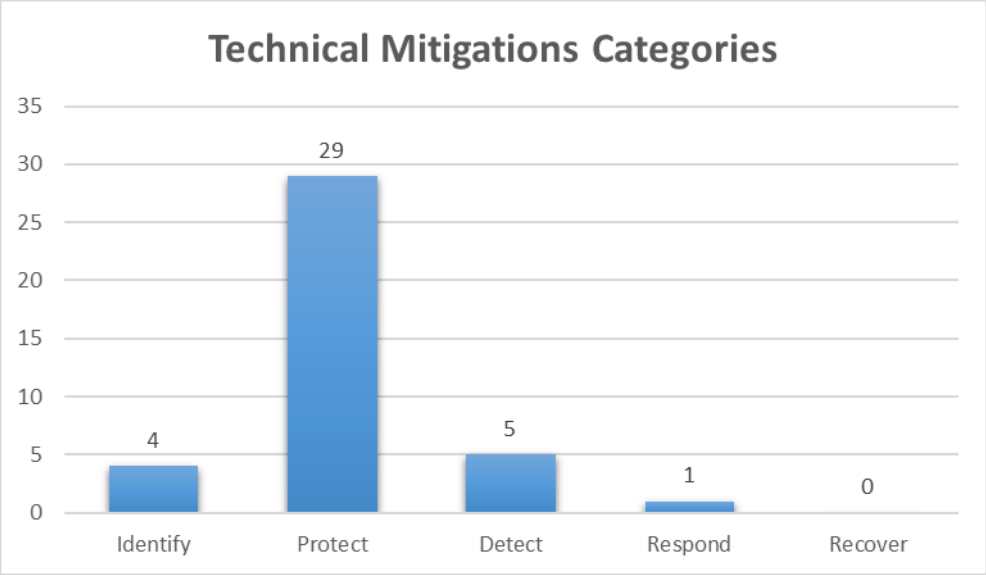


Figure 8: Identified Technical mitigations per category

The survey data revealed the following top 5 most frequently cited technical mitigations identified by experts:

- **Advanced Encryption in Communication Links and Data Storage**: This emphasizes the importance of robust encryption to protect data confidentiality during transmission and while at rest.
- **Extensive Code Analysis** (Static Analysis with Cybersecurity Rules): This highlights the need for thorough code review using automated tools configured with cybersecurity best practices to find potential vulnerabilities.
- **Intrusion Detection Mechanisms and Tools**: This underscores the importance of implementing systems that can detect and alert security personnel to suspicious activity on the network.
- **Proper Authentication Methods and Access Control**: This emphasizes the need for strong authentication mechanisms to verify user identities and restrict access to systems and data based on proper permissions.
- **Secure-by-Design Approach**: This highlights the importance of building security into the system design, adopting a "zero trust" approach that assumes no user or device is inherently trustworthy and requires verification before granting access.

In addition to the top 5, the poll found more useful technological mitigations. The need of having a thorough plan and strategy to guarantee continued adherence to security best practices is one such example (Item 24). This approach could entail using tools to stop known vulnerabilities from being introduced into new programs, keeping an up-to-date vulnerability database, and using resources such as the OWASP Top 10 [66] (a well-known list of web application security threats).

According to the survey, there may be advantages to switching from passwords to cryptographic keys, often known as passkeys (Item 33). Passkeys allow safe

authentication without requiring users to memorize or manually enter complicated passwords by combining public key cryptography with biometrics (facial recognition, fingerprint). This strategy seeks to improve overall security and remove the possibility of using weak or frequently used passwords.

3.6 Procedural Mitigations

The 31 procedural mitigations that the experts found are shown in Table 11, arranged from the most to the least frequently stated. One more time, NIST Cybersecurity Framework's five functions [65] served as the basis for classifying each mitigation technique.

Table 11: Procedural mitigations identified

#	Answers	Response Frequency	Category
1	**Enforcing security standards** (in satellite and ground systems)	33 %	Protect
2	**Security testing** (PenTest, FuzzTesting, Out-of-bounds, equivalence class partitioning test, buffer overflow, DoS tests, simulated attacks)	24 %	Protect
3	**Awareness trainings** to the developers (e.g. phishing, ransomware, and malware etc.)	24 %	Identify
4	**Conducting independent regular security audits**	24 %	Protect
5	**Ensure a SDLC (Secure Development Life Cycle) is integrated in the application development**	24 %	Protect
6	**Training on security aspects** considered within the different **domains and standards.** (1) **Training on V&V** of embedded systems from a hacker perspective. (2) **Training on security aspects** when **designing embedded systems**.	24 %	Identify
7	**Security requirements to be specified as early as possible** to avoid and detect potential vulnerabilities. These vulnerabilities might force design or architecture changes. For that reason, the soon the better.	14 %	Protect
8	(1) **Check of OSS libraries** and other third-party SW for SW **vulnerabilities**. (2) For integrated components (reuse, OS, used tools, …) **do a deep analysis and test all interfaces** (Zero Trust model)	14 %	Protect
9	**Vulnerability / Threats Analysis done before requirements are closed.** (1) Comprehensive assessment of vulnerability in Satellite Data Centres, particularly to prevent attacks in cloud solutions for data storage	14 %	Protect

#	Answers	Response Frequency	Category
10	**(1) Maintenance Plan with security contents** (incident response) (2) **Have user manuals, maintenance, and incident** resolution plans (3) **Cover security in installation/operation/maintenance documentation**	14 %	Protect
11	**More secure information and deliverables flow.**	10 %	Protect
12	**Robustness testing**	10 %	Protect
13	**Every user involved** in activities related to the project shall be **subjected to user authentication. (Zero Trust model)**	5 %	Protect
14	**Errata analysis**	5 %	Protect
15	**Security reviews**	5 %	Protect
16	**Take security lessons learned from other projects/missions/domains** into account.	5 %	Protect
17	**Organizational security culture, resources** (e.g. tools, training, processes, templates) and assessment	5 %	Identify
18	**Restricted/Protected access** to software development tools, developments environments (Secure Development Life Cycle), hardware tools, …	5 %	Protect
19	**Scanning repositories**	5 %	Protect
20	**Hardening machines**	5 %	Protect
21	**Enforce patching**	5 %	Protect
22	**Security scans of nodes**	5 %	Protect
23	**Force baseline migrations**	5 %	Protect
24	**No agile methodology in security critical development**	5 %	Protect
25	**Clearer requirements with rationales -** goal should be simpler more robust software.	5 %	Protect
26	**Shorter feedback loops** to address ISVV findings in timely fashion.	5 %	Protect
27	**Have guidelines to integrate cybersecurity layer with central software interfaces / data processing layer.**	5 %	Protect
28	**Integrate cybersecurity in the validation simulator.**	5 %	Protect
29	**Nominate cybersecurity manager for a project.**	5 %	Protect

#	Answers	Response Frequency	Category
30	**Simulated attacks sessions with specialists before launch/operations.**	5 %	Protect
31	**Define a set of approved libraries to be used by satellite manufacturers.**	5 %	Identify

The distribution of processual mitigations throughout the NIST Cybersecurity Framework categories is seen in Figure 9. With 27 responses, the "Protect" category is the most popular, much as the technical mitigations. In contrast to the technical mitigations, which had a greater variety of responses from other categories, all of the remaining responses in this case come under "Identify."

According to this statistics, two key areas should be given special attention:

- Putting preventive measures in place to guard against cyberattacks (which is consistent with the considerable number of answers in the "Protect" category).
- Increasing knowledge about risk management in cybersecurity from an organisational standpoint. This involves controlling risks to data, assets, people, and systems. Organisations can focus their efforts on developing a strong risk management plan that fits their business requirements by enhancing this understanding.

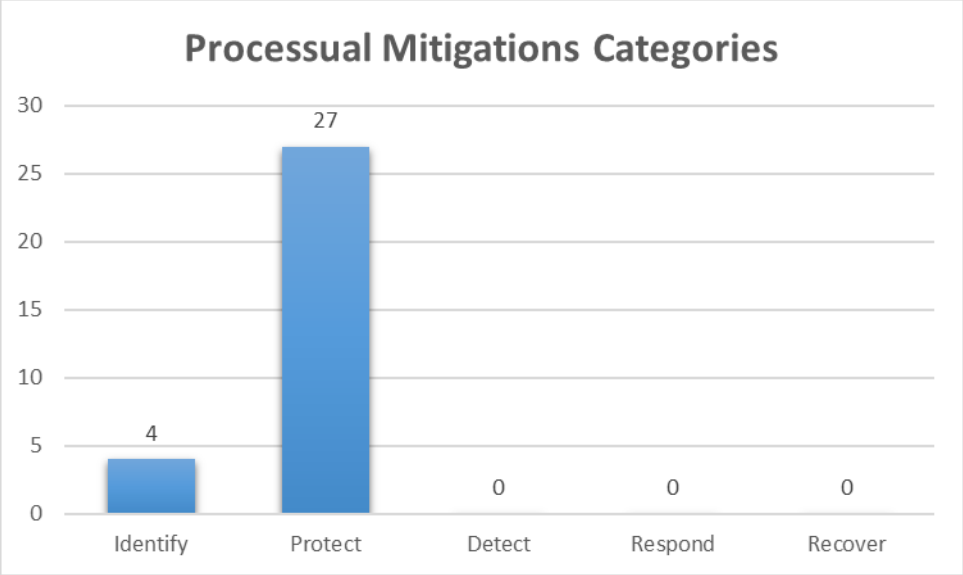


Figure 9: Identified Processual mitigations per category

The survey data revealed the following top 5 most frequently cited processual mitigations identified by experts:

- **Enforcing Security Standards**: This emphasizes the importance of implementing and enforcing robust security standards across both satellite and ground systems.

- **Comprehensive Security Testing**: This highlights the need for a variety of security testing methods, including penetration testing, fuzz testing, out-of-bounds testing, equivalence class partitioning testing, buffer overflow testing, denial-of-service testing, and simulated attack scenarios.
- **Developer Security Awareness Training**: This underscores the importance of providing developers with regular security awareness training to educate them on current threats like phishing, ransomware, and malware, and how to develop secure code.
- **Independent Regular Security Audits**: Regular independent security audits conducted by qualified personnel are crucial for finding potential vulnerabilities in systems and processes.
- **Secure Development Lifecycle (SDLC) Integration**: This emphasizes the importance of integrating a secure development lifecycle (SDLC) methodology into the application development process. An SDLC incorporates security best practices throughout the development stages to find and mitigate vulnerabilities early on.

The survey revealed some more intriguing results from the experts, in addition to the top five processual mitigations that were most mentioned.

The need of precisely specifying security requirements early and frequently throughout the project lifecycle is highlighted by one significant recommendation (Item 7). This prevents vulnerabilities from being found later in the development process, when fixing them can be far more costly and time-consuming. Early diagnosis reduces possible interruption and expense by enabling necessary changes to the project architecture.

The significance of carefully evaluating third-party software for vulnerabilities before to incorporating it into projects is another intriguing issue (Item 8). This entails staying away from unknown equipment, software, and parts and thoroughly examining and testing them to guarantee their security.

Lastly, Item 29 emphasises how important it is for a project team to have a dedicated cybersecurity specialist. This committed person can proactively detect and resolve any security threats, promote security best practices, and guarantee their application.

3.7 Standard and Resources

Table 12 presents the 19 cybersecurity standards and other resources identified by the experts, sorted from the most frequently mentioned to the least frequent. The categorization was done by separating the standards, procedures, tools and other resources.

Table 12: Cybersecurity standard and other resources

#	Answers	Response Frequency	Category
1	NIST (CSF, SP 800)	29 %	Standards/Norms
2	ESA (E40, Q80 + Handbook)	29 %	Standards/Norms
3	IEC 62443 (for control systems)	19 %	Standards/Norms
4	ISO 27000 Family (27001 and 27002)	19 %	Standards/Norms
5	NASA (STD-8739.8B, STD-2601, STD-1006A, among others)	14 %	Standards/Norms
6	CWE Top 25	14 %	Other Resources
7	MITRE tools - ATT&CK, Engage, D3FEND, CALDERA	10 %	Tools
8	CCSDS	5 %	Standards/Norms
9	CLC/TS 50701	5 %	Standards/Norms
10	ISO 21434	5 %	Standards/Norms
11	DO-326 (aviation cybersecurity)	5 %	Standards/Norms
12	Railways EN50129 and EN50701	5 %	Standards/Norms
13	SEI secure coding standards	5 %	Standards/Norms
14	SANS CWE Top 10	5 %	Other Resources
15	CyBOK	5 %	Processes
16	EITCA/IS IT Security Academy	5 %	Standards/Norms
17	CLOUD SECURITY ALLIANCE	5 %	Standards/Norms
18	**Cryptography techniques** - Handshake, private key exchange, identification of persons with challenges, etc.	5 %	Processes
19	OWASP resources	5 %	Other Resources

Figure 10 depicts the distribution of cybersecurity resources identified by space engineers according to four main categories: Standards/Norms, Processes, Tools and Other Resources.

- **Standards/Norms**: This category received the most mentions, showing a strong emphasis on adhering to proven cybersecurity guidelines and best practices specifically tailored for the space sector. Examples include recent revisions to ESA's E40 and Q80 standards to

incorporate cybersecurity aspects, and NASA's STD-8739.8B and STD-2601 standards.

- **Processes**: One of the processes mentioned is CyBOK (Cybersecurity Body of Knowledge) [67], a project by the University of Bristol that catalogs existing cybersecurity knowledge to enhance accessibility and education within the cybersecurity community.
- **Tools**: This category encompasses a variety of cryptography techniques used to protect data at rest (stationary) and in transit, such as handshakes and private key exchange. It also includes a reference to MITRE, particularly the ATT&CK framework [68]. ATT&CK and related tools (Engage [69], D3FEND [70], and CALDERA [71]) provide a knowledge base of adversary tactics, countermeasures, and framework to automated security assessments.
- **Other Resources**: Finally, this category includes references to OWASP resources [72] and top vulnerabilities listed by CWE (Common Weakness Enumeration) [64].

Overall, Figure 10 highlights the importance of a multi-layered approach to cybersecurity in space systems. This approach combines established standards, knowledge resources, and practical tools to address potential threats.

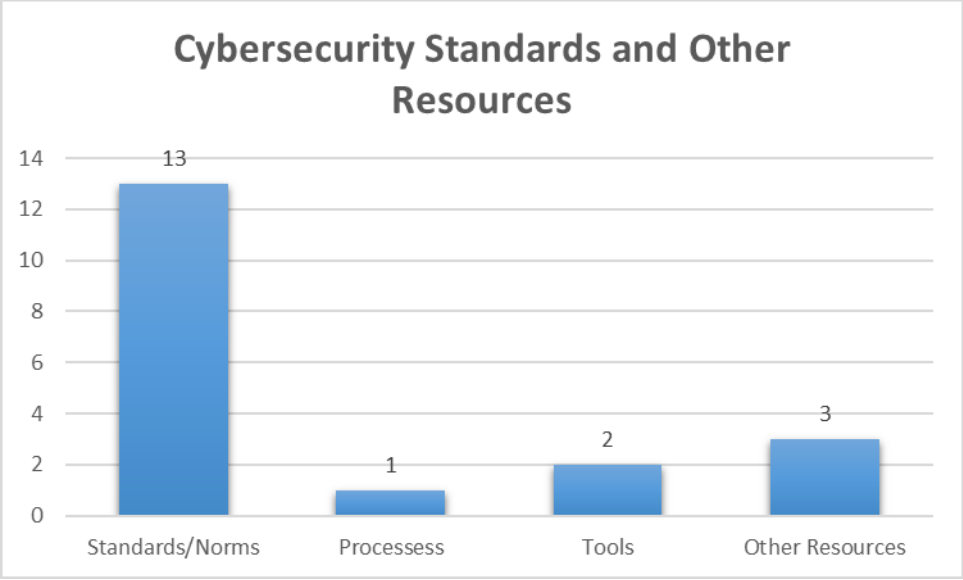


Figure 10: Cybersecurity standards and other resources categories

The survey data revealed the following top 5 most frequently cited cybersecurity standards and resources identified by experts:

- **NIST Cybersecurity Framework** (CSF) [65] and Special Publication 800 (SP 800) series: These resources provide a comprehensive approach to managing cybersecurity risk.

- **ESA standards E40** [7] **and Q80** [8], and accompanying Handbook: These European Space Agency standards focus on space systems and projects.
- **IEC 62443** (for control systems) [53]: This International Electrotechnical Commission standard addresses the specific security needs of industrial control systems.
- **ISO 27000 Family** [31] (including standards 27001 and 27002): This international standard offers a framework for implementing an Information Security Management System (ISMS).
- **NASA standards** [27] STD-8739.8B, STD-2601, STD-1006A, and others: These NASA-specific standards provide guidance for secure software development and secure coding practices.

These standards are a well-rounded selection, covering a variety of industries:

- The inclusion of IEC 62443 shows the importance of specialized standards for control systems.
- The ISO 27000 family provides a comprehensive approach to organizational cybersecurity posture.
- NIST publications are at the forefront of data security through robust cryptographic practices.

It is important to note that the survey also identified relevant standards from other sectors like aviation, automotive, and railway, indicating the growing emphasis on cybersecurity across various industries.

3.8 Most Vulnerable Segment

As shown in Section 2.2.1, Figure 2 depicts a simplified architecture of a space system. Each component within this architecture is considered a potential attack vector. Additionally, these components are often designed, manufactured, operated, and supported by different entities, introducing supply chain vulnerabilities.

The Space sector is generally comprised by four segments: **Ground**, **Link**, **Space**, and **User**. This segmentation is most found in American papers. The European Space Agency (ESA) combines the User and Ground segments into one, resulting in a three-segment system: **Ground/User**, **Link**, and **Space**.

As illustrated in Figure 11, according to the experts, the segment that is considered the most vulnerable to cyberattacks/cyberthreats is the ground segment due to the accessibility and existing interfaces, therefore more exposure exists to all kind of attacks (e.g., social engineering, unauthorized access), followed by the link/signal segment, which can also be access through the first one and that allows control of the satellites or unauthorized access to data.

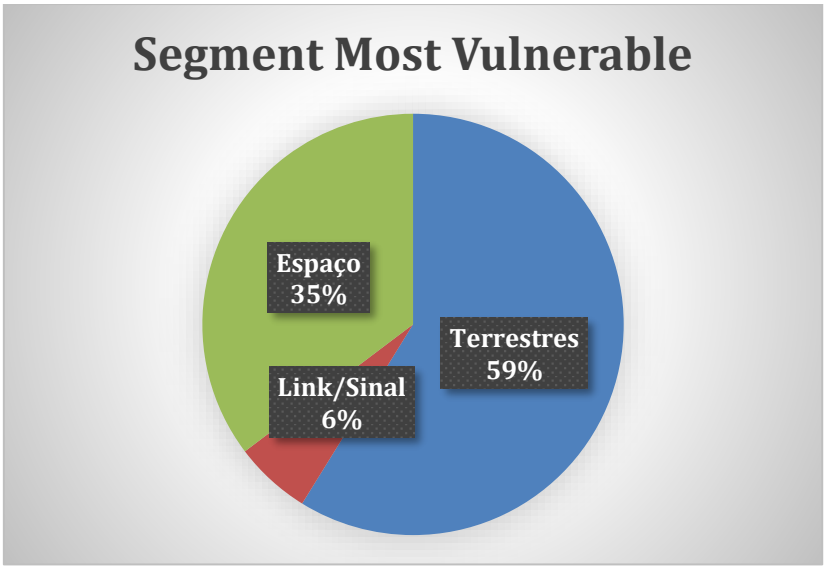


Figure 11: Segment most vulnerable results

3.9 Future Cybersecurity Concerns/Trends

Table 13 presents the 19 cybersecurity concerns and trends identified by the experts, sorted from the most frequently mentioned to the least frequent. The categorization of each concern/trend was developed for this report, as follows:

- Technological Evolution: This category includes concerns related to the rapid pace of technological change and the need for space systems cybersecurity to keep up with these changes.
- Training/Awareness: This category includes concerns related to the need for better training and awareness programs for space system players and other personnel involved in space system development in what concerns cybersecurity impacts.
- Regulatory – Political: This category includes concerns related to the role of government regulations and policies in shaping cybersecurity for space systems.
- Policy: This category includes concerns related to the need for clearer policies and guidelines around cybersecurity for space systems, including issues related to data sharing, incident response, and risk management.

Table 13: Future cybersecurity concerns/trends identified

#	Answers	Response Frequency	Category
1	Artificial Intelligence and Machine Learning use in cyber war.	33 %	Technology Evolution

#	Answers	Response Frequency	Category
2	Technical teams' acquaintance with cybersecurity concepts, analyses, and requirements. e.g. (1) Average programmer / architect not informed enough about cybersecurity and cryptography.	14 %	Training / Awareness
3	Political or geopolitical issues, causing cyberwarfare by powerful states/anarchists and climate fundamentalist movements	14 %	Regulatory - Political
4	Space debris and physical attacks (e.g. ASAT)	14 %	Regulatory - Political
5	Cybersecurity certification/legislation might become necessary (as for functional and safety)	10 %	Policy
6	International cooperation (especially in what concerns standards, best practices, methods, and tools)	10 %	Training / Awareness
7	The deployment of cybersecurity measurements may be cumbersome for the developers if not done properly	5 %	Training / Awareness
8	Security risk analysis is very important and needs to be fully documented	5 %	Policy
9	Threats Analysis should be performed and maintained like Hazard Analysis for safety critical systems.	5 %	Policy
10	Security shall be considered as a property of the system, as safety is considered today and thus part of the functional system	5 %	Training / Awareness
11	"Security is not an option" thus appropriate and formal processes need to be in place, as well as standards, testing, assessment…	5 %	Training / Awareness
12	Reuse of code - We tend to reuse more and more code, that sometimes is not developed according to the corresponding standards.	5 %	Policy
13	Autonomous systems	5 %	Technology Evolution
14	Tools need to be developed for both development and especially for testing cybersecurity requirements.	5 %	tools
15	IoT and emerging behaviours will clearly be targeted by hackers	5 %	Technology Evolution
16	We will only move forward in cybersecurity assurance when some large accident or incident happen. (reactive attitude)	5 %	Training / Awareness

#	Answers	Response Frequency	Category
17	Secure satellite communications (encrypted, protections against DoS, jamming or spoofing)	5 %	Technology Evolution
18	Supply chain security (development and V&V, use of static code analysis, threats and vulnerabilities analysis, use of expert's involvement, e.g. security specialists, security requirements specialists, penetration testers …)	5 %	Policy
19	A dedicated ECSS standard to deal with cybersecurity requirements, covering for example: 1. Training and awareness 2. Analysis (threat and vulnerability analysis as contribution to requirements baseline) 3. Security Requirements incorporated in Technical Specifications 4. Secure Design principles 5. Secure Coding (including secure coding rules) 6. Security V&V 7. Acceptance/Qualification/Certification 8. Security Updates / Maintenance 9. Documentation 10. Methods / Processes / Tools	5 %	Policy

As illustrated in Figure 12, the survey responses highlight a key concern among space engineers: the need for reinforced training and awareness of cybersecurity. Additionally, there is a strong emphasis on the importance of developing stricter standards that provide clear and robust security requirements.

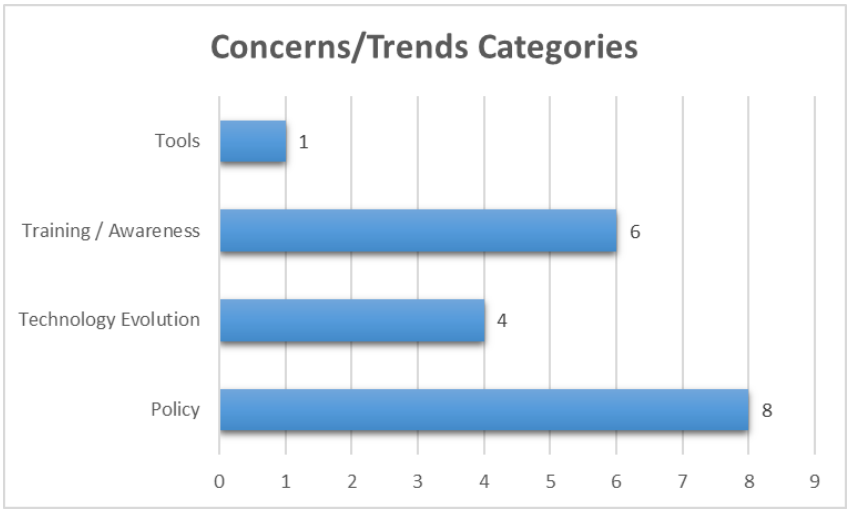


Figure 12: Concerns/Trends categories

The survey revealed a number of key cybersecurity concerns and trends named by space engineers/researchers. The top five most often cited issues are:

- **Integration of Artificial Intelligence (AI) and Machine Learning (ML) into cyberwarfare tactics:** Experts expressed significant concern about the potential use of AI and ML for malicious purposes.
- **Technical teams' lack of familiarity with cybersecurity concepts:** The survey highlighted a need for improved training and awareness of cybersecurity best practices among technical teams. This includes areas like vulnerability analysis, threat mitigation, and secure coding practices. (e.g., Average programmers and architects might not be informed enough about cybersecurity and cryptography).
- **Political and geopolitical motivations for cyberwarfare:** The survey showed concerns about cyberattacks launched by powerful states, anarchist groups, or climate activist movements.
- **Space debris and physical attacks (e.g., Anti-Satellite Weapons):** The possibility of physical attacks on space infrastructure through debris or dedicated anti-satellite weapons was also raised as a concern.
- **Need for stricter cybersecurity regulations and certifications:** Like functional safety standards, experts believe that there may be a need for mandatory cybersecurity certifications or legislation to enforce robust security practices.

