



SPACE THREAT LANDSCAPE

MARCH 2025

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors please use market@enisa.europa.eu

For media enquiries about this paper, please use press@enisa.europa.eu

EDITORS

Evangelos Rekleitis, ENISA

Monika Adamczyk, ENISA

ACKNOWLEDGEMENTS

We would like to thank the ENISA Advisory Group and the National Liaison Officers network for their valuable feedback.

We would also like to thank experts from the European Commission (DG CNECT) and the European Union Agency for the Space Programme (EUSPA), national authorities including the Belgian Institute for Postal Services and Telecommunications (BIPT, Belgium), Communications Regulation Commission (CRC, Bulgaria), National Agency for the Security of Information Systems (ANSSI, France), National Centre for Space Studies (CNES, France), Federal Office for Information Security (BSI, Germany), Ministry of Foreign Affairs and International Cooperation (Italy), National Cybersecurity Agency (ACN, Italy), Authority for Digital Infrastructure (Netherlands), Regulatory Authority for Electronic Communications and Postal Services (RATEL, Serbia), Ministry for Digital Transformation (Spain), private sector stakeholders including Thales and Rhea Cyber Security Services, and Expert Group Space of BSI Alliance for Cybersecurity (in particular: Aris Patronis, Christoph Möbius, Florian Göhler, Manuel Hoffmann, Max Roth, Sascha Fankhänel, Stefanie Grundner), and the ENISA colleagues: Nikolaos Tantouris and Dimitrios Papamartzivanos.



LEGAL NOTICE

This publication represents the views and interpretations of ENISA, unless stated otherwise. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to the Regulation (EU) No 2019/881. ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain ENISA as its source. Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication. ENISA maintains its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE

© European Union Agency for Cybersecurity (ENISA), 2025

This publication is licenced under CC-BY 4.0 "Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed, provided that appropriate credit is given and any changes are indicated".

For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

Luxembourg: Publications Office of the European Union, 2025

Linguistic version	Output format	Catalogue Number	ISBN	DOI
English	PDF Web	TP-01-25-007-EN-N	978-92-9204-696-5	10.2824/8841206



TABLE OF CONTENTS

1. INTRODUCTION	7
1.1 BACKGROUND AND CONTEXT	8
1.2 POLICIES & STANDARDS	10
1.3 SCOPE & OBJECTIVES	11
1.4 METHODOLOGY	12
1.5 TARGET AUDIENCE	13
1.6 STRUCTURE OF THE REPORT	13
2. COMMERCIAL SATELLITES LIFECYCLE MODEL	15
2.1. GENERIC LIFECYCLE MODEL AND ACTORS	16
3. ASSET TAXONOMIES	23
3.1. GROUND SEGMENT	25
3.2. SPACE SEGMENT	26
3.3. USER SEGMENT	27
3.4. HUMAN RESOURCES SEGMENT	28
4. SPACE THREATS	29
4.1. SPACE THREAT TRENDS	29
4.2. THREAT ACTORS	31
4.3. THREAT TAXONOMY METHODOLOGY	33
4.4. THREAT TAXONOMY	34
5. RISK ASSESSMENT	37
5.1. SCENARIO 1: COMMUNICATIONS PROTOCOL COMPROMISE VIA SOCIAL ENGINEERING	37
5.2. SCENARIO 2: EXPLOITING OBC/OBSW VULNERABILITIES VIA MALICIOUS CODE	40
5.3. SCENARIO 3: NETWORK INTRUSION DUE TO A LACK OF SECURITY PROTOCOLS AND MISCONFIGURATION	43



6. CYBERSECURITY CONTROL FRAMEWORK	47
6.1. CONTROLS TO THREATS MAPPING	50
7. CONCLUSIONS AND RECOMMENDATIONS	69
ANNEX A - LIST OF ACRONYMS AND ABBREVIATIONS	73
ANNEX B – DETAILED ASSET TAXONOMY	75
ANNEX C – SPACE THREAT TAXONOMY	85
ANNEX D – CYBERSECURITY CONTROL FRAMEWORK	96



EXECUTIVE SUMMARY

This report underlines the growing importance of cybersecurity considerations for the space industry, with an emphasis on commercial satellites. Previous years have witnessed several notable cyber-attacks aimed at the space industry, including large-scale satellite systems, with consequences being not only visible, but also potentially harmful for societies at large. At the same time, the growing body of EU frameworks regulating network and information security as well as resilience of critical and important sectors, recognises the space sector among essential entities, thus subjecting it to strict cybersecurity requirements that will be applicable from January 2025.

With this in mind, the primary objective of this report is to identify and assess the cybersecurity threat landscape for commercial satellites – exploring both existing and emerging challenges for the industry. This is achieved by focusing on cybersecurity aspects at each phase of the satellite lifecycle – development, deployment, operations, and decommissioning, and the stakeholders involved. The report defines a high-level reference architecture for commercial satellites presented in the form of a space assets taxonomy. The assets taxonomy is then matched against identified relevant threats and threat actors providing a space threat taxonomy, supplemented with possible risk scenarios and disruption models. Serving as a basic form of threat modelling, the scenarios, together with preceding sections, provide a baseline for designing a set of tailored cybersecurity controls derived from existing cybersecurity frameworks. The controls are aimed at providing guidance for strengthening resilience of commercial satellite operators.

The report is aimed at a wide target audience – which includes representatives of the public/government sector and the space industry, technical and cybersecurity communities, as well as academia, standardisation bodies, civil society organisations, and the interested public.

Among the key cybersecurity challenges faced by the commercial satellites industry, the report outlines:

- Supply chain risks, with the space sector heavily dependent on complex global supply chains;
- Use of third party Commercial Off-the-Shelf (COTS) components;
- Legacy systems, due to the remote nature and location of space systems;
- Limited visibility, again related to the remote nature of the space systems;
- Weak configuration, primarily found in the lack of cryptographic technologies;
- Human error, since space systems dependent on a high degree of human interaction in all phases of their lifecycle; and
- The threat of sophisticated cyber-attacks, launched by skilled and capable threat actors

To address these, some of the most notable recommended actions identified by the report include:

- Implementing security by default and by design principles;
- Analysis, testing, and hardening of COTS before and after introducing them into the production environment (operations);
- Strengthened physical security of all ground-based assets, as well as space assets prior to their launch;



- Deployment of validated and tested cryptographic technologies measures into space systems;
- Introduction of robust segmentation measures;
- Regular patching and hardening of space systems;
- Adopting a zero-trust approach; and
- Adopting sound and appropriate cyber hygiene practices.



1. INTRODUCTION

The United Nations Office for outer Space Affairs (UNOOSA) Index of Objects Launched into Outer Space counts a total of 17,852 objects, out of which 11,331 are currently registered having an 'in orbit' status.¹ As of 19 September 2024, the satellite tracking website "Orbiting Now" lists 10,786 active satellites in various Earth orbits.² Taking a closer look into satellite operators shows that the commercial space sector is taking the lead of the overall space landscape, with private companies owning most of the active satellites (over 60% among the top 10 satellite operators).³

Such rates of commercial exploitation of space, coupled with an increasing number of private companies also launching and operating Space-as-a-Service business models, have made the application of satellites a standard enabling practice across a myriad of sectors and solutions. This includes phones and internet access, critical communications, satellite TV and radio broadcast, land and water resources monitoring, precision farming, remote sensing, management of remote infrastructure, and logistics package tracking, amongst others. Satellites have also been defined as central to achieving the United Nations' Sustainable Development Goals (SDGs) at the global level⁴, as well as the objectives of the EU's green and digital transition⁵.

However, by becoming the backbone of some of the key modern economic activities, the new "space race" has also increased the potential for harmful effects of any loss of capability, no matter the cause, opening the door for new vulnerabilities in parallel. The use of off the shelf and open source hardware and software components, trends such as software-defined satellites, in-orbit reconfigurations, onboard intelligence, and quantum technologies are all making space assets and data increasingly susceptible to cyber-attacks. Considering recent forecasts of an average 2,800 satellite launches annually between 2023 and 2032 – the equivalent of 8 satellites per day⁶ - there is an urgent need to address the risks and threats faced by the space sector today, to ensure uninterrupted and effective communication in the future. And yet, despite general agreement that the space domain requires targeted attention, with the lack of analysis and control over space-based infrastructure recognised among key cybersecurity threats to emerge by 2030⁷, there is still a relative lack of detailed, sector-specific cybersecurity guidelines for commercial satellite operators. Apart from NASA's Best Practice Guide⁸ published in January 2024, the Security in space systems lifecycles standard⁹ published by the European Cooperation for Space Standardization (ECSS) in July 2024, and a number of technical standards and guidelines that can be leveraged to support resilience of different satellite components, processes, or lifecycle phases, satellite operators are generally governed

¹ Online Index of Objects Launched into Outer Space. United Nations Office for Outer Space Affairs. https://www.unoosa.org/oosa/osindex/index.aspx?lf_id=

² Active satellite orbiting data. Orbiting Now. <https://orbit-ing-now.com/>

³ Who owns all the satellites. SatelliteXplorer. <https://geoxc-apps.bd.esri.com/space/satellite-explorer/>

⁴ Space Supporting the Sustainable Development Goals. United Nations Office for Outer Space Affairs. <https://www.unoosa.org/oosa/en/ourwork/space4sdgs/index.html>

⁵ EU Space 4 green and digital transition. 2021. EUSPA. <https://www.euspa.europa.eu/newsroom-events/news/eu-space-4-green-and-digital-transition>

⁶ Euroconsult. 2023. Satellites to be Built & Launched, 26th edition. <https://digital-platform.euroconsult-ec.com/product/satellites-to-be-built-launched/>. Publicly available summary available here: <https://www.euroconsult-ec.com/press-release/four-tons-of-satellites-to-be-launched-daily-by-2032-demand-concentrates-by-a-handful-of-players/>

⁷ ENISA. 2023. ENISA Foresight Cybersecurity Threats for 2030. <https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030>

⁸ NASA. 19 January 2024. Space Security: Best Practices Guide (BPG). <https://swehb.nasa.gov/display/SWEHBVD/7.22+-+Space+Security%3A+Best+Practices+Guide?preview=/146540183/154501144/Space%20Security%20Best%20Practices%20Guide%20BPG%20REV%20B.pdf>

⁹ European Cooperation for Space Standardization. 1 July 2024. Space engineering – Security in space systems lifecycles. ECSS-E-ST-80C. <https://ecss.nl/standard/ecss-e-st-80c-space-engineering-security-in-space-systems-lifecycles/>



by national rules and regulations prescribed by the country of their establishment, despite their operations having a wider reach and, often, a global impact.

To this end, the aim of this report is to assess the cybersecurity threat landscape for the commercial satellite industry and to provide recommendations for effective and practical cybersecurity controls and mitigation strategies, considering the specific needs of commercial satellite operators.

1.1 BACKGROUND AND CONTEXT

Cyber-attacks on satellites can be executed from the ground and the attackers do not necessarily need to be spacefaring nations. Real-life events have shown that even large-scale systems are susceptible to hostile takeovers, with the 2022 Viasat satellite hack serving as a notable example, shutting down tens of thousands of modems across Europe and disrupting not only economic activities of several European countries but also lifeline functions such as emergency services.¹⁰ In 2022, researchers identified several vulnerabilities in commercial satellite infrastructure, enabling access to terminals^{11,12} as well as blind signal identification¹³. The need to better understand the threats and vulnerabilities of satellite systems has led to a decision by the U.S. government to allow a group of hackers to attack a satellite deployed in orbit, during the 2023 August DEF CON conference¹⁴, to identify further resilience measures that can be introduced.¹⁵

In the domain of space policy and satellite operations research, a number of publications have illustrated the severe consequences that can arise from targeted cyber attacks on critical space assets.¹⁶ They are further exacerbated with the recognised dual or multi-use of satellite infrastructure, whereby commercial technology intended for civilian use can nevertheless be weaponised in support of geopolitical goals.^{17,18} Finally, research into the potential consequences of successful cyberattacks on commercial satellites also suggests the potential of cascading effects including:

1. **Physical:** Potential misalignment of satellite orbits, increasing the risk of collision with other space objects and exacerbating the challenges of space debris mitigation. The implications of a collision cascade in space are significant, potentially **rendering orbits inaccessible and jeopardising the usability of entire regions of space.**¹⁹
2. **Economic:** A successful cyber intrusion resulting in a disruption of satellite services could lead to immediate and significant financial losses for businesses relying on uninterrupted communications and data transmission. Loss of satellite service in the industries that heavily depend on satellite connectivity, such as transportation, logistics, and remote monitoring, could result in **costly downtime, delays, and**

¹⁰ Howell O'Neil, P. 2022. Russia hacked an American satellite company one hour before the Ukraine invasion.

<https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/>

¹¹ Burgess, M. 10 August 2022. The Hacking of Starlink Terminals Has Begun. Wired. <https://www.wired.com/story/starlink-internet-dish-hack/>

¹² KU Leuven-COSIC. 2022. Starlink-FI. <https://github.com/KULeuven-COSIC/Starlink-FI>

¹³ Humphreys, T. et al. 2022. Signal Structure of the Starlink Ku-Band Downlink. Cornell University.

<https://arxiv.org/pdf/2210.11578>

¹⁴ See DEFCON. <https://defcon.org/index.html> and the linked article published on The Register:

https://www.theregister.com/2023/06/03/moonlighter_satellite_hacking/

¹⁵ Gedeon, J. 2023. For the first time, U.S. government lets hackers break into satellite in space. Politico.

<https://www.politico.com/news/2023/08/11/def-con-hackers-space-force-00110919>

¹⁶ Peeters, W. 2023. Cyberattacks on Satellites: An Underestimated Political Threat. LSE.

<https://www.lse.ac.uk/ideas/projects/space-policy/publications/Cyberattacks-on-Satellites>

¹⁷ Porras, D. 2023. Shared risks: An examination of universal space security challenges. Briefing paper for the United Nations Disarmament Commission. UNIDIR. <https://unidir.org/wp-content/uploads/2023/05/shared-risks-an-examination-of-universal-space-security-challenges-en-775.pdf>

¹⁸ European Commission, 2022. EU Space Strategy for Security and Defence. https://defence-industry-space.ec.europa.eu/eu-space-policy/eu-space-strategy-security-and-defence_en

¹⁹ Peeters, W. 2023. Cyberattacks on Satellites: An Underestimated Political Threat.

<https://www.lse.ac.uk/ideas/projects/space-policy/publications/Cyberattacks-on-Satellites>



inefficiencies, potentially leading to stock market shutdowns, air traffic halts, or supply chain disruption.²⁰

3. **Societal/Human:** Following a successful cyber incident against a space system, a trickle-down effect can result in **panic, food shortages, plundering, and social unrest**, depending on the extent and duration of impact. Disruptions to essential services dependent on space systems, such as commercial aviation, may generate **loss of human life and catastrophic consequences**.²¹
4. **Legal/Regulatory:** The compromise of sensitive information transmitted via satellites can lead to breaches of customer data and trade secrets, eroding trust in satellite-based services in the long run. Such incidents may also have **legal and regulatory repercussions, potentially leading to fines and reputational damage for satellite operators, businesses involved in satellite-dependent operations, as well as a cascading effect resulting in geopolitical tensions**.^{22,23,24}

As commercial satellites increasingly underpin vital global communications, navigation, and essential services, addressing the risks posed by malicious actors targeting these systems is of paramount importance. The above-mentioned cases show the need for developing dedicated reference materials to provide a baseline for better sectoral security and resilience of the commercial satellite sector.

When considering security in the context of satellite technologies, one needs to be aware that there are many entry points for malicious actors. These are dispersed across the satellite's lifecycle, which encompasses everything from an initial idea to project planning, development, transport, launch, operation, and final decommissioning. Each phase of the lifecycle includes a multitude of relevant assets and actors, many of which can be a potential source of vulnerabilities. It is therefore essential to secure satellite solutions and apply "security by design" and "security by default" concepts as prerequisites for attaining zero-trust principles. This implies ensuring that cybersecurity considerations are knitted into every phase of the lifecycle process, and assuming a level of security that is proportional to the value of the protected assets. To successfully achieve this, it is important to:

- understand the satellite lifecycle model;
- understand what needs to be secured (the assets that are subject to satellite specific threats and adversarial models);
- manage threats in a multi-party ecosystem in a comprehensive way by using interoperable models and taxonomies; and
- implement relevant cybersecurity controls based on risk models to ensure strengthened security of satellite infrastructure.

The introduction of minimum industry standards, based on "security by design" and "security by default" would also contribute to make cybersecurity attainable under the same or similar market conditions.

²⁰ Peeters, W. 2023. Cyberattacks on Satellites: An Underestimated Political Threat.

<https://www.lse.ac.uk/ideas/projects/space-policy/publications/Cyberattacks-on-Satellites>

²¹ Peeters, W. 2023. Cyberattacks on Satellites: An Underestimated Political Threat.

<https://www.lse.ac.uk/ideas/projects/space-policy/publications/Cyberattacks-on-Satellites>

²² Peeters, W. 2023. Cyberattacks on Satellites: An Underestimated Political Threat.

<https://www.lse.ac.uk/ideas/projects/space-policy/publications/Cyberattacks-on-Satellites>

²³ Khandelwal, S. 2015. Russian Hackers Hijack Satellite To Steal Data from Thousands of Hacked Computers

<https://thehackernews.com/2015/09/hacking-satellite.html>

²⁴ Nelson, N. 2023 How Hackers Can Hijack a Satellite <https://www.darkreading.com/cybersecurity-analytics/how-researchers-hijacked-a-satellite>



1.2 POLICIES & STANDARDS

This subsection provides a snapshot of relevant policies for this report, including current frameworks, policies, standards, and guidelines that have a significant impact on commercial satellite solutions.

At the EU level, the updated Directive on measures for a high common level of cybersecurity across the Union (NIS2 directive)²⁵ now encompasses space as a sector of high criticality, comprising operators of ground-based infrastructure that support space-based services, as well as telecom operators. This provides an initial high-level set of obligations pertaining to cybersecurity that satellite operators need to abide by. These obligations may be further specified in the context of the national transposition of the NIS2 Directive in line with the minimum harmonisation approach. Moreover, under Article 21(5) of the NIS2 Directive, the Commission is empowered to adopt implementing acts to lay down the technical and the methodological requirements of the required measures.

The Cyber Resilience Act (CRA), the first-ever EU-wide legislation addressing cybersecurity for products with digital elements, was published in the Official Journal on 20 November 2024²⁶. Aiming to ensure that all products with digital elements placed on the EU market meet stringent cybersecurity standards throughout their lifecycle, the CRA is expected to have a significant impact on the development, operations and decommissioning of space systems.

Box 1. Additional EU policies and initiatives aimed at increasing the level of security of space systems, products, and communication

EU Cybersecurity Act establishing the European Cybersecurity Certification Framework, a harmonised approach to European cybersecurity certification schemes to attest that ICT products, services, and processes comply with specified security requirements, protecting the availability, authenticity, integrity and confidentiality of data and functions enabled, throughout their lifecycle. (Regulation EU 2019/881)

Council Resolution on Encryption calling for joined efforts at EU level in the technology industry to ensure continued implementation and use of strong encryption technology to protect against cyber threats. (13084/1/20)

EU Secure Connectivity Programme setting the goals for an EU satellite constellation (IRIS2) to provide EU Member States with guaranteed access to highly secure, low-latency and global connectivity services for the protection of critical infrastructure, surveillance and support for external action or crisis management, along with military applications. The security of these communications will be based on advanced encryption technologies, including quantum cryptography, and enable the provision of commercial infrastructure to provide high-speed broadband connectivity in the EU and in strategic areas further afield.

Recommendation on a Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography (PQC) encouraging a harmonised EU-wide approach for the adoption of PQC for public administrations and critical infrastructures. (C(2024) 2393 final)

In terms of standardisation, the European Cooperation for Space Standardisation (ECSS)²⁷, a collaborative effort between the European Space Agency, national space agencies, and the European space industry associations plays a pivotal role. Facilitating management, engineering, product assurance, and sustainability in space projects and applications, ECSS focuses on developing standardised requirements to support European space activities.²⁸ Further work on standardisation is provided by the Consultative Committee for Space Data Systems (CCSDS), currently the only body that is combining communications and security.

²⁵ European Commission, 2023. Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive). <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

²⁶ Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). <http://data.europa.eu/eli/reg/2024/2847/oj>

²⁷ ECSS, 2023. ECSS Active Standards. <https://ecss.nl/standards/active-standards/>

²⁸ For example, ongoing work on the Space product assurance – Security in space systems lifecycles standard (ECSS-Q-ST-80-10C-DIR1)



CCSDS' Space Data Link Security (SDLS) protocol²⁹, at the data link layer of the Open Systems Intercommunication (OSI) stack, provides recommendations for ensuring confidentiality, integrity and authenticity of communication.³⁰ Further developments in the standardisation domain are also expected from organisations such as the Institute of Electrical and Electronics Engineers (IEEE) which is currently working on a standard that will define cybersecurity controls for space systems.³¹

Looking at EU's strategic partners, the United States' Space Policy Directive 5 (SPD-5)³², released in 2020, addresses the need for cybersecurity in space systems and directs federal agencies to collaborate with non-governmental space operators to establish cybersecurity-informed norms for space systems. SPD-5 has been a crucial milestone in establishing key cybersecurity principles for safeguarding space systems as it provides guidance on protecting space assets and supporting infrastructure from evolving cyber threats and mitigating the risk of harmful space debris caused by malicious cyber activities. Regarding standardisation, the National Institute of Standards and Technology (NIST) provides supporting materials for assessing and managing cybersecurity risk in the space domain with the Introduction to cybersecurity for commercial satellite operations³³ specifically focusing on cybersecurity risk management in the commercial satellite industry. The US has a dedicated Space Information Sharing and Analysis Center (Space ISAC), launched in 2019 under the sponsorship of NASA, U.S. Space Force (formerly Air Force Space Command), and the National Reconnaissance Office.³⁴

1.3 SCOPE & OBJECTIVES

The primary objective of this report is the identification and assessment of the cybersecurity threat landscape for the space sector, exploring both existing and emerging cybersecurity challenges in the satellite industry. By understanding potential cyber-related risks, threats, and vulnerabilities, the report aims to lay the groundwork for a trustworthy and uninterrupted deployment of commercial satellite systems and architecture.

Focus is placed on cybersecurity threats and vulnerabilities across the satellite lifecycle and associated actors and assets identified as crucial components of satellite systems. Specific objectives include:

- **Definition of a generic commercial space system lifecycle model as well as identification and an analysis of satellite assets taxonomy**, considering the stakeholders involved in respective lifecycle phases, interdependencies between the phases, groupings based on the lifecycle, as well as identifying their respective asset segments, i.e. ground-space-user;
- **Correlation of a list of threats, threat actors, and vulnerabilities**, mapping them against a list of identified satellite assets. By examining potential threats, this report aims to provide insights into the vulnerabilities that may exist within existing and developing satellite projects;
- **Description of sample cyber-attack scenarios** and failure models pertinent to various stages in the core commercial satellite lifecycle; and
- **Development of recommendations for effective and practical cybersecurity controls and mitigation strategies** for the commercial space industry, helping them

²⁹ CCSDS. July 2022. Space Data Link Security Protocol. CCSDS 355.0-B-2. <https://public.ccsds.org/Pubs/355x0b2.pdf>

³⁰ Note: CCSDS' protocols are presented in the form of recommendations and are not legally binding.

³¹ IEEE. Standard for Space System Cybersecurity. P3349. <https://standards.ieee.org/ieee/3349/11182/>

³² UG Government. 2020. Space Policy Directive 5 (SPD-5). <https://www.cisa.gov/resources-tools/resources/space-policy-directive-5>

³³ Scholl, M. & Suloway, T. NIST, 2023. Introduction to Cybersecurity for Commercial Satellite Operations. <https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8270.pdf>

³⁴ Space ISAC. <https://spaceisac.org/>



protect their assets and ensure the continued safe and secure operation of space infrastructure.

Overall, the Space Threat Landscape report endeavours to provide a holistic perspective on the cybersecurity challenges faced by commercial satellites. By identifying potential threats and vulnerabilities and providing a cybersecurity controls framework the report aims to equip stakeholders in the commercial satellite sector with the knowledge and insights needed to bolster the resilience and security of satellite systems in the face of evolving cyber threats.

1.4 METHODOLOGY

The report is compiled based on publicly available, open-source resources collected through desk research. This includes frameworks, standards and guidance published by international organisations, national space agencies and standardisation bodies, as well as taxonomies, white papers and research published by the technical community and academia. Striving for general applicability, collected data has been dissected, cross-examined, and grouped based on contextual similarities. Certain aspects such as satellite lifecycle actors are presented in a generic format allowing further tailoring based on the specific purpose and design of a satellite.

The approach employed for this report adheres to the methodology established by ENISA for its annual Threat Landscape assessments. Aligned with this methodology, the contents of the report were developed incrementally, starting with the definition of a reference lifecycle model and the identification of relevant infrastructure feeding into the asset taxonomy. This was followed by the identification of relevant threats and possible risk scenarios based on which relevant cybersecurity controls were defined.

The lifecycle was developed comparing existing satellite lifecycle models employed by ESA, ECSS, BSI, NASA, JAXA and NIST. These were analysed to create an overview of existing approaches and identify similar and/or overlapping phases, providing a baseline for the generic lifecycle model for commercial satellites.

The asset taxonomy is based on extensive literature survey of space infrastructures including frameworks published by national public and standardisation bodies, industry and technical communities and academic research. Identified assets were clustered and tagged to relevant segments based on common references and grouping found in the literature.

The threat taxonomy is based on an examination of space and wider cybersecurity industry threat assessments addressing the space sector, industry reports, national space agencies' and standardisation bodies' guidelines and toolkits providing recommendations for defending against specific threats, academic research and analysis of known attacks on space infrastructure. Identified threats were clustered mirroring ENISA's Threat Taxonomy. Linkages of threats to specific assets and their effects according to the CIA model (Confidentiality, Integrity, Availability) were made based on relations identified in the examined literature and the nature of the targeted assets. Threat actors are presented at a high-level and should be treated as hypothetical given the known challenges of clear attribution in the cyber domain.

The proposed reference cybersecurity controls framework was derived based on a thorough review of existing cybersecurity frameworks, standards and guidelines published by relevant national and international authorities and standardisation bodies. Identified controls were then analysed to determine common objectives and patterns, overlaps, outliers, and gaps, enabling high-level, contextual control clustering based on relevance for the commercial satellites' sector context.

For the purpose of collecting relevant information and consulting on findings and proposed models and recommendations, ENISA has engaged experts from the European Commission (DG CNECT) and the European Union Agency for the Space Programme (EUSPA), national

authorities including the Belgian Institute for Postal Services and Telecommunications (BIPT, Belgium), Communications Regulation Commission (CRC, Bulgaria), National Agency for the Security of Information Systems (ANSSI, France), National Centre for Space Studies (CNES, France), Federal Office for Information Security (BSI, Germany), Ministry of Foreign Affairs and International Cooperation (Italy), National Cybersecurity Agency (ACN, Italy), Authority for Digital Infrastructure (Netherlands), Regulatory Authority for Electronic Communications and Postal Services (RATEL, Serbia), Ministry for Digital Transformation (Spain), private sector stakeholders including Thales and Rhea Cyber Security Services, and Expert Group Space of BSI Alliance for Cybersecurity (in particular: Aris Patronis, Christoph Möbius, Florian Göhler, Manuel Hoffmann, Max Roth, Sascha Fankhänel, Stefanie Grundner).

Striving for broad applicability, the terminology employed within this report was built on the principles of ensuring holistic understanding, contextual relevance, knowledge integration, consistency, and easier updating and maintenance of the Space Threat Landscape report.

1.5 TARGET AUDIENCE

The target audience for the Space Threat Landscape report includes various stakeholders concerned with the cybersecurity threats related to commercial satellites and space-based technologies. These stakeholders can be broadly categorized as follows:

- **Public/governmental sector** (national and international level): Governing entities, space agencies, regulatory bodies, and authorities responsible for overseeing satellite operations, space policy, and national security.
- **Satellite industry**: Companies and organizations involved in the satellite industry, including satellite operators, manufacturers, service providers, and other stakeholders within the satellite ecosystem, including the Satellite Industry and Space/Satellite Technical Community (e.g. Supply Chain and Logistics Providers), the User Community and Satellite Industry (e.g. Telecommunications Providers), and other relevant industry players.
- **Space and satellite technical community**: Experts in space technology, satellite design, satellite operations, space mission planning, and related fields.
- **Cybersecurity community**: Professionals and organizations with expertise in cybersecurity, particularly as it relates to space and satellite systems.
- **Academia and research community**: Researchers, scholars, and educational institutions conducting studies and research in satellite technology and space-related cybersecurity.
- **Standardisation bodies**: Organisations and committees involved in setting standards and best practices for space and satellite technology security.
- **Civil society and the general public**: Individuals and organizations with an interest in space technology, satellite services, and the potential risks associated with space-based systems.
- **User community**: End users (consumers) of the services provided by space technology.

1.6 STRUCTURE OF THE REPORT

Following this Introduction, the report is structured as follows:

- Chapter 2 presents a generic lifecycle model for commercial satellite infrastructures, with relevant actors mapped to each of the lifecycle phases. The defined lifecycle phases are used as a baseline for subsequent definition of assets and relevant processes presented in succeeding chapters;
- Chapter 3 details the assets in the satellite ecosystem based on the lifecycle stages defined in Chapter 2 and categorises them in 22 asset sub-domains, across the

ground, space, and user segments, with the addition of a human resources segment to account for the human dimension;

- Chapter 4 introduces the threat taxonomy of satellite systems - where relevant threats are presented and mapped to corresponding assets that were introduced in Chapter 3;
- Chapter 5 presents a risk assessment via specific risk scenarios and highlights cybersecurity-related challenges to satellite systems;
- Chapter 6 outlines a proposed cybersecurity control framework tailored to the needs of commercial satellite operators, to address the threats identified in the threat taxonomy;
- Chapter 7 concludes the report providing a summary of findings, highlighting cybersecurity challenges related to satellites systems, and proposing a set of high-level recommendations for strengthening resilience of commercial satellite operators.



2. COMMERCIAL SATELLITES LIFECYCLE MODEL

To meaningfully address the different aspects of the space domain, a systematic and structured approach should be applied. This includes considering all phases that a typical satellite system goes through during its lifecycle. This chapter presents a generic satellite lifecycle model, highlighting the components and entities (processes and actors) related to each of the lifecycle phases, as a foundation for the development of a satellite asset taxonomy, identification of potential threats and applicable risk scenarios.

A study of lifecycle models for space projects employed by national space agencies shows that, despite variations in the ways in which actions are grouped into phases or the terminology employed, at their core these lifecycles remain the same, regardless of the ownership or intended use of the satellite systems, and whether they are commercial, military, or state-owned. These generally mirror a standard systems engineering process where the objectives and resources are first identified, followed by a definition of requirements, ultimately leading to system design and development³⁵. Another common trait of models employed by ESA, NASA and JAXA is the application of a phased approach where regular review cycles play a vital role in determining whether a given phase has met the necessary criteria to transition to the next one. For example, upon validation of design and manufacturing, the operation phase is launched by ensuring that all mission objectives are fulfilled. Once the goals of the mission are determined as complete or achieved, the system is decommissioned.

Satellite lifecycle models are fundamentally similar regardless of the intended use or ownership of a specific satellite.

Further analysis of additional lifecycle models employed by organisations such as BSI (i.e. IT-Grundschutz Profile for Space Infrastructures³⁶) or NIST (i.e. Introduction to Cybersecurity for Commercial Satellite Operations³⁷) shows that even the models that place stronger focus on cybersecurity aspects of satellite lifecycle operations nevertheless follow a similar phased logic.

Figure 1 - Illustrates the phases of the satellite lifecycle models employed by prominent organisations governing the space sector and cybersecurity.

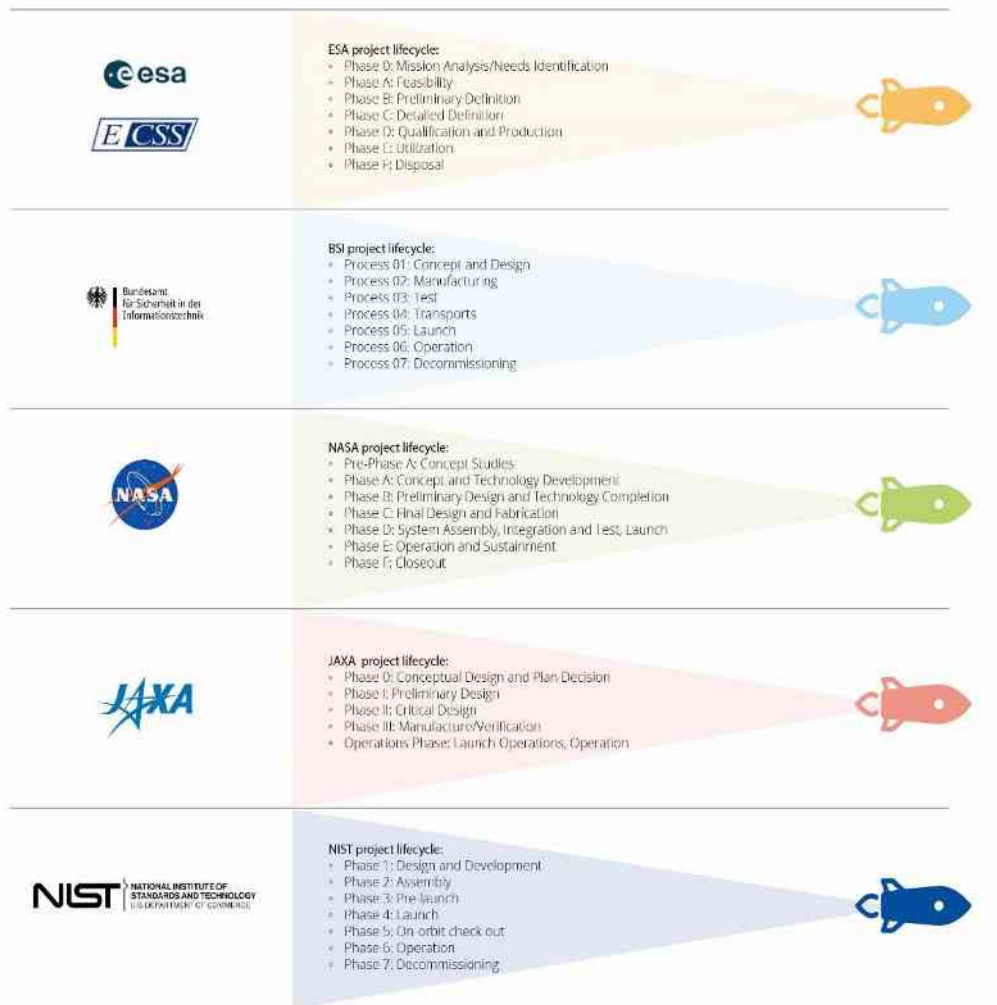
³⁵ Specifically, common phases of the standard systems engineering process include the following: Requirements analysis, Specifications, Design, Implementation, Test, and Maintenance, with Feedback as a cross-cutting element. Shiotani, B. 2018. Project Life-Cycle and Implementation for a class of small Satellites. https://s3vi.ndc.nasa.gov/ssri-kb/static/resources/SHIOTANI_B.pdf

³⁶ BSI, 2022, IT-Grundschutz Profile for Space Infrastructures. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/profiles/Profile_Space-Infrastructures.pdf?__blob=publicationFile&v=2

³⁷ Scholl, M. & Suloway, T. NIST, 2023. Introduction to Cybersecurity for Commercial Satellite Operations. <https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8270.pdf>



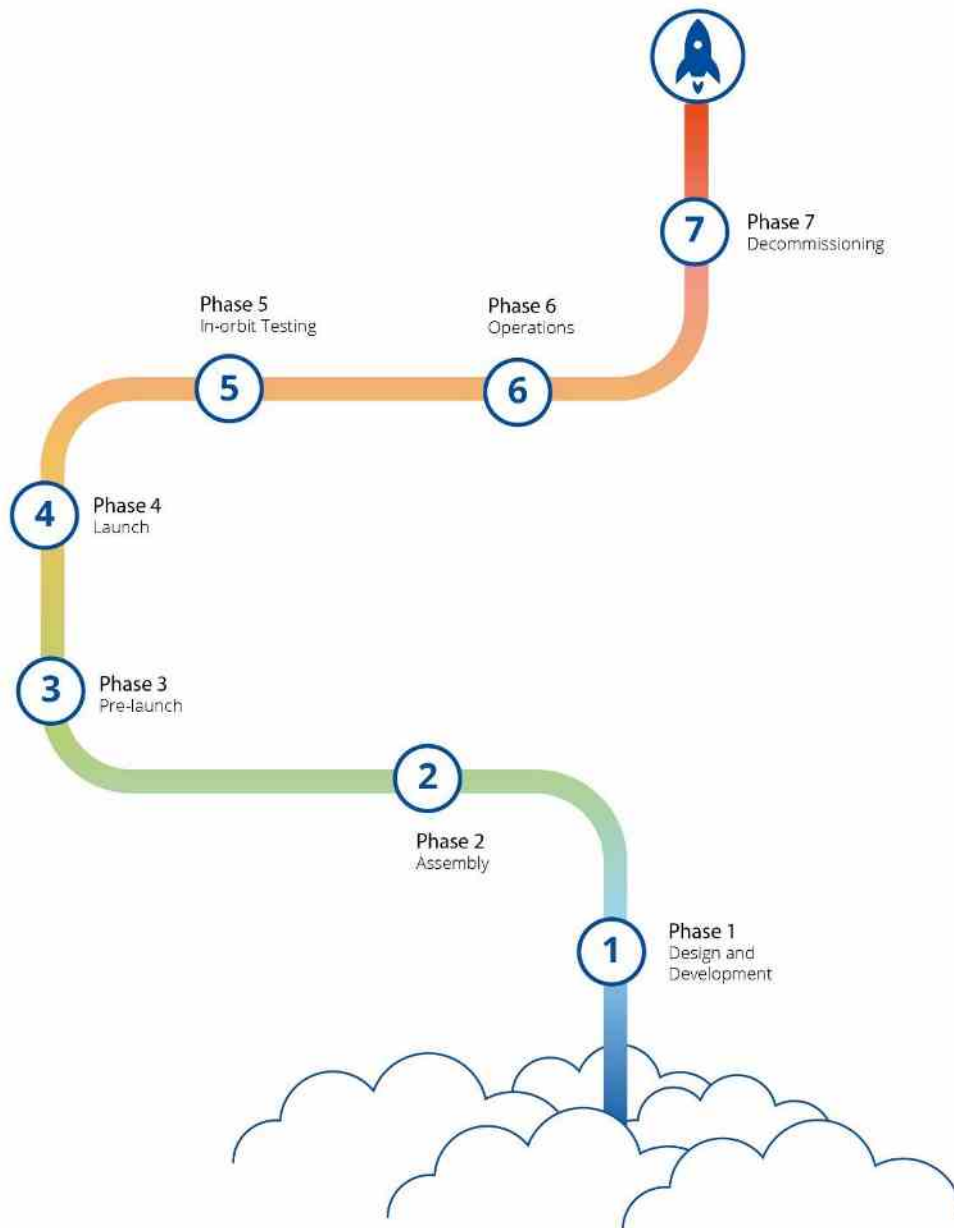
Figure 1: Phases of existing Satellite Lifecycle Models



2.1. GENERIC LIFECYCLE MODEL AND ACTORS

This section presents a generic satellite lifecycle model developed on the basis of existing common practice, enabling the identification of processes and actors related to each lifecycle phase. The below lifecycle is developed based on the assessment of different frameworks discussed above, and by using NIST's nomenclature as a generic skeleton.

Figure 2: Phases of a generic commercial Satellite Lifecycle Model



Within the above lifecycle, various actors can be engaged across a range of activities, depending on the nature and mission purpose of a specific satellite. Based on the existing knowledge and the current demands for workforce in the aerospace industry, several broader types of actors, each relevant to a different phase of the commercial satellite lifecycle, are outlined in this report.^{38,39,40,41,42}

³⁸ SpaceX, September 2021. Falcon User's Guide. <https://www.spacex.com/media/falcon-users-guide-2021-09.pdf>

³⁹ SpaceX. Rocket Crew list of open positions. <https://www.spacex.com/careers/jobs/>

⁴⁰ Rocket Crew. The biggest list of space jobs and aerospace from new space companies. <https://rocketcrew.space/>

⁴¹ Moiz, A. Indeed, July 2023. 22 Jobs in the Space Industry To Explore (Plus Duties). <https://www.indeed.com/career-advice/finding-a-job/jobs-in-space-industry>

⁴² NASA. List of featured careers. <https://www.nasa.gov/careers/featured-careers>

Actors include astronomers, atmospheric scientists, satellite operators, and engineers with a background ranging from aerospace engineering to cybersecurity, data, electronics, mechanics, and others. This group is essential for the initial design and development phases which form a foundation for successful development, operations, and retirement of a specific satellite. Other actors include test engineers who are responsible for ensuring that all the components are working as projected, as well as IT engineers that form the Satellite Operations Centre (SOC, also referred to as the Satellite Control Center - SCC) utilised for all sorts of in-orbit validations, custody management, mission execution, data and cybersecurity governance. While it is the SOC that primarily manage the satellite, during the retirement and disposal phases, aerospace engineers and scientists are reintroduced to manage its decommissioning. Finally, there are end users that benefit from satellites, including service consumers such as companies that utilise satellites to provide a specific service. The end users also include individual consumers that benefit from the services provided and/or enabled by commercial satellites, though in some cases they may be direct beneficiaries of a satellite solution as seen in the example of Starlink – a provider of wireless internet access⁴³.

Apart from scientists and engineers who participate in the design, construction and operations of satellite systems and their supporting infrastructure, there is also a multitude of additional supporting actors who are irreplaceable from a process perspective. These actors can be clustered into two broad categories: specialists in fields necessary for production, including e.g. chemistry, material sciences and power engineering/energetics, and specialists in fields necessary for project management, such as human resources, finances, procurement, general management and administration. While the role and efforts of those specialists and their contribution to the overall mission is not to be underestimated, their involvement is not thoroughly examined in this report as it does not in any way differ from their functioning in other projects in different fields and. Therefore, they are considered at a general level, as part of the business-as-usual component of space missions and the overall satellite lifecycle.

The following subsections provide a short description of each phase of the satellite lifecycle model and the individual actors involved.

2.1.1. Phase 1 – Design and Development

This phase covers definition of requirements and assessments to ensure that the new project meets the mission goals and objectives. During this phase, the project team will set the ground for ideas, mission concepts, cost, system-level requirements, and technology needs, and will examine the mission's overall feasibility. This leads to the creation of a mission concept review. Based on this concept, a list of system-level functional and security requirements is established and reviewed by technology experts with relevant expertise. The result of this process is the technical documentation, in which specific designs of satellite components are drafted.

During design and development, robust software and hardware design processes should also incorporate security aspects, including security by design and by default principles. To this end, developers must ensure that implemented security features are proportional to the value of the assets and associated risks in case of compromise, fulfilling a security by default approach. Secure coding practices must be followed from the outset to minimise both vulnerabilities and cyber threats. Rigorous security testing, including penetration testing and vulnerability assessments, should be performed to identify and address potential weaknesses during these early phases of development.