The survey identified other issues raised by the experts. One of those issues was the proposal for a dedicated ECSS standard to cover cybersecurity implementation in space systems. This aligns with item 19 of the survey responses, highlighting the importance of establishing clear guidelines to mitigate cyber risks. Additionally, experts emphasized the need for a cultural shift towards security. Space systems should prioritize cybersecurity as a fundamental property, not an afterthought (security-by-design). This requires integrating security considerations throughout the entire development process, including adhering to established standards and best practices as mentioned in items 10 and 11 of the survey.

3.10 DASIA Paper

A scientific paper entitled "Engineering and Assessing Cybersecurity for Space Systems," [15] derived from the findings of a cybersecurity survey, was authored and submitted, in February, to the Eurospace DASIA 2024 conference in Croatia, the preeminent industrial conference in the domain of European space data. The paper was presented by Dr. Nuno Silva, on May 28th, 2024 (Software session), and was well-received by the audience at the presentation. The audience has shown interest by requesting more information about the outcomes of the cybersecurity survey and by providing immediate feedback based on their industrial experience, this feedback was fully aligned with the collected data from the cybersecurity survey [14] that was only concluded after the mentioned conference.

3.11 Conclusions

The survey has confirmed the critical need for robust cybersecurity measures in space systems. The research highlights a concerning reality: real threats and vulnerabilities exist, and they pose a significant risk to these increasingly crucial and critical pieces of infrastructure.

The findings underscore the importance of integrating cybersecurity considerations throughout the entire development lifecycle, from the initial design to the verification and validation (V&V). This requires a collaborative effort among stakeholders in the space domain, ensuring that the critical infrastructure receives the necessary protection.

Given the ever-evolving nature of cyber threats and the nascent field of space cybersecurity, ongoing research and collaboration are even more crucial. By addressing potential limitations and fostering international cooperation, the space industry can build a future where critical space systems are secure and resilient.

These findings and insights from the cybersecurity literature was an asset to recommend adjustments and advancements to the existing space standards, particularly those established by ECSS which apply to the European space community, presented at Chapter 5.

4 SPACE SYSTEMS THREATS AND VULNERABILITIES

Like any other system, space systems are susceptible to both deliberate and inadvertent threats and vulnerabilities. The consequences of these risks can be wide-ranging, ranging from operations disruption and data integrity compromise to, in severe situations, endangering human life.

We can help resolve these problems and improve the cybersecurity of space systems by recognising and mitigating these threats and vulnerabilities.

So far, we have made progress on the first two internship objectives (Section 1.2): (1) Collect and Analyse State-of-the-Art Data and (2) Engage with Key Stakeholders. The completion of the cybersecurity survey marks the completion of the second objective. This chapter delves into the presentation of threats, threat actors, and vulnerabilities identified in the space sector through expert surveys and literature reviews, which aligns with the first internship objective.

4.1 Threats

A threat or cyberthreat is the possibility that a threat actor will impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals, by taking advantage of a space system's weakness, through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service [73].

Due to their widespread use, space systems are vulnerable to attacks from a variety of sources, ranging from amateur hackers to nation-state actors.

This heightened vulnerability has been exacerbated by the recent entry of private businesses into the space industry, including Jeff Bezos' Blue Origin and Elon Musk's SpaceX. Newer issues are brought about by the quick rise of new actors, some of which may lack the security expertise of more established ones.

The origins of new threats can be explained by four factors [74]:

- **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 13. 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.

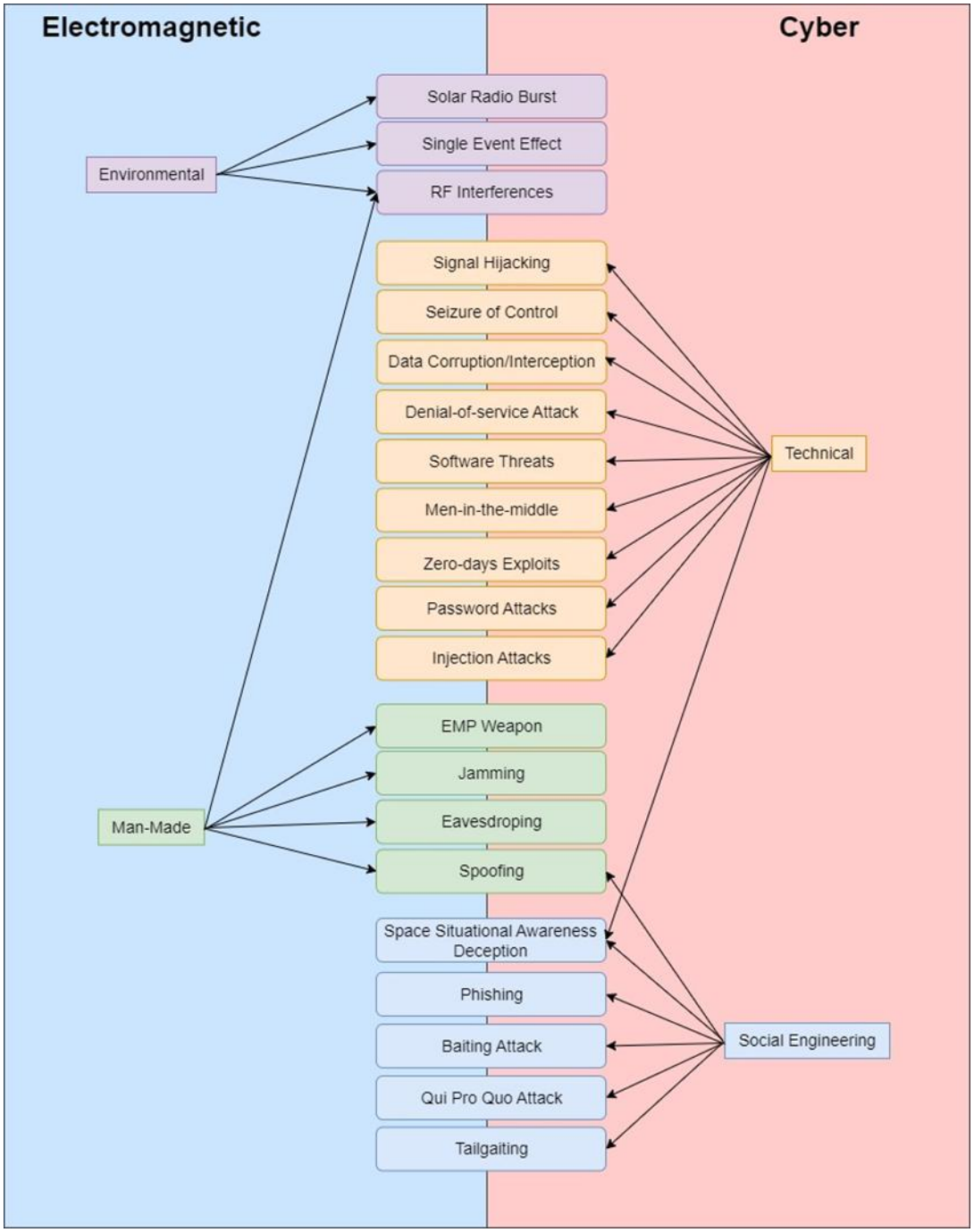


Figure 13: Digital Security Threats based on [19]

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.

Threat actors are shown in Table 14 along with their corresponding methods, skill levels, and goals to demonstrate the diversity of potential cybersecurity attacks.

Table 14: Threat actors behind the attacks

Threat Actor	**Description**	**Motivation**	**Skill** [75]	**Tactics**
Amateur Hackers	Threat actors who target systems to test their cyber skills and mostly for their enjoyment. [76]	Personal motivations	Low	Pre-existing tools and techniques
Cybercriminals	Individuals or groups that target computer systems for financial gain. [77]	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. [77]	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. [76]	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. [76]	Ideological or Political Religion	High	Social engineering, DoS, malware, SQL injection, Man-in-the-Middle attacks, and Stuxnet-like attacks. [78]
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. [76]	State-cyber espionage Technology Theft Geo-Political	Very High	Cyber warfare

As expected, since the rise of the digital era, the number of cyber incidents in space sector has increased exponentially, as shown in Figure 14. There has been a clear

trend of increasing cyber-capabilities, targeting space infrastructures, along with a rise in the number of actors capable of carrying out attacks. In the present day, nearly 30 states have demonstrated some degree of cyber-offensive counterspace capabilities [17].

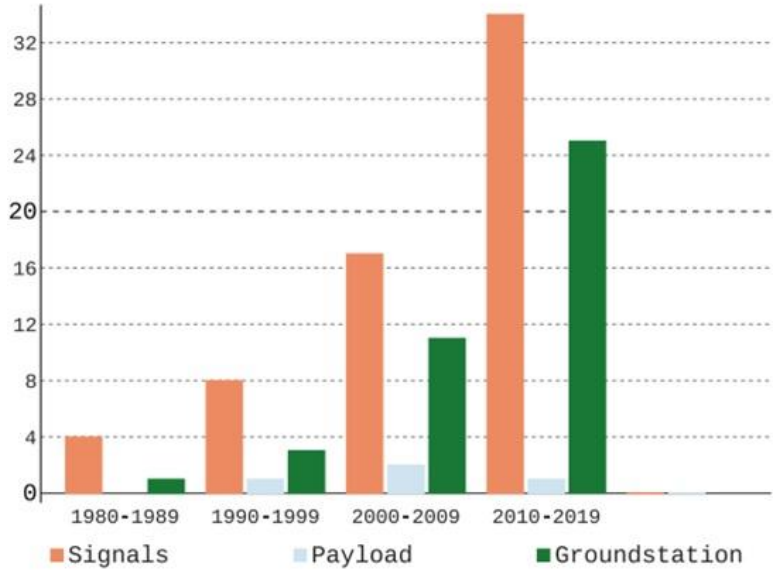


Figure 14: Target Segments by Decade based on [17]

The cyber incidents mentioned above occur for a variety of reasons. These reasons range from political motives to technological theft, espionage, or simply to spread terror. Figure 15 shows the number of incidents for each type of motivations, from 1980 to 2019. For more details about the incident reasons see [18].

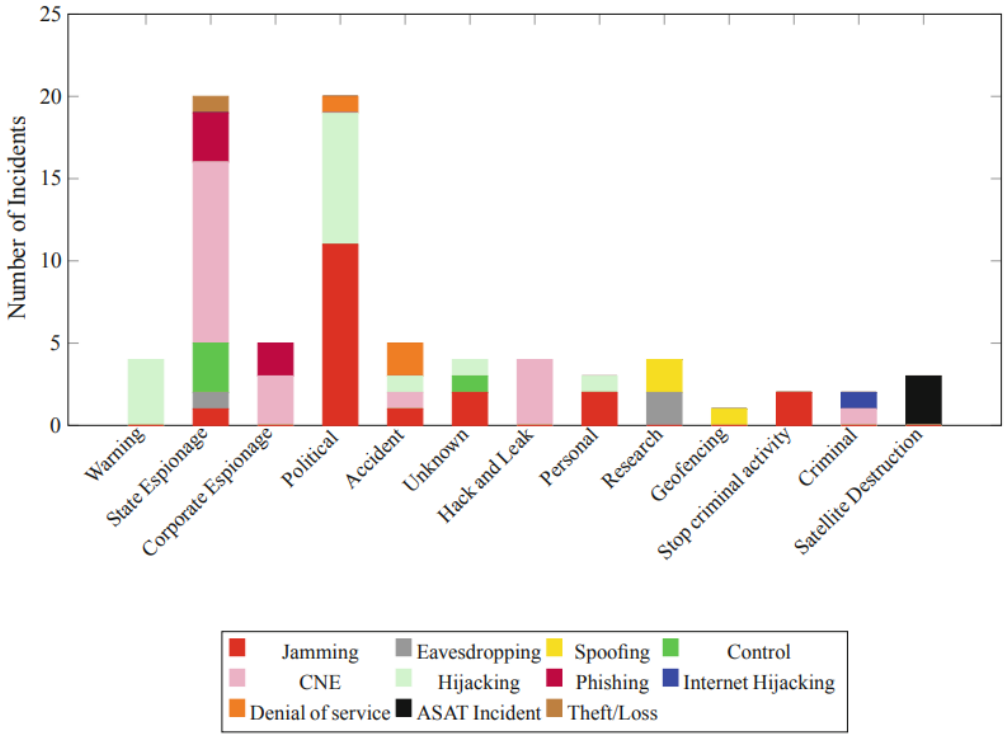


Figure 15: Motive and type of Satellite Incidents [18]

No matter what motivation is behind a cyberattack, 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 Anti-Satellite (ASAT) attack would result in the destruction of the entire satellite/satellite constellation. Figure 16 depicts the range of effects caused by some threats.

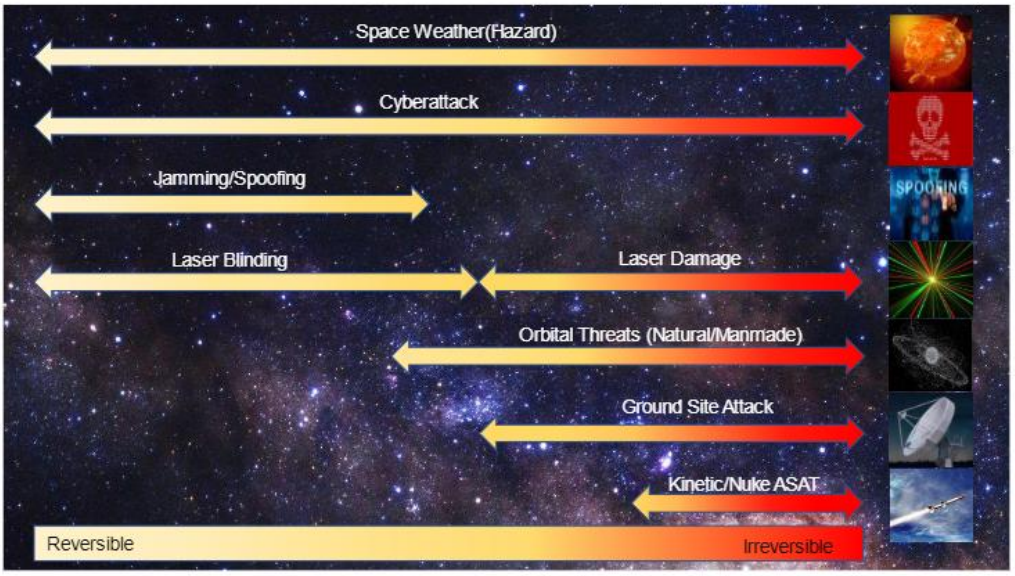


Figure 16: Range of effects cause by threats [23]

Some of these threats will be explained in the following subsections.

4.1.1 Electromagnetic Threats

Electromagnetic threats to space infrastructures 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**.

4.1.1.1 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.

T1 - 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 17. 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 to one of the GPS frequencies, the L2 frequency[1], and implementing new civilian codes, enhancing the stability and reliability of GNSS operations [79].

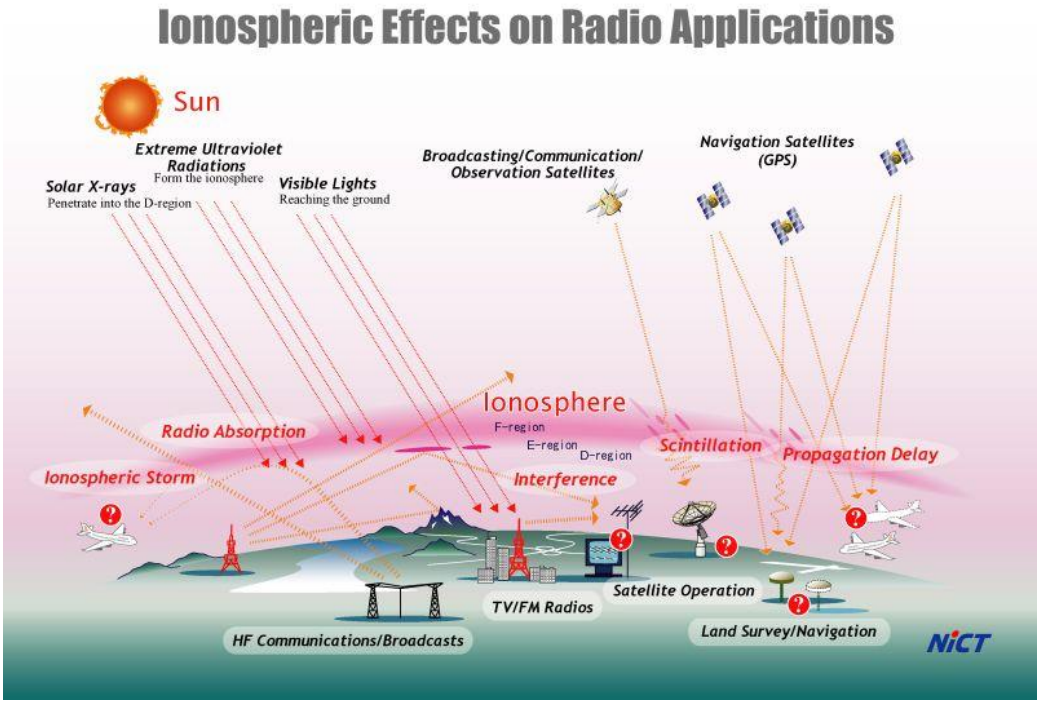


Figure 17: Solar radio burst effects on Space Infrastructure [80]

On the 6th of September 2017, the Sun expelled X-class flares that caused a coronal mass ejection (auroras) on Earth, affecting the performance of GNSS signals [81].

T2 - 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 [24]:

- **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

[1] The L2 frequency was implemented after the L1. It also has a military code and a civilian use code. The L2 uses the frequency 1227.60 MHz, which is faster than the L1. This allows the signal to better travel through obstacles such as cloud cover, trees, and buildings (more on obstacles here).

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.
- **Latch-up**: 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.

4.1.1.2 Man-Made

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

T3 - 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 18 depicts two primary types of jamming that can disrupt satellite communications [26]:

- **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.

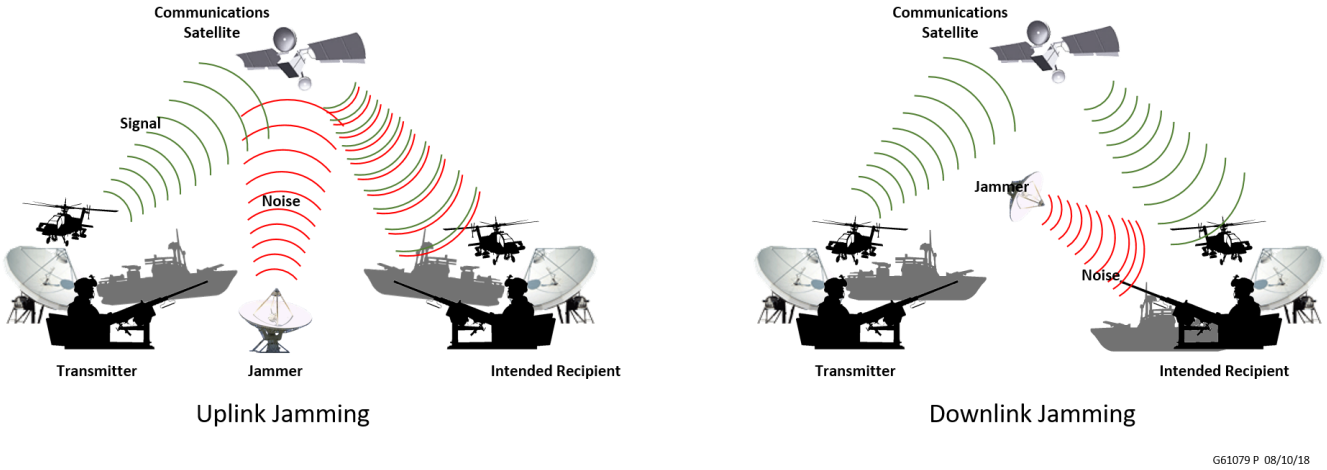


Figure 18: Jamming Threat [82]

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 caused delays in flights [83].

T4 - 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"** [74]. This involves broadcasting a copy of the signal that is either out of time or with corrupt

data, depicted in Figure 19. 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.

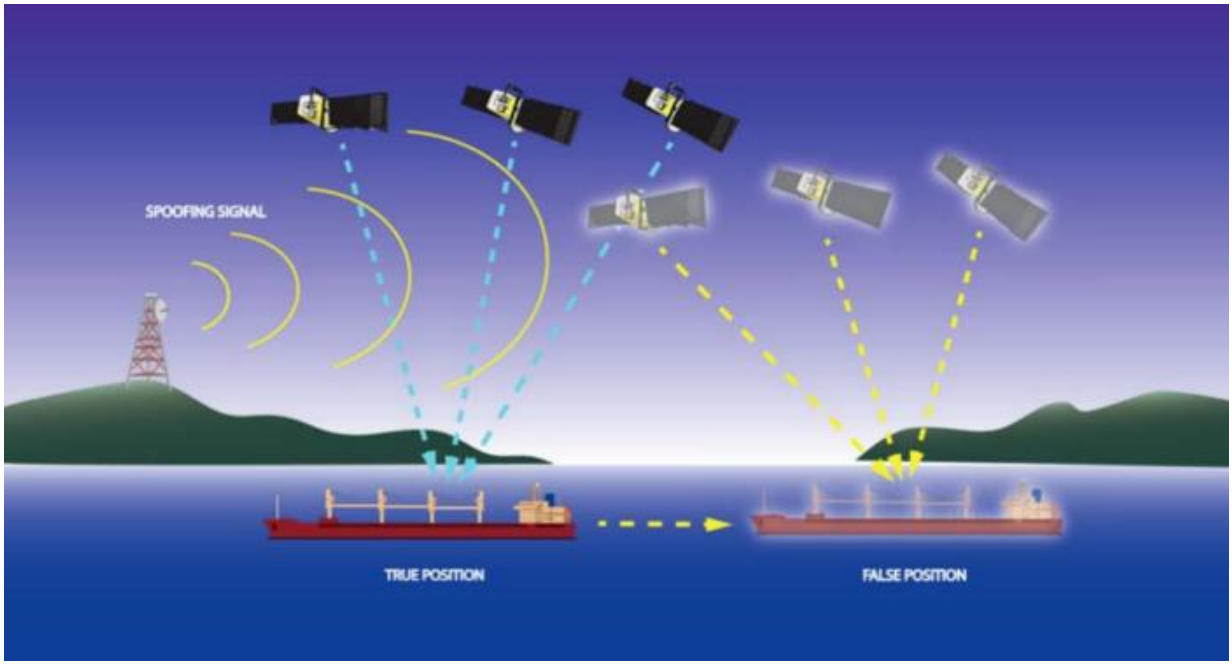


Figure 19: Spoofing threat [84]

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 [85].

T5 - Eavesdropping

Another electronic threat to consider is **eavesdropping**. This involves intercepting signals from satellites or other sources for monitoring purposes, as depicted in Figure 20. 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.

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 [86].

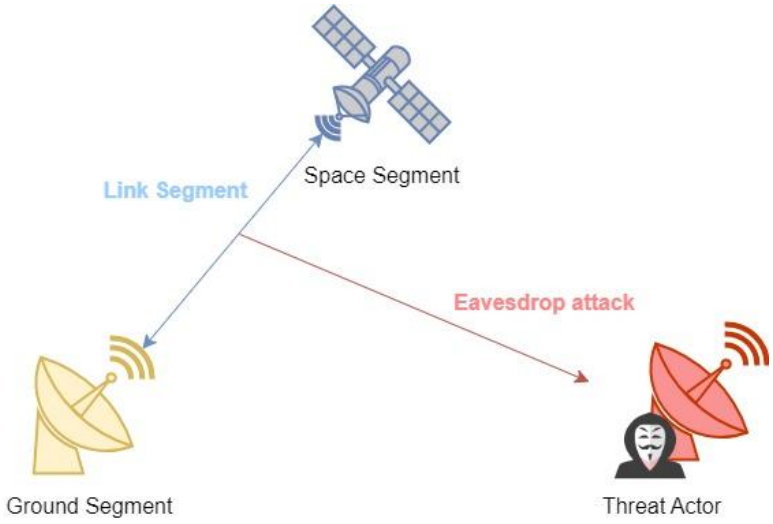


Figure 20: Eavesdrop attack on satellite communications

4.1.2 Cyber Threats

This type of threats 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**.

4.1.2.1 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.