Manufacturers and companies also need to account for the long lifetime of some spacecrafts and build redundancy and flexibility into their designs to address evolving cyber threats over the vehicle's operational lifespan. Existing operational systems should also consider using compensating controls to achieve desired security outcomes if legacy technologies are

⁴³ Starlink. SpaceX. <https://www.starlink.com/>

insufficient. Finally, supply chain management throughout the lifecycle should be assessed and governed utilising compliance forms and vendor vetting for cybersecurity standards employed prior to selecting specific vendors, who will provide satellite system components and services.

Actors

The design and development of a satellite requires a vast amount of knowledge, both theoretical and practical from differing scientific fields. Gathering, analysis and interpretation of such knowledge may involve astronomers, concerned with observation and analysis of processes and celestial bodies in the universe, physicists concerned with research of natural laws relevant for the design and development of satellites, atmospheric scientists, concerned with analysis of atmospheric phenomena and their relevance to the process and other various research and/or scientist profiles concerned with specific research tasks relevant to the process. Further, the design and development processes typically involve engineers from several differing fields. These include aerospace engineers, concerned with the overall development of the satellite; cybersecurity engineers, concerned with the security of a satellite's IT components; data engineers / scientists, concerned with the collection, processing and analysis and interpretation of any data relevant to the development process; electronics engineers, concerned with the development of electronic features and equipment; software engineers, concerned with the development of software needed for the functioning of a satellite; manufacturing engineers, concerned with the production of specific satellite components; mechanical engineers, concerned with the specific mechanical devices and features; propulsion engineers, concerned with the design of satellite propulsion systems; and test engineers, concerned with planning and conducting of testing of satellites or their components.⁴⁴

The design of a specific satellite may concern many differing aspects of engineering, IT, data science and other fields, depending on its defined mission.

2.1.2. Phase 2 - Assembly

The assembly phase involves the procurement and integration of space assets/components and integrating them to enable the spacecraft to perform its missions. Apart from the assets that are relevant to the spacecraft itself, this phase also applies to the assets that are needed to support satellite operations/control. Hence, the successful review of the preliminary design leads to the finalisation of the detailed design of the system, including the production of hardware and code software guaranteeing that it can meet the requirements. Once the critical design review is approved, hardware procurement and software coding are initiated.

Cybersecurity of the supply chain is one critical aspect in this phase. The procurement of spacecraft and ground/user components, from around the world demands careful validation of performance and cybersecurity functionality through tests and scheduled compliance audits. The hardware, firmware and software supply chain play a critical role in ensuring cybersecurity. While hardware modifications become limited once the spacecraft is launched, software modifications can often be conducted from the ground. Hence, addressing supply chain risks involves understanding supplier security and privacy policies, communicating requirements to suppliers, and engaging trusted vendors for all aspects of assembly. Organisations should establish secure communication channels with suppliers and ensure that components are not tampered with during transportation and assembly, as well as during mission execution (in the context of the software utilised). Continuous monitoring of the supply chain helps detect potential malicious activities. To ensure operational continuity in case of supply chain disruptions, organisations should consider supplier diversification, that is, maintaining a multi-supplier strategy.

⁴⁴ In the context of a lifecycles of specific satellites, the roles of actors may be combined e.g. mechanical engineer can also conduct tasks delegated here to a test engineer etc.

Actors

The manufacturing of a satellite requires the physical production of satellite components by manufacturing technicians. The act of assembly itself requires the engagement of various technical personnel, including mechanical, aerospace and electronic technicians tasked with assembly of devices and components, specific to their specialisation. These technicians are also key for the provision of feedback to various engineers and other actors relevant to the design and development of satellites, for the optimisation and improvement of the satellite design.

Based on the specific nature of individual satellites, further actors might be involved in the satellite's assembly, such as laser technicians, avionics technicians, robotics technicians and other actors.

2.1.3. Phase 3 – Pre-launch

Following the assembly phase, the pre-launch phase involves testing the satellite's functionality and establishing connectivity with ground control systems. At this point, focus is on the high-level integration of the satellite with the launch vehicle, the launch infrastructure, and the satellite operations centre. The testing of this integration and the functionalities of all the above mentioned is also conducted, mainly on the level of different elements of the system (hardware, software, and human). This phase is also known for system integration, validation, and verification (IVV), and some industry players refer to it as such. Regardless, this phase also entails the preparation of the system for deployment and for performing the launch of the system itself followed by obtaining authorisation for it to be used/deployed.

This phase is crucial for ensuring cybersecurity in satellite health and status monitoring systems. Operators must be vigilant about connectivity and access during pre-launch and control physical access to the vehicle during transit and storage at the launch facility. Cybersecurity is essential during this phase to ensure the integrity and confidentiality of the test environment and telemetry data. Operators should also validate the RF links and control access to critical satellite health and status monitoring systems.

Actors

Before the satellite is launched, its capabilities must be tested to assure that it operates according to its design. This task is usually delegated to test technicians, who test the various satellite avionic, electronic, and IT features. Their activities are managed by and reported to a launch authority, assisted by an operations safety manager, tasked with enforcing the security principles on the site of the launch.

The atmospheric scientists and space weather scientists are tasked with assessing natural conditions at the time of the launch to ensure a safe launch.

The route which the satellite and its carrier will follow to reach its destination in space must also be pre-planned. This is handled by flight dynamics engineers whose tasks are separated into two: knowing what the orbit injection characteristics delivered by the launcher will be and after injection (i.e.; separation of the spacecraft from the launcher), all the travel from the injection orbit to the final orbit (it lasts from a couple of days to half a year). Finally, the transportation of the satellite or its components is conducted by logistics and other support staff.

2.1.4. Phase 4 – Launch

Moving the space system to its operational environment involves launch devices and installations, fuel operations, and safety systems. Due to the complexities and costs associated with the launch, this phase is outsourced. Additionally, the launch also includes Early Orbit Phase when the spacecraft is transferred from its injection point to the final orbit position. This process can last up to 6 months.



During the launch phase, cyber threats could target launch devices and installations, fuel operations, and safety systems. Cybersecurity measures should be in place to protect critical launch infrastructure and control systems. Additionally, in instances where the launch phase is outsourced, supply chain risks also must be considered to mitigate any breaches and malicious intrusion during this phase.

Actors

During the launch phase, two different organisations are usually involved. One is the launcher company, while the other one is the spacecraft manufacturer - both working hand in hand, with the launch being managed by a launch director (usually on the launcher company side). His tasks are the overall management of the process, its multiple components and personnel. An operations safety manager is concerned with the secure course of the launch. IT related aspects of the launch are conducted by the satellite operations centre operators (SOC operators), managed by the centre's lead (SOC lead) and coordinated by the launch control lead, some of which can also be from the spacecraft manufacturer/operator side as these matters concern the satellite's operability.

The act of the launch is coordinated on-site by launch technicians, who ensure the correct course of its technical aspects.

2.1.5. Phase 5 – In-orbit Testing

Once in orbit, satellites undergo post-launch checks to verify system integrity and operational status. This phase can be split into two steps: the first one following the injection into the transfer orbit (i.e. to make sure that the systems needed during the transfer work as expected), and the second, following the transfer before delivery to the customer. While the satellite has already established links with the ground command and control system, during this phase, the transfer of command and control from the development to the operating organisation occurs. In both cases, the customer/operator requires particularly heightened cybersecurity measures to address changes in custody and potential vulnerabilities. The in-orbit testing phase is critical for ensuring that the satellite systems have survived the launch and are operational, but also because it may offer opportunities for malicious actors to exploit vulnerabilities during the transfer of custody.

Actors

The operations of the satellite in orbit, including the activities immediately after it reaches its destination and enters a business-as-usual stage of operations, can be a fully automated process. However, even automated processes should be supervised by humans. Hence, the process is monitored by SOC operators, in case when an unexpected event occurs, such as a malfunction of a satellite or an unanticipated natural condition. In cases where the process is not automated, SOC operators conduct all the required tasks manually. Their activities are coordinated by the SOC leader.

Depending on the nature of the satellite, the launch procedure, and the SOC, as well as other factors, a launch director and an operations safety manager can also be involved in this phase.

2.1.6. Phase 6 – Operations

In the operations phase, the satellite conducts mission-specific functions, such as sensing, information processing, data acquisition, and communication. Operations are managed via the ground stations and centres that are critical for functioning and mission execution. Cybersecurity is crucial to maintaining the confidentiality, integrity, and availability of sensitive data and communications. Assets/components such as command and data handling, ground control systems, communication modules, command and control interfaces, onboard computers and software, data cryptographic mechanisms, satellite payloads, and firmware/software updates play a vital role in securing the satellite's operations.

Actors

As with the in-orbit testing, this phase includes automated solutions and/or SOC operators, coordinated by the SOC leader. Their tasks include management of operations of both the satellite payload and bus.

The activities of SOC operators and the SOC leader can be supported by atmospheric scientists and space weather scientists, GIS analysts and other actors, depending on the nature of the satellite or in case of unexpected events occurring during its operations. Additionally, actors that typically work in the SOC include network and communication engineers, mission planners, payload operators, ground station operators, data analysts, logistics, support staff, and emergency response teams. Depending on the nature of a satellite, these actors can vary, but professionals working in the SOC collaborate closely to ensure the successful operations of a satellite throughout its mission.

2.1.7. Phase 7 – Decommissioning

Decommissioning is a high-risk process involving the post-mission disposition of satellites and space structures. When a satellite is decommissioned, it is either removed from the orbit or left in space but sent further away from Earth. In case the satellite is removed from the orbit, the process includes re-entry or re-orbiting, followed by recovery and post landing analysis to understand the impact of the landing process on the satellite's construction and materials. Proper handling of orbital debris and hazardous materials is essential, as are considerations for the secure handling and disposal of sensitive data, including intellectual property. Cybersecurity risks during decommissioning include data loss, corruption, unauthorised access and misuse by malicious actors, as well as potential physical threats to decommissioned systems. Improper decommissioning can also result in satellites becoming hijacked, broadcasting malicious signals, or posing a physical threat to other space assets through proximity operations or kinetic activity. Adherence to international standards, treaties, and domestic regulations is crucial.

Actors

The act of decommissioning is conducted by SOC operators, whose activities are coordinated by the SOC leader. They may be assisted by astronomers, atmospheric scientists, GIS analysts, and other actors, depending on the nature of the satellite to perform specific tasks in scope of decommissioning operations.

The post-landing analysis is conducted by topical experts, such as material scientists, mechanical engineers, physicists and others (as needed) to accurately assess the impact of the landing process on the satellite.



3. ASSET TAXONOMIES

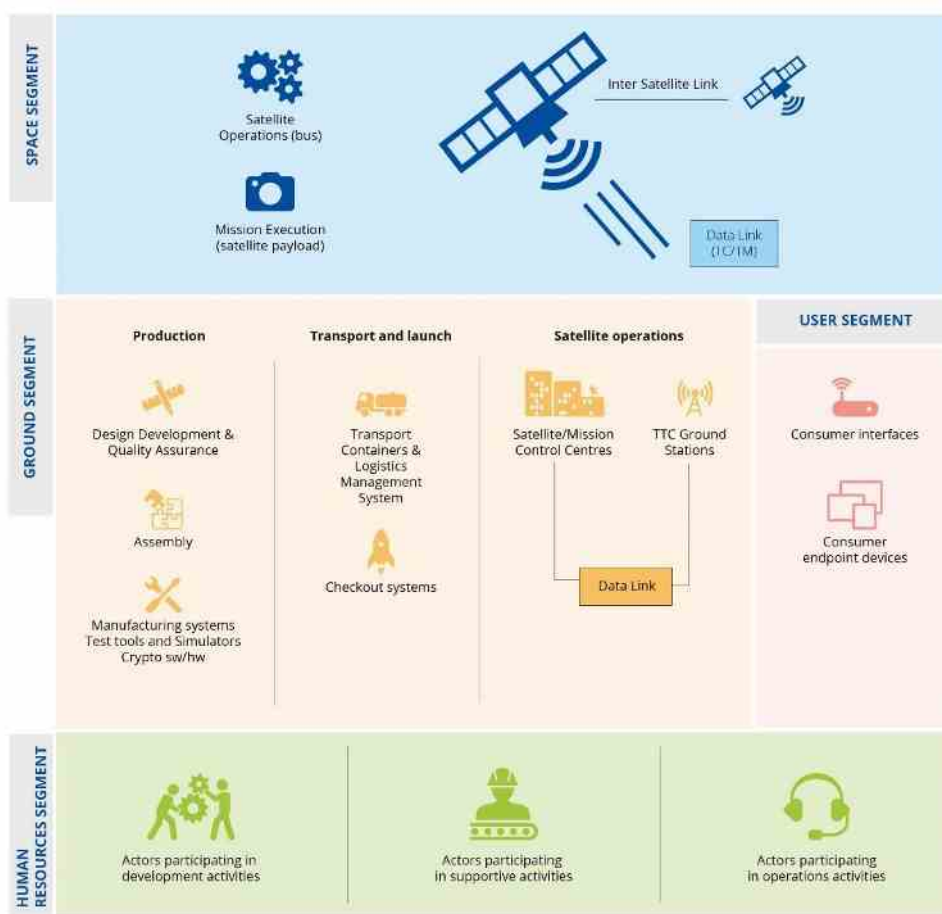
To ensure a streamlined and comprehensive approach, a **ground-space-user classification for the satellite taxonomy** is used and aligned with the lifecycle model described in the previous chapter. These three core segments are further broken down into categories, defined based on the specific process that related architecture supports, namely:

- Production
- Transportation
- Launch
- Satellite operations (from launch phase to decommissioning phase)
- Mission execution
- Consumer interfaces
- Consumer endpoint devices

The human dimension is addressed as a separate, horizontal 'human resources' segment to be considered across the entire asset taxonomy.



Figure 3: Asset Taxonomy⁴⁵



Although primarily focusing on the critical assets that underpin the operational aspects of satellites throughout their lifecycle, the taxonomy also identifies third party ground services supporting satellite missions, such as launch services, transportation, or manufacturing systems. However, because the third-party services differ significantly and are physical and digital structures of their own, therefore they fall out of the remit of this report and are included only on high-level to ensure a holistic view of the primary and secondary infrastructure. This also enables subsequent identification of specific threats, such as third-party compromise and supply chain intrusion.

A detailed assets taxonomy is provided in Annex B, further decomposing the segments and related categories outlined below into more specific asset subdomains and asset groups.

⁴⁵ Note: Production, transportation and launch are also commonly considered as part of satellite operations. They are labelled as separate categories here for ease of understanding the different process.

3.1. GROUND SEGMENT

Figure 4: Detailed Asset Taxonomy – Ground segment



This segment includes the terrestrial systems that facilitate communication, monitoring of satellite activities, and relaying of essential telemetry data, as well as brick and mortar facilities, manufacturing, logistics, and ultimately on-the-ground transportation.^{46,47, 48, 49, 50, 51,52, 53}

Categories defined in the Ground segment include:

- **Production** includes assets needed for satellite development. It emphasises the importance of secure practices and concept known as “security by design and by default”, as this category also covers assets required during planning, design and development, cryptographic technologies, testing, and simulations, all of which are critical for ensuring confidentiality, integrity, and availability of the system throughout its lifecycle and mission execution.
- **Transportation** includes assets that are being used for transportation of satellite components to the test and/or launch sites.
- **Launch** includes assets associated with launch sites and launch control centres. Launch is, in the case of commercial satellites, commonly outsourced to third parties and only assets relevant to the mission itself are listed in the subsequent asset taxonomy.

⁴⁶ Willbold, J., Schloegel, M., Vogeles, M., Gerhardt, M., Holz, T., Abbasi, A. 2023. Space Odyssey: An Experimental Software Security Analysis of Satellites. In IEEE Symposium on Security and Privacy. <https://willbold.com/paper/willbold2023spaceodyssey.pdf>.

⁴⁷ Manulis, M. et al. (2020). Cyber security in New Space: Analysis of Threats, Key Enabling Technologies, and Challenges. International Journal of Information Security. https://www.researchgate.net/publication/341331628_Cyber_security_in_New_Space_Analysis_of_threats_key_enabling_t_echnologies_and_challenges.

⁴⁸ BSI. (2023). Technical Guideline BSI TR-03184 Information Security for Space Systems. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03184/BSI-TR-03184_part1.pdf?__blob=publicationFile&v=2.

⁴⁹ NIST. 2022. Satellite Ground Segment: Applying the Cybersecurity Framework to Satellite Command and Control. <https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8401.pdf>.

⁵⁰ BSI, 2022, IT-Grundschutz Profile for Space Infrastructures. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/profiles/Profile_Space-Infrastructures.pdf?__blob=publicationFile&v=2.

⁵¹ ESA, 2020, ESA TECHNOLOGY TREE, Version 4.0. <https://esamultimedia.esa.int/multimedia/publications/STM-277/STM-277.pdf>.

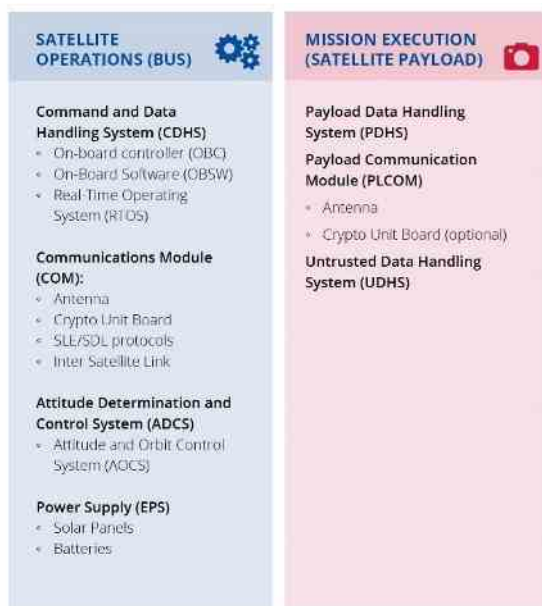
⁵² The Consultative Committee for Space Data Systems. 2023. Space Link Extension – Forward CLTU Service Specification. <https://public.ccsds.org/Pubs/912x1b5.pdf>.

⁵³ Quiquet, F. 2020. Description of the Elements of a Satellite Command and Control System. <https://www.spacesecurity.info/en/description-of-the-elements-of-a-satellite-command-and-control-system/>.

- **Satellite operations** include assets related to the management, control, and monitoring of satellites throughout the mission lifecycle. This includes control centres and ground control stations, which provide a secure link to the satellite. Additionally, this includes Earth stations/Gateways (e.g. internet connectivity where the gateway serves as a hub for transmitting/receiving signal from the orbiting assets and transforms it to terrestrial connectivity).

3.2. SPACE SEGMENT

Figure 5: Detailed Asset Taxonomy – Space segment



The Space segment contains satellite(s) orbiting the Earth.^{54, 55, 56, 57, 58, 59} It can include satellites that are operating independent of other satellites, several satellites orbiting the Earth arranged in a regular pattern (i.e. a satellite constellation), or satellites in completely different orbits but serving the same mission. Categories defined in the Space segment include:

- **Satellite operations (BUS)**, also referred to as the 'platform', include all assets required to operate and maintain a satellite in orbit. The satellite bus operates independently from the payload, which is mission-specific.
- **Mission execution (satellite payload)** includes assets needed to fulfil the mission. In some cases, payload systems rely on bus solutions to transmit and receive data and to communicate with ground stations and satellite/mission control centres. However, there is an increasing trend for keeping these two systems completely separated,

⁵⁴ ESA. Science and Exploration: Power.

https://www.esa.int/Science_Exploration/Human_and_Robotic_Exploration/Orion/Power

⁵⁵ Guven, U. Power System Design for Earth Orbiting Satellites. Aerospace Lectures.

<https://www.aerospacelectures.com/Power%20System%20Design%20for%20Earth-Orbiting%20Satellites.pdf>

⁵⁶ Ear, E., Remy, L.C.J., Feffer, A., Hu, S. 2023. Characterizing Cyber Attacks against Space Systems

with Missing Data: Framework and Case Study. <https://arxiv.org/pdf/2309.04878.pdf>

⁵⁷ BSI. 2023. Technical Guideline BSI TR-03184 Information Security for Space Systems.

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03184/BSI-TR-03184_part1.pdf?__blob=publicationFile&v=2

⁵⁸ Scholl, M. Suloway, T. 2023. Introduction to Cybersecurity for Commercial Satellite Operations.

https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=936776

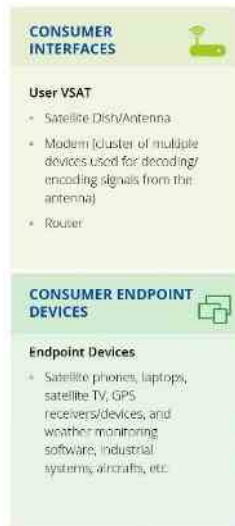
⁵⁹ Manulis, M. Bridges, C.P., Harrison, R., Sekar, V., Davis, A. 2020. Cyber security in New Space.

<https://link.springer.com/article/10.1007/s10207-020-00503-w>

especially for missions where a satellite has multiple payloads which serve different consumers.⁶⁰

3.3. USER SEGMENT

Figure 6: Detailed Asset Taxonomy – User segment



The User segment contains interfaces and devices that enable end users to access and benefit from the services provided by a satellite, ranging from communication and navigation to TV reception and industrial applications.⁶¹ Depending on the use-case, the scope of the User segment encompasses assets needed to reach the ground station (or the satellite directly) with the request for service, and to receive the communication from the satellite – enabling the service.^{62,63}

Categories defined in the User segment include:

- **Consumer interfaces** include terminals that enable users to interact with the satellite directly or with other ground station segments. Consumer interfaces rely on Very-small-aperture terminals (VSATs), comprised of smaller asset groups that include consumer antennas and modems connected to routers for dispersing the signal.^{64,65}
- **Consumer endpoint devices** include the physical assets needed to manage the consumer interfaces. This includes, for example, satellite phones, satellite television receivers, vehicles, industrial systems, aircrafts, etc.⁶⁶

⁶⁰ Willbold, J., Schloegel, M., Vogele, M., Gerhardt, M., Holz, T., Abbasi, A. 2023. Space Odyssey: An Experimental Software Security Analysis of Satellites. In IEEE Symposium on Security and Privacy. <https://willbold.com/paper/willbold2023spaceodyssey.pdf>.