T6 - 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, as depicted in Figure 21. This threat does not have a very steep learning curve and do not need significant resources to execute.

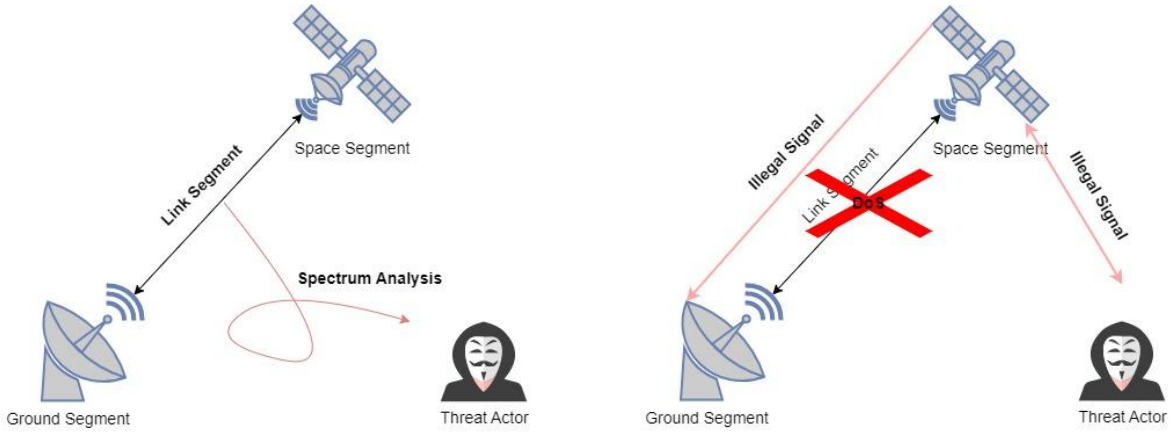


Figure 21: Spectrum analysis and Signal hijacking

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 [87].

T7 - 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 [19]. 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.

T8 - Denial-of-Service Attack

This attack method, known as a Denial-of-Service (DoS) or Distributed Denial-of-Service attack (DDoS) attacks, as illustrate in Figure 22, 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.

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 [88].

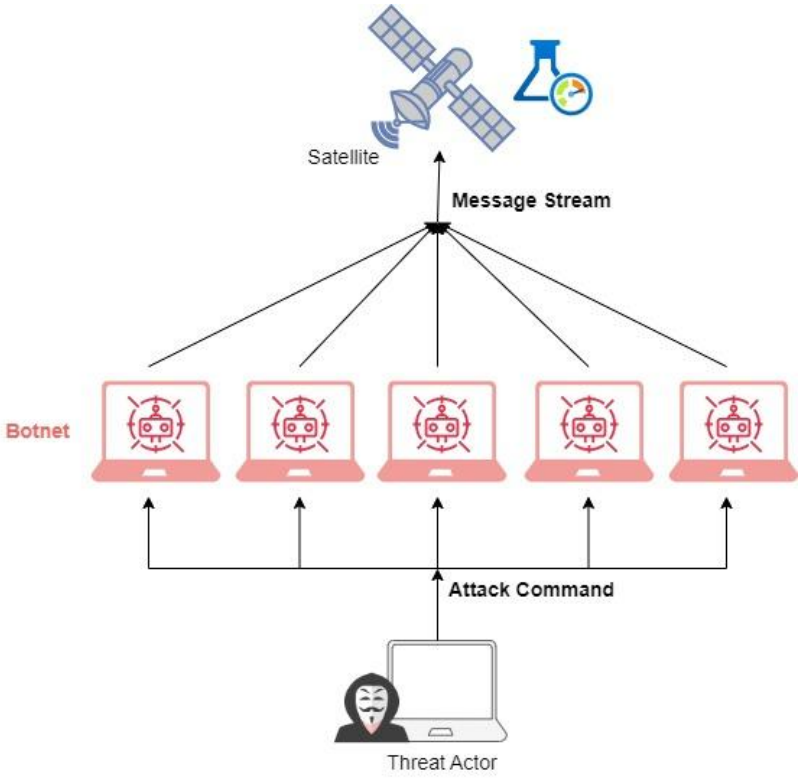


Figure 22: Illustration of a Distributed Denial-of-Service attack (botnet)

T9 - 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 [89]. 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.

T10 - Software Threats

The objectives of software threats are to gain control of internal organizational information systems. Once inside, they can access and exfiltrate sensitive information, all while remaining undetected. Malware is a prime example of a

software threat that can pose a significant risk to space systems. Figure 23 presents some examples of malwares.

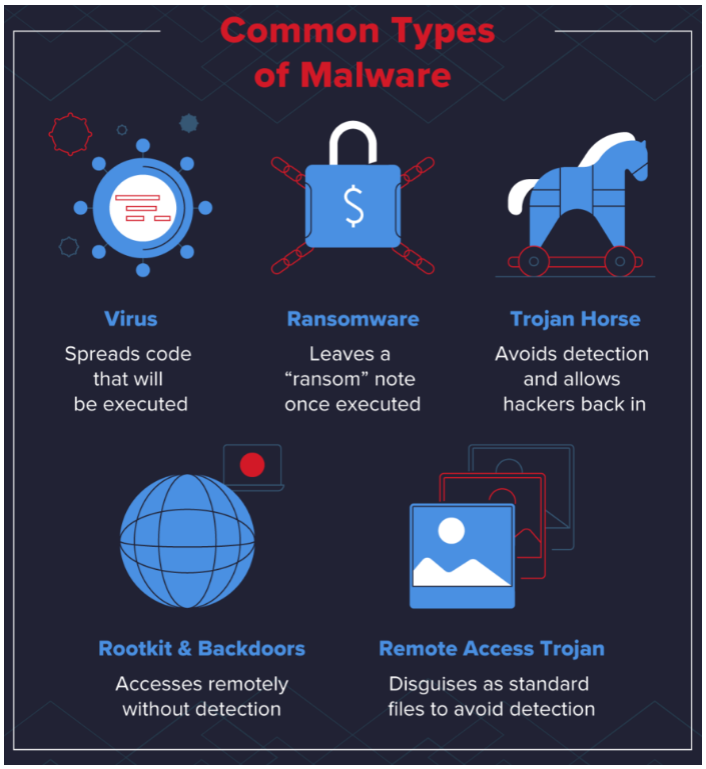


Figure 23: Types of Malware [90]

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 [91].

T11 - 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 [92]. 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.

T12 - 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 [92].

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 analyse past exploit data to set up a baseline for normal system behaviour. 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 [93].

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.

T13 - Password Attacks

Passwords function as the first line of defence, 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 [94].

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 [95].

T14 - 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.

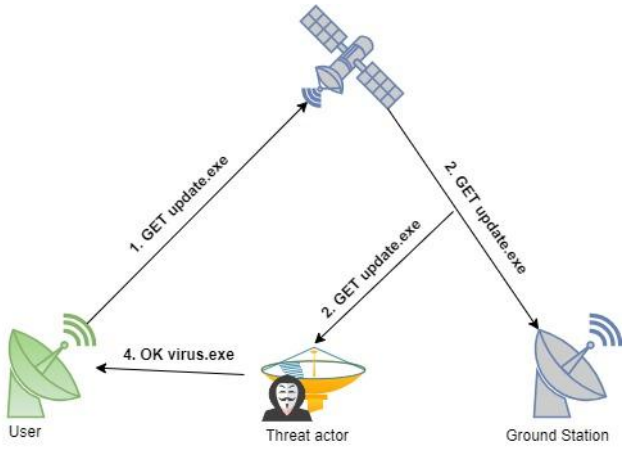


Figure 24: Example of an Injection attack

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 [19].

T15/T22 - Other Technical Threats

The following technical threats (see Table 13) were identified through the cybersecurity survey, presented at chapter 3.

Table 15: Threats identified by the specialists

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.

4.1.2.2 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.

T23 - 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 is 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 [96].

T24 - Baiting Attack

Threat actors place 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.

T25 - 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.

T26 - 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.

T27 - 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.

4.2 Vulnerabilities

A weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability [97]

Some of the primary weaknesses that present a serious risk to space systems are examined in the sections that follow.

4.2.1 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.

4.2.2 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 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.

4.2.3 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 [98]. 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 is 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 [99].

4.2.4 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.

4.2.5 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 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 [26].

4.2.6 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 [100].
- **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 [100].
- **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.

4.2.7 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 [41]:

- **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. The internet is interconnected, allowing for the free flow of information and data across borders.

4.2.8 Static Code Analysis Tools

Without static code analysis tools, developers could unintentionally add flaws to software that would have been detected right away by the SCA techniques. These flaws can then be used by attackers to obtain illegal access, steal information, or interfere with regular business processes.

4.2.9 Security Analysis (Threats and Vulnerabilities)

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

Failing to conduct a proper security analysis 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 assessed 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 is 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.

4.2.10 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, already mentioned in Sections 2.1.2 and 2.1.3, 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 the series of “IEC 62443 Security for industrial automation and control systems”, 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.

4.2.11 Security Design

Security design is a fundamental principle in cybersecurity, that comes after the identification of security requirements. It focuses on incorporating security measures throughout the entire development lifecycle of a system. Neglecting this crucial step has dire 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.

4.2.12 Security Implementation

Once security requirements are defined and the secure design is complete, it is 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 organizations 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 the code for known security weaknesses and bad coding practices, further strengthening the developer's security posture.

4.2.13 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 is 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.

4.2.14 Installation/Operation/Maintenance

Installation, Operations, 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 initiates once the system is completed and 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 is 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 paramount. 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 dire consequences for the organization's security posture.

4.2.15 Other Vulnerabilities

The following vulnerabilities were identified through the cybersecurity survey, presented in chapter 3

A summary of these vulnerabilities is presented in Table 16.

Table 16: Vulnerabilities identified by specialists

Vulnerabilities	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.

Vulnerabilities	Example
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.
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 considerable 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.

5 PROPOSALS TO IMPROVE CYBERSECURITY IN SPACE SECTOR ADDRESSING THREATS AND VULNERABILITIES

This chapter presents mitigations to the threats and vulnerabilities presented in Chapter 4, as well as recommendations to improve the ECSS-E-ST-40C [7] and ECSS-Q-ST-80C [8] standards. These two standards were proposed by Critical Software for analysis and recommendations for improvement because they are the two most relevant when creating space software for the European Space domain. This fulfills the internship objectives three (Propose Mitigations) and four (Produce Scientific Publications), as outlined in Section 1.2.

5.1 Proposals to Cope with Threats and Vulnerabilities

With the threats and vulnerabilities identified in the previous sections (Section 4.1 and 4.2), this new section presents proposals that aims to address these concerns by exploring effective methods to mitigate potential cyber risks of the space sector. By proactively addressing these challenges, we can ensure the continued safe and secure operation of space systems, fostering a more robust and resilient space environment and operations.

5.1.1 Mitigation Strategies for Cybersecurity Threats

Table 17 presents potential threats for the space system and their respective mitigations identified (Chapter 4) in literature and by engineering experts through the cybersecurity survey (Chapter 3).

In the first column ("#") simply numbers each threat for easy reference.

The second column ("Threat") describes the specific threat.

The third and last columns ("Solutions / Mitigations") list the strategies used to protect against each threat listed in the second column. Each strategy is accompanied by a identification that is an abbreviation of the threat that will mitigate.

For more information, Annex B.1 details threats and their respective mitigations.

Table 17: Threats proposed solutions

#	Threat	Solutions / Mitigations
T1	Solar Radio Burst	**SRB-1** – Increase Signal Power & New Civilian Codes
T2	SEE – Burnout	**SEE-1** – Protect Metal-Oxide-Semiconductor
	SEE – Functional Interrupt	**SEE-2** – Power-Cycling

#	Threat	Solutions / Mitigations
	SEE – Gate Rupture	**SEE-3** – Avoid SRAM and EEPROM
	SEE – Latch-up	**SEE-4** – Shutdown Power Supply
	SEE – Multiple Bit Upset	**SEE-5** – Employ Error-Correcting Codes
	SEE – Multiple Cell Upset	**SEE-6** – Increase Spacing.
	SEE – Transient Errors	**SEE-7** – Employ Redundant Techniques
T3	Jamming	**JAM-1** - Time-Frequency Filtering Mask **JAM-2** - Adaptive Notch Filter **JAM-3** - Short-Time Fourier Transform (STFT) **JAM-4** - ACM and DWT Filtering **JAM-5** - Spatial Filtering, Polarization Diversity, and Adaptive Adjustment **JAM-6** - Spectral Self-Coherence Beamforming **JAM-7** - Spatial-Temporal Interference Projection **JAM-8** - Regret Minimization Framework & Game-Theoretical Approach
T4	Spoofing	**SPOO-1** - Navigation Message Authentication (NMA) **SPOO-2** - Chips Message Robust Authentication (CHIMERA) **SPOO-3** - Timed Efficient Stream Loss-tolerant Authentication (TESLA) **SPOO-4** - Cross sensor´s information **SPOO-5** - Y-code **SPOO-6** - C/N0 Monitoring **SPOO-7** - Absolute Power Monitoring
T5	Eavesdropping	**EAV-1** - On-Board Encryption **EAV-2** - New Cryptographic techniques
T6	Signal Hijacking	**SH-1** - Spread Spectrum **EAV-1** - On-Board Encryption **EAV-2** - New Cryptographic techniques

#	Threat	Solutions / Mitigations
T7	Data Corruption and Interception	**DC&I-1** - Advanced Encryption Standard (AES) **DC&I-2** - Triple Data Encryption Standard (3DES) **DC&I-3** - Rivest-Shamir-Adleman (RSA) **DC&I-4** - Elliptic Curve Cryptography (ECC) **DC&I-5** - Secure Hash Algorithm (SHA) **DC&I-6** - Intrusion Detection and Prevention Systems
T8	Denial-of-Service	**DoS-1** - Traffic Filtering and Rate Limiting **DoS-2** - Intrusion Detection and Prevention Systems (IDPS) **DoS-3** - Geolocation Filtering **DoS-4** - Hardening Satellite Software and Firmware **DoS-5** - Redundancy and Failover Mechanisms **DoS-6** - Use DDoS-resistant services **DoS-7** - Distribute servers geographically and topologically **DoS-8** - Configure firewalls and routers to drop Internet Control Message Protocol (ICMP) packets and block DNS **DoS-9** - Protect DNS servers
T9	Web Spoofing	**WS-1** - Use Strong Authentication **WS-2** - Securely Store Secrets **WS-3** - Protect Credentials During Transmission **WS-4** - Secure Authentication Cookies with SSL/TLS **WS-5** - Implement Packet Filtering **WS-6** - Avoid Host-based Authentication **WS-7** - Use HTTPS **WS-8** - Filter ICMP packets **WS-9** - Use Random Sequence Numbers and Reduce Initial TTLs (Time-to-Live) **WS-10** - Employ Encryption **WS-11** - Avoid Authentication based Solely on IP

#	Threat	Solutions / Mitigations
T10	Software Threats	**ST-1** - Keep software, internet browser, and operating system up to date
		ST-2 - Use Safe Search Tools
		ST-3 - Use Security Software and Antivirus
		ST-4 - Install NoScript (or a similar extension) on browser
		ST-5 - Acceptance Testing
		ST-6 - System Evaluation
		ST-7 - Continuous Threat Monitoring, Continuous Risk Management
		ST-8 - Run-Time Security Monitoring
		ST-9 - Auditing
		ST-10 - Supply Chain Confidence
T11	Man-in-the-Middle	**MITM-1** - Avoid using Wi-Fi connections that are not password-protected
		MITM-2 - Avoid using public networks for sensitive transactions
		MITM-3 - Log out of applications immediately when not in use
		MITM-4 - Use strong encryption, such as a VPN
T12	Zero-days Exploits	**ZDE-1** - Vulnerability Databases
		ZDE-2 - Machine Learning for Anomaly Detection
		ZDE-3 - Space System Information Sharing and Analysis Center (ISAC)
T13	Password Attacks	**PA-1** - Passkeys
T14	Injection Attacks	**IATT-1** - Apply the principle of least privilege
		IATT-2 - Avoid dynamic SQL
		IATT-3 - Validate input data
T15	Source Code Tampering	**SCT-1** - Extensive code analysis
		SCT-2 - Zero code smells and zero warnings objective
		SCT-3 - Protection of software development environments
		SCT-4 - Extensive V&V
		SCT-5 - Specific security assessment of the design/code
		SCT-6 - Integrity checks

#	Threat	Solutions / Mitigations
T16	Spacecraft Configuration Modification	**SCM-1** - Intrusion detection mechanisms **SCM-2** - Robust FDIR configuration **SCM-3** - Proper authentication methods and access control **SCM-4** - CRCs for all data transmission **SCM-5** - Give an ID to every entity in the system **SCM-6** - Telecommands acceptance is subject to validation **SCM-7** - Periodically change the CRC/checksum/cryptography algorithms **SCM-8** - Authentication on software patch **SCM-9** - Accept telecommands and download telemetry only when flying above certain regions
T17	Bad Design	**BD-1** - Secure-by-design approach **BD-2** - Take security lessons **BD-3** - Every user involved in activities related to the project shall be subjected to user authentication
T18	Speed Up Development / Pressure	**SUD/P-1** - Good and Secure Development Practices
T19	Lack of Certification	**LCSS-1** – Have a Comprehensive Certification Processes that Include Cybersecurity Aspects
T20	Lack of Vulnerability / Threat Analysis	**LV&TA-1** - Awareness trainings **LV&TA-2** - Security testing **LV&TA-3** - Enforcing security standards **LV&TA-4** - Conducting independent regular security audits **LV&TA-5** - Ensure a SDLC is integrated in the application development **LV&TA-6** - Training on security aspects, V&V **LV&TA-7** - Check of OSS libraries vulnerabilities **LV&TA-8** - Vulnerability / Threats Analysis done before requirements are closed **LV&TA-9** - Security reviews
T21	Exploit Development Tools	**EDT-1** - Security reviews **EDT-2** - Check of OSS libraries vulnerabilities **EDT-3** - Robustness testing **EDT-4** - Do a deep analysis and test all interfaces (Zero Trust model) **EDT-5** - Conducting independent regular security audits **EDT-6** - Security testing

#	Threat	Solutions / Mitigations
T22	Unmitigated Errata	**UE-1** – Errata Analysis **UE-2** – Security Reviews
T23-27	Social Engineering	**SE-1** - Awareness and Training **SE-2** - Technical Controls **SE-3** - Policies, Procedures, and Governance **SE-4** - Incident Response and Reporting

5.1.2 Mitigation Strategies for Cybersecurity Vulnerabilities

Table 18 presents potential vulnerabilities for the space system and their respective mitigations identified (Chapter 4) in literature and by engineering experts through the cybersecurity survey.

The first column ("Vulnerability") describes the specific vulnerabilities.

The second and last columns ("Solutions / Mitigations") list the strategies used to protect against each threat listed in the first column.

For more information, Annex B.2 details the vulnerabilities and their respective mitigations.

Table 18: Vulnerabilities proposed solutions

Vulnerability	Solutions / Mitigations
Human Factor	Social Engineering mitigations: **SE-1** - Awareness and Training **SE-2** - Technical Controls **SE-3** - Policies, Procedures, and Governance **SE-4** - Incident Response and Reporting
Development Life Cycle	**SSDLC-1 -** Microsoft Security Development Lifecycle **SSDLC-2 -** Software Security Touchpoints **SSDLC-3 -** Software Assurance Forum for Excellence in Code (SAFECode) **SSDLC-4 -** NIST Secure Software Development Framework

Vulnerability	Solutions / Mitigations
Supply Chain	**SC-1** - Enforce Cybersecurity Requirements **SC-2** - Supply Chain Risk Management **SC-3** - Obtain Products from Trusted Suppliers **SC-4** - Component Maintenance **SC-5** - Software Bill of Materials **SC-6** - Harden the Build Environment **SC-7** - Promoting Security in Government Contracts **SC-8** - Regulatory Framework for Private Sector Activities **SC-9** - Use of Advanced Technology
Commercial-off-the-Shelf	**COTS-1** – Security Analysis
Technological Evolution	**TE-1** - Software-Defined Radio **TE-2** - Cloud Computing **TE-3** - Optical Communication **TE-4** - Quantum Key Distribution **TE-5** - Ground Station as a Service
Static Code Analysis Tools	**SCA-1** - Static Code Analysis
Security Analysis	**SA-1** - Threat Modelling **SA-2 -** Network Security Monitoring **SA-3** - Vulnerability Scanning **SA-4** - Penetration Testing **SA-5** - Input Validation **SA-6** - Independent Regular Security Audits **SA-7** - Fuzz Testing **SA-8** - Static Code Analysis **SA-9** - Security Testing
Security Requirements	**SR-1** - Security Requirements Analysis

Vulnerability	Solutions / Mitigations
Security Design	**SD-1** - Economy of Mechanism **SD-2** - Fail-Safe **SD-3** - Complete Mediation **SD-4** - Open Design **SD-5** - Separation of Privilege **SD-6**- Least Privilege **SD-7** - Least Common Mechanism **SD-8** - Psychological Acceptability **SD-9** - Work Factor **SD-10** - Compromise Recording
Security Implementation	**SI-1** - Code Reviews **SI-2** - Threat Modelling **SI-3** - Security Testing
Security Testing	**SecT-1** - Security Requirements Testing **SecT-2** - Threat Mitigation Testing **SecT-3** - Vulnerability Testing **SecT-4** - Penetration Testing **SecT-5** - Independence of Testers
Installation/Operation/Maintenance	**IOM-1** - Security Checks **IOM-2** - Secure Configuration and Integration **IOM-3** - Access Controls and Authentication Mechanisms **IOM-4** - User Training **IOM-5** - Monitor System **IOM-6** - Regular Updates **IOM-7** - Routine System Maintenance **IOM-8** – Security Patches **IOM-9** - Regular Vulnerability Assessments **IOM-10** - Incident Response Plans

Vulnerability	Solutions / Mitigations
Software bugs with security impacts	**SB-1** - Extensive code analysis **SB-2** - Security testing **SB-3** - Extensive V&V of the embedded device against fuzz inputs **SB-4** - Built-in or self-tests to ensure application and data integrity **SB-5** - Perform input validation **SB-6** - Integrity checks for all data, configurations, inputs to the system **SB-7** - Conducting independent regular security audits **SB-8** - Security reviews
Weak development process	**WDP-1** - Ensure a SDLC (Secure Development Life Cycle) is integrated in the application development. **WDP-2** - No agile methodology in security critical development
Read and write operations in memory	**R&W-1** - Robustness testing
Software update	**SU-1** - Authentication on software patch **SU-2** - Enforce patch management
Weak software development protection	**WSDP-1** - Protection of software development environments **WSDP-2** - Every user involved in activities related to the project shall be subjected to user authentication. (Zero Trust model)
Debug ports not protected	**DP-1** - Access to target memories through unprotected debug ports.
Bad code practices	**BCP-1** - Extensive code analysis **BCP-2** - Zero code smells and zero warnings objective
Lack of security acceptance plan	**LSAP-1** - 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	**WSI&DF-1** - More secure information and deliverables flow. **WSI&DF-2** - Use of certified tools
Weak secure boundary parameter	**WSBP-1** - Robustness testing **WSBP-2** - Extensive code analysis
Weak password policies	**WPP-1** - Use cryptographic keys instead of passwords.
High turnover of contractors	**HTC-1** - Create a baseline workforce to be trained in cybersecurity.

Vulnerability	Solutions / Mitigations
Use of dynamic memory	**UDM-1** - Exclude dynamic memory in space systems.
Deserialization of untrusted data	**DUD-1** - Security reviews
Integer overflow of wraparound	**IOW-1** - Extensive code analysis
Improper monitoring in ground and space segment	**IM-1** - Intrusion detection mechanisms **IM-2** - Robust FDIR configuration **IM-3** - Firewall
Poor management of the exchange data	**PMED-1** - Advanced encryption **PMED-2** - Proper authentication methods and access control.

5.2 Proposals to Change/Improve/Integrate Specific Requirements into the ECSS E40 & Q80

This section builds on the previous Sections 5.1.1 and 5.1.2, where space systems threats, vulnerabilities and associated mitigations have been identified/proposed and promotes the exercise of mapping the proposed mitigations to the existing ECSS standards for space software engineering and space software quality assurance (ECSS-E-ST-40C [7] and ECSS-Q-ST-80C [8]). The aim of this section is the proposal of generic requirements of the two mentioned ECSS standards in complement to the current software engineering requirements already listed in those standards.

The proposed recommendations for the ECSS standards (Table 19 and Table 20) have been derived only for the threats and vulnerabilities that are not mitigated in those standards and that are applicable to software (subject of ECSS standards selected for analyses - ECSS-E-ST-40C [7] and ECSS-Q-ST-80C [8]). The tables contain the threats and vulnerabilities mitigation in the first column as presented in Section 5.1 and the proposal for standards requirements in the second column which were developed by the current work.

5.2.1 ECSS-E-ST-40C & ECSS-Q-ST-80C

The European Space Agency objectives are to develop the space capability of the European members and from that share benefits to the citizens of the old continent and the rest of the world.