⁶¹ NIST. 2023. Introduction to Cybersecurity for Commercial Satellite Operations. <https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8270.pdf>.

NIST. 2023. Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN). <https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8441.pdf>.

⁶³ Quiquet, F. 2020. Description of the Elements of a Satellite Command and Control System.

<https://www.spacesecurity.info/en/description-of-the-elements-of-a-satellite-command-and-control-system/>

⁶⁴ Ocean Web. 2022. A guide to maritime VSAT. <https://www.oceanweb.com/a-guide-to-maritime-vsats/>

⁶⁵ Gartner. Very Small Aperture Terminal (VSAT). <https://www.gartner.com/en/information-technology/glossary/vsat-very-small-aperture-terminal#:~:text=A%20very%20small%20aperture%20terminal,communication%20network%2C%20excluding%20broadcast%20television.>

⁶⁶ NIST. 2023. Introduction to Cybersecurity for Commercial Satellite Operations. <https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8270.pdf>

3.4. HUMAN RESOURCES SEGMENT

Figure 7: Detailed Asset Taxonomy – Human Resources segment



Human Resources comprise the human dimension of the asset taxonomy, embedded across the entire satellite lifecycle. It is the staff's vigilance and compliance with different security protocols that create an integral layer for protecting mission-critical assets and ensuring security by design and by default throughout the lifecycle.

Asset subdomains defined in the Human resources segment are directly related to the actor clusters identified against the different phases of the satellite lifecycle, and include:

- Actors participating in development activities;
- Actors participating in supporting tasks; and
- Actors participating in satellite operations.

4. SPACE THREATS

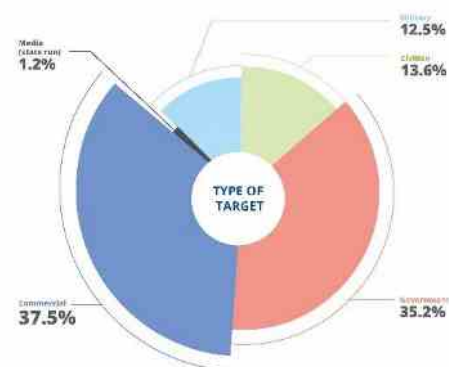
Satellite systems and related services are an integral component of modern life, supporting a wide range of critical applications, from communications to navigation and Earth observation. Increased reliance on satellite technology also exposes these systems to a growing array of cybersecurity threats. Understanding the threat landscape for satellite systems is therefore crucial for safeguarding their operations and ensuring continued, uninterrupted provision of relevant satellite-based services. This chapter delves into the web of threats facing satellite systems, examining different threat actors, threat categories, and possible tactics, techniques, and procedures (TTPs), compiled in a threat taxonomy.

4.1. SPACE THREAT TRENDS

The Space Attacks Open Database Project⁶⁷ provides a detailed compilation of publicly known attacks on satellites, covering the period between 1977 and 2019. However, despite the immense growth of the space sector over the past years⁶⁸, there seems to be a lack of consolidated data on cybersecurity incidents taking place during this period. The lack of analysis, together with the lack of control of space-based infrastructure and objects, was also recognised by ENISA's 2023 Foresight report⁶⁹, listing it in the top 10 threats.

Supplementing the Space Attacks Open Database Project findings with additional insight from publicly available reports on individual cybersecurity incidents in the space domain indicates that the majority of the space-based attacks took place on commercial and government targets – as illustrated in Figure 8. These are followed by targets on the military and civilian sectors, and one identified attack on state-run media outlets. Due to their nature and spread, some of these attacks contain overlaps in terms of target categories. While the database does not specify differentiators between these categories, it is assumed that the difference lies in the party that actually owns/operates the asset (making the difference between government, civilian, and military).

Figure 8: Target categories of known attacks in the space domain



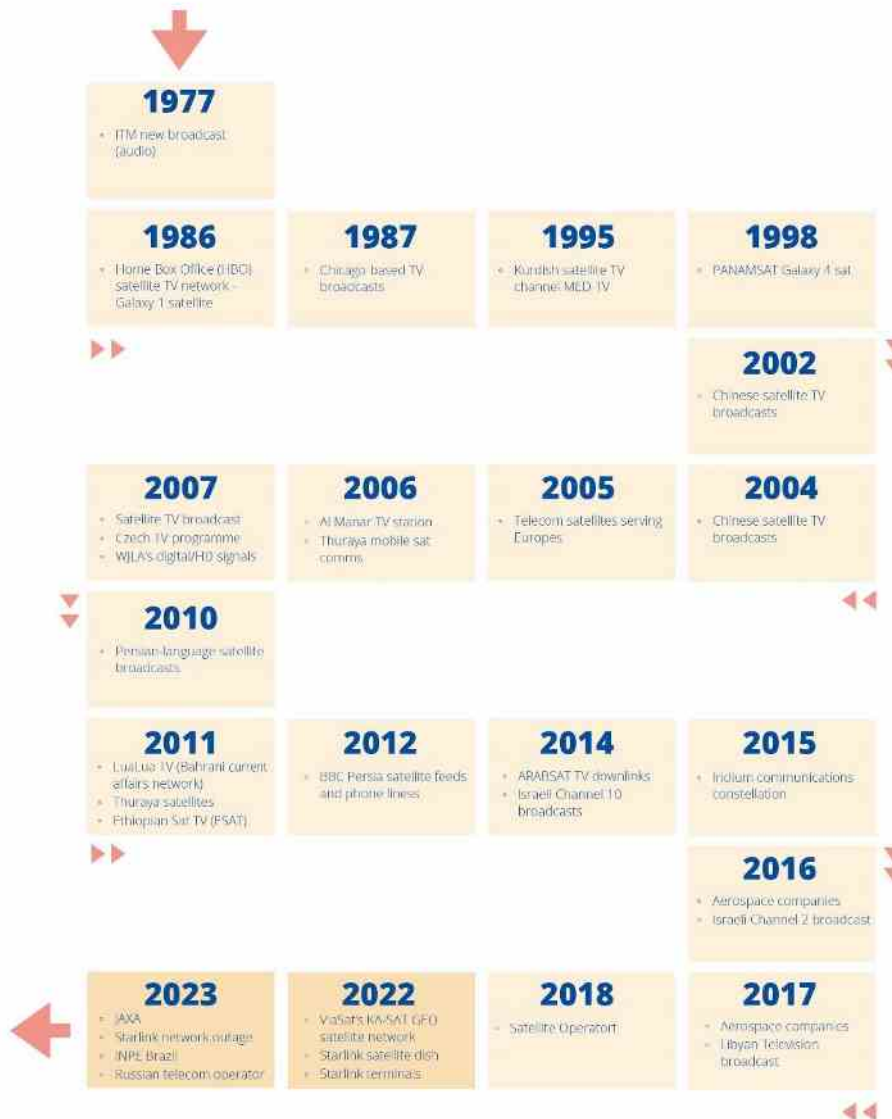
⁶⁷ Space Security Community. Space Attacks Open Database Project. <https://www.spacesecurity.info/en/space-attacks-open-database/>

⁶⁸ UNOOSA statistics on the annual number of objects launched into space indicate a 300+% increase of objects launched into space for this timeframe, from less than 600 objects launched in 2019, to over 2500 objects launched in 2023, the majority of these being commercial assets. Online Index of Objects Launched into Outer Space. United Nations Office for Outer Space Affairs. https://www.unoosa.org/oosa/osoindex/index.aspx?lf_id=

⁶⁹ ENISA. 2023. ENISA Foresight Cybersecurity Threats for 2030. <https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030>

As illustrated in Figure 9 below, attacks on commercial satellite infrastructure have had a consistent presence throughout the observed period. Although the updated ENISA's 2024 Foresight report no longer lists space-related threats in the top 10, the lack of analysis and control of space-based infrastructure and objects still figures prominently, taking 11th place. Inspecting technological trends, the report recognises that as the number of satellites in space grows so does our dependency on space infrastructures.⁷⁰ Consequently, a rise in the number of attacks against satellites can also be expected.

Figure 9: Examples of known attacks on commercial satellite infrastructure/s (timeline)

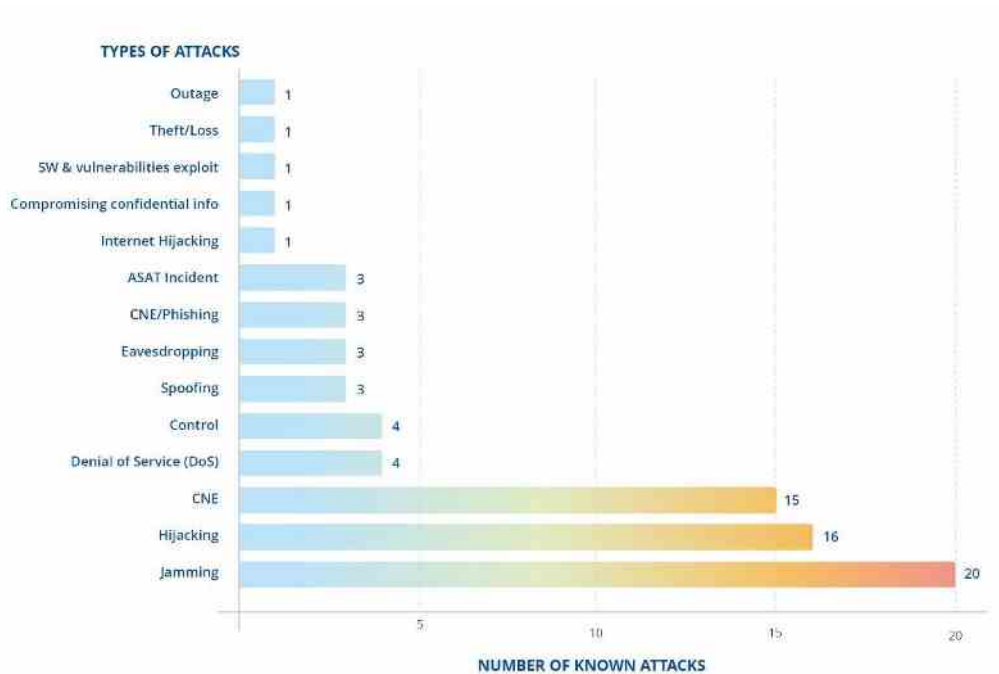


Jamming was among the most frequent materialised threats according to the database, the effects of which can range from disrupting access to a satellite to affecting Global Navigation Satellite Systems (GNSS) used for services such as GPS, followed by hijacking and Computer Network Exploitation (CNE). Attacks aimed at control functions, as well as spoofing, eavesdropping and the employment of anti-satellite weapons (ASATs) were far less frequent

⁷⁰ ENISA. 2024. Foresight Cybersecurity Threats For 2030 - Update 2024: Extended report.
<https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-extended-report>

during the observed period. The figure below presents a breakdown of the attack types identified.

Figure 10: Breakdown of known attacks on satellites per attack type



Visibility of space threat trends is expected to improve with developments such as the obligation to report all significant incidents prescribed by the NIS2 Directive, which now includes space, telecoms in the scope of sectors of high criticality and other relevant critical sectors such as the manufacturing of e.g. computer, electronic and optical products, machinery, transport equipment, and equipment n.e.c.⁷¹, thereby providing a more complete picture of the threat landscape impacting satellite operations. The recent establishment of the EU Space Information Sharing Centre (ISAC)⁷² is also expected to encourage more proactive information and knowledge sharing about security-related information, incidents, cyber trends, vulnerabilities, and threats among commercial space operators. In turn, this will reflect on the number of known incidents, with an expected upward trend compared to previous years as more cyber-relevant events will be officially recorded.

4.2. THREAT ACTORS

The growing commercialisation of the space domain opens the door to a wide array of threat actors, motivated by different traits and with varying levels of capabilities, including:

State-nexus actors, who rely on government resources to achieve their objectives. Primarily engaged in espionage and disruption, state-nexus actors are sometimes directed by the military, intelligence or state control apparatus of their country and often spend considerable time investigating their targets to identify weaknesses and entry points. In addition to other states, state-nexus actors can also target other organisations for sensitive data or conduct operations to obtain funding for their country.

⁷¹ INSPIRE registry: Manufacturing not elsewhere classified (n.e.c.)

<https://inspire.ec.europa.eu/codelist/EconomicActivityNACEValue/C.32.99>

⁷² EU Space ISAC <https://www.euspa.europa.eu/eu-space-programme/eu-space-and-security/eu-space-isac>

Cybercrime actors and hacker-for-hire actors, primarily motivated by financial gain. Mainly targeting data or infrastructure, cybercrime actors often employ social engineering and either steal from their victims, engage in extortion, or aim to monetise the stolen information. As a subcategory of cybercrime actors, hacker-for hire actors contribute to the professionalisation of the cybercrime market, including services to state-nexus actors, often providing access to environments or cybercriminal services (e.g. ransomware-as-a-service).

Private Sector Offensive Actors (PSOA), who are engaged in the cyber-surveillance industry. Focused on enabling other actors (e.g. governments, private individuals) to gain a competitive advantage against their peers, PSOAs specialise in developing and selling cyberweapons to their clients, equipping them with advanced cyber capabilities.

Hactivists (a.k.a. Civil Activists), whose primary goal is to extract and expose data or disrupt business operations for ideological reasons or to draw attention to a specific cause, advocating for political or social change.

Hackers, comprising a diverse set of malicious actors' subgroups that vary in their motivation, objectives, skillsets and capabilities. These may range from Cyberwarriors and Cyber Fighters to Blackhat hackers/Crackers, but can also include Cyber Vandals and Script Kiddies.

Disgruntled Employees or Insider Attackers, who have detailed insight of the organisation and its systems. This includes staff, contractors, vendors, customers, or former employees.

Untrained/Reckless Employees, who may not have the intention to cause harm but may still do so as a result of negligence or insufficient training.

With the above, different threat actors can exercise various types of attacks regardless of the resources of their supporting organisation - if any. This is further corroborated with examples of different threats, discussed below, which do not necessarily require significant resources to perform successful cyber-attacks.

When conducting a risk assessment, the threat actors most relevant for the specific use case should be identified. This involves delving into the characteristics of each identified threat actor category/type, including their motivations, capabilities, and objectives. The provided descriptions are inconclusive and serve as a foundational starting point for a more in-depth analysis.

More details on the abovementioned threat actors, their motives, means, and opportunities is provided in the ENISA Threat Landscape 2024⁷³, and in ENISA's Methodology for Sectoral Cybersecurity Assessment⁷⁴.

⁷³ ENISA. September 2024. ENISA Threat Landscape 2024. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>

⁷⁴ ENISA. 2021. Methodology for Sectoral Cybersecurity Assessments. <https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment>

4.3. THREAT TAXONOMY METHODOLOGY

The taxonomy presented below is based on a comparative analysis of academic^{75, 76, 77, 78, 79, 80, 81, 82} and industrial (including relevant government agencies)^{83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93} resources deliberating on the types of threats and attack tactics, techniques, and procedures (TTPs) applicable to the space domain and publicly available information on known attacks on satellite infrastructure. These are then clustered in common threat categories and inspected for their impact on confidentiality, integrity and availability (CIA). As a final step, identified threats are mapped against the relevant asset categories and subdomains identified in Chapter 3.

The threat taxonomy strictly focuses on assets for which a direct cyber-relevant threat has been identified, resulting in disruption or destruction of satellite infrastructure and/or services. Assets that are at risk solely from physical threats are not further addressed.

Important to note is that there is no universally accepted standard for a threat taxonomy, and competing approaches are still emerging.⁹⁴ This is evident in the literature examined for the purpose of this report where classifications of threats and relevant TTPs and attack vectors employed in the materialisation of these threats somewhat overlap. The presented taxonomy therefore focuses on the common threat clusters identified across the addressed information sources, while common TTPs and attack vectors form the parts of the description of these.

⁷⁵ Baram, G. and Wechsler, O. 2020. Cyber Threats to Space Systems. Current Risks and the Role of NATO. Joint Air Power Competence Centre. <https://www.iapcc.org/essays/cyber-threats-to-space-systems/>

⁷⁶ Bichler, S. F. 2015. Mitigating Cyber Security Risk in Satellite Ground Systems. Air Command and Staff College. <https://apps.dtic.mil/sti/pdfs/AD1012754.pdf>

⁷⁷ Garino, B. and Gibson, J. 2018. Space System Threats. Aerospace Security. <https://aerospace.csis.org/wp-content/uploads/2018/09/Space-System-Threats.pdf>

⁷⁸ Manulis, M. et al. (2020). Cyber security in New Space: Analysis of Threats, Key Enabling Technologies, and Challenges. International Journal of Information Security. https://www.researchgate.net/publication/341331628_Cyber_security_in_New_Space_Analysis_of_threats_key_enabling_technologies_and_challenges

⁷⁹ Matei, V.C. 2021. Cybersecurity Analysis for the Internet-Connected Satellites. Uppsala Universitet. <https://uu.diva-portal.org/smash/get/diva2:1622956/FULLTEXT01.pdf>

⁸⁰ Livingstone, D. and Lewis, P. 2016. Space, the Final Frontier for Cybersecurity? Chatham House. <https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf>

⁸¹ Varadharajan, V. and Suri, N. 2022. Security Challenges when Space Merges with Cyberspace. Cornell University. <https://arxiv.org/pdf/2207.10798>

⁸² Willbold, J., Schloegel, M., Voge, M., Gerhardt, M., Holz, T., Abbasi, A. 2023. Space Odyssey: An Experimental Software Security Analysis of Satellites. In IEEE Symposium on Security and Privacy. <https://willbold.com/paper/willbold2023spaceodyssey.pdf>

⁸³ Aerospace Corporation. Space Attack Research & Tactic Analysis (SPARTA). <https://sparta.aerospace.org/>

⁸⁴ Bailey, B. et al. 2019. Defending Spacecraft in the Cyber Domain. Center for Space Policy and Strategy. https://aerospace.org/sites/default/files/2019-11/Bailey_DefendingSpacecraft_11052019.pdf

⁸⁵ Bailey, B. 2020. Establishing Space Cybersecurity Policy, Standards, and Risk Management Practices. Aerospace Corporation. https://aerospace.org/sites/default/files/2020-10/Bailey%20SPD5_20201010%20V2_formatted.pdf

⁸⁶ BSI. (2023). Technical Guideline BSI TR-03184 Information Security for Space Systems. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03184/BSI-TR-03184_part1.pdf?__blob=publicationFile&v=2

⁸⁷ The Consultative Committee for Space Data Systems. 2022. Security Threats Against Space Missions. CCSDS 350.1-G-3. <https://public.ccsds.org/Pubs/350x1g3.pdf>

⁸⁸ Bingen, K. Johnson, K. and Young, M. 2023. Space Threat Assessment 2023. Center for Strategic & International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-04/230414_Bingen_Space_Assessment.pdf?VersionId=oMsUS8MupLbZi3BISPrqPCKd5jDejZnJ

⁸⁹ ESPI. 2022. ESPI Report 84 - The war in Ukraine from a space cybersecurity perspective. <https://www.espi.or.at/wp-content/uploads/2022/10/ESPI-Report-84.pdf>

⁹⁰ Fortinet. August 2022. Global Threat Landscape Report. A Semiannual Report by FortiGuard Labs. <https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-1h-2022.pdf>

⁹¹ Scholl, M. & Suloway, T. NIST, 2023. Introduction to Cybersecurity for Commercial Satellite Operations. <https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8270.pdf>

⁹² UK Space Agency. 2020. Cyber Security Toolkit. https://assets.publishing.service.gov.uk/media/5ec298a3e90e071e2f955ebc/Space_cyber_toolkit_final_v4.pdf

⁹³ White House. 2020. Memorandum on Space Policy Directive-5 – Cybersecurity Principles for Space Systems. <https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/>

⁹⁴ ENISA. 2021. Methodology for Sectoral Cybersecurity Assessments. <https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment>

4.4. THREAT TAXONOMY

For the purpose of the threat taxonomy, high-level threat categories have been derived from ENISA's threat taxonomy⁹⁵, which serves as a baseline for mapping the space threat landscape.

This includes the following threat categories:

- **Nefarious Activity/Abuse (NAA)**: "intended actions that target ICT systems, infrastructure, and networks by means of malicious acts with the aim to either steal, alter, or destroy a specified target".
- **Eavesdropping/Interception/ Hijacking (EIH)**: "actions aiming to listen, interrupt, or seize control of a third party communication without consent".
- **Physical Attacks (PA)**: "actions which aim to destroy, expose, alter, disable, steal or gain unauthorised access to physical assets such as infrastructure, hardware, or interconnection".
- **Unintentional Damage (UD)**: unintentional actions causing "destruction, harm, or injury of property or persons and results in a failure or reduction in usefulness".
- **Failures or malfunctions (FM)**: "partial or full insufficient functioning of an asset (hardware or software)".
- **Outages (OUT)**: "unexpected disruptions of service or decrease in quality falling below a required level".
- **Disaster (DIS)**: "a sudden accident or a natural catastrophe that causes great damage or loss of life".
- **Legal (LEG)**: "legal actions of third parties (contracting or otherwise), in order to prohibit actions or compensate for loss based on applicable law".

In addition to the above, threats stemming from the **legacy infrastructure (LEI)** are also present. Although legacy is a challenge for all information technology enabled systems, the nature of space infrastructure - where assets are not physically reachable yet need to provide services at a specified level of output and quality for protracted periods of time, makes this an important feature to consider in relation to the developing cyber threat landscape. The extended use of commercial off-the-shelf software (COTS) for different satellite components^{96, 97, 98, 99} adds a further layer of complexity to the management of the satellite infrastructure. Apart from standard supply chain risks resulting from – among other – the reliance on COTS, threats in the context of legacies may materialise via an exploit of vulnerabilities arising during the satellite's infrastructure lifecycle. Some of these might have been unknown or were not considered as relevant during the design, assembly, and initial operational phases, which may result in unpatched or outdated legacy COTS components¹⁰⁰.