In what concerns standards, ESA cooperates with the European Cooperation for Space Standardization (ECSS), promoting a coherent set of user-friendly space standards for use by the agency. With regards to cybersecurity, ECSS are including

some requirements in ECSS-E-ST-40C and ECSS-Q-ST-80C, which are still ongoing a public review, particularly, in the case of the second standard.

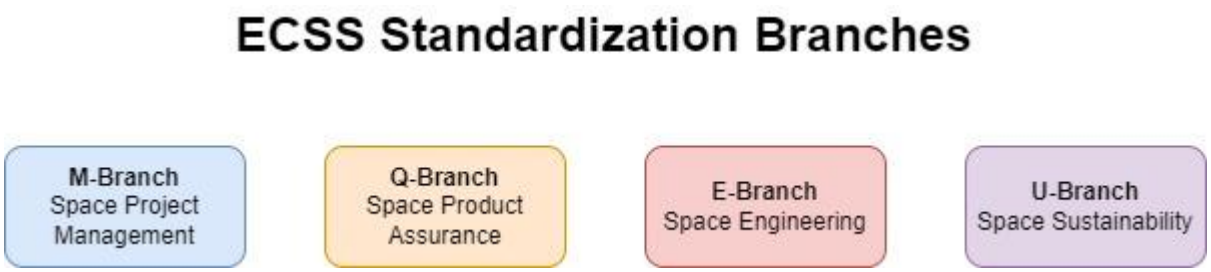


Figure 25: ECSS Standardization Branches

ECSS-E-40 focuses on software that belongs to space systems and is developed within the scope of space projects. Its applicability encompasses all segments of space systems, including space, launch, and ground segments. Furthermore, it covers the entire software engineering lifecycle, including requirements definition, design, production, verification and validation (V&V), installation, operations, and maintenance. This standard has seen a recent introduction of security aspects that will make this standard more robust in cybersecurity. Final publication of the new version is still pending approval at the moment of writing of this report.

Through the Q-80 standard, users leverage a set of software product assurance requirements for developing and maintaining the software component of firmware in space systems, including space, launch, and ground segments [8].

Like the E-40 standard, Q-80 is currently undergoing review, updates and approval to align with ECSS-E-ST-40C and incorporate new software security assurance requirements.

5.2.2 Gap Analyse of the ECSS E40 & Q80

A gap analysis was performed by searching the entire document for mentions of the terms "cybersecurity" and "security" to identify missing elements. Based on the threats, vulnerabilities, and their respective mitigations identified in Section 5.1, generic requirements were derived to address these gaps. The following sections will present those proposed requirements that was missing. It is important to note that not all threats and vulnerabilities were considered, as the scope of these standards is limited to space software development and product assurance.

5.2.3 Safeguarding ECSS E40 & Q80: Addressing Threats

This section presents several proposals aimed at enhancing the cybersecurity standards of the European Cooperation for Space Standardization (ECSS), specifically focusing on ECSS-E-ST-40 (6 March 2009) [7]and ECSS-Q-ST-80 (15 February 2017) [8], to address critical gaps in the current standards and provide a more comprehensive framework for mitigating cybersecurity risks in space systems. The proposals listed in column "Proposal" of Table 19 and Table 20 are based on

the threats, vulnerabilities, and their respective mitigations identified in Sections 5.1.1 and 5.1.2.

The proposals have been categorized into three types:

- **E40-P-xx**: Proposals primarily related to the E40 standard, focusing on software development.
- **Q80-P-xx**: Proposals primarily related to the Q80 standard, focusing on software assurance.
- **OTH-P-xx**: Proposals that fall outside the scope of both E40 and Q80.

Table 19 presents the proposed generic requirements to cope with the identified threats, mainly based on their associated mitigations. It should be noted that these requirements should be applied whenever necessary (i.e., when cybersecurity is applicable, which is not the case for all types of space applications).

Since ECSS E40 and Q80 are focused on software, mitigations for electromagnetic threats, such as Solar Radio Bursts, Single Event Effects, Jamming, Spoofing, and Eavesdropping, are not considered. Additionally, given that these standards are essentially software oriented, and the following cyber threats affect the systems, these were not included in the referred standards: Signal Hijacking, Denial-of-Service, Web Spoofing, Man-in-the-Middle attacks, Zero-Day Exploits, Password Attacks, and Injection Attacks.

Table 19: Threats, mitigations and respective requirements proposals

Mitigation	Proposal
DC&I-1 - Advanced Encryption Standard (AES): A widely used symmetric encryption algorithm for securing sensitive data. In ground segment security, AES-counter mode is often employed to further enhance security and system performance. AES utilizes three key sizes (128, 192, and 256 bits), the selection of which should align with the required security standards. DC&I-2 - Triple Data Encryption Standard (3DES): A symmetric encryption algorithm that applies the Data Encryption Standard (DES) cipher three times to each data block using three different keys. However, 3DES performs poorly compared to AES, as it is considerably slower. DC&I-3 - Rivest-Shamir-Adleman (RSA): A widely used asymmetric encryption algorithm for secure data transmission. It employs a pair of keys: one public key for encryption and one private key for decryption. RSA is primarily used for digital signatures but is also valued for protecting sensitive data, including login credentials, in satellite communication systems. DC&I-4 - Elliptic Curve Cryptography (ECC): A public key encryption technique based on elliptic curve theory, offering strong security with relatively small key sizes. Compared to RSA, ECC provides equivalent security with smaller keys, making it a lightweight cryptographic technique ideal for satellites with resource constraints. DC&I-5 - Secure Hash Algorithm (SHA): A family of cryptographic hash functions used to generate unique, fixed-size message digests for data integrity verification. The resulting hash code is virtually impossible to reverse-engineer. DC&I-6 - Intrusion Detection and Prevention Systems: the use these systems onboard spacecraft, employing signatures and machine learning, can help detect and prevent cyber intrusions.	**E40-P-01**: A Requirement on data integrity protection, intrusion detection and prevention. **Q80-P-01**: A Requirement on V&V of data integrity protection, intrusion detection and prevention

Mitigation	Proposal
ST-1 - Keep software, internet browser, and operating system up to date: Regularly apply security patches and updates to address vulnerabilities that could be exploited by malware. ST-2 - Use safe search tools that warn about malicious sites: These tools can help avoid clicking on links or visiting websites that may harbour malware. ST-3 - Use security software and antivirus: Install and regularly update reputable security software to detect and remove malware. ST-4 - Install NoScript (or a similar extension) on browser: This extension can help prevent malicious scripts from running on websites. ST-5 - Acceptance testing: This involves thoroughly testing the software to ensure it meets all functional and non-functional requirements, including security requirements, before deployment. It helps identify any potential vulnerabilities or issues that might be exploited by malware. ST-6 - System evaluation: This involves independent verification and validation (IV&V) and code analysis to assess the system's security posture and identify any potential weaknesses or vulnerabilities. ST-7 - Continuous threat monitoring, continuous risk management: This involves continuously monitoring the system for potential threats and vulnerabilities, and proactively managing risks to mitigate the likelihood or impact of a security incident. ST-8 - Run-time security monitoring: Monitoring the system during operation to detect any suspicious activity or potential attacks in real time. ST-9 - Auditing: Periodically reviewing the system's security controls and processes to ensure they are effective and compliant with relevant regulations and standards. ST-10 - Supply chain confidence: Establishing trust and ensuring the security of the entire software supply chain, from development to deployment, to minimize the risk of introducing vulnerabilities through third-party components or services.	**E40-P-02**: A Requirement on the toolset environment and its protection, namely, that tools are up to date, known security issues are analysed and documented. **E40-P-03**: A Requirement on supply chain protection (see **E40-P-10**, **Q80-P-14**). **Q80-P-02**: A Requirement on V&V of the toolset environment and its protection, namely, that tools are up to date, known security issues are analysed and documented. **Q80-P-03**: A Requirement on V&V of the supply chain protection (see **E40-P-10**, **Q80-P-14**).
SCT-1 - Extensive code analysis (static analysis with cybersecurity rules) SCT-2 - Zero code smells and zero warnings objective (from static analysis tools) SCT-3 - Protection of software development environments SCT-4 - Extensive V&V of the embedded device against fuzz inputs SCT-5 - Specific security assessment of the design/code SCT-6 - Integrity checks for all data, configurations, inputs to the system	**Q80-P-04**: Verify that code smells and warnings are checked, fixed or justified. **Q80-P-05**: Check that specific security assessments are performed on design and code.

Mitigation	Proposal
SCM-1 - Intrusion detection mechanisms SCM-2 - Robust FDIR configuration SCM-3 - Proper authentication methods and access control SCM-4 - CRCs for all data transmission SCM-5 - Give an ID to every entity in the system SCM-6 - Telecommands acceptance is subject to validation SCM-7 - Periodically change the CRC/checksum/cryptography algorithms SCM-8 - Authentication on software patch SCM-9 - Accept telecommands and download telemetry only when flying above certain regions.	**E40-P-04**: A Requirement on intrusion detection and prevention, data integrity and authentication, and access control and geographical restrictions. **Q80-P-06**: A Requirement on V&V of intrusion detection and prevention, data integrity and authentication, and access control and geographical restrictions. **Q80-P-07**: A requirement on V&V of FDIR configurations.
BD-1 - Secure-by-design approach (Zero trust solutions) BD-2 - Take security lessons learned from other projects/missions/domains into account. BD-3 - Every user involved in activities related to the project shall be subjected to user authentication. (Zero Trust model)	**E40-P-05**: A Requirement on secure-by-design approach, lessons learned from other domains and development environment authentication and access control. **Q80-P-08**: A Requirement on V&V of secure-by-design approach, lessons learned from other domains and development environment authentication and access control.
SUD/P-1 - Prioritizing speed over thoroughness in design, code analysis, and testing can leave vulnerabilities in the final product. This must be tackled with the opposite, by following the good and secure development practices.	**OTH-P-01**: A Requirement on prioritize thoroughness in development processes and adherence to secure development practices.
LCSS-1 - Unlike industries like aviation (FAA) and railways (TUV), space systems lack comprehensive certification processes that include cybersecurity aspects	**OTH-P-02**: Recommend an independent cybersecurity assessment perform by ESA or the prime contractors. **Q80-P-09**: Reinforce that ISVV shall perform an independent cybersecurity analysis.

Mitigation	Proposal
LV&TA-1 - Awareness trainings LV&TA-2 - Security testing LV&TA-3 - Enforcing security standards LV&TA-4 - Conducting independent regular security audits LV&TA-5 - Ensure a SDLC is integrated in the application development. LV&TA-6 - Training on security aspects, V&V LV&TA-7 - Check of OSS libraries vulnerabilities. LV&TA-8 - Vulnerability / Threats Analysis done before requirements are closed. LV&TA-9 - Security reviews	**E40-P-06**: A Requirement on vulnerability management, security reviews, and reinforce awareness and training, all referent to vulnerability / threat analysis. **Q80-P-10**: A Requirement on V&V of vulnerability management, security reviews, and reinforce awareness and training, all referent to vulnerability / threat analysis. (See also **E40-P-09**, **Q80-P-13**)
EDT-1 - Security reviews EDT-2 - Check of OSS libraries vulnerabilities. EDT-3 - Robustness testing EDT-4 - Do a deep analysis and test all interfaces (Zero Trust model) EDT-5 - Conducting independent regular security audits EDT-6 - Security testing	**E40-P-07**: A Requirement on Security Reviews and Testing, and Comprehensive Analysis and Testing, referring to development tools (tools assessment or certified tools). **Q80-P-11**: A Requirement on V&V of Security Reviews and Testing, and Comprehensive Analysis and Testing, referring to development tools (tools assessment or certified tools).
UE-1 - Errata analysis UE-2 - Security reviews	**E40-P-08**: A Requirement on Errata Analysis and Mitigation, referring to unmitigated errata. **Q80-P-12**: A Requirement on V&V of Errata Analysis and Mitigation, referring to unmitigated errata.

5.2.4 Safeguarding ECSS E40 & Q80: Addressing Vulnerabilities

Table 20 presents the proposed generic requirements to cope with the identified vulnerabilities, mainly based on their associated mitigations. It should be noted that these requirements should be applied whenever necessary (i.e., when cybersecurity is applicable, which is not the case for all types of space applications).

Some of the vulnerabilities identified in Section 5.1.2 were not considered because they are out of scope for ECSS E40 and Q80. These vulnerabilities relate to, e.g., human factors, legacy software, training, and fostering a cybersecurity culture.

Table 20: Vulnerabilities, mitigations and respective requirements proposals

Mitigation	Proposal
SSDLC -1 - Microsoft Security Development Lifecycle (SDL): A comprehensive process that covers security practices throughout the entire software development lifecycle, from planning to maintenance. SSDLC -2 - Software Security Touchpoints: A lightweight framework that focuses on key security activities at critical points in the development process. SSDLC -3 - Software Assurance Forum for Excellence in Code (SAFECode): A collaborative effort by leading software companies to develop and promote best practices for software assurance. SSDLC -4 - NIST Secure Software Development Framework (SSDF): A set of fundamental, sound, and secure software development practices based on established secure software development practice documents.	**E40-P-09**: A Requirement on Implementing Comprehensive SSDLC Frameworks, referring to development life cycle. **Q80-P-13**: A Requirement on V&V of Implementing Comprehensive SSDLC Frameworks, referring to development life cycle.

Mitigation	Proposal
SC-1 - Enforce Cybersecurity Requirements: Impose strict cybersecurity requirements for commercial technologies and off-the-shelf components used in both civilian and military space assets. Frameworks like the Cybersecurity Maturity Model Certification (CMMC) could be adopted. SC-2 - Supply Chain Risk Management (SCRM): Establish a robust SCRM program incorporating software assurance methods to minimize the likelihood of malware introduction into components and modules. SC-3 - Obtain Products from Trusted Suppliers: Prioritize suppliers with a proven track record of security and quality assurance. Verify their compliance with relevant cybersecurity standards and practices. SC-4 - Component Maintenance: Continuously monitor integrated components for any unauthorized modifications. Address known vulnerabilities identified by the team, community, or supplier through regular updates and patches. Maintain direct communication between the supplier and customer to ensure timely updates and support. SC-5 - Software Bill of Materials (SBOM): Maintain a detailed list of third-party components to facilitate validation and vulnerability identification. SC-6 - Harden the Build Environment: Ensure that the environment used to build and assemble components is secure and free from potential vulnerabilities. SC-7 - Promoting Security in Government Contracts: Enforce strict cybersecurity standards in government contracts to incentivize commercial vendors to prioritize security in their products, potentially leading to industry-wide improvements. SC-8 - Regulatory Framework for Private Sector Activities: Create a regulatory framework to manage the growing private sector space activities, ensuring compliance with existing space treaties like the Outer Space Treaty while promoting industry efforts to strengthen cybersecurity and collaboration. SC-9 - Use of Advanced Technology: Leverage advanced technologies like blockchain to enhance the security, authenticity, and integrity of software and hardware throughout the supply chain. The decentralized and immutable nature of blockchain can bring transparency, security, and traceability to every component.	**E40-P-10**: A Requirement on Enforcing Cybersecurity Requirements, Supply Chain Risk Management, Component Maintenance and Security, Regulatory Framework and Industry-Wide Improvements and Leveraging Advanced Technologies, referring to supply chain. **Q80-P-14**: A Requirement on V&V of Enforcing Cybersecurity Requirements, Supply Chain Risk Management, Component Maintenance and Security, Regulatory Framework and Industry-Wide Improvements and Leveraging Advanced Technologies, referring to supply chain.

Mitigation	Proposal
COTS-1 – Security Analysis: Black-box testing techniques such as fuzzing, boundary value analysis, and equivalence partitioning can be employed to assess the product's robustness. Additionally, ensuring compliance with established security guidelines, like Security Technical Implementation Guides (STIGs), and regularly checking for and addressing vulnerabilities listed in the OWASP Top Ten is essential for maintaining a secure system	**E40-P-11**: A Requirement on Security Analysis and Testing, referring to COTS. **E40-P-12**: A Requirement requesting security analysis and assessments for all types of reused software. **Q80-P-15**: A Requirement on V&V of Security Analysis and Testing, referring to COTS. **Q80-P-16**: A Requirement on V&V of security analysis and assessments for all types of reused software.
TE-1 - Software-Defined Radio (SDR): SDRs offer software control over functions traditionally performed by hardware, such as filtering, modulation, and mixing. This reduces the reliance on hardware, freeing up space for other components, and enables low-cost signal authentication solutions like fingerprint embedding, which acts as an authentication tag over message waveforms. TE-2 - Cloud Computing: Shifting data processing and storage from personal computers to secure data centers, accessible via the internet, enhances flexibility, availability, and redundancy. This allows for better management of customer scheduling needs through browser applications and provides protection against cyberattacks. TE-3 - Optical Communication: Moving away from traditional radio frequency (RF) communication, optical communication uses visible light for satellite communication. This technology is less vulnerable to jamming and other RF-based electronic warfare tactics. TE-4 - Quantum Key Distribution (QKD): This emerging field of cryptography holds the key to future-proofing encryption. While traditional encryption algorithms could be compromised by powerful quantum computers in the future, QKD utilizes quantum mechanics to establish secret keys with unconditional post-quantum security. TE-5 - Ground Station as a Service (GSaaS): This method aims to reduce the cost of acquiring infrastructure by enabling users to communicate with, process data from, control, and monitor satellites via the cloud using a simple laptop or desktop computer.	**OTH-P-03**: New technologies need to be fully assessed from security perspectives (threats and vulnerabilities analysis, interface impact with other technologies, risk analysis)

Mitigation	Proposal
SA-1 - Threat Modelling: This involves systematically identifying and assessing potential threats to a system, analysing their potential impact, and developing strategies to mitigate those risks. SA-2 - Network Security Monitoring: By analysing network traffic with tools like packet sniffers, security teams can extract data to be analysed, enabling the detection and prevention of attacks. SA-3 - Vulnerability Scanning: Automated tools scan the system for known vulnerabilities, such as outdated software or misconfigurations. SA-4 - Penetration Testing: This involves simulating real-world attacks to identify and exploit vulnerabilities in a system's defences, providing a more comprehensive assessment of the system's security posture. SA-5 - Input Validation: Rigorous validation of user input helps prevent injection attacks and other vulnerabilities arising from unexpected or malicious data. SA-6 - Independent Regular Security Audits: Periodically conducting independent security audits by external experts helps identify vulnerabilities and ensures compliance with industry best practices. SA-7 - Fuzz Testing: This software testing technique uncovers implementation bugs by injecting "random" or invalid input and analysing the system's behaviour. SA-8 - Static Code Analysis: This involves analysing the source code without executing it to identify potential issues, bad practices, and vulnerabilities. SA-9 - Security Testing: This encompasses various techniques like performance testing, simulated attacks (including buffer overflow and DoS testing), and equivalence class partitioning tests to assess a system's security posture under different conditions.	**E40-P-13**: A Requirement on Threat Modelling and Risk Assessment, Network Security Monitoring and Input Validation, referring to security analysis. **Q80-P-17**: A Requirement on V&V of Threat Modelling and Risk Assessment, Network Security Monitoring, Vulnerability Scanning and Testing, Input Validation, referring to security analysis. (See also **E40-P-16**, **E40-P-17**, for code analysis and **Q80-P-20**, **Q80-P-21**, for additional security testing techniques)
SR-1 - Security Requirements Analysis: The first step is to identify and classify systems to assess their potential threats and vulnerabilities. After compiling a list of threats, a risk assessment is conducted to evaluate the likelihood and potential impact of each, allowing for the identification of the most significant risks.	**E40-P-14**: A Requirement on security requirements analysis, referring to security requirements. **Q80-P-18**: A Requirement on V&V of security requirements analysis, referring to security requirements.

Mitigation	Proposal
SD-1 - Economy of Mechanism: Design simplicity minimizes attack surfaces and aids code inspection. SD-2 - Fail-Safe Defaults: Deny access by default, then grant permissions explicitly. Prioritize allowlists over denylists to prevent unauthorized access. SD-2 - Complete Mediation: Check every access to every object, every time. Defence in depth is key. SD-3 - Open Design: Security should rely on secret keys, not on obscurity. SD-4 - Embrace Kerckhoff's principle, which states that a cryptographic system's security depends solely on the secrecy of its keys. SD-5 - Separation of Privilege: Multiple layers of protection, using different mechanisms, enhance security. SD-6 - Least Privilege: Grant programs and users the minimum necessary rights (need-to-know basis). SD-7 - Least Common Mechanism: Minimize shared components to limit the impact of a successful attack. SD-8 - Psychological Acceptability: Balance security and usability to ensure user adoption. SD-9 - Work Factor: Consider the attacker's resources when evaluating security measures. SD-10 - Compromise Recording: Logging and evidence collection are vital for incident response.	**E40-P-15**: A Requirement to reinforce the 10 principles of a secure design. **Q80-P-19**: A Requirement on V&V of the 10 principles of a secure design.
SI-1 - Code Reviews: Conducting thorough code reviews by peers or security experts to identify potential issues that might have been missed by automated tools. SI-2 - Threat Modelling: Identifying potential threats and vulnerabilities early in the development process to proactively mitigate risks. SI-3 - Security Testing: Performing security testing, including penetration testing and fuzz testing, to simulate real-world attacks and assess the system's resilience.	**E40-P-16**: A Requirement on Threat Modelling to be performed on development process to mitigate security risks. **E40-P-17**: A Requirement on Code Reviews focused on security topics. **Q80-P-20**: A Requirement on V&V of Threat Modelling to be performed on development process to mitigate security risks. **Q80-P-21**: A Requirement on V&V of Code Reviews focused on security topics.

Mitigation	Proposal
SecT-1 - Security Requirements Testing SecT-2 - Threat Mitigation Testing SecT-3 - Vulnerability Testing SecT-4 - Penetration Testing SecT-5 - Independence of Testers	**E40-P-18**: A Requirement on a Comprehensive Security Testing that shall be included in the test plan. **Q80-P-22**: A Requirement on V&V of the Comprehensive Security Testing that shall be included in the test plan.

Mitigation	Proposal
Installation: IOM-1 - Security Checks: Conduct thorough pre-installation security checks on all hardware and software components. IOM-2 - Secure Configuration and Integration: Ensure secure configuration and integration with existing infrastructure. IOM-3 - Access Controls and Authentication Mechanisms: Implement access controls and authentication mechanisms to restrict unauthorized access. **Operation**: IOM-4 - User Training: Provide comprehensive user training to prevent accidental misconfigurations or misuse. IOM-5 - Monitor System: Monitor system logs for suspicious activity and potential security breaches. IOM-6 - Regular Updates: Regularly update software and firmware to address vulnerabilities. **Maintenance**: IOM-7 - Routine System Maintenance: Perform routine system maintenance to prevent malfunctions and ensure optimal performance. IOM-8 – Security Patches: Apply security patches and updates promptly to protect against emerging threats. IOM-9 - Regular Vulnerability Assessments: Conduct regular vulnerability assessments and penetration testing to identify and address weaknesses. IOM-10 - Incident Response Plans: Develop and test incident response plans to quickly address any security breaches.	**E40-P-19**: A Requirement on security checks before installation, secure configuration and integration with the existing infrastructure and access control and authentication mechanism during installation. **E40-P-20**: A Requirement on user training concerning security, monitoring the system for security concerns and regular security updates. **E40-P-21**: A Requirement for routine system maintenance, security patches, regular vulnerability assessments and incident response plans. **Q80-P-23**: A Requirement on V&V of security checks before installation, secure configuration and integration with the existing infrastructure and access control and authentication mechanism during installation. **Q80-P-24**: A Requirement on V&V of user training concerning security, monitoring the system for security concerns and regular security updates. **Q80-P-25**: A Requirement on V&V of routine system maintenance, security patches, regular vulnerability assessments and incident response plans.

Mitigation	Proposal
SB-1 - Extensive code analysis SB-2 - Security testing SB-3 - Extensive V&V of the embedded device against fuzz inputs SB-4 - Built-in or self-tests to ensure application and data integrity SB-5 - Perform input validation SB-6 - Integrity checks for all data, configurations, inputs to the system SB-7 - Conducting independent regular security audits SB-8 - Security reviews	**Q80-P-26**: A Requirement on analysing any software issue for potential security impacts (Data Integrity and Input Validation, Independent Security Audits, Reviews, Code Analysis and Security Testing).
WDP-1 - Ensure a SDLC (Secure Development Life Cycle) is integrated in the application development. WDP-2 - No agile methodology in security critical development	**OTH-P-04**: A Requirement on Cautious Use of Agile Methodologies, to avoid a weak development process. (see also E40-P-09 and Q80-P-13)
SU-1 - Authentication on software patch SU-2 - Enforce patch management	**E40-P-22**: A Requirement on Authentication and Patch Management, referring to software update. **Q80-P-27**: A Requirement on V&V of Authentication and Patch Management, referring to software update.
WSDP-1 - Protection of software development environments WSDP-2 - Every user involved in activities related to the project shall be subjected to user authentication. (Zero Trust model)	(See **E40-P-05**, **Q80-P-08**, for authentication and **E40-P-02**, **E40-P-03**, **Q80-P-02**, **Q80-P-03** for software development environment protection.)
DP-1 - Access to target memories through unprotected debug ports.	**Q80-P-28**: A Requirement to ensure that debug ports are disabled for flight software.
BCP-1 - Extensive code analysis BCP-2 - Zero code smells and zero warnings objective	**Q80-P-29**: A Requirement on verify that code smells and warnings are checked, fixed or justified.

Mitigation	Proposal
LSAP-1 - 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.	**Q80-P-30**: A Requirement to ensure that security and unusual are covered by the acceptance plan.
WSI&DF-1 - More secure information and deliverables flow. WSI&DF-2 - Use of certified tools	**E40-P-23**: One Requirement to ensure the secure delivery of all project information.(see also **E40-P-07**, **Q80-P-11**)
WPP-1 - Use cryptographic keys instead of passwords.	**E40-P-24**: A Requirement to ensure a strong password policy or cryptographic keys.
HTC-1 - Create a baseline workforce to be trained in cybersecurity.	**OTH-P-05**: A Requirement on comprehensive and documented cybersecurity training.
DUD-1 - Security reviews	**E40-P-25**: A Requirement to ensure secure deserialization of untrusted data. **Q80-P-31**: A Requirement on V&V of the secure deserialization of untrusted data.
IM-1 - Intrusion detection mechanisms IM-2 - Robust FDIR configuration IM-3 - Firewall	**E40-P-26**: A Requirement to ensure intrusion detection in the flight software if needed. **OTH-P-06**: A Requirement to ensure intrusion detection and firewall protection to ground systems. (See **E40-P-04**, **Q80-P-06**, **Q80-P-07**)
PMED-1 - Advanced encryption PMED-2 - Proper authentication methods and access control	(see **E40-P-01**, **Q80-P-01**)

In total, 63 proposals have been presented, being:

- 26 requirements proposed for ECSS-E-ST-40C,
- 31 requirements proposed for ECSS-E-ST-Q-80C, and
- 6 requirements proposed other engineering/project/contract areas.

These proposals address key vulnerabilities and threats identified in previous research and analysis and intend to help the space industry in strengthening the security of space systems.

Lastly, these proposed requirements should be seen as such (proposals) to help the respective (E40 and Q80) ECSS Working Groups into improving the cybersecurity engineering of space systems.

6 CONCLUSION

The objectives of this internship were to collect and analyse state-of-the-art data on cybersecurity threats, vulnerabilities, and respective solutions in the space sector, to engage with key stakeholders, to propose mitigations, to develop recommendations and propose them to standards, to produce scientific publications, and to disseminate the findings. The research questions were formulated to explore the current state of space cybersecurity (**RQ-01**), to identify threats and vulnerabilities (**RQ-02**), to propose mitigation strategies (**RQ-03**), and to develop recommendations to improve existing space standards (**RQ-04**).

The findings of this study revealed that the space sector faces numerous threats and vulnerabilities that can lead to severe consequences, such as economic loss or loss of life. The internship cybersecurity survey identified a total of 61 different threats and vulnerabilities and has shown that specialists share the consensus that substantial efforts are required to address potential cybersecurity threats and vulnerabilities. The neglecting of cybersecurity reinforcement within the space sector is substantial, and significant efforts are required to make the space sector cyber secure.

The first internship objective (**Collect and Analyse State-of-the-Art Data**) was fulfilled by conducting a comprehensive literature review. The literature review revealed that improvements should be made to existing standards, and standards workgroups have been established to develop specific cybersecurity standards for the sector and improve existing engineering standards. A relevant set of threats and vulnerabilities applicable to the space sector was also compile based on the literature review.

The second objective (**Engage with Key Stakeholders**) was fulfilled by establishing contact with teams involved in space systems, software development and validation to draw a picture of cybersecurity subject in the space sector. The targeted survey on "Cybersecurity Challenges and Solutions for Space Systems" distributed to relevant stakeholders provided valuable insights and data (threats, vulnerabilities, mitigations, standards, tools and concerns) on the current state of space cybersecurity and promoted the engagement with specific stakeholders of the space sector.

The third objective (**Propose Mitigations**) was fulfilled by proposing mitigation strategies to address the identified threats and vulnerabilities. It shall be noted that mitigation strategies already exist for most of the threats and vulnerabilities identified in this study (from the literature review and the cybersecurity survey). However, investing in cybersecurity education is essential to strengthen the overall security posture of the space sector. Other measures include promoting joint work and technology transfer across the cybersecurity community (namely between academia and industry), treating cybersecurity as a mandatory property of systems/software engineering, adopting a proactive cybersecurity posture, and integrating

cybersecurity topics into space engineering standards (as recommended and mandatory requirements).

The fourth objective (**Develop Recommendations and Standards**) was fulfilled by drafting recommendations to improve existing space standards. One of the outcomes of this internship was the development of 63 improvement proposals for two key European space standards (ECSS), which have the potential to significantly enhance the state of cybersecurity in space. Currently, the proposed requirements for ECSS standards can be mapped to and integrated in ECSS-E-ST-40C [7] and ECSS-Q-ST-80C [8] which newer versions will already contain basic cybersecurity elements, but can also enable the definition of templates for cybersecurity support documentation, as ECSS DRDs (e.g., Threats and Vulnerabilities Analyses Report) that can be included in these standards.

The fifth objective (**Produce Scientific Publications**) was fulfilled by preparing and submitting one scientific paper detailing the literature review, state-of-the-art, and threats/vulnerabilities study for space systems. The "Engineering and Assessing Cybersecurity for Space Systems" paper was accepted and presented at DASIA 2024 in Croatia.

The sixth objective (**Disseminate Findings**) was fulfilled by sharing the cybersecurity survey summary report with the identified stakeholders (and survey participants), including key contacts at ESA, NASA, and other relevant industries, to foster collaboration and raise awareness of the research findings. Consequently, an invitation was received to join an IEEE standards working group, the "IEEE SA WG on space systems cybersecurity" [101].

In conclusion, the proposed improvements (requirements) to existing space standards based on these requirements can contribute to a more robust cybersecurity posture in the space sector. One of the results of this work was to increase cybersecurity awareness within Critical Software and provide materials to improve the awareness for the space sector. Future work could study the impact of AI in the space sector cybersecurity and continue to improve cybersecurity organizational process standards, tools and best practices. The proposed mitigation strategies and recommendations can serve as a starting point to safeguarding space systems by defining and implementing robust cybersecurity requirements to address the identified threats and vulnerabilities. The same knowledge base can be used to define new (cybersecurity) testing strategies and create a cybersecurity test set (e.g. to support penetration testing) to apply for Critical Software´s systems and those of third parties. Additionally, this knowledge can help improve and mature the cybersecurity team training at Critical Software, aiming to protect not only the organization from cyberthreats but also the developed systems (software).

REFERENCES

[1] "Computer Security Resource Center," NIST, [Online]. Available: https://csrc.nist.gov/glossary/term/authentication. [Accessed 03 February 2025].

[2] "Computer Security Resource Center," NIST, [Online]. Available: https://csrc.nist.gov/glossary/term/availability. [Accessed 03 February 2025].

[3] "Computer Security Resource Center," NIST, [Online]. Available: https://csrc.nist.gov/glossary/term/confidentiality. [Accessed 03 February 2025].

[4] "Computer Security Resource Center," NIST, [Online]. Available: https://csrc.nist.gov/glossary/term/cybersecurity. [Accessed 03 February 2025].

[5] "Computer Security Resource Center," NIST, [Online]. Available: https://csrc.nist.gov/glossary/term/integrity. [Accessed 03 February 2025].

[6] "Computer Security Resource Center," NIST, [Online]. Available: https://csrc.nist.gov/glossary/term/cyber_threat. [Accessed 03 February 2025].

[7] “ECSS-E-ST-40C – Software (6 March 2009),” European Cooperation for Space Standardization, [Online]. Available: https://ecss.nl/standard/ecss-e-st-40c-software-general-requirements/. [Accessed 9 April 2024].

[8] "ECSS-Q-ST-80C Rev.1 – Software product assurance (15 February 2017)," European Cooperation for Space Standardization, [Online]. Available: https://ecss.nl/standard/ecss-q-st-80c-rev-1-software-product-assurance-15-february-2017/. [Accessed 9 April 2024].

[9] P. Sousa, "Literature Review and State-of-the-art Study on Cybersecurity for Space or Similar Domains," CSW-2024-TNR-01442, V 1.0, Critical Software, S.A., 2024.

[10] P. Sousa, "Analysis of Practices and International Standards Related to Cybersecurity," CSW-2024-TNR-01469, V 1.0, Critical Software, S.A., 2024.

[11] P. Sousa, "Space systems threats and vulnerabilities," CSW-2024-TNR-01468, V 1.0, Critical Software, S.A., 2024.

[12] P. Sousa, "Proposals to Cope with Threats and Vulnerabilities," CSW-2024-TNR-03939, V 1.0, Critical Software, S.A., 2024.

[13] P. Sousa, "Proposal to Change/Improve/Integrate Specific Requirements into the ECSS E40 & Q80," CSW-2024-TNR-04549, V 1.0, Critical Software, S.A., 2024.

[14] P. Sousa, "Report - Cybersecurity Survey," CSW-2024-TNR-03904, V 1.0, Critical Software, S.A., 2024.

[15] P. Sousa, J. Cunha and N. Silva, "Engineering and Assessing Cybersecurity for Space Systems," in *DAta Systems in Aerospace*, Opatija, 2024.

[16] Viasat, Inc., "KA-SAT Network cyber attack overview," Viasat, 30 March 2022. [Online]. Available: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview. [Accessed 16 November 2024].

[17] J. Pavur and I. Martinovic, "Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight," *Journal of Cybersecurity,* pp. 1-17, 2022.

[18] M. Manulis, P. C. Bridges, R. Harrison, V. Sekar and A. Davis, "Cyber security in New Space," *International Journal of Information Security*, p. 24, 2020.

[19] G. Falco, “Cybersecurity Principles for Space Systems,” *Journal of Aerospace Computing, Information and Communication,* pp. 1-10, December 2018.

[20] R. Sujeetha, H. Das, T. Dhelawat and M. Tanveer, "Cyber-Space and Its Menaces," in *2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN)*, Pondicherry, 2019.

[21] S. Pazouki and A. Aydeger, "Securing International Space Station Against Recent Cyber Threats," in *Proceedings of Seventh International Congress on Information and Communication Technology* , London, 2023.

[22] A. Elmarady and K. Rahouma, "Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk Assessment," *IEEE Access,* vol. 9, 2021.

[23] K. Thangavel, J. Plotnek, A. Gardi and R. Sabatini, "Understanding and Investigating Adversary Threats and Countermeasures in the Context of Space Cybersecurity," in *IEEE/AIAA 41st Digital Avionics Systems Conference (DASC)*, Portsmouth, 2022.

[24] G. Falco and N. Boschetti, "A Security Risk Taxonomy for Commercial Space Missions," in *AIAA Ascend 2021*, Las Vegas, 2021.

[25] N. Boschetti, N. Gordon and G. Falco, "Space Cybersecurity Lessons Learned from The ViaSat Cyberattack," in *Conference: AIAA Ascend 2022,* Las Vegas, 2022.

[26] V. Varadharajan and N. Suri, "Security challenges when space merges with cyberspace," *Space Policy*, vol. 67, 2024.

[27] NASA, "NASA Technical Standards System," NASA, [Online]. Available: https://standards.nasa.gov/NASA-Technical-Standards. [Accessed 16 November 2024].

[28] "Consultative Committee for Space Data Systems," Consultative Committee for Space Data Systems, [Online]. Available: https://public.ccsds.org/default.aspx. [Accessed 20 March 2024].

[29] "Standard for Space System Cybersecurity," IEEE Standards Association, [Online]. Available: https://standards.ieee.org/ieee/3349/11182/. [Accessed 21 March 2024].

[30] "Gregory Falco, LEED AP," LinkedIn, [Online]. Available: https://www.linkedin.com/in/gregoryfalco/. [Accessed 16 November 2024].

[31] "ISO/IEC 27000 family - Information security management," International Organization for Standardization, [Online]. Available: https://www.iso.org/standard/iso-iec-27000-family. [Accessed 9 April 2024].

[32] "ISO," International Organization for Standardization, [Online]. Available: https://www.iso.org/home.html. [Accessed 23 January 2024].

[33] "NIST," National Institute of Standards and Technology, [Online]. Available: https://www.nist.gov/. [Accessed 11 January 2024].

[34] "Aerospace Security," [Online]. Available: https://aerospace.csis.org/the-private-sectors-assessment-of-u-s-space-policy-and-law/. [Accessed 21 March 2024].

[35] "FCC Seeks Comment on Cybersecurity Recommendations for Communications Providers," Hogan Lovells, 23 April 2015. [Online]. Available: https://www.hoganlovells.com/en/publications/fcc-seeks-comment-on-cybersecurity-recommendations-for-communications-providers_1. [Accessed 16 November 2024].

[36] "Global Cybersecurity Agenda (GCA)," international Telecommunication Union, [Online]. Available: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx. [Accessed 16 November 2024].

[37] "New FAA Regulations Target Cybersecurity Vulnerabilities in Aircraft Design," Jones Day, 16 September 2024. [Online]. Available: https://www.jonesday.com/en/insights/2024/09/new-faa-regulations-target-cybersecurity-vulnerabilities-in-aircraft-design. [Accessed 16 November 2024].

[38] "Delegated regulation - 2022/1645 - EN - EUR-Lex," EUR-Lex, [Online]. Available: https://eur-lex.europa.eu/eli/reg_del/2022/1645/oj. [Accessed 16 November 2024].

[39] S. Shelhorse, D. Meshulam, J. Gilluly, R. Plesco and A. Serwin, "SEC addresses cybersecurity risk in proposed rules for the investment management industry," DLA Piper, [Online]. Available: https://www.dlapiper.com/pt-br/insights/publications/2022/02/sec-addresses-cybersecurity-risk. [Accessed 16 November 2024].

[40] "Insights from the 2021 Cyber Coordination Groups," Financial Conduct Authority, [Online]. Available: https://www.fca.org.uk/publications/research/cyber-coordination-groups-insights-2021. [Accessed 16 November 2024].

[41] "7 trends that could shape the future of cybersecurity in 2030," World Economic Forum , 3 March 2023. [Online]. Available: https://www.weforum.org/agenda/2023/03/trends-for-future-of-cybersecurity/. [Accessed 23 April 2024].

[42] "Space Critical Infrastructure: Breaking the Binary Debate and a Call for Space Council Action," SpaceNews, [Online]. Available: https://spacenews.com/space-critical-infrastructure-breaking-the-binary-debate-and-a-call-for-space-council-action/. [Accessed 23 May 2024].

[43] "Debate Over Space as a Critical Infrastructure in Europe Takes Center Stage at Cysat," Via Satellite, [Online]. Available: https://www.satellitetoday.com/cybersecurity/2024/04/24/debate-over-space-as-a-critical-infrastructure-in-europe-takes-center-stage-at-cysat/. [Accessed 23 May 2024].

[44] P. LIONNET, "The current structure of the European space manufacturing sector," JANUARY 2021. [Online]. Available: https://eurospace.org/wp-content/uploads/2021/01/structure-of-the-space-manufacturing-sector-v2021.pdf. [Accessed 14 December 2023].

[45] M. S. Turan, "Lightweight Crypto, Heavyweight Protection," NIST, 13 January 2021. [Online]. Available: https://www.nist.gov/blogs/taking-measure/lightweight-crypto-heavyweight-protection. [Accessed 22 March 2024].

[46] D. D´Souza, "$178 Billion Flows into Space Investments in Past 10 Years," 19 February 2021. [Online]. Available: https://www.investopedia.com/space-economy-seen-nearly-usd178-billion-in-investments-since-2011-5113282. [Accessed 18 January 2024].

[47] T. Harford, "The CubeSat revolution changing the way we see the world," BBC, 17 July 2019. [Online]. Available: https://www.bbc.com/news/business-48533945. [Accessed 20 December 2023].

[48] "Nanosats Database," [Online]. Available: https://www.nanosats.eu/. [Accessed 20 December 2023].

[49] U. Ogono, "What Cyber Security Processes Does a Cyber Security Analyst Need to Know?," Career Karma, 4 September 2022. [Online]. Available: https://careerkarma.com/blog/cyber-security-processes-and-methods/#:~:text=What%20Are%20the%20Five%20Steps%20of%20the%20Cyber,4%20Respond%20to%20Incidents%20...%205%20Recovery%20. [Accessed 23 March 2024].

[50] "What Is Access Management? Risks, Technology, and Best Practices," Frontegg, 28 May 2023. [Online]. Available: https://frontegg.com/guides/access-management. [Accessed 24 March 2024].

[51] J. Holdsworth and M. Kosinski, "What is incident response?," IBM, 20 August 2024 . [Online]. Available: https://www.ibm.com/topics/incident-response. [Accessed 24 March 2024].

[52] M. Antunes and B. Rodrigues, Introduction to Cybersecurity, FCA, 2022.

[53] "ISA/IEC 62443 Series of Standards," International Society of Automation, [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards. [Accessed 24 May 2024].

[54] Frankfurt Solutions, "Automotive Cybersecurity – ISO/SAE 21434," Frankfurt Solutions, 17 July 2020. [Online]. Available: https://www.frankfurtsolutions.com/en/2020/07/17/automotive-cybersecurity/. [Accessed 25 November 2024].

[55] "ISO/SAE 21434:2021," ISO, [Online]. Available: https://www.iso.org/standard/70918.html. [Accessed 23 March 2024].

[56] D. EkertJürgen, D. Dobaj and A. Salamun, "Cybersecurity Verification and Validation Testing in Automotive," *Journal of Universal Computer Science*, vol. XXVII, no. 8, pp. 850-867, 2021.

[57] "OWASP SAMM," OWASP, [Online]. Available: https://owasp.org/www-project-samm/. [Accessed 24 March 2024].

[58] "Building Security In Maturity Model (BSIMM)," Synopsys, [Online]. Available: https://www.synopsys.com/software-integrity/software-security-services/bsimm-maturity-model.html. [Accessed 24 March 2024].

[59] "Common Criteria," Common Criteria, [Online]. Available: https://www.commoncriteriaportal.org/index.cfm. [Accessed 24 March 2024].

[60] "Other Publications," Common Criteria, [Online]. Available: https://www.commoncriteriaportal.org/cc/index.cfm. [Accessed 24 March 2024].

[61] "About the Common Criteria," Common Criteria, [Online]. Available: https://www.commoncriteriaportal.org/ccra/index.cfm. [Accessed 24 March 2024].

[62] Anwita, "5 Best Cybersecurity tools in 2024," Sprinto, 7 May 2024. [Online]. Available: https://sprinto.com/blog/best-cybersecurity-tools/#:~:text=Types%20of%20cybersecurity%20tools%201%20Network%20security%20monitoring,sniffers%20...%208%20Antivirus%20software%20...%20Mais%20itens. [Accessed 24 March 2024].

[63] "Security Requirements for Cryptographic Modules," NIST, [Online]. Available: https://csrc.nist.gov/pubs/fips/140-3/final. [Accessed 05 February 2025].

[64] "Common Weakness Enumeration," Common Weakness Enumeration, [Online]. Available: https://cwe.mitre.org/index.html. [Accessed 16 November 2024].

[65] "The CSF 1.1 Five Functions," National Institute of Standards and Technology, 26 February 2024. [Online]. Available: https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions. [Accessed 5 June 2024].

[66] OWASP, "OWASP Top Ten," OWASP, [Online]. Available: https://owasp.org/www-project-top-ten/. [Accessed 25 November 2024].

[67] "Knowledgebase – CyBOK v1.1," CyBok, [Online]. Available: https://www.cybok.org/knowledgebase1_1/. [Accessed 10 April 2024].

[68] "ATT&CK," MITRE , [Online]. Available: https://attack.mitre.org/. [Accessed 10 April 2024].

[69] "Engage," MITRE, [Online]. Available: https://engage.mitre.org/defenders/. [Accessed 10 April 2024].

[70] "D3FEND," MITRE, [Online]. Available: https://d3fend.mitre.org/. [Accessed 10 April 2024].

[71] "Caldera," MITRE, [Online]. Available: https://caldera.mitre.org/. [Accessed 10 April 2024].

[72] "OWASP," OWASP Foundation, [Online]. Available: https://owasp.org/. [Accessed 10 April 2024].

[73] NIST, "Computer Security Resource Center," NIST, [Online]. Available: https://csrc.nist.gov/glossary/term/cyber_threat. [Accessed 16 November 2024].

[74] F. Quiquet, "What are the threats to space systems?," Space & Cybersecurity, 18 May 2020. [Online]. Available: https://www.spacesecurity.info/en/what-are-the-threats-to-space-systems/. [Accessed 7 March 2024].

[75] The Aerospace Corporation, "Protecting Space Systems from Cyber Attack," Medium, 31 March 2022. [Online]. Available: https://medium.com/the-aerospace-corporation/protecting-space-systems-from-cyber-attack-3db773aff368. [Accessed 22 April 2024].

[76] SentinelOne, "What is a Threat Actor? Types & Examples," SentinelOne, 26 June 2021. [Online]. Available: https://www.sentinelone.com/cybersecurity-101/threat-intelligence/threat-actor/#:~:text=Threat%20Actor%20Types%20and%20Attributes%201%201.%20Cybercriminals,5.%20Insider%20Threats%20...%206%206.%20Hackers%20. [Accessed 22 April 2024].

[77] IBM, "What is a threat actor?," IBM, [Online]. Available: https://www.ibm.com/topics/threat-actor. [Accessed 22 April 2024].

[78] S. Iftikhar, "Cyberterrorism as a global threat: a review on repercussions and countermeasures," pp. 14-16, 2024.

[79] Y. V. Yasyukevich, A. S. Yasyukevich and E. I. Astafyeva, "How modernized and strengthened GPS signals enhance the system performance during solar radio bursts," *GPS Solutions,* vol. 25, 2021.

[80] Chillymanjaro, "Solar radio bursts," The Watchers, 7 September 2011. [Online]. Available: https://watchers.news/2011/09/07/solar-radio-bursts/. [Accessed 23 April 2024].

[81] H. Sato, N. Jakowski, J. Berdermann, K. Jiricka, A. Heßelbarth, D. Banyś and V. Wilken, "Solar Radio Burst Events on 6 September 2017 and Its Impact on GNSS Signal Frequencies," pp. 1-11, 2019.

[82] The Hughes Team, "Securing SATCOM: Modernizing Military Systems for Smarter Adversaries," Hughes, 5 September 2018. [Online]. Available: https://www.hughes.com/resources/insights/satellite-broadband/securing-satcom-modernizing-military-systems-smarter. [Accessed 8 March 2024].

[83] "GPS Jammer Delays Flights in France," Resilient Navigation and Timing Foundation, 15 September 2017 . [Online]. Available: https://rntfnd.org/2017/09/15/gps-jammer-delays-flights-in-france/. [Accessed 23 April 2024].

[84] The Editorial Team, "Vessels navigating in China report GPS spoofing incidents," Safety4Sea, 2 January 2020. [Online]. Available: https://safety4sea.com/vessels-navigating-in-china-report-gps-spoofing-incidents/. [Accessed 8 March 2024].

[85] H. Lied, "GPS freaking out? Maybe you're too close to Putin," NRKbeta, 18 September 2017. [Online]. Available: https://web.archive.org/web/20170925202637/https:/nrkbeta.no/2017/09/18/gps-freaking-out-maybe-youre-too-close-to-putin/. [Accessed 23 April 2024].

[86] J. Porup, "It's Surprisingly Simple to Hack a Satellite," VICE, 21 August 2015. [Online]. Available: https://www.vice.com/en/article/its-surprisingly-simple-to-hack-a-satellite/. [Accessed 23 April 2024].

[87] T. Staff, "Hamas hacks into Israeli TV and threatens: 'Terror will never end'," The Times of Israel, 12 March 2016. [Online]. Available: https://www.timesofisrael.com/hamas-hacks-israeli-tv-the-terror-will-never-end/. [Accessed 22 April 2024].

[88] "BBC fears Iranian cyber-attack over its Persian TV service," The Guardian, 2012. [Online]. Available: https://www.theguardian.com/media/2012/mar/14/bbc-fears-iran-cyber-attack-persian. [Accessed 23 April 2024].

[89] T. Moes, "Spoofing Examples (2024): The 4 Worst Attacks of All Time," SoftwareLab, January 2024. [Online]. Available: 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. [Accessed 23 April 2024].

[90] M. Buckbee, "Malware Protection: Basics and Best Practices," Varonis, 4 April 2022. [Online]. Available: https://www.varonis.com/blog/malware-protection. [Accessed 23 April 2024].

[91] P. Muncaster, "German space centre endures cyber attack," The Register, 15 April 2014 . [Online]. Available: https://www.theregister.com/2014/04/15/dlr_attacked_china_apt_trojans/. [Accessed 23 April 2024].

[92] "Types of cyberthreats," IBM, 25 March 2024. [Online]. Available: https://www.ibm.com/think/topics/cyberthreats-types. [Accessed 22 April 2024].