Finally, as an overarching prerequisite for most of the threats identified above, the **acquisition of capabilities** by adversaries is also recognised as a threat vector by the SPARTA matrix¹⁰¹

⁹⁵ ENISA. 2016. ENISA Threat Taxonomy. <https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view>

⁹⁶ ESPI. 2022. ESPI Report 84 - The war in Ukraine from a space cybersecurity perspective. <https://www.espi.or.at/wp-content/uploads/2022/10/ESPI-Report-84.pdf>

⁹⁷ Willbold, J., Schloegel, M., Vogele, M., Gerhardt, M., Holz, T., Abbasi, A. 2023. Space Odyssey: An Experimental Software Security Analysis of Satellites. In IEEE Symposium on Security and Privacy. <https://willbold.com/paper/willbold2023spaceodyssey.pdf>

⁹⁸ Manulis, M. et al. (2020). Cyber security in New Space: Analysis of Threats, Key Enabling Technologies, and Challenges. International Journal of Information Security. https://www.researchgate.net/publication/341331628_Cyber_security_in_New_Space_Analysis_of_threats_key_enabling_technologies_and_challenges.

⁹⁹ Peeters, W. 2022. Cyberattacks on Satellites: An Underestimated Political Threat. LSE Ideas. <https://www.lse.ac.uk/ideas/projects/space-policy/publications/Cyberattacks-on-Satellites>

¹⁰⁰ Manulis, M. et al. (2020). Cyber security in New Space: Analysis of Threats, Key Enabling Technologies, and Challenges. International Journal of Information Security. https://www.researchgate.net/publication/341331628_Cyber_security_in_New_Space_Analysis_of_threats_key_enabling_technologies_and_challenges.

¹⁰¹ Aerospace Corporation. Space Attack Research & Tactic Analysis (SPARTA). <https://sparta.aerospace.org/>



and the ESA SPACE-SHIELD¹⁰², both of which are based on the MITRE ATT&CK framework and tailored to the space domain. Acquisition of capabilities refers to the ability of threat actors to acquire and employ the necessary skills and/or resources to achieve their objectives. This may relate to various types of offensive activities aimed at any satellite lifecycle asset, ranging from the acquisition of infrastructure (e.g. ground infrastructure, space infrastructure), to specific software (e.g. advanced malware, decryptors) or tools (e.g. specific anti-satellite assets, such as anti-satellite weapons - ASAT).

Figure 11 provides an overview of the high-level threat categories for the space domain. A breakdown of specific threats within each of these categories is presented below in Figure 12. Details on each of the identified threats, their impact on CIA, and respective affected assets is provided in Annex B. Several overlaps of specific threats across the threat categories exist, as these can be a result of both nefarious activities as well as unintentional damage. The threat taxonomy presented in this report is aimed for general applicability for any orbit.¹⁰³

Figure 11: Space Threat Taxonomy



¹⁰² European Space Agency. Space Attacks and Countermeasures Engineering Shield (SPACE-SHIELD). <https://spaceshield.esa.int/>

¹⁰³ For a detailed assessment of Low Earth Orbit (LEO) constellations, commonly used in the current space setup in Europe, please refer to ENISA's targeted report on LEOs. ENISA, 2024. Low Earth Orbit (LEO) SATCOM Cybersecurity Assessment. <https://www.enisa.europa.eu/publications/low-earth-orbit-leo-satcom-cybersecurity-assessment>

Figure 12: Detailed Space Threat Taxonomy



5. RISK ASSESSMENT

This chapter presents three risk scenarios aimed at illustrating the potential impact of adverse events on commercial satellite infrastructure and the services they provide.¹⁰⁴ These hypothetical scenarios consider the defined generic lifecycle model, assets taxonomy and taxonomy of threats as presented in this report. Examples of real-life incidents involving satellite infrastructure, derived from the literature review for preceding steps, have also been taken into account. Each scenario specifies the threat(s) that are materializing, the assets at risk, and the potential threat actor(s) considering generally assumed capacity and possible motivations behind the threat actor clusters. Cascading effects are presented through the escalation path, and impact is considered through the CIA triad, supplemented with wider impact considerations presented in the form of a high-level PESTLE analysis. When conducting a risk assessment, identified relevant threats should be classified considering their impact, likelihood, intentionality, and cascading effects.¹⁰⁵

5.1. SCENARIO 1: COMMUNICATIONS PROTOCOL COMPROMISE VIA SOCIAL ENGINEERING

Assumptions on the context:

- Commercial broadcasting satellite (TV and radio).
- In-house, on-prem operations centre.
- Insufficient staff awareness.
- Weak network segmentation.

The scenario covers several ground-related threats that can result with an attacker taking control over the Telemetry, Tracking, and Command (TTC) ground station and communication protocols and ultimately hijacking the satellite and/or obtaining the ability to modify mission values. The scenario emphasises the growing risk of satellite hijacking to either disable the satellite or broadcast a malicious signal.

As depicted in Figure 14, the first step is to gather information on employees, identify potential targets, and launch a spearphishing campaign in order to secure initial access. A link in the phishing email leads an employee to download a malicious file, which enables the attacker to access the network. Once inside the network, the attacker exploits the lack of segmentation, moving laterally and gaining access to credentials stored in memory. In parallel, the attacker conducts network reconnaissance to identify satellite control systems, configurations, and communications protocols to direct the next attack. The extracted valid credentials are then used to penetrate the mission control software. The attacker thus obtains access to information about configurations and signal amplification mechanisms at one of the TTC ground stations connected to the mission control centre. Access to such information enables the attacker to exfiltrate sensitive data related to satellite communication protocols and encryption keys. Assuming that the systems have a vulnerable SDLS protocol, the attacker can gain access to critical information including Authentication, Encryption, and Authenticated Encryption. As a result of such a vulnerability, the attacker obtains knowledge about data link protocols connecting the operations centre and the TTC ground station enabling either eavesdropping on

¹⁰⁴ The risk scenarios provide a limited sample of possible attack technique chains. For more information, research conducted by Department of Computer Science at the University of Colorado can be consulted, which identified 72 attack tactic chains and 4,076 attack technique chains. Ear, E., Remy, L.C.J., Feffer, A., Hu, S. 2023. Characterizing Cyber Attacks against Space Systems with Missing Data: Framework and Case Study. <https://arxiv.org/pdf/2309.04878.pdf>

¹⁰⁵ For additional guidance, the ISO 31000 Risk management standard can be used.



the communication or compromising the signal, thus impacting the satellite's confidentiality, integrity, and availability. With control over the mission control software, the attacker can also intentionally crash the satellite, causing physical damage to the satellite itself as well as other satellites in the constellation or further afield.

It is important to stress that beyond the owned Ground station and the Ground Station as a Service (GSaaS) models, where ground stations belong to authenticated players, operators may face additional challenges related to ground station security. Open networks like SatNOGS¹⁰⁶, often supporting open-source missions, rely on voluntary contributions, raising significant concerns about the level of trust that can be placed in such diverse and potentially unverified ground stations. The risk of malicious or compromised ground stations within these networks cannot be discounted. Furthermore, while the focus is often on the communication links between the ground station and the satellite, the security of links and protocols between ground stations is equally critical. These inter-ground station communications, often used for coordination and data sharing, represent another potential attack vector that requires careful consideration and robust security measures.

Figure 13: Scenario 1 – Communications protocol compromise via social engineering



Table 1: Scenario 1 – Communications protocol compromise via social engineering

Communications protocol compromise	IMPACT (CIA)
	Crucial: the compromise of communication protocols between the satellite operations centre, TTC ground station, and the satellite itself, grants the attacker access to the majority of assets related to satellite operations and mission execution. Once compromised, the attacker can eavesdrop on all

¹⁰⁶ SatNOGS Open Source global network of satellite ground-stations. <https://satnogs.org/>

communication, modify onboard values, cause disruption by manipulating the satellite's bus, or continue to penetrate into the satellite bus-payload link and modify the payload to leak confidential information. Compromised communication protocols lead to multiple mission-specific assets being compromised, amounting to a critical impact level with all three CIA categories – confidentiality, integrity, and availability – affected.

As this cybersecurity incident looks into the compromise of communication protocols between the ground and satellite infrastructure, impacts on CIA are as follows:

CONFIDENTIALITY

The breach and compromise of SLE/SDL protocols jeopardises confidentiality of data transmitted between the satellite operations centre, ground stations, and the satellite itself. Sensitive or client privileged information, as well as corporate interests of the satellite operator, become vulnerable to unauthorised access. The ability to eavesdrop on communication channels allows attackers to gather intelligence, which could lead to strategic disadvantages, leak of proprietary technology, as well as commercial espionage.

INTEGRITY

The ability to laterally move within the network and eventually gain control over communication protocols, both on the ground and in the satellite itself, grants the attacker the ability to disrupt the integrity of satellite services. With access to SLE/SDL protocols the attacker can alter critical parameters and commands to compromise transmitted data. Such activities could lead to incorrect satellite positioning, incorrect sensor readings, and execution of malicious commands. Loss of data integrity has a negative impact on trust in the information transmitted and makes it difficult for operators to distinguish between genuine and manipulated commands and telemetry.

AVAILABILITY

With the scenario escalating, the attacker can rely on compromised communication protocols to ultimately disrupt the availability of satellite services, as well as the satellite itself. The attacker can hijack the satellite to broadcast malicious signal, as well as crash it or render it inoperable, thus impacting and disrupting the payload and the services provided. As such, compromised availability not only affects the mission itself, but can also trickle down to the sectors relying on the satellite, potentially leading to both financial and legal consequences.

THREAT CLUSTER	ASSETS AFFECTED	THREAT ACTORS
• Social Engineering • Malicious code/ software/ activity: Network exploit • Abuse/ Falsification of rights • Unauthorised access • Interception of communication • Hijacking	• Satellite Operations Centre • TTC Ground • SLE/SDL • Satellite bus • Satellite payload	• Untrained/ Reckless Employees • (Organized) Cyber Crime actors • State-Sponsored Attackers/Government Spies

BROADER IMPACT (PESTLE)

POLITICAL

- Potential for strained relations between countries if the breach is used for promotion of political propaganda via compromised payload or is traced back to state-sponsored groups.

ECONOMIC

- TV and radio broadcasters, satellite operators and consumers could suffer financial losses due to disrupted services.
- The costs of mitigating the attack and restoring services could be substantial.

SOCIAL

- It could lead to the disruption of information flow and the public could lose access to important news, potentially leading to misinformation.
- Spreading disinformation or propaganda can lead to social unrest.

ENVIRONMENTAL

- The incident may raise concerns of space debris if the corrupted satellite becomes uncontrollable or changes trajectory.

ESCALATION PATH

1. The attacker gathers information on the satellite centre's employees and selects possible targets for a spearphishing campaign.
2. The attacker sends **spearphishing** emails containing malicious attachments to the selected employees of the **satellite control centre**. One employee that opens the attachment, would trigger **malware payload**. With this, the attacker would establish an initial foothold in the facility's internal network.
3. The attacker could further exploit **vulnerable systems and the lack of network segmentation** to access credentials stored in memory and conduct **credentials dumping**.
4. Credentials are then extracted, including details on privileged accounts within the network. The attacker filters valid credentials that are associated with **satellite control systems**.
5. The attacker then conducts **network reconnaissance** to identify **satellite control systems**, configurations, and communications protocols, which are later used to gain control over **TTC ground stations** and antennas.
6. The attacker utilises **valid credentials** to move laterally within the network and access the **mission control software**.
7. The attacker collects information about the satellite communication equipment – specifically, the **antenna configurations** and signal amplification mechanisms at one of the **TTC ground stations** connected to the mission control centre.
8. The attacker manages to **exfiltrate sensitive data** related to satellite communication protocols and encryption keys, therefore gaining the ability for corrupting **SLE/SDL protocols** between the operations centre, the TTC ground station, and the satellite. Eventually, the attacker could corrupt the **satellite bus and payload**.

5.2. SCENARIO 2: EXPLOITING OBC/OBSW VULNERABILITIES VIA MALICIOUS CODE

Assumptions on the context:

- Commercial satellite constellation providing internet coverage (broadband satellite service).
- Weak perimeter protection (assembly and/or transportation) and, in case these are provided by third parties, lack of vendor/third party security audit and due diligence.
- Weak hardening procedures after the assembly phase.
- Weak software configuration and data processing controls.

This scenario covers several ground – and space – related threats designed to take control over the satellite bus and specifically On-Board Controller (OBC), On-Board Software (OBSW), and subsequently the Real Time Operating System (RTOS). The scenario emphasises the threat of unauthorised physical access that can be exploited to plant malicious software which can corrupt satellite's operations and on-board system once in orbit. Hence, the scenario points out oversights such as inadequate hardening procedures after assembly, which allow for an IO device (for example a USB drive) to be plugged in and transfer malicious code. Finally, the scenario showcases how software misconfiguration during production leads to vulnerabilities, ultimately enabling threat materialisation during operations.

For this threat to materialise, the attacker first needs to gain unauthorised physical access to the satellite's assembly line or transport container to implant malicious code using an IO interface (e.g. a USB port) to install malicious software modelled to exploit existing vulnerabilities caused by software misconfigurations in the OBC and OBSW. Specifically, as satellite systems process

large quantities of data, the malware prevents sanitisation of data inputs manipulating the OBC and OBSW by injecting random and inconsistent data. The malicious data eventually creates errors in the RTOS system. The repetitive requests caused by the malware would lead to compromise of the logical storage, which would reach its full limit by causing resource exhaustion. This enables the attacker to modify the satellite's parameters opening new opportunities for further tampering with its reset and update procedures. With the ability to modify parameters, the attacker can compromise the TM/TC data at the satellite's COM and attempt to hijack the satellite or engage in eavesdropping. Meanwhile, unable to detect the source of such erratic behaviour of the satellite's bus and find a way to correct it, the mission control centre ultimately loses control of the space segment.

Figure 14: Scenario 2 – Exploiting OBC/OBSW vulnerabilities via malicious code



Table 2: Scenario 2 – Exploiting OBC/OBSW vulnerabilities via malicious code

Exploiting OBC/OBSW vulnerabilities via malicious code	IMPACT (CIA)
	Crucial: the injection of random and inconsistent errors into the satellite's system creates a highly unpredictable operational environment, compromising the satellite's reliability and overall performance. Due to software misconfiguration in the space segment, the ground team is unable to efficiently identify and patch the vulnerability until the point when it is too late for any restart to occur due to resource exhaustion. Combined with communication failures and system malfunctions this would result in significant disruption of the satellite's services, affecting integrity and availability. Ultimately, attackers can exploit other assets such as COM, and impact confidentiality and availability of the satellite.

As this cybersecurity incident looks into the compromise of satellite BUS, impacts on CIA are as follows:

CONFIDENTIALITY

If the TM/TC data at the satellite's COM is compromised, interception of communication is enabled allowing the attacker to engage in eavesdropping, thus violating data confidentiality.

INTEGRITY

The malware's continuous presence and manipulation of the satellite's software results in an unpredictable operational environment and compromised data integrity. As the software transmits corrupted telemetry and executes malicious commands, decision-making at the mission control centre can be incorrect. Due to the resource exhaustion and challenges in resetting the satellite, the mission control centre cannot discern false readings and manipulated data from genuine ones, ultimately jeopardising the trustworthiness of the space segment.

AVAILABILITY

The persistent malware corrupting the data ultimately exhausts the system's resources and memory, rendering the satellite inoperable. As the satellite's performance deteriorates, computational sensing becomes unreliable or ceases altogether. As the scenario escalates, the attacker may compromise other assets such as COM to hijack the satellite or crash it.

THREAT CLUSTER	ASSETS AFFECTED	THREAT ACTORS
• Unauthorised physical access • Sabotage through hardware/software • Malicious code/ software/ activity: Software and vulnerabilities' exploit • Software misconfiguration • Resource exhaustion • Unauthorised modification: Parameters • Seizure of control: Satellite bus • Hijacking	• Assembly/Manufacturing systems/Transport container • Satellite BUS (OBC, OBSW, RTOS, COM)	• State-Sponsored Attackers/ Government Spies • Cyber Terrorists • Disgruntled Employees or Insider Attackers

BROADER IMPACT (PESTLE)

POLITICAL

- Depending on the beneficiaries of the satellite providing internet coverage, political concerns could arise if the attacker was to use it for espionage or communication sabotage.
- Political implications could also arise if the malicious actor gaining unauthorised physical access was found to be working on behalf of another country.

SOCIAL

- In remote or conflict-affected areas where alternative communication infrastructure is limited could hinder emergency response effort as well as access to potentially life-saving information.
- A collapse of internet-providing satellites would create an information vacuum, leading to uncertainty and potential panic.

TECHNOLOGICAL

- Services that rely on the internet, from streaming to cloud computing, would be unavailable.
- Potential disruptions in any autonomous systems relying on internet connection.

ENVIRONMENTAL

- Losing control of the space segment could potentially contribute to the creation of space debris in a situation where a threat actor taking control of a satellite would change its course and cause it to collide with another satellite.

ESCALATION PATH

1. The attacker gains **unauthorised physical access** to the satellite's **assembly line or transport container** and implants **malicious code** via the satellite's USB port.
2. The **malware** exploits computational systems, including **OBC and OBSW**, which are vulnerable to common software faults.
3. Once the satellite is in orbit and begins to process large quantities of data, the **malware triggers malicious injection into OBC & OBSW** injecting random and inconsistent errors into the system.
4. The **malware compromises logical storage**, until the full limit is reached, and then modifies the satellite's parameters enabling further **tampering with its reset and update procedures**.
5. As a result of the above, malware causes the satellite to continue to operate with random errors, causing persistent unreliability, with the source of the errors undetected, malware maintains control and disrupt satellite functionality.
6. Ultimately, the **malware compromises space assets by exploiting existing vulnerabilities**, while the security teams struggle to identify the source of errors, leaving them without clear evidence of malicious software implanted during ground operations.
7. As a result of the **software misconfiguration** and the inability of security teams to patch the vulnerability, the scenario can escalate where the attacker ultimately gains control of the satellite.

5.3. SCENARIO 3: NETWORK INTRUSION DUE TO A LACK OF SECURITY PROTOCOLS AND MISCONFIGURATION

Assumptions on the context:

- Commercial navigation satellite that is part of a low Earth orbit (LEO) satellite constellation providing positioning, navigation, and timing (PNT) signals.
- Subpar incident/natural disaster response plan.
- Ignoring security procedures for adding COTS in production environment (operations) in favour of business continuity.

The scenario covers several ground-related threats that emphasise how improper security planning and ignoring security procedures combined with environmental hazards could be used by attackers to gain access to VSATs to eavesdrop on confidential information, leak or corrupt the data, or even corrupt firmware to launch ransomware attacks. The scenario emphasises how growing risks of environmental hazards, such as fires and floods, coupled with subpar security planning and compliance, can disrupt the secure communication chain between the satellite and the end-users.

A major hailstorm has seriously damaged a terminal ground station of a commercial satellite operator providing navigation services. Namely, the company's VSAT antennas have been badly affected, causing failure of services provided to end users in a specific region. Since the company does not employ a mesh network, it is forced to acquire a new set of VSATs as a means of quickly restoring services. New VSATs are procured through a trusted third-party provider and are immediately put into operational use to cut any financial losses. Thus, with business continuity placed before security, the conduct of necessary hardening of the acquired infrastructure is skipped. However, the company's IT team quickly discovers a vulnerability within the newly acquired network infrastructure, allowing for remote code execution. Specifically, unused ports on the VSATs modem unit are not configured as per the manufacturer's recommendations and are left open for accepting packets. As the new VSAT are already being installed, the management is faced with the decision whether to first shut down the network before it is patched (it needs to be patched in multiple places and properly tested, with further security procedures carried out); patch immediately without proper testing; or keep

business as usual until the patch is ready and deployed. The management realises that another shutdown of operations will cause further disruption and financial losses and opts for the second option - patching without testing. This leaves the ports open and with no testing performed - undetected, and creating a potential entry point for malicious actors.

This vulnerability is picked up by a malicious actor during a random port scanning. The malicious actor exploits this misconfiguration to tap into the network, realising further weaknesses in the form of improper network segmentation, allowing smooth lateral movement across mission critical satellite components. This enables the attacker to intercept communication between the newly deployed VSATs and the end users. Having this access enables the attacker to leak collected data, corrupt it, launch subsequent man-in-the-middle attacks or implant ransomware by corrupting the VSAT firmware. In a worst-case scenario, combined with weak network segmentation, the attacker can even reach and compromise the systems of end users relying on the affected VSATs in case weak network segmentation is also present on the receiving (end user) end.

Figure 15: Scenario 3 – Network intrusion due to a lack of security protocols and misconfiguration



Table 3: Scenario 3 – Network intrusion due to a lack of security protocols and misconfiguration

Network intrusion due to a lack of security	IMPACT (CIA)
	Crucial: as a result of natural disasters, the lack of, or subpar, incident response plan leads to “quick fix” solutions where business continuity is placed ahead of security. With this, introduction of new equipment also highlights the need for complying to the security programme and clear guidelines on controls for securing COTS. A failure to comply to security controls and harden COTS, increases the likelihood of

different ports being left open on VSAT's modem and router. Scanning ports to check which ones are open, is not a complex task and does not require any significant skills, resulting in a myriad of potential attackers (from "script kiddies" to state-sponsored groups). Furthermore, the assumption that the network is not properly segmented, enables the attacker to freely move around systems and target specific protocols - such as communication between the provider of the service and the user in this case. This scenario showcases how ignoring compliance and security procedures in favour of business continuity results with an attacker being able to eavesdrop on the communication, as well as have the ability to leak the client-privileged data, use it to launch man-in-the-middle attacks against the users, or corrupt firmware of the VSAT to potentially engage in ransomware attack.