[93] "What is a Zero-day Attack? - Definition and Explanation," Kaspersky, [Online]. Available: https://www.kaspersky.com/resource-center/definitions/zero-day-exploit. [Accessed 23 April 2024].

[94] "Six Types of Password Attacks & How to Stop Them," Onelogin, [Online]. Available: https://www.onelogin.com/learn/6-types-password-attacks. [Accessed 23 April 2024].

[95] C. Harris, "The Most Significant Password Breaches Of 2021," Expert Insights, 22 April 2024. [Online]. Available: https://expertinsights.com/insights/the-most-significant-password-breaches/. [Accessed 23 April 2024].

[96] J. O'Leary, J. Kimble, K. Vanderlee and N. Fraser, "Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware," Mandiant, 20 September 2017. [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/apt33-insights-into-iranian-cyber-espionage/. [Accessed 23 April 2024].

[97] "National Vulnerability Database - Vulnerabilities," NIST, [Online]. Available: https://nvd.nist.gov/vuln. [Accessed 29 November 2024].

[98] Microsoft, "Microsoft Digital," 2023.

[99] "Microsoft Digital Defense Report 2023," Microsoft, 2023. [Online]. Available: https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023. [Accessed 23 April 2024].

[100] M. Holmes, "10 Defining Moments in Cybersecurity and Satellite in 2023," Via Satellite, 22 January 2024. [Online]. Available: https://interactive.satellitetoday.com/via/january-february-2024/10-defining-moments-in-cybersecurity-and-satellite-in-2023/. [Accessed 23 April 2024].

[101] IEEE Standard Association, "P3349 - Space System Cybersecurity Working Group," IEEE Standard Association, [Online]. Available: https://sagroups.ieee.org/3349/. [Accessed 20 November 2024].

[102] GIS Resources, GIS Resources, 3 March 2022. [Online]. Available: https://gisresources.com/everything-you-need-to-know-about-gps-l1-l2-and-l5-frequencies/. [Accessed 25 June 2024].

[103] ESA, "GPS Signal Plan," ESA Navipedia, [Online]. Available: https://gssc.esa.int/navipedia/index.php/GPS_Signal_Plan. [Accessed 25 June 2024].

[104] H. Pirayesh and H. Zeng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials,* vol. 24, no. 2, pp. 767 - 809, 14 March 2022.

[105] CCSDS, "Security Threats against Space Missions," 2022.

[106] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen and G. Lachapelle, "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques," *International Journal of Navigation and Observation,* July 2012.

[107] Analog Devices, "An Introduction to Spread-Spectrum Communications," Analog Devices, 18 February 2003. [Online]. Available: https://www.analog.com/en/resources/technical-articles/introduction-to-spreadspectrum-communications--maxim-integrated.html. [Accessed 27 June 2024].

[108] S. Salim, N. Moustafa and M. Reisslein, "Cybersecurity of Satellite Communications Systems: A Comprehensive Survey of the Space, Ground, and Links Segments," *IEEE Communications Surveys & Tutorials,* 3 June 2024.

[109] N. Khatwani, "IP Spoofing and it’s Countermeasures.," Medium, 19 September 2020. [Online]. Available: https://medium.com/@namrata_khatwani/ip-spoofing-and-its-countermeasures-755fe0aa7116. [Accessed 1 July 2024].

[110] M. Zaoui, B. Yousra, S. Yassine, M. Yassine and O. Karim, "A Comprehensive Taxonomy of Social Engineering Attacks and Defense Mechanisms: Toward Effective Mitigation Strategies," *IEEE Access,* vol. 12, pp. 72224 - 72241, 20 May 2024.

[111] "Cyber Range," Ciberbit, [Online]. Available: https://www.cyberbit.com/platform/cyber-range/. [Accessed 17 July 2024].

[112] A. Ibrahim, Y. Fernando, M. S. Shaharudin, Y. Ganesan, N. H. Ahmad, A. Amran and L. k. Loon, "Aerospace Supply Chains Using Blockchain Technology: Implications for Sustainable Development Goals," *Sustainable Operations, Logistics and Supply Chain Management's Lab,* 2024.

[113] Cyber Defense Agency, "Securing The Software Supply Chain," August 2022. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF. [Accessed 5 July 2024].

[114] N. Boschetti, C. Smethurst, G. Epiphaniou, C. Maple, J. Sigholm and G. Falco, "Ground Station as a Service Reference Architectures and Cyber Security Attack Tree Analysis," in *IEEE Aerospace Conference Proceedings*, 2023.

[115] J. Saltzer and M. Schroeder, "The protection of information in computer systems," *Proceedings of the IEEE,* vol. 63, no. 9, pp. 1278 - 1308, 1975.

[116] "A04:2021 – Insecure Design," OWASP , 2021. [Online]. Available: https://owasp.org/Top10/A04_2021-Insecure_Design/. [Accessed 16 July 2024].

ANNEXES

ANNEX A. SUPPORT MATERIAL

This annex introduces the technical notes generated throughout this internship. These technical notes serve as supplementary material for this final internship report and are listed as follows:

A.1 TN01 – Literature Review and State-of-the-Art Study on Cybersecurity for Space or Similar Domains

This technical note (CSW-2024-TNR-01442-Technical-Note-01-State-of-the-art-Cybersecurity.pdf) presents a detailed analysis of the state-of-the-art cybersecurity in the Space sector, discussing the current landscape of Space Systems and the associated cybersecurity processes and tools [9].

A.2 TN02/03 - Analysis of Practices and International Standards

This technical note (CSW-2024-TNR-01469-Technical-Note-02-Cybersecurity-Standards.pdf) presents a detailed analyses of cybersecurity standards, generic and sector-specific (Space, automotive, railway and aviation) [10].

A.3 TN04 - Space System Threats and Vulnerabilities

This technical note (CSW-2024-TNR-01468-Technical-Note-04-Space-System-Threats-and-Vulnerabilities.pdf) provides a list of Space Sector threats and vulnerabilities [11].

A.4 TN05 - Proposals to Cope with Threats and Vulnerabilities

This technical note (Technical Note 05 - Proposals to Cope with Threats and Vulnerabilities.pdf) provides the proposed mitigation strategies for Space System Threats and Vulnerabilities [12].

A.5 TN06 - Proposal to Change/Improve/Integrate Specific Requirements into the ECSS E40 & Q80

This technical note (CSW-2024-TNR-04549-Technical-Note-06-Proposals-to-Change-Improve-Integrate-Specific-Requirements-into-the-ECSS-E40-&-Q80.pdf) details the analysis of European software space engineering standards to identify

cybersecurity gaps and suggests specific requirements to improve the cybersecurity capabilities of space systems, based on a literature review and survey responses [13].

A.6 Survey on Cybersecurity Challenges and Solutions for Space Systems Report

This report (CSW-2024-TNR-03904-Report-Cybersecurity-Survey.pdf) presents a detailed analysis of expert responses on Space Sector Cybersecurity survey [14].

A.7 DASIA Paper - Engineering and Assessing Cybersecurity for Space Systems

Using the results gathered from the survey, a paper was produced that analyses the main challenges and considerations concerning cybersecurity for space systems. This paper highlights the urgent need for collaborative efforts among stakeholders to safeguard critical infrastructures within the space domain [15].

ANNEX B. THREATS AND VULNERABILITIES MITIGATIONS

The following subsections present the threats and vulnerabilities and their respective mitigations in more detail.

B.1 Threats Mitigation

The categorization divides threats into two primary groups: electromagnetic threats, encompassing issues like direct energy attacks or electromagnetic interference, and cyber threats targeting software, hardware, or communication infrastructure of space systems.

B.1.1 ELECTROMAGNETIC THREATS SOLUTIONS

The following threats focus on electromagnetic threats, specifically those originating from both environmental and man-made sources.

B.1.1.1 Environmental

Solutions focus on threats arising from natural phenomena.

B.1.1.1.1 Solar Radio Bursts

The Global Positioning System (GPS) utilizes three primary L-band frequencies for civilian use, ranging from 1 to 2 GHz: L1, L2, and L5. Additionally, there's civilian codes, Course Acquisition (C/A) and military-exclusive P-Code and a more modern M code. These codes that are crucial for [102]:

- **Calculating distance**: The codes help receivers determine the distance between themselves and the satellite.
- **Identifying messages**: Codes distinguish between different types of transmitted information.
- **Security**: Codes like the M code enhance transmission security through exclusivity, authentication, and confidentiality (along with streamlined key distribution).

With GPS modernization, new civilian signals have been introduced: L1C, L2C, and L5. Here's a breakdown of the frequencies and their purposes [103]:

- **L1** (1575.42 MHz): Primarily used for tracking GPS satellite location.
- **L1C** (similar frequency to L1): Designed for interoperability with Europe's Galileo system, it offers higher power and advanced security features.
- **L2** (1227.60 MHz): Used to monitor the health of GPS satellites.
- **L2C** (similar frequency to L2): Designed to meet commercial needs for dual-frequency receivers, improving accuracy.

- **L5** (1176.45 MHz): Improves accuracy for civilian applications like aircraft precision approach guidance.

SRD-1 Mitigation – Increase Signal Power & New Civilian Codes: Solutions to mitigate the effects mentioned earlier are already in use. These include increasing the transmitted signal power at the L2 frequency and implementing new civilian codes, both of which enhance the stability and reliability of GNSS (Global Navigation Satellite System) operations during solar events [79].

B.1.1.1.2 Single Event Effects

The deposition of charged particles within a satellite, originating from cosmic events, direct ionization, and nuclear interactions, can cause significant damage to satellite hardware. Effects range from complete component destruction to more subtle errors like bit flips in memory cells or registers. [24]

Catastrophic Single Events:

- **Burnout**: High currents triggered by ionizing particles can overheat and permanently damage components.
    - **SEE-1 Mitigation**: Protect metal-oxide-semiconductor field-effect transistors (MOSFETs) with radiation-hardened designs to withstand larger linear energy transfer (LET).
- **Functional Interrupt**: This event causes unexpected loss of functionality or changes the state of a device, similar to a Single Event Upset (SEU).
    - **SEE-2 Mitigation**: Power-cycling the device typically restores functionality, though some damage may be permanent.
- **Gate Rupture**: The impact of ionizing particles damages the gate dielectric of a transistor, leading to insulator breakdown and increased temperature. Devices using non-volatile static random-access memories (SRAM) and electrically erasable programmable read-only memories (EEPROMs) are particularly vulnerable.
    - **SEE-3 Mitigation**: Avoid using SRAM and EEPROM technologies in radiation-sensitive environments.
- **Latch-up**: This event creates a low-resistance path between power and ground due to ionizing particles, resulting in high currents, vaporized metals, and potentially permanent damage.
    - **SEE-4 Mitigation**: Rapidly disconnect power to prevent further damage from high currents.

Non-Catastrophic Single Events:

- **Multiple Bit Upset** (MBU): This event primarily affects memory components. Ionizing particles flip multiple bits within the same data word.

    - **SEE-5 Mitigation**: Employ error-correcting codes (ECC) and distribute data bits non-contiguously in memory.
- **Multiple Cell Upset** (MCU): Ionizing particles cause multiple bits within an integrated circuit to flip state simultaneously.
    - **SEE-6 Mitigation**: Increase spacing between transistors in integrated circuit design.
- **Transient Errors**: Ionizing particles induce temporary errors in a circuit's combinational logic, with increased likelihood at faster operating speeds.
    - **SEE-7 Mitigation**: Employ techniques like circuit redundancy and voting to correct for transient errors.

B.1.1.2 Man-made

These threats can also be caused by human interference, potentially leading to disruptions of operations and alterations to data transmitted from the satellite.

B.1.1.2.1 Jamming

Jamming interferes with RF communications by transmitting radio signals on the same frequency as legitimate communications, effectively overpowering them. This disruption interrupts transmissions between satellites, or between satellites and ground stations.

To mitigate this threat, various anti-jamming techniques can be employed [104] [105]:

Signal Processing Techniques:

- **JAM-1 - Time-Frequency Filtering Mask**: This technique leverages the unique characteristics of jamming and GPS signals in both the time and frequency domains. The filter identifies and suppresses the jamming signal's energy while allowing the GPS signal to pass through.
- **JAM-2 - Adaptive Notch Filter**: This filter continuously detects, estimates the frequency of, and blocks single-tone continuous jamming signals. Its adaptability allows it to adjust to changes in the jamming signal's frequency.
- **JAM-3 - Short-Time Fourier Transform** (STFT): By analysing signals in both time and frequency domains, STFT enhances the notch filter's ability to respond quickly to changes in jamming frequencies and handle wider jamming bandwidths.
- **JAM-4 - ACM and DWT Filtering**: This two-step process uses an Approximate Conditional Mean (ACM) filter to estimate the true GPS signal, followed by a Discrete Wavelet Transform (DWT) filter to further refine the signal and remove jamming components. This approach has demonstrated

the ability to maintain a high signal-to-noise ratio (SNR), even under severe jamming conditions.

Antenna Array Techniques:

- **JAM-5 - Spatial Filtering, Polarization Diversity, and Adaptive Adjustment**: Antenna arrays utilize multiple antennas to pinpoint the desired GPS signal, suppress jamming signals from other directions, and adapt to changing jamming tactics.
- **JAM-6 - Spectral Self-Coherence Beamforming**: This technique amplifies the GPS signal based on its self-coherent properties while cancelling out the jamming signal, which typically lacks such patterns.
- **JAM-7 - Spatial-Temporal Interference Projection**: This method differentiates between the GPS and jamming signals based on their spatial and temporal characteristics, projecting the received signal onto a subspace orthogonal to the jamming signal to effectively eliminate it.
- **JAM-8 - Regret Minimization Framework & Game-Theoretical Approach**: This combines decision-making under uncertainty with game theory to develop a system where users can quickly adapt their strategies to maximize successful communication despite jamming.

B.1.1.2.2 Spoofing

Spoofing involves transmitting counterfeit signals that mimic legitimate GPS signals to deceive receivers and gain unauthorized access.

To safeguard against this threat, various cryptographic techniques can be employed [18] [106]

- **SPOO-1 - Navigation Message Authentication** (NMA): This mechanism ensures the authenticity and integrity of navigation data using either symmetric or asymmetric key encryption.
- **SPOO-2 - Chips Message Robust Authentication** (CHIMERA): A hybrid of NMA and spreading code authentication, CHIMERA uses the P-224 elliptic curve digital signature algorithm for added security.
- **SPOO-3 - Timed Efficient Stream Loss-tolerant Authentication** (TESLA): Used in the Galileo GNSS system, TESLA, combined with Message Authentication Code (MAC), verifies the origin and identity of messages.
- **SPOO-4 – Cross sensor´s information**: sensors like inertial measurement units (IMUs) and vehicle odometers can help detect spoofing by cross-checking data against GNSS measurements. Discrepancies between sensor readings can indicate a potential spoofing attack.

- **SPOO-5 – Y-code**: Military GPS signals are further protected by an encrypted binary code known as the Y-code. This code significantly enhances security, making it extremely difficult to spoof these signals without access to the Y-code.
- **SPOO-6 - C/N0 monitoring**: C/N0, or Carrier-to-Noise density ratio, is a measure of the strength of a received GPS signal relative to background noise. C/N0 monitoring is a valuable tool in anti-spoofing techniques. By tracking the history and behaviour of C/N0, GPS receivers can detect sudden anomalies that may indicate a spoofing attack, allowing for timely intervention and protection of GPS-based navigation systems.
- **SPOO-7 - Absolute Power Monitoring**: GPS signal strength decreases as it travels through the atmosphere and other obstacles (a phenomenon known as path loss). This decrease is highly variable and depends on factors like distance, terrain, and weather conditions. On Earth, the maximum power of a legitimate GPS signal at the L1 frequency (used by civilian GPS devices) is around -153 dBW (decibel-watts). If a receiver detects a signal significantly stronger than this, it strongly suggests a spoofing attack.

The authors of [106] provide a comprehensive survey of over a dozen additional GPS defence techniques against spoofing. These include analysing power variations relative to receiver movement, comparing L1/L2 power levels, and examining differences in signal direction of arrival, among others.

B.1.1.2.3 Eavesdropping

Eavesdropping involves the interception of signals from satellites or other sources for monitoring purposes, often referred to as signals intelligence (SIGINT). SIGINT can be further divided into two categories:

- **Communications Intelligence** (COMINT): Focuses on intercepting and analysing voice communications.
- **Electronic Intelligence** (ELINT): Focuses on intercepting and analysing other types of radio signals, such as radar emissions or telemetry data.

To protect against eavesdropping, strong signal encryption is crucial. To mitigate such a threat there are various mitigation techniques [17]:

- **EAV-1 - On-Board Encryption**: One traditional method involves employing on-board encryption capabilities with pre-shared secret keys between the ground station and satellite. This ensures only authorized parties can decrypt and understand the messages. However, this approach is vulnerable if the shared key is compromised.
- **EAV-2 – New Cryptographic techniques**: Newer approaches, such as public-key cryptography and quantum key distribution, can overcome the vulnerabilities of pre-shared keys.

- **Public-Key Cryptography**: Utilizes a pair of keys – a public key for encryption (known to everyone) and a private key for decryption (known only to the recipient). This eliminates the need for pre-sharing secret keys.
- **Quantum Key Distribution** (QKD): This cutting-edge technology leverages principles of quantum mechanics to securely distribute encryption keys between the satellite and ground systems, offering the potential for virtually unbreakable encryption.

B.1.2 Cyber Threats Solutions

The following threats focus on cyber threats, which can target both technical vulnerabilities and exploit social engineering tactics.

B.1.2.1 Technical

Cyber threats exploit technical vulnerabilities in software to gain unauthorized access to systems and data.

B.1.2.1.1 Signal Hijacking

Signal hijacking consists of an unauthorized takeover of a transmission channel to cause disruption or spread malicious content. This can occur if the command and control (C2) link is poorly encrypted. Therefore, the first step in mitigation is to implement robust signal encryption. The solutions for this involve the same techniques already identified in eavesdropping mitigations.

Additionally, **spread spectrum** can be implemented to further enhance security.

SH-1 - Spread Spectrum: Spread spectrum intentionally expands signal bandwidth by injecting a higher frequency signal, causing the transmitted signal to appear as noise. The process involves a spreading operation (injecting a spread-spectrum code) before transmission and a dispreading operation (removing the code) at the receiver. The same code, known at both ends of the channel, is essential for successful communication [107].

B.1.2.1.2 Data Corruptions and Interception

Data corruption and interception are critical security threats in the space sector, targeting communication channels between satellites and ground stations.

- **Data interception** refers to the unauthorized access and capture of data transmitted between a satellite and a ground station.
- **Data corruption** involves the unauthorized alteration or modification of data transmitted between a satellite and a ground station.

To mitigate these threats, it is essential to use robust cryptographic algorithms, such as those mentioned in eavesdropping mitigations, to ensure data transmitted or stored remains secure and confidential. In addition to the encryption techniques

already identified, several others can help protect data in transit and at rest, including [108]:

- **DC&I-1 - Advanced Encryption Standard** (AES): A widely used symmetric encryption algorithm for securing sensitive data. In ground segment security, AES-counter mode is often employed to further enhance security and system performance. AES utilizes three key sizes (128, 192, and 256 bits), the selection of which should align with the required security standards.
- **DC&I-2 - Triple Data Encryption Standard** (3DES): A symmetric encryption algorithm that applies the Data Encryption Standard (DES) cipher three times to each data block using three different keys. However, 3DES performs poorly compared to AES, as it is considerably slower.
- **DC&I-3 - Rivest-Shamir-Adleman** (RSA): A widely used asymmetric encryption algorithm for secure data transmission. It employs a pair of keys: one public key for encryption and one private key for decryption. RSA is primarily used for digital signatures but is also valued for protecting sensitive data, including login credentials, in satellite communication systems.
- **DC&I-4 - Elliptic Curve Cryptography** (ECC): A public key encryption technique based on elliptic curve theory, offering strong security with relatively small key sizes. Compared to RSA, ECC provides equivalent security with smaller keys, making it a lightweight cryptographic technique ideal for satellites with resource constraints.
- **DC&I-5 - Secure Hash Algorithm** (SHA): A family of cryptographic hash functions used to generate unique, fixed-size message digests for data integrity verification. The resulting hash code is virtually impossible to reverse-engineer.
- **DC&I-6 - Intrusion Detection and Prevention Systems**: the use these systems onboard spacecraft, employing signatures and machine learning, can help detect and prevent cyber intrusions [23].

B.1.2.1.3 Denial-Of-Service

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.

Mitigating denial-of-service (DoS) attacks on satellites is a significant challenge due to the unique constraints and vulnerabilities of space-based systems. However, several strategies can be employed to enhance resilience against such attacks [20] [23], (see Section 3.5), [105]:

Network-Level and Satellite Mitigation:

- **DoS-1 - Traffic Filtering and Rate Limiting**: Implementing filtering mechanisms at ground stations or network gateways can help detect and block suspicious traffic patterns indicative of a DoS attack. Rate limiting can restrict the number of requests from a single source, preventing overwhelming legitimate traffic.
- **DoS-2 - Intrusion Detection and Prevention Systems** (IDPS): IDPS can monitor network traffic for signs of malicious activity, such as sudden spikes in traffic or unusual packet patterns, and automatically trigger mitigation actions.
- **DoS-3 - Geolocation Filtering**: Filtering traffic based on geographic origin can help block attacks originating from known malicious sources or regions. (survey mitigations)
- **DoS-4 - Hardening Satellite Software and Firmware**: Regularly updating and patching satellite software and firmware can help address vulnerabilities that could be exploited in a DoS attack.
- **DoS-5 - Redundancy and Failover Mechanisms**: Building redundancy into critical satellite components and systems can ensure continued operation even if some components are overwhelmed or disabled by an attack.

Ground-Level Mitigation:

- **DoS-6 - Use DDoS-resistant services**: This ensures you have enough bandwidth to handle traffic spikes caused by malicious activity.
- **DoS-7 - Distribute servers geographically and topologically**: Distributing servers across different locations makes it harder for attackers to target and successfully attack your infrastructure.
- **DoS-8 - Configure firewalls and routers to drop Internet Control Message Protocol** (ICMP) packets and block DNS.
- **DoS-9 - Protect your DNS servers**: DNS servers are often targeted in DoS attacks. Using measures like DDoS-resistant DNS providers can help mitigate this risk.

B.1.2.1.4 Web Spoofing

In the network domain, spoofing is a deceptive tactic where cybercriminals gain unauthorized access to systems by impersonating trusted entities. Common types of spoofing include [109]:

- **Email Spoofing**: Forging email headers to make messages appear as if they originated from a different sender.
- **IP Spoofing**: Masking the true source IP address of network traffic.

- **Website Spoofing**: Creating fake websites that mimic legitimate ones to steal information or distribute malware.

To mitigate the risks of spoofing attacks, several countermeasures can be taken [109] [105]:

- **WS-1 - Use strong authentication**: Implement multi-factor authentication (MFA) and avoid relying solely on passwords.
- **WS-2 - Securely store secrets**: Avoid storing passwords or other sensitive data in plaintext. Use encryption or hashing techniques.
- **WS-3 - Protect credentials during transmission**: Encrypt credentials when sending them over networks.
- **WS-4 - Secure authentication cookies with SSL/TLS**: Use HTTPS to protect authentication cookies and ensure secure transmission of sensitive data.
- **WS-5 - Implement packet filtering**: Analyse and discard incoming/outgoing packets with suspicious source/sender IP addresses.
- **WS-6 - Avoid host-based authentication**: Use encrypted connections (e.g., SSH) for remote logins and authentication.

While detecting IP spoofing is difficult for end users, they can minimize their risk of other types of spoofing by taking the following precautions [109] [105]:

- **WS-7 - Use HTTPS for secure browsing**: Ensure websites have valid SSL/TLS certificates to protect against eavesdropping and tampering.
- **WS-8 - Filter ICMP packets**: ICMP (Internet Control Message Protocol) can be used in some spoofing attacks, so filtering them can add a layer of protection.
- **WS-9 - Use random sequence numbers and reduce initial TTLs** (Time-to-Live): This can make it harder for attackers to guess sequence numbers and exploit vulnerabilities in network protocols.
- **WS-10 - Employ encryption**: Use encryption tools to protect sensitive data during transmission and storage.
- **WS-11 - Avoid authentication based solely on IP**: Rely on stronger authentication methods that are not easily spoofed.

B.1.2.1.5 Software Threats

Software threats, such as malware, are designed to infiltrate and control organizational information systems, identify sensitive data, exfiltrate that data back to adversaries, and conceal their activities. These threats pose a significant risk to space systems.