CONFIDENTIALITY

The attacker's ability to access the network and eavesdrop on the communication between the service provider (VSAT) and the end-users, compromises confidentiality. The attacker can gain access to sensitive information such as intellectual property, credentials, and proprietary data. Leaking this data can be exploited for malicious purposes.

INTEGRITY

With access to the VSATs, attackers can perform man-in-the-middle attacks, given the ability to modify and corrupt data exchanged between the service provider and the users. Access to VSATs enables attackers to deceive users, manipulate certain transactions, and inject malicious content. This can lead to issues such as fraud, misinformation, legal actions against the VSAT provider, and loss of customer base due to eroded trust in the former's systems.

AVAILABILITY

With the ability to corrupt firmware, attackers can move laterally across the network and exploit this to access additional systems and solutions. Such capability is likely to lead to ransomware attacks where attackers encrypt essential data and disrupt the functionality of the systems.

THREAT CLUSTER	ASSETS AFFECTED	THREAT ACTORS
- Environmental Hazard - Software misconfiguration - Malicious code/ software/activity: Network exploit - Unauthorised access - Compromising confidential information (data breaches): Exfiltration - Man-in-the-Middle - Abuse of leaked data - Firmware corruption	- TTC Ground - VSAT - Antenna - User VSAT - User Endpoint Devices	(Organised) Cyber Crime actors - Blackhat Hackers/Crackers - Cyber Vandals/Cyber Punks
BROADER IMPACT (PESTLE)		
ECONOMIC - Economic losses in sectors reliant on precise navigation (e.g. shipping, aviation, ride-sharing). - Financial losses for satellite-based service providers due to service disruptions and loss of customer trust. SOCIAL - Public dismay in societies highly reliant on PNT, especially if key services like navigation, communications, or emergency services are affected.		
ESCALATION PATH		

- 
- A solid red vertical bar is positioned to the left of the list items.
1. An **environmental disaster** damages **VSAT antennas** providing services to a specific region.
 2. The company scatters to quickly replace these, **disregarding security protocols** for hardening the devices, including modems and routers connected to the VSATs.
 3. An attacker **scanning for open ports** identifies this vulnerability and takes advantage of it, gaining **unauthorised access into the network**.
 4. Once within the network, the attacker has the ability to **conduct reconnaissance** and or prepare for subsequent **eavesdropping** or attacking campaigns.
 5. **Weak network segmentation** allows the attacker lateral movements across mission critical components, posing as a threat to end users as well in case the latter's **network is not properly segmented/patched/secured**.
 6. The ability to **eavesdrop** on the communication exchange between the **VSAT and the end-user**, provides the attacker with the opportunity to **leak confidential information**.
 7. The attacker also gains the ability to conduct **man-in-the-middle attacks**, to **corrupt the data** exchanged between the subject company and its clients, or to launch **subsequent ransomware attacks by corrupting firmware**.

6. CYBERSECURITY CONTROL FRAMEWORK

This chapter aims to provide clear and concise recommendations on the implementation and use of appropriate cybersecurity controls, presented in the form of a sample cybersecurity control framework. The listed controls are derived from existing EU regulations¹⁰⁷, international cybersecurity frameworks^{108, 109}, cybersecurity profiles tailored to the space sector^{110, 111, 112, 113}, best practice guides¹¹⁴, taxonomies of countermeasures¹¹⁵, and national guidelines^{116, 117, 118}. They are mapped against specific threats identified in the threat taxonomy and applied across relevant phases of the lifecycle. Aiming for general applicability, the controls can be further tailored depending on the nature and needs of a specific mission.

In total, the control framework contains 125 individual controls, grouped into 18 control clusters. These are:

- **Policies and procedures:** addressing the governance aspects of space missions in the context of cybersecurity. The objective is to ensure that relevant information and cyber security processes are in defined, documented, approved by management, communicated to all relevant parties and, ultimately, implemented. Having clear policies and procedures in place ensures that all stakeholders are aware of the security requirements, as well as their obligations, roles, and responsibilities for implementing and/or adhering to these.
- **Compliance:** addressing the wider business environment of satellite operators in relation to legal and regulatory requirements. These include sector-specific regulations and requirements for critical entities, as well as obligations related to protection of privacy and intellectual property rights, and extra-territorial jurisdiction. An important component of verifying and maintaining compliance are independent reviews of information security (audits) to identify any gaps and relevant mitigation measures.
- **Risk management:** addressing how risks are identified, assessed, and mitigated throughout the lifecycle. Controls in this cluster include threat modelling to identify the

¹⁰⁷ Namely, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive).

¹⁰⁸ International Organisation for Standardisation (ISO), 2022. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

¹⁰⁹ National Institute of Standards and Technology (NIST), 2024. The NIST Cybersecurity Framework (CSF) 2.0. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

¹¹⁰ Scholl, M. and Suloway, T. 2023. Introduction to Cybersecurity for Commercial Satellite Operations. NIST. NIST IR 8270. <https://csrc.nist.gov/pubs/ir/8270/final>

¹¹¹ Bartock, M. et al. 2023. Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services. NIST. NIST IR 8323 Rev. 1. <https://csrc.nist.gov/pubs/ir/8323/r1/final>

¹¹² Lightman, S. Suloway, T. and Brule, J. 2022. Satellite Ground Segment - Applying the Cybersecurity Framework to Satellite Command and Control. NIST. NIST IR 8401. <https://csrc.nist.gov/pubs/ir/8401/final>

¹¹³ McCarthy, J. et al. 2023. Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN). NIST. NIST IR 8441. <https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8441.ipd.pdf>

¹¹⁴ National Aeronautics and Space Administration (NASA), 2024. Space Security: Best Practice Guide (BPG). <https://swehb.nasa.gov/display/SWEHBVD/7.22+-+Space+Security%3A+Best+Practices+Guide>

¹¹⁵ Aerospace Corporation. Space Attack Research & Tactic Analysis (SPARTA). SPARTA Countermeasures. <https://sparta.aerospace.org/countermeasures/SPARTA>

¹¹⁶ Federal Office for Information Security (BSI), 2022. IT-Grundschutz Profile for Space Infrastructures: Minimum Protection for Satellites Covering their Entire Life Cycle. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/profiles/Profile_Space-Infrastructures.pdf?__blob=publicationFile&v=2

¹¹⁷ Federal Office for Information Security (BSI), 2023. Technical Guideline BSI TR-03184 Information Security for Space Systems - Part 1: Space segment

¹¹⁸ Ministry of Economy, Trade and Industry (METI) Cybersecurity Guidelines for Commercial Space Systems



attack surface, criticality analysis to determine critical functions and data flows and prioritise mitigation measures, and Business Impact Analysis (BIA) to assess the potential impact and likelihood of identified threats. The objective is to establish a comprehensive risk management framework, including Third Party (supply chain) risk management practices.

- **Security by Design and by Default:** promoting Secure Development Lifecycle (SDLC) practices and the principles of security by design and by default. Controls in this cluster address aspects of coding standards and configuration management, change management and separation of environments to prevent lateral movement in case of a breach.
- **Environmental and Physical security:** primarily aimed at ensuring physical protection of ground segment infrastructure and satellite components during transport to prevent unauthorised access and tampering.
- **Network security:** primarily aimed at supporting the establishment of resilient communication flows. Controls in this cluster include access-based segmentation of the network, authenticated encryption (with associated data), and disabling physical ports and non-critical backdoor commands, among others. The objective is to establish and maintain the integrity and confidentiality of communication.
- **Data security:** addressing the confidentiality, integrity, and availability of data in all forms (rest, transit, use), throughout the information lifecycle. Controls in this cluster include identification of information assets, classification, and labelling, as well as measures for Data Loss Prevention (DLP) and ensuring a defined process for backup.
- **Vulnerability management:** aimed at ensuring that technical vulnerabilities are identified, validated and recorded and that there are defined processes to address these. Controls in this cluster address aspects such as vulnerability scanning, malware protection, software and protocol updates¹¹⁹, integrity checks¹²⁰ and assurance, and prevention against installation of unauthorised software.
- **Access management (zero trust):** aimed at ensuring data and information system confidentiality and integrity, preventing unauthorised access. Controls in this cluster address aspects of identity management, access rights, authentication and authorisation and session termination, among others. The cluster accounts for both physical and logical access management practices and is built on zero-trust principles, including least privilege and verification of all access requests (internal and external) prior to granting access to the network and other assets.
- **Asset management:** concerned with appropriate management of assets throughout their lifecycle, including systems, hardware, software, services, and data. Controls in this cluster include establishment and maintenance of an up-to-date asset inventory, prioritisation of assets based on their classification, criticality, resources, and impact on

¹¹⁹ Software and protocol updates, especially when distributed across multiple ground stations, require robust integrity checks. The update process and its management are critical, particularly when multiple ground stations are involved, to ensure continuity even while the satellite is in orbit. Update protocols must guarantee the integrity of the software update after the consolidation of all received packets. Update protocol resilience in the presence of untrusted Ground Stations is especially important as missions might rely on open networks (e.g. SatNOGS) that rely on voluntary contributions, raising significant concerns about the level of trust that can be placed in such diverse and potentially unverified ground stations.

¹²⁰ Integrity checks are crucial for maintaining satellite operational integrity. This includes secure boot mechanisms to ensure the correct image is loaded at each startup. Furthermore, vetted backup operational images and a robust recovery process are essential to mitigate the impact of failures (whether due to malicious actions or natural events like geomagnetic storms) and prevent the satellite from becoming inoperable.

the mission, and resulting security requirements such as maintenance, return, and secure disposal or re-use of equipment.

- **Supply Chain management:** aimed at ensuring resilience of the supply chain including outsourced developments, provision of services, as well as procurement and use of COTS. Controls in this cluster include the use of Service Level Agreements (SLAs) to define and monitor Third Party adherence to defined obligations, measures to ensure supply chain security, as well as to ensure that third party software and hardware can be analysed for known vulnerabilities to inform further actions.
- **Monitoring and Alerting:** aimed at ensuring that mission critical components or systems and logs are monitored on a continuous basis to enable timely alerting in case of suspicious or anomalous activity, feeding into response capabilities. Good practice and controls in this domain include network and communications monitoring, intrusion detection and prevention measures and tools, as well as the deployment of Security Information and Event Management (SIEM) solutions.
- **Incident Response:** aimed at establishing baseline capabilities for responding to detected events and incidents to contain and/or mitigate malicious activity. Controls in this cluster include defining incident thresholds to inform required actions, incident response procedures in the form of an Incident Response Plan, as well as considerations of how information on a detected incident is communicated to relevant stakeholders and the public, as required.
- **Business Continuity Management/Disaster Recovery:** aimed at supporting continuity of critical operations in case of disruption, and/or a return to normal operations following an incident. Controls in this cluster include having defined requirements for critical services delivery, as well as sufficient capacity, redundancy and/or backup options to ensure availability.
- **Capacity building:** addressing the human resources segment, controls in this cluster aim to ensure that relevant stakeholders are provided with sufficient knowledge and awareness to perform their tasks while maintaining vigilance in relation to cybersecurity threats and risks. This includes training and awareness raising measures, as well as collecting cyber threat intelligence and information sharing.
- **Testing:** aimed at ensuring that the processes and procedures in place, as well as the software and hardware deployed are regularly tested to ensure that, once implemented, these function as expected. Testing is an important component of the control framework as it enables proactive identification of gaps that needs to be addressed. Controls in this cluster include testing detection processes, simulations of attack scenarios, software and hardware testing and code analysis, among others.
- **Continuous improvement:** applicable to all aspects of the lifecycle, this control cluster promotes employing feedback loops in terms of feeding the results of testing, reviews and audits back into the existing cybersecurity framework to ensure existing processes are proactively improved.
- **Defence capabilities:** primarily aimed at establishing active defence capabilities to respond to attacks. Controls in this cluster include capabilities such as manoeuvrability, use of deception and decoys, and measures to protect filters, shutters, but also antenna nulling and the use of defensive jammers and spoofers.

6.1.CONTROLS TO THREATS MAPPING

The tables below provide a mapping of relevant cybersecurity controls to each of the threats clusters and threats identified in the Threat Taxonomy. A description and more details on each of the controls making up the Control Framework is provided in Annex D.

6.1.1. Controls for addressing threats from nefarious activity/abuse (NAA)

Table 4: Controls for addressing threats from nefarious activity/abuse (NAA)

THREAT	CONTROL TITLE	CONTROL
Abuse of leaked data	Legal, statutory, regulatory, and contractual requirements	Legal, statutory, regulatory, and contractual requirements relevant to information security and the organization's approach to meet these requirements are identified, documented, and kept up to date.
	Independent review of information security	Independent review(s) of information security (auditing) are conducted
	Data Loss Prevention	Data Loss Prevention (DLP) solutions and measures are employed
	OSAM Dual Authorization	Multi-factor authentication is employed for OSAM servicers
Abuse/ falsification of rights	Threat modelling	Threat modelling is employed to identify and reduce the attack surface
	Risk management	Risk management processes and procedures are defined and implemented
	Installation of software on operational systems	Procedures for software installation on operational systems are defined and implemented
	Computing Device Authentication	Computing devices are authenticated before network connections are established
	Access control	Access control policies and procedures are defined and documented
	Identity management	Identities are managed throughout their lifecycle
	Authentication information management	Allocation and management of authentication information governed by a management process, including guidance for personnel on proper handling.
	Access rights	Access control policies and procedure determining access rights to information and associated assets are defined and implemented
	Authentication	Authentication procedures are defined and documented
	Multi factor authentication	The zero-trust concept is applied to access management
	Insider Threat Protection	Insider Threat procedures and guidelines are defined and documented
	Restricted zones access	Informal meeting places within restricted zones are defined
	Password security	A password policy and guidelines are defined and documented
	Asset Inventory	An asset inventory if established and maintained
	Return of assets	A procedure for asset management following termination of cooperation is defined and documented
	Continuous Personnel Monitoring	Personnel activity is monitored to detect anomalous behaviours
	Cybersecurity awareness and training	Cybersecurity is included in human resources practices and personnel are provided with awareness and training
	OSAM Dual Authorization	Multi-factor authentication is employed for OSAM servicers
	Simulation Testing	The resilience of segments is tested using attack simulations across the lifecycle
	Process ID whitelisting	Process ID whitelisting is employed in the satellite
	Communications Security	Secure communication protocols are employed to prevent unauthorized disclosure of, and detect changes to information
Compromising confidential information (data breaches): Exfiltration	Information classification and labelling	Information is classified according to the assessed risk level and confidentiality, integrity, and availability needs (CIA), and labelled accordingly
	Data Management	Data is protected in all states (rest, transit, use)
	Data Loss Prevention	Data Loss Prevention (DLP) solutions and measures are employed
	Backup	There is a defined and implemented process for conducting, maintaining, and testing backup of information
	Information Lifecycle	Information assets are identified and described across their lifecycle, considering all relevant processes
	Data masking	Data masking is employed to obfuscate original, sensitive data
	Real-time physics model-based system verification	Real-time physics model-based system is used to verify data input and control sequence changes
	Protocol Update / Refactoring	Protocols are updated based on emerging threats and vulnerabilities
	Integrity Checking and Assurance	Integrity checking mechanisms are used to verify software, firmware, and information integrity

	Return of assets	A procedure for asset management following termination of cooperation is defined and documented
	Equipment maintenance	Procedures and processes for equipment maintenance are defined and implemented
	Secure disposal or re-use of equipment	Procedures and processes for disposal/re-use of equipment are defined and implemented
	Asset lifecycle management	Guidelines and procedures for the asset management lifecycle are defined and documented
	Network and Communications Monitoring Function	Communications are monitored to identify cybersecurity events and verify the effectiveness of protective measures
	Reinforcement Learning	A reinforcement learning agent is deployed to detect anomalous events
	Security Information and Event Management (SIEM) / Security Operations Center (SOC)	Logs of security-relevant events are integrated into a Security Information and Event Management (SIEM) system
	Network and Communications Monitoring Function	Communications are monitored to identify cybersecurity events and verify the effectiveness of protective measures
Denial of Service (DoS)	System redundancy & backup	Redundancy is introduced for critical infrastructure and data is backed up
	Capacity to ensure availability	The required level of availability and capacity for the ground segment is maintained and established
	Secure Development Lifecycle	Rules for the secure development of software and systems should be established and applied.
Data Modification	Tamper Protection	Physical inspection of hardware is performed to identify potential tampering
	Disable Physical Ports	Physical ports are disabled prior to operations
	Resilient Position, Navigation, and Timing	Authentication mechanisms to verify GNSS information sources are in place
	Communication Physical Medium	Alternate physical mediums for networking are in place to mitigate network security concerns
	Traffic Flow Security	Traffic flow security and confidentiality measures are in place to mitigate traffic analysis attacks
	On-board Message Encryption	Encryption of the message and the space link
	Secret Shares	Secret shares are employed
	Data encryption	Transmitted data (bus-payload link) is encrypted
	Information classification and labelling	Information is classified according to the assessed risk level and confidentiality, integrity, and availability needs (CIA), and labelled accordingly
	Data Management	Data is protected in all states (rest, transit, use)
	Data Loss Prevention	Data Loss Prevention (DLP) solutions and measures are employed
	Backup	There is a defined and implemented process for conducting, maintaining, and testing backup of information
	Information Lifecycle	Information assets are identified and described across their lifecycle, considering all relevant processes
	Real-time physics model-based system verification	Real-time physics model-based system is used to verify data input and control sequence changes
	Process ID whitelisting	Process ID whitelisting is employed in the satellite
	A tamper resistant body	A tamper resistant body is used when producing a sensor node
	Integrity Checking and Assurance	Integrity checking mechanisms are used to verify software, firmware, and information integrity
	Remote access management	Remote access management procedure and processes are defined and documented
	Secure disposal or re-use of equipment	Procedures and processes for disposal/re-use of equipment are defined and implemented
	Asset lifecycle management	Guidelines and procedures for the asset management lifecycle are defined and documented
	Cloud Cybersecurity Measures	SLAs are in place external services and cloud providers
	Network and Communications Monitoring Function	Communications are monitored to identify cybersecurity events and verify the effectiveness of protective measures
	Event detection communication	Event detection is communicated to stakeholders
	Anomaly detection	Event data is correlated from multiple sources and communicated; Inappropriate or malicious activity within the mission's systems is detected
	Mission Cyber Actor Actions Detection	An on-board cyber actor actions detection function is in place
	Reinforcement Learning	A reinforcement learning agent is deployed to detect anomalous events

	Incident Thresholds	Incident thresholds are defined and documented based on an understanding of potential impact
	Cabling security	A secure cabling protocol is defined
	Information sharing	Information is actively shared to achieve broader cybersecurity situational awareness
	Machine Learning Data Integrity	Data integrity testing is performed on AI/ML training datasets
	Detection Processes	Detection processes are continuously improved
	Filtering and Shuttering	Filters and shutters are employed to protect sensors from laser dazzling and blinding
	Anti-counterfeit Hardware	Anti-counterfeit policy and procedures are defined and implemented
	Deception and Decoys	Deception and decoys are employed for defensive capabilities
Electro magnetic interference	Coding Standard	Secure coding principles for software development are defined and implemented to ensure proper security constructs are in place
Firmware corruption	Cybersecurity-Safe Mode	Secure vehicle fault management functions and safe mode operations are implemented to enable a cyber-safe mode when threats are detected
	Installation of software on operational systems	Procedures for software installation on operational systems are defined and implemented
	Vulnerability scanning	Vulnerability scanning is used to identify vulnerabilities
	Software Updates	Regular software updates are performed to mitigate exploitation risk
	Integrity Checking and Assurance	Integrity checking mechanisms are used to verify software, firmware and information integrity
	Dynamic Code Analysis	Dynamic Code Analysis is performed to identify software/firmware weaknesses and vulnerabilities
Identity Theft	Secure Workload-to-Workload Authenticator	Procedures for secure authentication integration protocol are defined and documented
	Threat modelling	Threat modelling is employed to identify and reduce the attack surface
	Risk management	Risk management processes and procedures are defined and implemented
	Installation of software on operational systems	Procedures for software installation on operational systems are defined and implemented
	Computing Device Authentication	Computing devices are authenticated before network connections are established
	Access control	Access control policies and procedures are defined and documented
	Identity management	Identities are managed throughout their lifecycle
	Authentication information management	Allocation and management of authentication information governed by a management process, including guidance for personnel on proper handling.
	Access rights	Access control policies and procedure determining access rights to information and associated assets are defined and implemented
	Authentication	Authentication procedures are defined and documented
	Multi factor authentication	The zero-trust concept is applied to access management
	Insider Threat Protection	Insider Threat procedures and guidelines are defined and documented
	Restricted zones access	Informal meeting places within restricted zones are defined
	Password security	A password policy and guidelines are defined and documented
	Asset Inventory	An asset inventory if established and maintained
	Return of assets	A procedure for asset management following termination of cooperation is defined and documented
	Equipment maintenance	Procedures and processes for equipment maintenance are defined and implemented
	Continuous Personnel Monitoring	Personnel activity is monitored to detect anomalous behaviours
	Cybersecurity awareness and training	Cybersecurity is included in human resources practices and personnel are provided with awareness and training
	OSAM Dual Authorization	Multi-factor authentication is employed for OSAM servicers
	Simulation Testing	The resilience of segments is tested using attack simulations across the lifecycle
	Transmission security	Transmission security solutions and measures are employed to protect communication transmission