To mitigate the risks of software threats, adhere to the following best practices [20] [105]:

- **ST-1 - Keep your software, internet browser, and operating system up to date**: Regularly apply security patches and updates to address vulnerabilities that could be exploited by malware.
- **ST-2 - Use safe search tools that warn you about malicious sites**: These tools can help you avoid clicking on links or visiting websites that may harbour malware.
- **ST-3 - Use security software and antivirus**: Install and regularly update reputable security software to detect and remove malware.
- **ST-4 - Install NoScript (or a similar extension) on your browser**: This extension can help prevent malicious scripts from running on websites.
- **ST-5 - Acceptance testing**: This involves thoroughly testing the software to ensure it meets all functional and non-functional requirements, including security requirements, before deployment. It helps identify any potential vulnerabilities or issues that might be exploited by malware.
- **ST-6 - System evaluation**: This involves independent verification and validation (IV&V) and code analysis to assess the system's security posture and identify any potential weaknesses or vulnerabilities.
- **ST-7 - Continuous threat monitoring, continuous risk management**: This involves continuously monitoring the system for potential threats and vulnerabilities, and proactively managing risks to mitigate the likelihood or impact of a security incident.
- **ST-8 - Run-time security monitoring**: Monitoring the system during operation to detect any suspicious activity or potential attacks in real time.
- **ST-9 - Auditing**: Periodically reviewing the system's security controls and processes to ensure they are effective and compliant with relevant regulations and standards.
- **ST-10 - Supply chain confidence**: Establishing trust and ensuring the security of the entire software supply chain, from development to deployment, to minimize the risk of introducing vulnerabilities through third-party components or services.

B.1.2.1.6 Man-in-the-Middle

A man-in-the-middle (MITM) attack is a cyberattack where a threat actor secretly positions themselves between two communicating parties. The attacker's goal is to eavesdrop on the communication, potentially intercepting or manipulating data without either party's knowledge.

To minimize the risk, users should [20]:

- **MITM-1 - Avoid using Wi-Fi connections that are not password-protected**: Open Wi-Fi networks are more vulnerable to MITM attacks.
- **MITM-2 - Avoid using public networks for sensitive transactions**: Use a trusted and secure network (e.g., your home Wi-Fi) when conducting online banking or sharing sensitive information.
- **MITM-3 - Log out of applications immediately when not in use**: This prevents unauthorized access in case your session is hijacked.
- **MITM-4 - Use strong encryption, such as a VPN**: While an attacker can still intercept encrypted messages, they will be unable to read or alter the data without the encryption key.

B.1.2.1.7 Zero-Days-Exploits

A zero-day exploit is a cyberattack that targets a software vulnerability unknown to the software vendor or security researchers. The term "zero-day" refers to the fact that developers have zero days to address the flaw before it's exploited.

While there is no immediate fix for a zero-day exploit, several proactive measures can mitigate the risk [14]:

- **ZDE-1 - Vulnerability Databases**: Utilizing resources like the National Institute of Standards and Technology (NIST) National Vulnerability Database can expedite the identification and patching of known vulnerabilities, potentially preventing them from becoming zero-day exploits.
- **ZDE-2 - Machine Learning for Anomaly Detection**: Machine learning algorithms can analyse past exploit data to establish a baseline of normal system behaviour. Any deviations from this baseline might signal a potential zero-day attack.
- **ZDE-3 - Space System Information Sharing and Analysis Center (ISAC)**: Establishing a Space System Information Sharing and Analysis Center (ISAC) would be a significant step in this direction [19]. This will enable cooperation between the public and private space sectors, along with the academic community, is crucial for mitigating zero-day threats

The key functions of such an ISAC would include [19]:

- **Information Sharing**: Encouraging participation from government agencies (e.g., the U.S. Department of Defence, NASA) and private sector space organizations to foster information sharing and collaboration on cybersecurity threats and best practices.
- **Timely Vulnerability Disclosure**: Requiring member entities to promptly disclose vulnerability and attack information within a predefined timeframe,

similar to the European Union's General Data Protection Regulation's 72-hour breach notification requirement.

- **Curated Best Practices**: Developing and maintaining a central repository of cybersecurity standards and best practices specific to space systems, with input and contributions from ISAC members.
- **Cross-Sector Threat Sharing**: Sharing relevant threat information with other critical sectors that rely on space systems (e.g., telecommunications, finance) to ensure comprehensive preparedness and response.

B.1.2.1.8 Password Attacks

Passwords serve as the first line of defence, protecting data access from unauthorized individuals. Over time, password requirements have become more stringent.

Hackers employ various methods to crack passwords, including:

- **Phishing**: Deceptive emails or messages designed to trick users into revealing their passwords or clicking malicious links.
- **Man-in-the-middle (MitM) attacks**: Attackers intercept communications to steal data, including passwords.
- **Brute-force attacks**: Automated software rapidly tries numerous username and password combinations to gain access to an account.
- **Dictionary attacks**: Hackers use lists of common words and phrases to guess passwords.
- **Credential stuffing**: Hackers test stolen username and password combinations from other breaches, hoping they work on different platforms.
- **Keyloggers**: Malicious software that records keystrokes, including passwords.

While passwords are considered a primary defence, they are also a vulnerability. Complex password requirements often lead users to write down passwords, making them susceptible to discovery by malicious actors.

A potential solution is to move beyond passwords and adopt cryptographic keys, often called passkeys.

- **PA-1 – Passkeys:** Passkeys leverage public key cryptography and biometrics (like fingerprints or facial recognition) for secure authentication without the need to remember or manually enter complex passwords. This approach aims to eliminate the risk of weak or reused passwords and enhance overall security [14] .

B.1.2.1.9 Injection Attacks

Injection attacks are a common and powerful threat, targeting vulnerabilities in web applications, databases, and other systems that rely on user input.

To withstand these attacks, the following measures are recommended [RD-12]:

- **IATT-1 - Apply the principle of least privilege**: Grant database users only the minimum permissions necessary to perform their tasks. This limits the potential damage if an attacker gains access.
- **IATT-2 - Avoid dynamic SQL**: If possible, use parameterized queries or prepared statements to prevent attackers from injecting malicious SQL code.
- **IATT-3 - Validate input data**: Implement rigorous input validation at the application level to ensure that user-supplied data conforms to expected formats and does not contain malicious code. Use a whitelist approach to allow only specific, safe input values.

B.1.2.1.10 Social Engineering

These threats exploit people's psychological vulnerabilities. Attackers manipulate and deceive victims into compromising systems, often by tricking them into installing malware or revealing login credentials.

Detecting social engineering attacks is increasingly difficult. The use of artificial intelligence (AI) in such attacks can make them harder to recognize, as attackers can craft sophisticated and personalized messages to deceive victims. Additionally, social engineering relies on manipulating human psychology, making it challenging to predict or prevent all potential scenarios.

To mitigate this threat, organizations can implement comprehensive cybersecurity strategies, as depicted in Figure 26:

- **SE-1 - Awareness and Training**: Educate employees and individuals about social engineering tactics, including common red flags and how to respond to suspicious requests.
- **SE-2 - Technical Controls**: Implement multi-factor authentication, email filtering, web filtering, and intrusion detection systems to bolster security and detect potential threats.
- **SE-3 - Policies, Procedures, and Governance**: Establish clear policies outlining acceptable use of systems and data, procedures for handling sensitive information, and a governance framework to oversee cybersecurity practices.
- **SE-4 - Incident Response and Reporting**: Develop a clear process for reporting and responding to suspected or confirmed social engineering incidents, including steps for containment, damage assessment, and recovery.

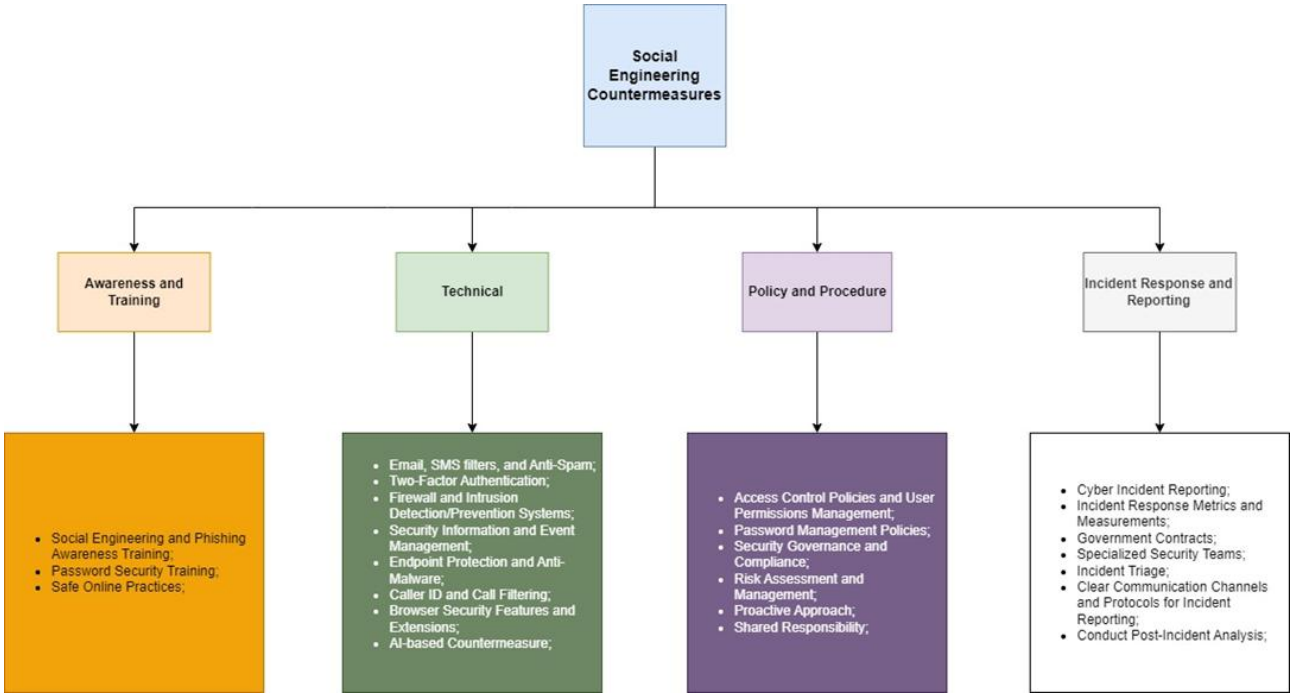


Figure 26: Mitigation Strategies for Social Engineering [110]

The following topics will go more in detail about the cybersecurity strategies.

B.1.2.1.10.1 Awareness and Training

Educating all personnel within an organization is crucial, as they are often the primary targets of social engineering attacks. Providing employees with the tools to protect themselves and the company is essential. To achieve this, comprehensive social engineering and phishing awareness training should be conducted.

This training should educate employees about the various types of social engineering techniques and keep them updated on the latest tactics and defence strategies. Simulated attacks, such as sending employees internal phishing emails, links, or attachments, or organizing a game that playfully "penalizes" those who leave their computers unlocked (for example, by requiring them to buy donuts for the team [19]), can be used to assess their awareness and preparedness [110].

Password security training is equally important. Employees should be taught best practices for creating strong passwords, the risks of reusing passwords, and the importance of avoiding password sharing [110] .

Additionally, training on safe online practices is vital. This includes raising awareness about the risks of opening unknown attachments, analysing email headers for potential red flags, hovering over links to verify their legitimacy before clicking, and refraining from sharing personal information online [19] [110] .

To achieve advanced cybersecurity proficiency, organizations can leverage solutions like "cyber ranges," immersing employees in hyper-realistic simulated attacks to enhance awareness, skills, and teamwork. A prime example is the Cyberbit Cyber

Range [111], an on-demand platform offering a comprehensive catalogue of cyber-attacks, as shown in Figure 27.

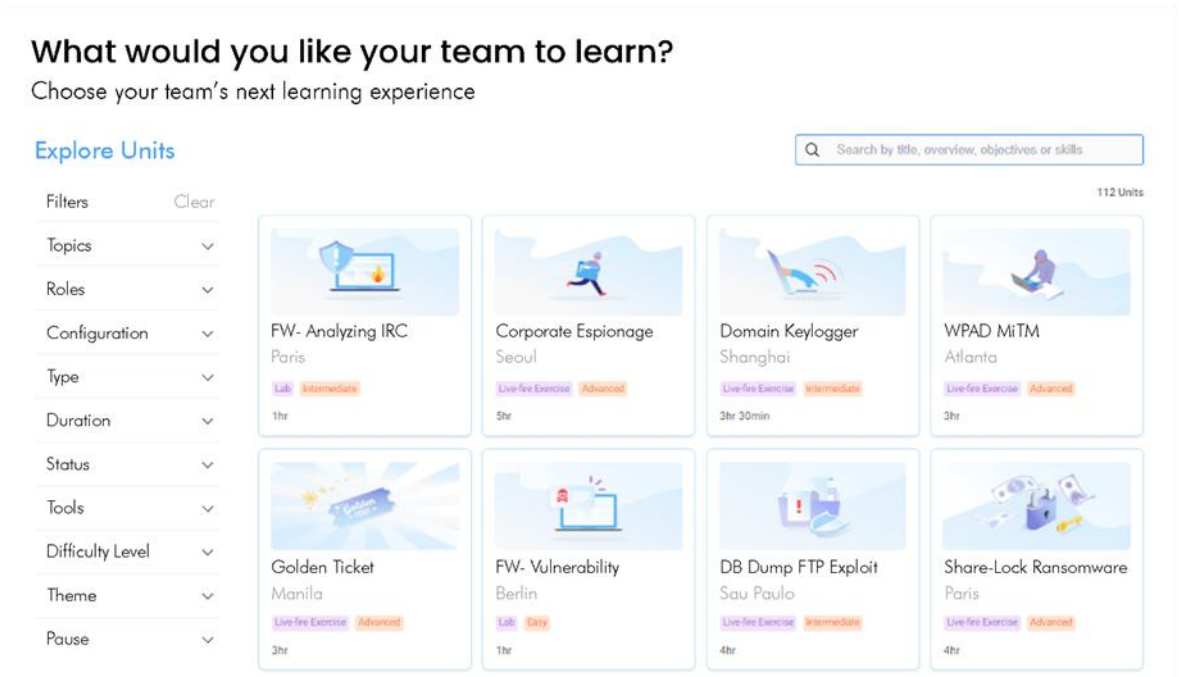


Figure 27: Catalogue of cyber-attacks [111]

This enables teams to recognize and respond effectively to various threats while learning industry best practices through the integration of NIST, NICE, CREST, and MITRE ATT&CK frameworks. Suitable for Red, Blue, or Purple teams, it caters to all skill levels, from beginner to advanced.

The platform also supports attack simulations against cloud-native and hybrid environments, utilizing industry-standard tools like Wireshark, McAfee, Carbon Black, and others depicted in Figure 28.

Figure 28: Commercial tools used by Cyberbit Cyber Range [111]

The exercises within this framework run on corporate-grade virtual networks, helping to identify challenges teams may face during incident detection, investigation, and response. To further strengthen this solution, it continuously assesses employees' real-time cyber performance during simulations.

The Cyberbit Cyber Range also offers a unique feature: simulated attacks on operational technology (OT). It provides a full-scale, emulated OT network and end-to-end simulations of IT-to-OT attacks, adding another layer of realism and complexity to the training environment, as depicted in Figure 5

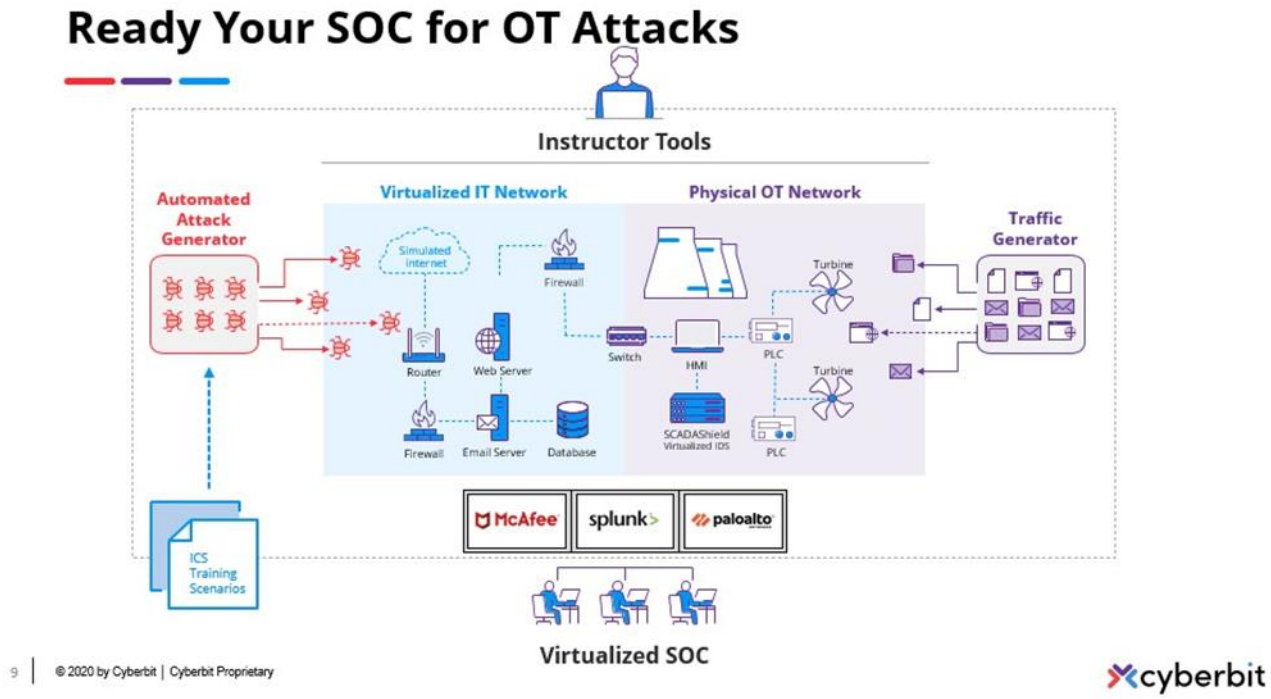


Figure 29: OT networks simulation attacks [111]

By implementing comprehensive awareness training programs and promoting a culture of security, organizations can significantly reduce their vulnerability to social engineering attacks.

B.1.2.1.10.2 Technical Controls

Once personnel are aware of the dangers, introducing software to enhance prevention further adds significant value. Examples of such technical controls include [110]:

Email, SMS filters, and Anti-Spam Solutions: These tools analyse incoming messages to identify and block phishing emails and spam containing malicious links or attachments.

- **Two-Factor Authentication** (2FA): Implementing 2FA strengthens access security by requiring an additional form of identification (such as a code from an authenticator app) beyond a password.
- **Firewall and Intrusion Detection/Prevention Systems** (IDPS): Employ a well-configured firewall to monitor and block unauthorized intrusions or malicious activities. IDPS actively scan network traffic for suspicious patterns and can take immediate action to protect systems.

- **Security Information and Event Management** (SIEM) **Solutions**: SIEM solutions aggregate and analyse security logs from various sources, enabling faster detection and response to suspicious activities.

Endpoint Protection and Anti-Malware Solutions: Installing antivirus software, VPNs (Virtual Private Networks), and other endpoint protection tools safeguards user devices from malware and unauthorized access.

- **Caller ID and Call Filtering Solutions**: These solutions help identify and block fraudulent or spoofed calls, preventing social engineering attacks through phone communication.
- **Browser Security Features and Extensions**: Configure web browsers to enhance security by activating all available security features. Install extensions to block untrusted websites and restrict access to sites without valid certifications (e.g., those lacking HTTPS).
- **AI-based Countermeasures**: Leveraging AI can be a powerful defence against attacks that utilize AI. AI-powered tools can analyse communication patterns, identify anomalies, examine messages and links, flag potential threats, and scan data for breach indicators. Additionally, AI can streamline incident response by automating tasks and learning from past incidents to improve future security measures.

B.1.2.1.10.3 Policies, Procedures, and Governance

Regarding the establishment of policies, procedures, and governance mechanisms, the following should be considered [19] [110].

- **Access Control Policies and User Permissions Management**: Define and manage employee privileges and access to organizational resources. This minimizes the risk of unauthorized access and ensures appropriate access to systems, applications, and data.
- **Password Management Policies**: Establish clear guidelines and best practices for creating, storing, and changing passwords. Promote good password hygiene to ensure secure authentication.
- **Acceptable Use Policies**: Define acceptable behaviour and actions when using organizational resources, systems, and networks. Emphasizing security responsibilities and potential liabilities for breaches is crucial. Legislation should incentivize responsible parties to take necessary measures to secure their systems.
- **Security Governance and Compliance**: Establish a robust framework for managing security risks, implementing controls, ensuring compliance with relevant regulations and standards, and overseeing the effectiveness of social engineering mitigation techniques.

- **Risk Assessment and Management**: Develop a process for identifying and assessing vulnerabilities and potential risks, prioritizing them based on their potential impact, and implementing appropriate controls and mitigation techniques.
- **Proactive Approach**: Policymakers must take a proactive stance on space cybersecurity, rather than waiting for major cyberattacks to occur before enacting relevant legislation.
- **Shared Responsibility**: Policies concerning critical infrastructure security should also encompass the third-party infrastructure upon which it relies. For example, space systems should be held to the same security standards as the critical infrastructure they support.

B.1.2.1.10.4 Incident Response and Reporting

Responding to and reporting social engineering attacks in detail is crucial for organizations and the broader cyber community to evolve their mitigation strategies. To achieve this, the following activities should be undertaken:

- **Cyber Incident Reporting**: Similar to 32 Code of Federal Regulations Part 236, a rule should be established mandating that space asset organizations report all cyber incidents that have impacted or could potentially impact national security. This rule should include clear steps and instructions for timely reporting.
- **Incident Response Metrics and Measurements**: Utilize metrics to assess the effectiveness and efficiency of incident response efforts. This helps identify areas for improvement and optimize future responses.
- **Government Contracts**: Government contracts with space asset organizations should require contractors to comply with specific cybersecurity metrics, such as Key Performance Parameters (KPPs) and Key Performance Indicators (KPIs). These KPPs can specify the system's cybersecurity categorization for availability, integrity, and confidentiality, and should include appropriate cyber attributes within the system survivability KPPs based on applicable cybersecurity controls.
- **Specialized Security Teams**: Establish separate teams of cybersecurity specialists for mission systems and internal networks/server systems (operational technology vs. information technology). This is crucial due to the distinct operating environments, security skills, and expertise required for each. These teams would be responsible for effectively and promptly responding to any cyber threat, especially social engineering incidents.
- **Incident Triage**: Develop a process to analyse and categorize incidents based on impact, severity, and urgency. This prioritization facilitates the

implementation of targeted response efforts and the allocation of necessary resources.

- **Clear Communication Channels and Protocols for Incident Reporting**: Establish secure and easily accessible communication channels through which employees can promptly report incidents.
- **Conduct Post-Incident Analysis**: Thoroughly reviewing and analysing attacks helps identify weaknesses in current strategies and informs improvements for future defences.

B.1.2.1.11 **Other Technical Threats**

The following technical threats were identified through the cybersecurity survey titled "Survey on Cybersecurity Challenges and Solutions for Space Systems" [14] conducted among space sector specialists. A summary of these threats and respected mitigations is presented in Table 4:

Table 21: Threats and respective mitigations identify by the experts

Threat	Mitigation
Source Code Tampering	**SCT-1 -** Extensive code analysis (static analysis with cybersecurity rules)
	SCT-2 - Zero code smells and zero warnings objective (from static analysis tools)
	SCT-3 - Protection of software development environments
	SCT-4 - Extensive V&V of the embedded device against fuzz inputs
	SCT-5 - Specific security assessment of the design/code
	SCT-6 - Integrity checks for all data, configurations, inputs to the system
Spacecraft configuration modification	**SCM-1 -** Intrusion detection mechanisms
	SCM-2 - Robust FDIR configuration
	SCM-3 - Proper authentication methods and access control
	SCM-4 - CRCs for all data transmission
	SCM-5 - Give an ID to every entity in the system
	SCM-6 - Telecommands acceptance is subject to validation
	SCM-7 - Periodically change the CRC/checksum/cryptography algorithms
	SCM-8 - Authentication on software patch
	SCM-9 - Accept telecommands and download telemetry only when flying above certain regions
Bad design	**BD-1 -** Secure-by-design approach (Zero trust solutions)
	BD-2 - Take security lessons learned from other projects/missions/domains into account
	BD-3 - Every user involved in activities related to the project shall be subjected to user authentication (Zero Trust model)

Threat	Mitigation
Speed up development / pressure	**SUD/P-1** - Prioritizing speed over thoroughness in design, code analysis, and testing can leave vulnerabilities in the final product. This must be tackled with the opposite, by following the good and secure development practices.
Lack of certification of space systems	**LCSS-1 -** Unlike industries like aviation (FAA) and railways (TUV), space systems lack comprehensive certification processes that include cybersecurity aspects.
Lack of vulnerability / threat analysis	**LV&TA-1 -** Awareness trainings **LV&TA-2 -** Security testing **LV&TA-3 -** Enforcing security standards **LV&TA-4 -** Conducting independent regular security audits **LV&TA-5 -** Ensure a SDLC is integrated in the application development **LV&TA-6 -** Training on security aspects, V&V **LV&TA-7 -** Check of OSS libraries vulnerabilities **LV&TA-8 -** Vulnerability / Threats Analysis done before requirements are closed **LV&TA-9 -** Security reviews
Exploit development tools	**EDT-1 -** Security reviews **EDT-2 -** Check of OSS libraries vulnerabilities **EDT-3 -** Robustness testing **EDT-4 -** Do a deep analysis and test all interfaces (Zero Trust model) **EDT-5 -** Conducting independent regular security audits **EDT-6 -** Security testing
Unmitigated errata	**UE-1 -** Errata analysis **UE-2 -** Security reviews

B.2 Vulnerabilities Mitigation

This chapter delves into the proposed mitigation techniques designed to address the identified vulnerabilities and enhance the overall security posture of space systems.