Jamming	Cryptography & Crypto Key Management	Rules for the use of cryptography are defined and implemented; On-board messages are encrypted
	Critical Telemetry Points Monitoring	Critical telemetry points are monitored for malicious activities
	Space-Based Radio Frequency Mapping	Space-based RF mapping is in place to monitor and analyse the RF environment
	Defensive Jamming and Spoofing	Jammers and spoofers are employed for defensive operations
	Antenna Nulling and Adaptive Filtering	Antenna nulling and adaptive filtering are employed for defensive operations
	Adaptive Risk Response and Resource Allocation Function	Continuous process of qualitative and quantitative mission security risk analysis and risk response is conducted for the duration of the mission
Malicious code/ software/activity: Cryptographic exploit	Risk management	Risk management processes and procedures are defined and implemented
	Cybersecurity-Safe Mode	Secure vehicle fault management functions and safe mode operations are implemented to enable a cyber-safe mode when threats are detected
	Transport Security	Transport from the integration hall to the test stations, between different facilities, and to the start facility is secured
	Communications Security	Secure communication protocols are employed to prevent unauthorized disclosure of, and detect changes to information
	Cryptography & Crypto Key Management	Rules for the use of cryptography are defined and implemented; On-board messages are encrypted
	On-board Message Encryption	Encryption of the message and the space link
	Power Masking	Power masking is used to protect secret keys
	Satellite Unit RF Encryption	Encryption of RF link
	Data encryption	Transmitted data (bus-payload link) is encrypted
	Data Loss Prevention	Data Loss Prevention (DLP) solutions and measures are employed
	Vulnerability Management	Vulnerability management processes and procedures are defined and implemented
	Threat modelling	Threat modelling is employed to identify and reduce the attack surface
	Criticality Analysis	Criticality analysis is performed to identify critical functions, components, and data flows
	Cybersecurity-Safe Mode	Secure vehicle fault management functions and safe mode operations are implemented to enable a cyber-safe mode when threats are detected
Malicious code/ software/activity: Malicious injection	Backdoor Commands	Non-critical backdoor commands are disabled
	Resilient Position, Navigation, and Timing	Authentication mechanisms to verify GNSS information sources are in place
	Access-based network segmentation	The network is segmented into subnetworks to prevent unauthorised access
	Data encryption	Transmitted data (bus-payload link) is encrypted
	Malware Protection	Mission operated systems employ malicious code protection mechanisms to detect and eradicate malicious code
	Installation of software on operational systems	Procedures for software installation on operational systems are defined and implemented
	Software Updates	Regular software updates are performed to mitigate exploitation risk
	Protocol Update / Refactoring	Protocols are updated based on emerging threats and vulnerabilities
	Network and Communications Monitoring Function	Communications are monitored to identify cybersecurity events and verify the effectiveness of protective measures
	Event detection communication	Event detection is communicated to stakeholders
	Mission Cyber Actor Actions Detection	An on-board cyber actor actions detection function is in place
	Reinforcement Learning	A reinforcement learning agent is deployed to detect anomalous events
	Incident Response Plan	Procedures and processes for Incident Response are defined and documented
	Incident Thresholds	Incident thresholds are defined and documented based on an understanding of potential impact
	Incident Recovery Plan	Procedures and processes for Incident Recovery are defined and documented
	Critical Services Delivery Requirements	Resilience requirements to support delivery of critical services are established for all operating states
	Static Code Analysis	Static Code Analysis is performed to identify system-relevant weaknesses
	Deception and Decoys	Deception and decoys are employed for defensive capabilities
	Antenna Nulling and Adaptive Filtering	Antenna nulling and adaptive filtering are employed for defensive operations

Malicious code/ software/activity: Network exploit

Secure Workload-to-Workload Authenticator	Procedures for secure authentication integration protocol are defined and documented
Threat modelling	Threat modelling is employed to identify and reduce the attack surface
Criticality Analysis	Criticality analysis is performed to identify critical functions, components, and data flows
Adaptive Risk Response and Resource Allocation Function	Continuous process of qualitative and quantitative mission security risk analysis and risk response is conducted for the duration of the mission
Risk management	Risk management processes and procedures are defined and implemented
Configuration Management	Configurations, including security configurations, are defined, documented, implemented, monitored, and reviewed.
Cybersecurity-Safe Mode	Secure vehicle fault management functions and safe mode operations are implemented to enable a cyber-safe mode when threats are detected
Change Management	Change management procedures are defined and documented
Tamper Protection	Physical inspection of hardware is performed to identify potential tampering
Communications Security	Secure communication protocols are employed to prevent unauthorized disclosure of, and detect changes to information
Transmission security	Transmission security solutions and measures are employed to protect communication transmission
Disable Physical Ports	Physical ports are disabled prior to operations
Backdoor Commands	Non-critical backdoor commands are disabled
Resilient Position, Navigation, and Timing	Authentication mechanisms to verify GNSS information sources are in place
Smart Contracts	Smart contracts are used to enforce security protocols
Communication Physical Medium	Alternate physical mediums for networking are in place to mitigate network security concerns
Traffic Flow Security	Traffic flow security and confidentiality measures are in place to mitigate traffic analysis attacks
Access-based network segmentation	The network is segmented into subnetworks to prevent unauthorised access
Cryptography & Crypto Key Management	Rules for the use of cryptography are defined and implemented; On-board messages are encrypted
On-board Message Encryption	Encryption of the message and the space link
Secret Shares	Secret shares are employed
Satellite Unit RF Encryption	Encryption of RF link
Data encryption	Transmitted data (bus-payload link) is encrypted
Malware Protection	Mission operated systems employ malicious code protection mechanisms to detect and eradicate malicious code
Vulnerability scanning	Vulnerability scanning is used to identify vulnerabilities
Computing Device Authentication	Computing devices are authenticated before network connections are established
Remote access management	Remote access management procedure and processes are defined and documented
Intrusion Detection and Prevention	On-board Intrusion detection/prevention systems (IDP/IPS) are employed to detect and respond to threats and attacks
Anomaly detection	Event data is correlated from multiple sources and communicated; Inappropriate or malicious activity within the mission's systems is detected
Incident Response Plan	Procedures and processes for Incident Response are defined and documented
Incident Thresholds	Incident thresholds are defined and documented based on an understanding of potential impact
Incident Recovery Plan	Procedures and processes for Incident Recovery are defined and documented
Cabling security	A secure cabling protocol is defined
Critical Services Delivery Requirements	Resilience requirements to support delivery of critical services are established for all operating states
Capacity to ensure availability	The required level of availability and capacity for the ground segment is maintained and established
Detection Processes	Detection processes are continuously improved
Deception and Decoys	Deception and decoys are employed for defensive capabilities
Assessment & Authorization concept	Assessment & Authorization (A&A) procedures and processes are defined and documented

Malicious code/ software/activity: Software and vulnerabilities exploit	Threat modelling	Threat modelling is employed to identify and reduce the attack surface
	Criticality Analysis	Criticality analysis is performed to identify critical functions, components, and data flows
	Coding Standard	Secure coding principles for software development are defined and implemented to ensure proper security constructs are in place
	Secure Development Lifecycle	Rules for the secure development of software and systems should be established and applied.
	Cybersecurity-Safe Mode	Secure vehicle fault management functions and safe mode operations are implemented to enable a cyber-safe mode when threats are detected
	Separation of Environments	The development, testing and production environments are separated and secured
	Change Management	Change management procedures are defined and documented
	Access-based network segmentation	The network is segmented into subnetworks to prevent unauthorised access
	Data encryption	Transmitted data (bus-payload link) is encrypted
	Malware Protection	Mission operated systems employ malicious code protection mechanisms to detect and eradicate malicious code
	Vulnerability Management	Vulnerability management processes and procedures are defined and implemented
	Installation of software on operational systems	Procedures for software installation on operational systems are defined and implemented
	Vulnerability scanning	Vulnerability scanning is used to identify vulnerabilities
	Security Testing Results	Results of penetration testing, and vulnerability scanning are used to build report and vulnerability repositories
	Software Updates	Regular software updates are performed to mitigate exploitation risk
	Protocol Update / Refactoring	Protocols are updated based on emerging threats and vulnerabilities
	Software Source Control	The use of binary or machine-executable code is controlled
	ASIC/FPGA Manufacturing	Trusted hardware development is ensured
	Integrity Checking and Assurance	Integrity checking mechanisms are used to verify software, firmware, and information integrity
	Access rights	Access control policies and procedure determining access rights to information and associated assets are defined and implemented
	Software Version Numbers	Version numbers of COTS or Open-Source are protected
	Software Bill of Materials	The Software Bill of Materials (SBOM) is generated to identify known vulnerabilities
	Outsourced development	Activities related to outsourced system development are monitor and reviewed
	Incident Response Plan	Procedures and processes for Incident Response are defined and documented
	Incident Thresholds	Incident thresholds are defined and documented based on an understanding of potential impact
	Incident Recovery Plan	Procedures and processes for Incident Recovery are defined and documented
	Critical Services Delivery Requirements	Resilience requirements to support delivery of critical services are established for all operating states
	Cyber threat intelligence	Cyber threat intelligence is collected and analysed
	Dynamic Code Analysis	Dynamic Code Analysis is performed to identify software/firmware weaknesses and vulnerabilities
	Static Code Analysis	Static Code Analysis is performed to identify system-relevant weaknesses
	Detection Processes	Detection processes are continuously improved
	Deception and Decoys	Deception and decoys are employed for defensive capabilities
	Long Duration Testing	Long Duration Testing is performed to identify race conditions and time-based attacks
	Coding Standard	Secure coding principles for software development are defined and implemented to ensure proper security constructs are in place
Manipulation of hardware and software: Zero-Day exploit	Secure Development Lifecycle	Rules for the secure development of software and systems should be established and applied.
	Installation of software on operational systems	Procedures for software installation on operational systems are defined and implemented
	Security Information and Event Management (SIEM) / Security Operations Center (SOC)	Logs of security-relevant events are integrated into a Security Information and Event Management (SIEM) system
	Dynamic Code Analysis	Dynamic Code Analysis is performed to identify software/firmware weaknesses and vulnerabilities
	Static Code Analysis	Static Code Analysis is performed to identify system-relevant weaknesses

Preventing services	Criticality Analysis	Criticality analysis is performed to identify critical functions, components and data flows
	Secure Development Lifecycle	Rules for the secure development of software and systems should be established and applied.
	Cybersecurity-Safe Mode	Secure vehicle fault management functions and safe mode operations are implemented to enable a cyber-safe mode when threats are detected
	Separation of Environments	The development, testing and production environments are separated and secured
	Cryptography & Crypto Key Management	Rules for the use of cryptography are defined and implemented; On-board messages are encrypted
	Power Masking	Power masking is used to protect secret keys
	Data Loss Prevention	Data Loss Prevention (DLP) solutions and measures are employed
	Remote access management	Remote access management procedure and processes are defined and documented
	Software Supply Chain Integrity	Technical measures are in place to ensure integrity of the supply chain
	Incident Response Plan	Procedures and processes for Incident Response are defined and documented
	Incident Recovery Plan	Procedures and processes for Incident Recovery are defined and documented
	Critical Services Delivery Requirements	Resilience requirements to support delivery of critical services are established for all operating states
	Criticality Analysis	Criticality analysis is performed to identify critical functions, components, and data flows
Resource exhaustion	Access-based network segmentation	The network is segmented into subnetworks to prevent unauthorised access
	On-board Message Encryption	Encryption of the message and the space link
	Access control	Access control policies and procedures are defined and documented
	Relay Protection	Relay and replay-resistant authentication mechanisms and employed
	System redundancy & backup	Redundancy is introduced for critical infrastructure and data is backed up
	Software and Hardware Testing Function	End to end testing is performed according to documented procedures
	Dynamic Code Analysis	Dynamic Code Analysis is performed to identify software/firmware weaknesses and vulnerabilities
	Deception and Decoys	Deception and decoys are employed for defensive capabilities
Seizure of control	Configuration Management	Configurations, including security configurations, are defined, documented, implemented, monitored, and reviewed.
	Secure Development Lifecycle	Rules for the secure development of software and systems should be established and applied.
	Cybersecurity-Safe Mode	Secure vehicle fault management functions and safe mode operations are implemented to enable a cyber-safe mode when threats are detected
	Secure Command Mode(s)	Spacecraft protection is enhanced by additional protection modes
	Change Management	Change management procedures are defined and documented
	Transport Security	Transport from the integration hall to the test stations, between different facilities, and to the start facility is secured
	Tamper Protection	Physical inspection of hardware is performed to identify potential tampering
	Access-based network segmentation	The network is segmented into subnetworks to prevent unauthorised access
	Data Loss Prevention	Data Loss Prevention (DLP) solutions and measures are employed
	Real-time physics model-based system verification	Real-time physics model-based system is used to verify data input and control sequence changes
	Protocol Update / Refactoring	Protocols are updated based on emerging threats and vulnerabilities
	Access control	Access control policies and procedures are defined and documented
	Authentication information management	Allocation and management of authentication information governed by a management process, including guidance for personnel on proper handling.
	Access rights	Access control policies and procedure determining access rights to information and associated assets are defined and implemented
	Remote access management	Remote access management procedure and processes are defined and documented
	Multi factor authentication	The zero-trust concept is applied to access management
	Asset lifecycle management	Guidelines and procedures for the asset management lifecycle are defined and documented
	Intrusion Detection and Prevention	On-board Intrusion detection/prevention systems (IDP/IPS) are employed to detect and respond to threats and attacks

	Physical Seizure	Space traffic control and debris mitigation protocols are established
Social Engineering	Secure Workload-to-Workload Authenticator	Procedures for secure authentication integration protocol are defined and documented
	Threat modelling	Threat modelling is employed to identify and reduce the attack surface
	Risk management	Risk management processes and procedures are defined and implemented
	Installation of software on operational systems	Procedures for software installation on operational systems are defined and implemented
	Access control	Access control policies and procedures are defined and documented
	Identity management	Identities are managed throughout their lifecycle
	Authentication information management	Allocation and management of authentication information governed by a management process, including guidance for personnel on proper handling.
	Access rights	Access control policies and procedure determining access rights to information and associated assets are defined and implemented
	Authentication	Authentication procedures are defined and documented
	Multi factor authentication	The zero-trust concept is applied to access management
	Insider Threat Protection	Insider Threat procedures and guidelines are defined and documented
	Restricted zones access	Informal meeting places within restricted zones are defined
	Password security	A password policy and guidelines are defined and documented
	Asset Inventory	An asset inventory if established and maintained
	Return of assets	A procedure for asset management following termination of cooperation is defined and documented
	Equipment maintenance	Procedures and processes for equipment maintenance are defined and implemented
	Continuous Personnel Monitoring	Personnel activity is monitored to detect anomalous behaviours
	Cybersecurity awareness and training	Cybersecurity is included in human resources practices and personnel are provided with awareness and training
	Simulation Testing	The resilience of segments is tested using attack simulations across the lifecycle
	Transmission security	Transmission security solutions and measures are employed to protect communication transmission
Spoofing	Cryptography & Crypto Key Management	Rules for the use of cryptography are defined and implemented; On-board messages are encrypted
	Network and Communications Monitoring Function	Communications are monitored to identify cybersecurity events and verify the effectiveness of protective measures
	Critical Telemetry Points Monitoring	Critical telemetry points are monitored for malicious activities
	Space-Based Radio Frequency Mapping	Space-based RF mapping is in place to monitor and analyse the RF environment
	Defensive Jamming and Spoofing	Jammers and spoofers are employed for defensive operations
	Antenna Nulling and Adaptive Filtering	Antenna nulling and adaptive filtering are employed for defensive operations
	Third Party risk management	Cyber supply chain risk management processes are defined and implemented
Supply Chain Compromise	Backdoor Commands	Non-critical backdoor commands are disabled
	ASIC/FPGA Manufacturing	Trusted hardware development is ensured
	Supplier Security Management	Supplier or Third-Party compliance with relevant security standards is reviewed
	Software Version Numbers	Version numbers of COTS or Open-Source are protected
	Software Bill of Materials	The Software Bill of Materials (SBOM) is generated to identify known vulnerabilities
	Software Supply Chain Integrity	Technical measures are in place to ensure integrity of the supply chain
	Cloud Cybersecurity Measures	SLAs are in place external services and cloud providers
	Outsourced development	Activities related to outsourced system development are monitor and reviewed
	Information sharing	Information is actively shared to achieve broader cybersecurity situational awareness

Theft of authentication information	Secure Workload-to-Workload Authenticator	Procedures for secure authentication integration protocol are defined and documented
	Threat modelling	Threat modelling is employed to identify and reduce the attack surface
	Adaptive Risk Response and Resource Allocation Function	Continuous process of qualitative and quantitative mission security risk analysis and risk response is conducted for the duration of the mission
	Risk management	Risk management processes and procedures are defined and implemented
	Transport Security	Transport from the integration hall to the test stations, between different facilities, and to the start facility is secured
	Communications Security	Secure communication protocols are employed to prevent unauthorized disclosure of, and detect changes to information
	Smart Contracts	Smart contracts are used to enforce security protocols
	Secret Shares	Secret shares are employed
	Power Masking	Power masking is used to protect secret keys
	Installation of software on operational systems	Procedures for software installation on operational systems are defined and implemented
	Computing Device Authentication	Computing devices are authenticated before network connections are established
	Access control	Access control policies and procedures are defined and documented
	Identity management	Identities are managed throughout their lifecycle
	Authentication information management	Allocation and management of authentication information governed by a management process, including guidance for personnel on proper handling.
	Access rights	Access control policies and procedure determining access rights to information and associated assets are defined and implemented
	Authentication	Authentication procedures are defined and documented
	Multi factor authentication	The zero-trust concept is applied to access management
	Insider Threat Protection	Insider Threat procedures and guidelines are defined and documented
	Restricted zones access	Informal meeting places within restricted zones are defined
	Password security	A password policy and guidelines are defined and documented
	Asset Inventory	An asset inventory is established and maintained
	Return of assets	A procedure for asset management following termination of cooperation is defined and documented
	Equipment maintenance	Procedures and processes for equipment maintenance are defined and implemented
	Network and Communications Monitoring Function	Communications are monitored to identify cybersecurity events and verify the effectiveness of protective measures
	Intrusion Detection and Prevention	On-board Intrusion detection/prevention systems (IDP/IPS) are employed to detect and respond to threats and attacks
	Continuous Personnel Monitoring	Personnel activity is monitored to detect anomalous behaviours
	Cybersecurity awareness and training	Cybersecurity is included in human resources practices and personnel are provided with awareness and training
	OSAM Dual Authorization	Multi-factor authentication is employed for OSAM servicers
	Simulation Testing	The resilience of segments is tested using attack simulations across the lifecycle
Unauthorised modification: Parameters	Adaptive Risk Response and Resource Allocation Function	Continuous process of qualitative and quantitative mission security risk analysis and risk response is conducted for the duration of the mission
	Risk management	Risk management processes and procedures are defined and implemented
	Separation of Environments	The development, testing and production environments are separated and secured
	Communications Security	Secure communication protocols are employed to prevent unauthorized disclosure of, and detect changes to information
	Malware Protection	Mission operated systems employ malicious code protection mechanisms to detect and eradicate malicious code
	Integrity Checking and Assurance	Integrity checking mechanisms are used to verify software, firmware and information integrity
	Software Supply Chain Integrity	Technical measures are in place to ensure integrity of the supply chain
	Cloud Cybersecurity Measures	SLAs are in place external services and cloud providers
	Event detection communication	Event detection is communicated to stakeholders
	Anomaly detection	Event data is correlated from multiple sources and communicated; Inappropriate or malicious activity within the mission's systems is detected
	Mission Cyber Actor Actions Detection	An on-board cyber actor actions detection function is in place
	Critical Telemetry Points Monitoring	Critical telemetry points are monitored for malicious activities

	Reinforcement Learning	A reinforcement learning agent is deployed to detect anomalous events
	Space-Based Radio Frequency Mapping	Space-based RF mapping is in place to monitor and analyse the RF environment
	Continuous Personnel Monitoring	Personnel activity is monitored to detect anomalous behaviours
	Dependency Confusion	Protections are in place for mitigating dependency confusion
	Software Mission Assurance	Assurance activities are performed according to documented procedures
	Software and Hardware Testing Function	End to end testing is performed according to documented procedures
	Dynamic Code Analysis	Dynamic Code Analysis is performed to identify software/firmware weaknesses and vulnerabilities
	Static Code Analysis	Static Code Analysis is performed to identify system-relevant weaknesses
	Machine Learning Data Integrity	Data integrity testing is performed on AI/ML training datasets
	OSAM Dual Authorization	Multi-factor authentication is employed for OSAM servicers
	Simulation Testing	The resilience of segments is tested using attack simulations across the lifecycle
	Detection processes are tested	Event detection processes are tested to ensure they are operating as intended
Unauthorised use of equipment	Detection Processes	Detection processes are continuously improved
	Secure Workload-to-Workload Authenticator	Procedures for secure authentication integration protocol are defined and documented
	Threat modelling	Threat modelling is employed to identify and reduce the attack surface
	Risk management	Risk management processes and procedures are defined and implemented
	Transport Security	Transport from the integration hall to the test stations, between different facilities, and to the start facility is secured
	Installation of software on operational systems	Procedures for software installation on operational systems are defined and implemented
	Computing Device Authentication	Computing devices are authenticated before network connections are established
	Access control	Access control policies and procedures are defined and documented
	Identity management	Identities are managed throughout their lifecycle
	Authentication information management	Allocation and management of authentication information governed by a management process, including guidance for personnel on proper handling.
	Access rights	Access control policies and procedure determining access rights to information and associated assets are defined and implemented
	Authentication	Authentication procedures are defined and documented
	Multi factor authentication	The zero-trust concept is applied to access management
	Insider Threat Protection	Insider Threat procedures and guidelines are defined and documented
	Restricted zones access	Informal meeting places within restricted zones are defined
	Password security	A password policy and guidelines are defined and documented
	Asset Inventory	An asset inventory is established and maintained
	Return of assets	A procedure for asset management following termination of cooperation is defined and documented
	Equipment maintenance	Procedures and processes for equipment maintenance are defined and implemented
	Secure disposal or re-use of equipment	Procedures and processes for disposal/re-use of equipment are defined and implemented
	Continuous Personnel Monitoring	Personnel activity is monitored to detect anomalous behaviours
	Cybersecurity awareness and training	Cybersecurity is included in human resources practices and personnel are provided with awareness and training
	Simulation Testing	The resilience of segments is tested using attack simulations across the lifecycle