B.2.1 HUMAN FACTOR

The human factor represents a significant vulnerability in space systems and critical infrastructure across various industries. Humans design and build software and hardware, inevitably introducing vulnerabilities where human intervention occurs. Humans are also targets for cyberattacks, particularly social engineering. To mitigate these risks, organizations must invest heavily in building a strong cybersecurity culture and training their employees to be vigilant against the ever-present dangers.

B.2.2 DEVELOPMENT LIFE CYCLE

The lifespan and security requirements of space missions vary widely. Some missions may last 5 years, while others may operate for 25 years or more. To address these diverse needs, it is essential to adopt distinct secure software development lifecycles (SSDLCs) to avoid long-term problems.

Several examples of SSDLC frameworks exist, both in the space domain and other industries. The technical note on state-of-the-art cybersecurity for space and other domains identifies four prominent SSDLC frameworks [9]:

- **SSDLC -1 - Microsoft Security Development Lifecycle** (SDL): A comprehensive process that covers security practices throughout the entire software development lifecycle, from planning to maintenance.
- **SSDLC -2 - Software Security Touchpoints**: A lightweight framework that focuses on key security activities at critical points in the development process.
- **SSDLC -3 - Software Assurance Forum for Excellence in Code** (SAFECode): A collaborative effort by leading software companies to develop and promote best practices for software assurance.
- **SSDLC -4 - NIST Secure Software Development Framework** (SSDF): A set of fundamental, sound, and secure software development practices based on established secure software development practice documents.

By tailoring the choice of SSDLC framework to the specific needs and constraints of each space mission, organizations can significantly improve the security and resilience of their software systems over the long term.

B.2.3 Supply Chain

The supply chain is a significant vulnerability for space organizations. Space systems consist of numerous components often manufactured by diverse companies

worldwide, which may operate under varying cybersecurity regulations and enforcement. This inconsistency introduces potential vulnerabilities that malicious actors could exploit.

To protect the supply chain, the sector could implement the following measures [19] [26] [112] [113] [105]:

- **SC-1 - Enforce Cybersecurity Requirements**: Impose strict cybersecurity requirements for commercial technologies and off-the-shelf components used in both civilian and military space assets. Frameworks like the Cybersecurity Maturity Model Certification (CMMC) could be adopted.
- **SC-2 - Supply Chain Risk Management** (SCRM): Establish a robust SCRM program incorporating software assurance methods to minimize the likelihood of malware introduction into components and modules.
- **SC-3 - Obtain Products from Trusted Suppliers**: Prioritize suppliers with a proven track record of security and quality assurance. Verify their compliance with relevant cybersecurity standards and practices.
- **SC-4 - Component Maintenance**: Continuously monitor integrated components for any unauthorized modifications. Address known vulnerabilities identified by the team, community, or supplier through regular updates and patches. Maintain direct communication between the supplier and customer to ensure timely updates and support.
- **SC-5 - Software Bill of Materials** (SBOM): Maintain a detailed list of third-party components to facilitate validation and vulnerability identification. Examples of SBOM formats include:
    - The Linux Foundation's Software Package Data Exchange (SPDX)
    - OWASP CycloneDX
    - NIST Software Identification Tags
- **SC-6 - Harden the Build Environment**: Ensure that the environment used to build and assemble components is secure and free from potential vulnerabilities.
- **SC-7 - Promoting Security in Government Contracts**: Enforce strict cybersecurity standards in government contracts to incentivize commercial vendors to prioritize security in their products, potentially leading to industry-wide improvements.
- **SC-8 - Regulatory Framework for Private Sector Activities**: Create a regulatory framework to manage the growing private sector space activities, ensuring compliance with existing space treaties like the Outer Space Treaty while promoting industry efforts to strengthen cybersecurity and collaboration.
- **SC-9 - Use of Advanced Technology**: Leverage advanced technologies like blockchain to enhance the security, authenticity, and integrity of software and

hardware throughout the supply chain. The decentralized and immutable nature of blockchain can bring transparency, security, and traceability to every component [RD-20].

B.2.4 Commercial-off-the-Shelf

The rapid increase in the number of actors participating in the space sector is largely due to the availability of affordable commercial-off-the-shelf (COTS) software and hardware. Small companies can now easily enter the space domain by purchasing these products and assembling them without the need to develop software from scratch. However, COTS products are often highly complex, composed of millions of lines of code, with their inner workings not always clear to the user.
Therefore, thorough security analysis is crucial.

COTS-1 – Security Analysis: Black-box testing techniques such as fuzzing, boundary value analysis, and equivalence partitioning can be employed to assess the product's robustness. Additionally, ensuring compliance with established security guidelines, like Security Technical Implementation Guides (STIGs), and regularly checking for and addressing vulnerabilities listed in the OWASP Top Ten is essential for maintaining a secure system [18].

B.2.5 Technological Evolution

Since the space sector supports society and various industries, including critical ones, depend on it, any disruption to its operations can have worldwide repercussions, causing severe impacts on individuals and businesses alike. Therefore, it's imperative that the space sector remains at the forefront of technological evolution, particularly in the realm of cybersecurity.
Here are some examples of technological advancements that have enhanced cybersecurity in the space sector [18].:

- **TE-1 - Software-Defined Radio** (SDR): SDRs offer software control over functions traditionally performed by hardware, such as filtering, modulation, and mixing. This reduces the reliance on hardware, freeing up space for other components, and enables low-cost signal authentication solutions like fingerprint embedding, which acts as an authentication tag over message waveforms.
- **TE-2 - Cloud Computing**: Shifting data processing and storage from personal computers to secure data centers, accessible via the internet, enhances flexibility, availability, and redundancy. This allows for better management of customer scheduling needs through browser applications and provides protection against cyberattacks.
- **TE-3 - Optical Communication**: Moving away from traditional radio frequency (RF) communication, optical communication uses visible light for satellite communication. This technology is less vulnerable to jamming and other RF-based electronic warfare tactics.

- **TE-4 - Quantum Key Distribution** (QKD): This emerging field of cryptography holds the key to future-proofing encryption. While traditional encryption algorithms could be compromised by powerful quantum computers in the future, QKD utilizes quantum mechanics to establish secret keys with unconditional post-quantum security [112].
- **TE-5 - Ground Station as a Service** (GSaaS): This method aims to reduce the cost of acquiring infrastructure by enabling users to communicate with, process data from, control, and monitor satellites via the cloud using a simple laptop or desktop computer [114].

B.2.6 Static Code Analysis Tools

Organizations heavily rely on information technology, necessitating proactive measures to safeguard their confidential data. Cybersecurity tools play a vital role by continuously monitoring computer systems and networks, helping companies and individuals maintain data privacy and security.
One such tool is Static Code Analysis (SCA), along with threat/vulnerability detection tools.

SCA-1 - Static Code Analysis: These tools play a crucial role in preventing vulnerabilities by analysing source code to identify potential issues, bad practices, and vulnerabilities before they are exploited.

B.2.7 Security Analysis (Threats and Vulnerabilities)

This step focuses on identifying and understanding potential threats and vulnerabilities within a system. It is crucial for organizations, particularly those in the space sector, to conduct thorough security analyses before finalizing requirements. Several methods can be employed to perform this task effectively (from report of the survey) [9] [14]:

- **SA-1 - Threat Modelling**: This involves systematically identifying and assessing potential threats to a system, analysing their potential impact, and developing strategies to mitigate those risks.
- **SA-2 - Network Security Monitoring**: By analysing network traffic with tools like packet sniffers, security teams can extract data to be analysed, enabling the detection and prevention of attacks.
- **SA-3 - Vulnerability Scanning**: Automated tools scan the system for known vulnerabilities, such as outdated software or misconfigurations.
- **SA-4 - Penetration Testing**: This involves simulating real-world attacks to identify and exploit vulnerabilities in a system's defences, providing a more comprehensive assessment of the system's security posture.
- **SA-5 - Input Validation**: Rigorous validation of user input helps prevent injection attacks and other vulnerabilities arising from unexpected or malicious data.

- **SA-6 - Independent Regular Security Audits**: Periodically conducting independent security audits by external experts helps identify vulnerabilities and ensures compliance with industry best practices.
- **SA-7 - Fuzz Testing**: This software testing technique uncovers implementation bugs by injecting "random" or invalid input and analysing the system's behaviour.
- **SA-8 - Static Code Analysis**: This involves analysing the source code without executing it to identify potential issues, bad practices, and vulnerabilities.
- **SA-9 - Security Testing**: This encompasses various techniques like performance testing, simulated attacks (including buffer overflow and DoS testing), and equivalence class partitioning tests to assess a system's security posture under different conditions.

B.2.8 Security Requirements

Security requirements analysis is a critical process for protecting information and systems from cyber threats. To achieve this, it is essential to develop well-defined security requirements during the project design phase. This systematic process involves identifying, documenting, and refining the security needs of a system or organization.

SR-1 - Security Requirements Analysis: The first step is to identify and classify systems to assess their potential threats and vulnerabilities. After compiling a list of threats, a risk assessment is conducted to evaluate the likelihood and potential impact of each, allowing for the identification of the most significant risks.

Based on these identified threats and risks, specific security requirements are established. Organizations can leverage commonly used cybersecurity standards, such as IEC 62443 [53], to guide the development of these requirements.

B.2.9 Security Design

Based on the study and paper, titled "The Protection of Information in Computer Systems" done by Jerome H. Saltzer and Michael D. Schroeder in the 70s [115], to have a good security design it must follow ten principles highlighted by the authors. The main secure design principles are the following:

1. **Economy of Mechanism**: Design simplicity minimizes attack surfaces and aids code inspection.
2. **Fail-Safe Defaults**: Deny access by default, then grant permissions explicitly. Prioritize allowlists over denylists to prevent unauthorized access.
3. **Complete Mediation**: Check every access to every object, every time. Defence in depth is key.
4. **Open Design**: Security should rely on secret keys, not on obscurity. Embrace Kerckhoff's principle, which states that a cryptographic system's security depends solely on the secrecy of its keys.

5. **Separation of Privilege**: Multiple layers of protection, using different mechanisms, enhance security.
6. **Least Privilege**: Grant programs and users the minimum necessary rights (need-to-know basis).
7. **Least Common Mechanism**: Minimize shared components to limit the impact of a successful attack.
8. **Psychological Acceptability**: Balance security and usability to ensure user adoption.
9. **Work Factor**: Consider the attacker's resources when evaluating security measures.
10. **Compromise Recording**: Logging and evidence collection are vital for incident response.

These principles remain crucial guides in modern secure design. Following them can help avoid common vulnerabilities, but they must be complemented by secure implementation practices. The OWASP Top 10's inclusion of "Insecure Design" [116] emphasizes the ongoing importance of design-level security.

B.2.10 Security Implementation

In the security implementation phase of software development, the primary goal is to translate security requirements and design decisions into actual code. This critical stage demands meticulous attention to detail and a proactive approach to identify and mitigate potential vulnerabilities.

Adhering to secure coding guidelines and standards is paramount in this phase. These guidelines and standards, often established by industry organizations or internal teams, provide developers with a roadmap for writing code that is resistant to common security flaws.

Static Code Analysis tools are automated software solutions that analyse source code without executing it. They play a crucial role in the security implementation phase by acting as a vigilant second eye, scanning the code for potential security weaknesses and coding flaws that might have been missed during manual reviews (see Section 4.2.8).

Besides secure coding practices and SCA tools, organizations should consider other security measures during the implementation phase, such as:

- **SI-1 - Code Reviews**: Conducting thorough code reviews by peers or security experts to identify potential issues that might have been missed by automated tools.
- **SI-2 - Threat Modelling**: Identifying potential threats and vulnerabilities early in the development process to proactively mitigate risks.
- **SI-3 - Security Testing**: Performing security testing, including penetration testing and fuzz testing, to simulate real-world attacks and assess the system's resilience.

B.2.11 Security Testing

Security validation and testing is a systematic process of evaluating the effectiveness of security controls in a system or organization. It serves as a form of proactive defence, testing the security of a system to identify weaknesses before attackers can exploit them.

The IEC 62443-4-1 standard [10] includes a section that focuses on documenting the outcomes of all security testing. This documentation helps verify whether the security requirements are being met, ensuring the product is effectively maintained throughout its real-world use. Table 5 details tests that can be performed to assess if the applied security strategy is robust and well-established.

Table 22: IEC 62443-4-1 Security Verification and Validation Testing [53]

Security Verification & Validation Testing	Examples
SecT-1 - Security Requirements Testing	• Functional testing of security requirements • Performance and scalability testing Boundary/edge condition, stress and malformed or unexpected input test
SecT-2 - Threat Mitigation Testing	• Create and execute mitigation plans Create and execute plans for attempting to thwart each mitigation
SecT-3 - Vulnerability Testing	• Attack surface analysis • Black box known vulnerability scanning Dynamic runtime resource management testing
SecT-4 - Penetration Testing	• Password cracking • Privilege escalation Exploiting software vulnerabilities
SecT-5 - Independence of Testers	• Security consulting firms • Freelance security researchers Internal audit teams with dedicated security expertise

B.2.12 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.

Mitigating risks throughout the Installation, Operation, and Maintenance (IOM) phases is crucial for the security and longevity of any system. Key considerations include (see Section 4.2.14)

Installation:

- **IOM-1 - Security Checks**: Conduct thorough pre-installation security checks on all hardware and software components.

- **IOM-2 - Secure Configuration and Integration**: Ensure secure configuration and integration with existing infrastructure.
- **IOM-3 - Access Controls and Authentication Mechanisms**: Implement access controls and authentication mechanisms to restrict unauthorized access.

Operation:

- **IOM-4 - User Training**: Provide comprehensive user training to prevent accidental misconfigurations or misuse.
- **IOM-5 - Monitor System**: Monitor system logs for suspicious activity and potential security breaches.
- **IOM-6 - Regular Updates**: Regularly update software and firmware to address vulnerabilities.

Maintenance:

- **IOM-7 - Routine System Maintenance**: Perform routine system maintenance to prevent malfunctions and ensure optimal performance.
- **IOM-8 – Security Patches**: Apply security patches and updates promptly to protect against emerging threats.
- **IOM-9 - Regular Vulnerability Assessments**: Conduct regular vulnerability assessments and penetration testing to identify and address weaknesses.
- **IOM-10 - Incident Response Plans**: Develop and test incident response plans to quickly address any security breaches.

B.2.13 Other Vulnerabilities

The following vulnerabilities were identified through the cybersecurity survey titled "Survey on Cybersecurity Challenges and Solutions for Space Systems" (see Chapter 3), conducted among the space sector specialists.

Table 23: Vulnerabilities and respective mitigations identified by the experts

Vulnerability	Mitigation
Software bugs with security impacts	**SB-1** - Extensive code analysis **SB-2** - Security testing **SB-3** - Extensive V&V of the embedded device against fuzz inputs **SB-4** - Built-in or self-tests to ensure application and data integrity **SB-5** - Perform input validation **SB-6** - Integrity checks for all data, configurations, inputs to the system **SB-7** - Conducting independent regular security audits **SB-8** - Security reviews

Vulnerability	Mitigation
Using of weak development process	**WDP-1** - Ensure a SDLC (Secure Development Life Cycle) is integrated in the application development. **WDP-2** - No agile methodology in security critical development
Read and write operations in memory	**R&W-1** - Robustness testing
Software update	**SU-1** - Authentication on software patch **SU-2** - Enforce patch management
Weak software development protection	**WSDP-1** - Protection of software development environments **WSDP-2** - Every user involved in activities related to the project shall be subjected to user authentication. (Zero Trust model)
Debug ports not protected	**DP-1** - Access to target memories through unprotected debug ports.
Bad code practices	**BCP-1** - Extensive code analysis **BCP-2** - Zero code smells and zero warnings objective
Lack of security acceptance plan	**LSAP-1** - 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	**WSI&DF-1** - More secure information and deliverables flow. **WSI&DF-2** - Use of certified tools
Weak secure boundary parameter	**WSBP-1** - Robustness testing **WSBP-2** - Extensive code analysis
Weak password policies	**WPP-1** - Use cryptographic keys instead of passwords.
High turnover of contractors	**HTC-1** - Create a baseline workforce to be trained in cybersecurity.
Use of dynamic memory	**UDM-1** - Exclude dynamic memory in space systems.
Deserialization of untrusted data	**DUD-1** - Security reviews
Integer overflow of wraparound	**IOW-1** - Extensive code analysis
Improper monitoring in ground and space segment	**IM-1** - Intrusion detection mechanisms **IM-2** - Robust FDIR configuration **IM-3** - Firewall
Poor management of the exchange data	**PMED-1** - Advanced encryption **PMED-2** - Proper authentication methods and access control.

ANNEX C. SURVEY ON CYBERSECURITY CHALLENGES AND SOLUTIONS FOR SPACE SYSTEM

The following subsections introduce the survey questions and the message in LinkedIn advertising the survey.

C.1 Survey Questions

The following text is the introductory text used in the survey titled "Cybersecurity Challenges and Solutions for Space Systems".

"As our reliance on space-based technologies continues to grow, safeguarding these applications against cyber threats becomes not only a matter of technological prowess but also a critical element in preserving the integrity, functionality, and security of space missions. Cybersecurity has been considered a key element of space software development and operations in the last years, reflected mostly in updated software development and V&V standards. For example, the ECSS have been considering and including more and more cybersecurity requirements in the set of European Space Standards, especially the upcoming versions of **ECSS-E-ST-40** and **ECSS-Q-ST-80**, which will already include significant amount of cybersecurity related requirements.

The objective of this survey is to capture several stakeholders/experts view on the cybersecurity challenges, particularly in what concerns vulnerabilities, threats and mitigations / solutions to tackle the potential cybersecurity threats that affect space systems.

Note: if you do not work with space systems directly, please consider that "space systems" can also be interpreted as safety-critical embedded or ground systems.

Confidentiality Note: all answers will be anonymized and not relatable to any individual or institution, however, we recommend that you to not provide any confidential information in your answers."

Table 24 depicts the questions presented in the survey titled "Cybersecurity challenges and solutions for space systems".

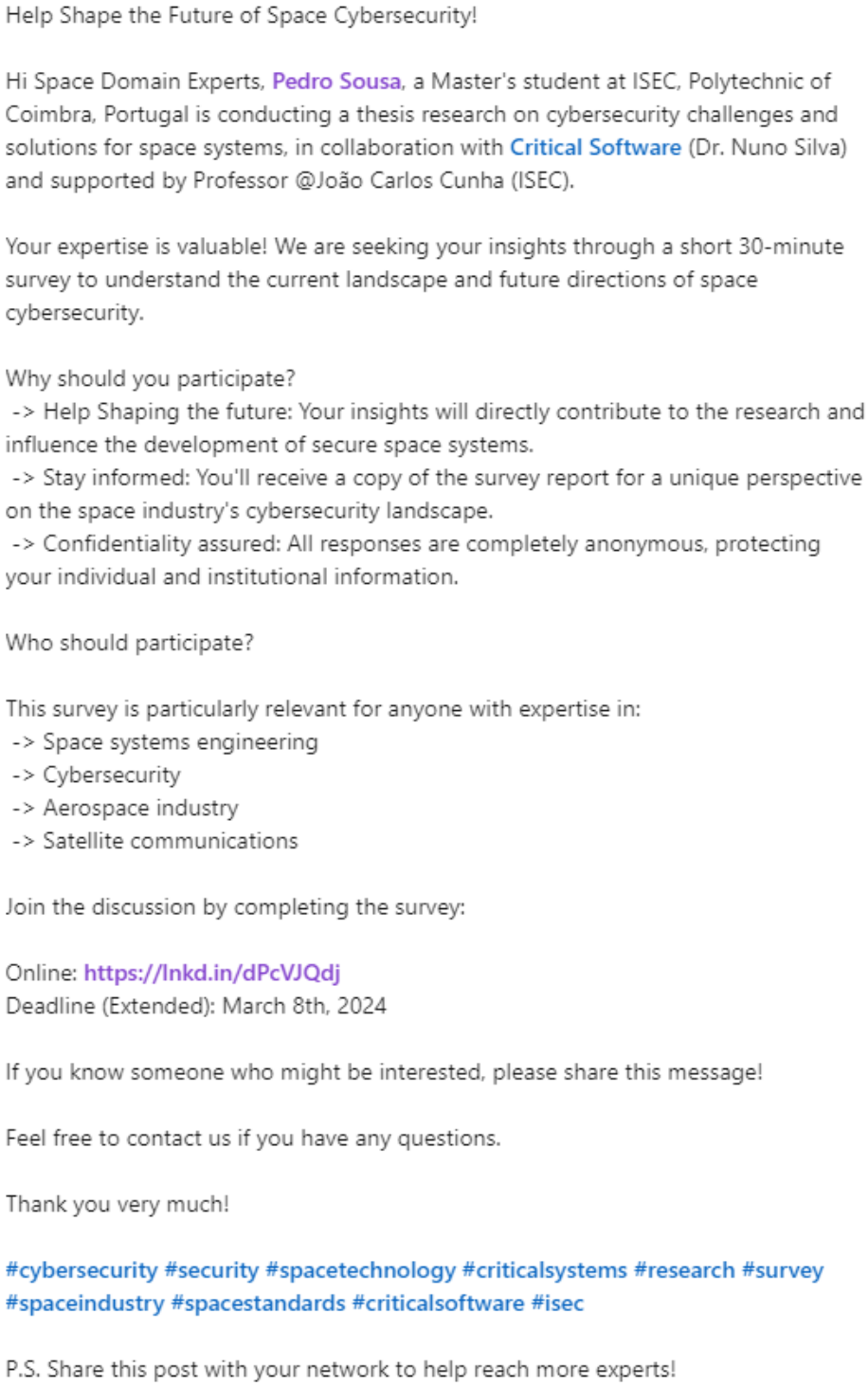
Table 24: Survey Questions and respective rationale

Number	Question	Rationale
1	List up to 5 of the most common or severe vulnerabilities that you believe affect space or ground systems (or embedded real-time systems).	To collect the perception of the experts on which are the most common vulnerabilities that impact security of space systems.

Number	Question	Rationale
2	List up to 5 cybersecurity threats that you consider relevant for space or ground systems (or embedded real-time systems).	To identify which are the main existing threats to space systems.
3	Identify up to 5 Technical Mitigations that are applied or could be applied to prevent cybersecurity problems in space or ground systems.	To collect functional level solutions and mitigations related to security vulnerabilities and threats and to start creating a catalogue of security related mitigations.
4	Identify up to 5 Processual Mitigations that are applied or could be applied to prevent cybersecurity problems in space or ground systems.	To collect process level solutions and mitigations related to security vulnerabilities and threats and to start creating a catalogue of security related mitigations in terms of process.
5	List the standards or cybersecurity resources used to ensure compliance and security of space or ground systems.	To identify which standards are being used, which are useful and which tools/resources are applicable and can serve as support to future cybersecurity assurance.
6	Select the segment of space systems that do you think are most vulnerable to cybersecurity threats. (Ground, Space or Link/Signal)	To identify which segment is more vulnerable.
7	Any other cybersecurity concerns/trends that you see in the short/middle term (up to 10 years from now) for safety-critical embedded systems, particularly space systems.	To identify potential emerging challenges or additional concerns not covered with the previous 5 questions.

C.2 Linkedin Message

Figure 30 depicts the publication done in LinkedIn to attract more participation to the cybersecurity survey.



Help Shape the Future of Space Cybersecurity!

Hi Space Domain Experts, Pedro Sousa, a Master's student at ISEC, Polytechnic of Coimbra, Portugal is conducting a thesis research on cybersecurity challenges and solutions for space systems, in collaboration with Critical Software (Dr. Nuno Silva) and supported by Professor @João Carlos Cunha (ISEC).

Your expertise is valuable! We are seeking your insights through a short 30-minute survey to understand the current landscape and future directions of space cybersecurity.

Why should you participate?
-> Help Shaping the future: Your insights will directly contribute to the research and influence the development of secure space systems.
-> Stay informed: You'll receive a copy of the survey report for a unique perspective on the space industry's cybersecurity landscape.
-> Confidentiality assured: All responses are completely anonymous, protecting your individual and institutional information.

Who should participate?

This survey is particularly relevant for anyone with expertise in:
-> Space systems engineering
-> Cybersecurity
-> Aerospace industry
-> Satellite communications

Join the discussion by completing the survey:

Online: https://lnkd.in/dPcVJQdj
Deadline (Extended): March 8th, 2024

If you know someone who might be interested, please share this message!

Feel free to contact us if you have any questions.

Thank you very much!

#cybersecurity #security #spacetechnology #criticalsystems #research #survey #spaceindustry #spacestandards #criticalsoftware #isec

P.S. Share this post with your network to help reach more experts!

Figure 30: LinkedIn message

Instituto Superior
de Engenharia