6.1.2. Controls for addressing threats from eavesdropping / interception / hijacking (EIH)

Table 5: Controls for addressing threats from eavesdropping/interception/hijacking (EIH)

THREAT	CONTROL TITLE	CONTROL
Hijacking	Transmission security	Transmission security solutions and measures are employed to protect communication transmission
	Resilient Position, Navigation, and Timing	Authentication mechanisms to verify GNSS information sources are in place
	Communication Physical Medium	Alternate physical mediums for networking are in place to mitigate network security concerns
	Traffic Flow Security	Traffic flow security and confidentiality measures are in place to mitigate traffic analysis attacks
	Access-based network segmentation	The network is segmented into subnetworks to prevent unauthorised access
	Cryptography & Crypto Key Management	Rules for the use of cryptography are defined and implemented; On-board messages are encrypted
	On-board Message Encryption	Encryption of the message and the space link
	Satellite Unit RF Encryption	Encryption of RF link
	Installation of software on operational systems	Procedures for software installation on operational systems are defined and implemented
	Computing Device Authentication	Computing devices are authenticated before network connections are established
	Network and Communications Monitoring Function	Communications are monitored to identify cybersecurity events and verify the effectiveness of protective measures
	Software and Hardware Testing Function	End to end testing is performed according to documented procedures
	Antenna Nulling and Adaptive Filtering	Antenna nulling and adaptive filtering are employed for defensive operations
Interception of communication	Adaptive Risk Response and Resource Allocation Function	Continuous process of qualitative and quantitative mission security risk analysis and risk response is conducted for the duration of the mission
	Risk management	Risk management processes and procedures are defined and implemented
	Communications Security	Secure communication protocols are employed to prevent unauthorized disclosure of, and detect changes to information
	Transmission security	Transmission security solutions and measures are employed to protect communication transmission
	Resilient Position, Navigation, and Timing	Authentication mechanisms to verify GNSS information sources are in place
	Communication Physical Medium	Alternate physical mediums for networking are in place to mitigate network security concerns
	Access-based network segmentation	The network is segmented into subnetworks to prevent unauthorised access
	Cryptography & Crypto Key Management	Rules for the use of cryptography are defined and implemented; On-board messages are encrypted
	On-board Message Encryption	Encryption of the message and the space link
	Satellite Unit RF Encryption	Encryption of RF link
	Data encryption	Transmitted data (bus-payload link) is encrypted
	Protocol Update / Refactoring	Protocols are updated based on emerging threats and vulnerabilities
	Session Termination	Procedures for session termination are established
	Network and Communications Monitoring Function	Communications are monitored to identify cybersecurity events and verify the effectiveness of protective measures

Man-in-the-Middle	Adaptive Risk Response and Resource Allocation Function	Continuous process of qualitative and quantitative mission security risk analysis and risk response is conducted for the duration of the mission
	Risk management	Risk management processes and procedures are defined and implemented
	Communications Security	Secure communication protocols are employed to prevent unauthorized disclosure of, and detect changes to information
	Transmission security	Transmission security solutions and measures are employed to protect communication transmission
	Resilient Position, Navigation, and Timing	Authentication mechanisms to verify GNSS information sources are in place
	Communication Physical Medium	Alternate physical mediums for networking are in place to mitigate network security concerns
	Cryptography & Crypto Key Management	Rules for the use of cryptography are defined and implemented; On-board messages are encrypted
	On-board Message Encryption	Encryption of the message and the space link
	Satellite Unit RF Encryption	Encryption of RF link
	Data encryption	Transmitted data (bus-payload link) is encrypted
	Session Termination	Procedures for session termination are established
	Network and Communications Monitoring Function	Communications are monitored to identify cybersecurity events and verify the effectiveness of protective measures
	Critical Telemetry Points Monitoring	Critical telemetry points are monitored for malicious activities
Network manipulation (Bus-Payload Link)	Adaptive Risk Response and Resource Allocation Function	Continuous process of qualitative and quantitative mission security risk analysis and risk response is conducted for the duration of the mission
	Risk management	Risk management processes and procedures are defined and implemented
	Communications Security	Secure communication protocols are employed to prevent unauthorized disclosure of, and detect changes to information
	Access-based network segmentation	The network is segmented into subnetworks to prevent unauthorised access
	Cryptography & Crypto Key Management	Rules for the use of cryptography are defined and implemented; On-board messages are encrypted
	On-board Message Encryption	Encryption of the message and the space link
	Satellite Unit RF Encryption	Encryption of RF link
	Data encryption	Transmitted data (bus-payload link) is encrypted
Network traffic manipulation (TC)	Network and Communications Monitoring Function	Communications are monitored to identify cybersecurity events and verify the effectiveness of protective measures
	Adaptive Risk Response and Resource Allocation Function	Continuous process of qualitative and quantitative mission security risk analysis and risk response is conducted for the duration of the mission
	Risk management	Risk management processes and procedures are defined and implemented
	Communications Security	Secure communication protocols are employed to prevent unauthorized disclosure of, and detect changes to information
	Transmission security	Transmission security solutions and measures are employed to protect communication transmission
	Resilient Position, Navigation, and Timing	Authentication mechanisms to verify GNSS information sources are in place
	Smart Contracts	Smart contracts are used to enforce security protocols
	Communication Physical Medium	Alternate physical mediums for networking are in place to mitigate network security concerns
	Access-based network segmentation	The network is segmented into subnetworks to prevent unauthorised access
	Cryptography & Crypto Key Management	Rules for the use of cryptography are defined and implemented; On-board messages are encrypted
	On-board Message Encryption	Encryption of the message and the space link
	Satellite Unit RF Encryption	Encryption of RF link
	Protocol Update / Refactoring	Protocols are updated based on emerging threats and vulnerabilities
	Integrity Checking and Assurance	Integrity checking mechanisms are used to verify software, firmware and information integrity
	Network and Communications Monitoring Function	Communications are monitored to identify cybersecurity events and verify the effectiveness of protective measures
	Critical Telemetry Points Monitoring	Critical telemetry points are monitored for malicious activities
	Detection Processes	Detection processes are continuously improved

Position detection (telemetry)	Adaptive Risk Response and Resource Allocation Function	Continuous process of qualitative and quantitative mission security risk analysis and risk response is conducted for the duration of the mission
	Risk management	Risk management processes and procedures are defined and implemented
	Communications Security	Secure communication protocols are employed to prevent unauthorized disclosure of, and detect changes to information
	Transmission security	Transmission security solutions and measures are employed to protect communication transmission
	Resilient Position, Navigation, and Timing	Authentication mechanisms to verify GNSS information sources are in place
	Access-based network segmentation	The network is segmented into subnetworks to prevent unauthorised access
	Cryptography & Crypto Key Management	Rules for the use of cryptography are defined and implemented; On-board messages are encrypted
	On-board Message Encryption	Encryption of the message and the space link
	Satellite Unit RF Encryption	Encryption of RF link
	Data encryption	Transmitted data (bus-payload link) is encrypted
	Protocol Update / Refactoring	Protocols are updated based on emerging threats and vulnerabilities
	Network and Communications Monitoring Function	Communications are monitored to identify cybersecurity events and verify the effectiveness of protective measures
	Mission Cyber Actor Actions Detection	An on-board cyber actor actions detection function is in place
	Critical Telemetry Points Monitoring	Critical telemetry points are monitored for malicious activities
Replay of recorded authentic communication traffic	Adaptive Risk Response and Resource Allocation Function	Continuous process of qualitative and quantitative mission security risk analysis and risk response is conducted for the duration of the mission
	Risk management	Risk management processes and procedures are defined and implemented
	Communications Security	Secure communication protocols are employed to prevent unauthorized disclosure of, and detect changes to information
	Transmission security	Transmission security solutions and measures are employed to protect communication transmission
	Resilient Position, Navigation, and Timing	Authentication mechanisms to verify GNSS information sources are in place
	Smart Contracts	Smart contracts are used to enforce security protocols
	Cryptography & Crypto Key Management	Rules for the use of cryptography are defined and implemented; On-board messages are encrypted
	On-board Message Encryption	Encryption of the message and the space link
	Satellite Unit RF Encryption	Encryption of RF link
	Data encryption	Transmitted data (bus-payload link) is encrypted
	Relay Protection	Relay and replay-resistant authentication mechanisms and employed
	Network and Communications Monitoring Function	Communications are monitored to identify cybersecurity events and verify the effectiveness of protective measures
	Critical Telemetry Points Monitoring	Critical telemetry points are monitored for malicious activities
Unauthorised access	Intellectual property rights	Procedures and processes for protecting intellectual property are defined and documented
	Adaptive Risk Response and Resource Allocation Function	Continuous process of qualitative and quantitative mission security risk analysis and risk response is conducted for the duration of the mission
	Risk management	Risk management processes and procedures are defined and implemented
	Communications Security	Secure communication protocols are employed to prevent unauthorized disclosure of, and detect changes to information
	Transmission security	Transmission security solutions and measures are employed to protect communication transmission
	Backdoor Commands	Non-critical backdoor commands are disabled
	Smart Contracts	Smart contracts are used to enforce security protocols
	Traffic Flow Security	Traffic flow security and confidentiality measures are in place to mitigate traffic analysis attacks
	Access-based network segmentation	The network is segmented into subnetworks to prevent unauthorised access
	Cryptography & Crypto Key Management	Rules for the use of cryptography are defined and implemented; On-board messages are encrypted
	On-board Message Encryption	Encryption of the message and the space link
	Power Masking	Power masking is used to protect secret keys
	Satellite Unit RF Encryption	Encryption of RF link
	Data encryption	Transmitted data (bus-payload link) is encrypted

	Malware Protection	Mission operated systems employ malicious code protection mechanisms to detect and eradicate malicious code
	Integrity Checking and Assurance	Integrity checking mechanisms are used to verify software, firmware, and information integrity
	Equipment maintenance	Procedures and processes for equipment maintenance are defined and implemented
	Software Supply Chain Integrity	Technical measures are in place to ensure integrity of the supply chain
	Network and Communications Monitoring Function	Communications are monitored to identify cybersecurity events and verify the effectiveness of protective measures
	Intrusion Detection and Prevention	On-board Intrusion detection/prevention systems (IDP/IPS) are employed to detect and respond to threats and attacks
	Event detection communication	Event detection is communicated to stakeholders
	Anomaly detection	Event data is correlated from multiple sources and communicated; Inappropriate or malicious activity within the mission's systems is detected
	Mission Cyber Actor Actions Detection	An on-board cyber actor actions detection function is in place
	Critical Telemetry Points Monitoring	Critical telemetry points are monitored for malicious activities
	Reinforcement Learning	A reinforcement learning agent is deployed to detect anomalous events
	Space-Based Radio Frequency Mapping	Space-based RF mapping is in place to monitor and analyse the RF environment
	Dependency Confusion	Protections are in place for mitigating dependency confusion
	Software Mission Assurance	Assurance activities are performed according to documented procedures
	Software and Hardware Testing Function	End to end testing is performed according to documented procedures
	Dynamic Code Analysis	Dynamic Code Analysis is performed to identify software/firmware weaknesses and vulnerabilities
	Static Code Analysis	Static Code Analysis is performed to identify system-relevant weaknesses
	Long Duration Testing	Long Duration Testing is performed to identify race conditions and time-based attacks
	OSAM Dual Authorization	Multi-factor authentication is employed for OSAM servicers
	Simulation Testing	The resilience of segments is tested using attack simulations across the lifecycle
	Detection processes are tested	Event detection processes are tested to ensure they are operating as intended
	Detection Processes	Detection processes are continuously improved

6.1.3. Controls for addressing threats from physical attacks (PA)

Table 6: Controls for addressing threats from physical attacks (PA)

THREAT	CONTROL TITLE	CONTROL
Coercion, extortion, or corruption	Secure Workload-to-Workload Authenticator	Procedures for secure authentication integration protocol are defined and documented
	Threat modelling	Threat modelling is employed to identify and reduce the attack surface
	Risk management	Risk management processes and procedures are defined and implemented
	Access control	Access control policies and procedures are defined and documented
	Access rights	Access control policies and procedure determining access rights to information and associated assets are defined and implemented
	Authentication	Authentication procedures are defined and documented
	Insider Threat Protection	Insider Threat procedures and guidelines are defined and documented
	Asset Inventory	An asset inventory is established and maintained
	Return of assets	A procedure for asset management following termination of cooperation is defined and documented
	Continuous Personnel Monitoring	Personnel activity is monitored to detect anomalous behaviours
	Cybersecurity awareness and training	Cybersecurity is included in human resources practices and personnel are provided with awareness and training

Damage/ Destruction of segment assets	Transport Security	Transport from the integration hall to the test stations, between different facilities, and to the start facility is secured
	Disable Physical Ports	Physical ports are disabled prior to operations
	Security Testing Results	Results of penetration testing and vulnerability scanning are used to build report and vulnerability repositories
	Manoeuvrability	Satellite evasive manoeuvre protocols are implemented
	Deception and Decoys	Deception and decoys are employed for defensive capabilities
	Physical Seizure	Space traffic control and debris mitigation protocols are established
	Defensive Dazzling/Blinding	Laser systems are employed to dazzle or blind the optical or infrared sensors of ASAT weapons.
Damage/ Destruction of the satellite via the use of ASAT	Protective Technology	Mechanisms to ensure resilience requirements are defined and employed
	Manoeuvrability	Satellite evasive manoeuvre protocols are implemented
	Deception and Decoys	Deception and decoys are employed for defensive capabilities
	Physical Seizure	Space traffic control and debris mitigation protocols are established
	Defensive Dazzling/Blinding	Laser systems are employed to dazzle or blind the optical or infrared sensors of ASAT weapons.
Loss during shipping	Protective Technology	Mechanisms to ensure resilience requirements are defined and employed
	Transport Security	Transport from the integration hall to the test stations, between different facilities, and to the start facility is secured
Sabotage through hardware/software	System redundancy	Redundancy is introduced for critical infrastructure and data is backed up
	Anti-counterfeit Hardware	Anti-counterfeit policy and procedures are defined and implemented
	Disable Physical Ports	Physical ports are disabled prior to operations
Unauthorised physical access	Security Testing Results	Results of penetration testing, and vulnerability scanning are used to build report and vulnerability repositories
	Transport Security	Transport from the integration hall to the test stations, between different facilities, and to the start facility is secured

6.1.4. Controls for addressing threats from unintentional damage (UD)

Table 7: Controls for addressing threats from unintentional damage (UD)

THREAT	CONTROL TITLE	CONTROL
Lack of segregation	Access-based network segmentation	The network is segmented into subnetworks to prevent unauthorised access
	Data encryption	Transmitted data (bus-payload link) is encrypted
Operating errors	Cybersecurity-Safe Mode	Secure vehicle fault management functions and safe mode operations are implemented to enable a cyber-safe mode when threats are detected
	Critical Services Delivery Requirements	Resilience requirements to support delivery of critical services are established for all operating states
	Software and Hardware Testing Function	End to end testing is performed according to documented procedures
	Detection processes are tested	Event detection processes are tested to ensure they are operating as intended
Software misconfiguration	Configuration Management	Configurations, including security configurations, are defined, documented, implemented, monitored, and reviewed.
	Coding Standard	Secure coding principles for software development are defined and implemented to ensure proper security constructs are in place
	Secure Development Lifecycle	Rules for the secure development of software and systems should be established and applied.
	Backdoor Commands	Non-critical backdoor commands are disabled

	Vulnerability Management	Vulnerability management processes and procedures are defined and implemented
	Installation of software on operational systems	Procedures for software installation on operational systems are defined and implemented
	Vulnerability scanning	Vulnerability scanning is used to identify vulnerabilities
	Security Testing Results	Results of penetration testing and vulnerability scanning are used to build report and vulnerability repositories
	Software Updates	Regular software updates are performed to mitigate exploitation risk
	Protocol Update / Refactoring	Protocols are updated based on emerging threats and vulnerabilities
	Software Source Control	The use of binary or machine-executable code is controlled
	ASIC/FPGA Manufacturing	Trusted hardware development is ensured
	Integrity Checking and Assurance	Integrity checking mechanisms are used to verify software, firmware, and information integrity
	Dynamic Code Analysis	Dynamic Code Analysis is performed to identify software/firmware weaknesses and vulnerabilities
Inadequate security planning/ management	Information Security Policies	An Information Security Policy (ISP) and other relevant cybersecurity policies and guidelines are defined and documented (e.g. change management policy, remote access policy, incident response, and other)
	Information security roles and responsibilities	Information security roles and responsibilities are defined
	Resource allocation	Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies.
	Assessment & Authorization concept	Assessment & Authorization (A&A) procedures and processes are defined and documented
	Business Impact Analysis (BIA)	Business Impact Analysis (BIA) is conducted to identify and assess potential impacts of threats and the likelihood of their occurrence. It is crucial process for BCM that identifies and evaluates the potential effects of disruptions on critical business operations. BIA informs the BCM strategy, ensuring that roles and responsibilities are clearly defined, with teams assigned to mitigate risks and implement effective recovery measures in the event of a disruption.
	Separation of Environments	The development, testing and production environments are separated and secured
	Data Management	Data is protected in all states (rest, transit, use)
	Integrity Checking and Assurance	Integrity checking mechanisms are used to verify software, firmware and information integrity
	Asset Inventory	An asset inventory is established and maintained
	Asset prioritisation	Guidelines for asset prioritisation are defined
	Public relations management during incidents	Information distribution during an incident is centralised and coordinated.
	Incident Response Plan	Procedures and processes for Incident Response are defined and documented
	Incident Thresholds	Incident thresholds are defined and documented based on an understanding of potential impact
	Incident Recovery Plan	Procedures and processes for Incident Recovery are defined and documented
	Critical Services Delivery Requirements	Resilience requirements to support delivery of critical services are established for all operating states
	System redundancy	Redundancy is introduced for critical infrastructure and data is backed up
	Software Mission Assurance	Assurance activities are performed according to documented procedures
	Software and Hardware Testing Function	End to end testing is performed according to documented procedures
	Long Duration Testing	Long Duration Testing is performed to identify race conditions and time-based attacks
	Machine Learning Data Integrity	Data integrity testing is performed on AI/ML training datasets
	Simulation Testing	The resilience of segments is tested using attack simulations across the lifecycle
	Detection processes are tested	Event detection processes are tested to ensure they are operating as intended

6.1.5. Controls for addressing threats from failures or malfunctions (FM)

Table 8: Controls for addressing threats from failures or malfunctions (FM)

THREAT	CONTROL TITLE	CONTROL
Failure of air conditioning or water supply	Emergency power sources	Emergency power generators and UPS systems are in place - power chain is available and dimensioned properly
Failure of Cloud infrastructure	Cloud Cybersecurity Measures	SLAs are in place external services and cloud providers
Failure of communication networks	Adaptive Risk Response and Resource Allocation Function	Continuous process of qualitative and quantitative mission security risk analysis and risk response is conducted for the duration of the mission
	Risk management	Risk management processes and procedures are defined and implemented
	Security of Power Systems	Power randomization and power consumption obfuscation techniques are employed
	Communications Security	Secure communication protocols are employed to prevent unauthorized disclosure of, and detect changes to information
	Traffic Flow Security	Traffic flow security and confidentiality measures are in place to mitigate traffic analysis attacks
	Emergency power sources	Emergency power generators and UPS systems are in place - power chain is available and dimensioned properly
Failure of power supply	Security of Power Systems	Power randomization and power consumption obfuscation techniques are employed
	Emergency power sources	Emergency power generators and UPS systems are in place - power chain is available and dimensioned properly
	Cabling security	A secure cabling protocol is defined
	Capacity to ensure availability	The required level of availability and capacity for the ground segment is maintained and established
Rogue hardware	Transport Security	Transport from the integration hall to the test stations, between different facilities, and to the start facility is secured
	Anti-counterfeit Hardware	Anti-counterfeit policy and procedures are defined and implemented
	Restricted zones access	Informal meeting places within restricted zones are defined
	Software Supply Chain Integrity	Technical measures are in place to ensure integrity of the supply chain

6.1.6. Controls for addressing threats from outages (OUT)

Table 9: Controls for addressing threats from outages (OUT)

THREAT	CONTROL TITLE	CONTROL
Personnel absence	Continuous Personnel Monitoring	Personnel activity is monitored to detect anomalous behaviours
Security services failure	Security of Power Systems	Power randomization and power consumption obfuscation techniques are employed
	Security Information and Event Management (SIEM) / Security Operations Center (SOC)	Logs of security-relevant events are integrated into a Security Information and Event Management (SIEM) system
	Emergency power sources	Emergency power generators and UPS systems are in place - power chain is available and dimensioned properly
	Capacity to ensure availability	The required level of availability and capacity for the ground segment is maintained and established

6.1.7. Controls for addressing threats from disasters (DIS)

Table 10: Controls for addressing threats from disasters (DIS)

THREAT	CONTROL TITLE	CONTROL
Atmospheric hazards	Transport Security	Transport from the integration hall to the test stations, between different facilities, and to the start facility is secured
	System redundancy	Redundancy is introduced for critical infrastructure and data is backed up
Environmental hazards	Transport Security	Transport from the integration hall to the test stations, between different facilities, and to the start facility is secured
	System redundancy	Redundancy is introduced for critical infrastructure and data is backed up

6.1.8. Controls for addressing threats from legal aspects (LEG)

Table 11: Controls for addressing threats from legal aspects (LEG)

THREAT	CONTROL TITLE	CONTROL
Data leaks	Legal, statutory, regulatory, and contractual requirements	Legal, statutory, regulatory, and contractual requirements relevant to information security and the organization's approach to meet these requirements are identified, documented, and kept up to date.
	Intellectual property rights	Procedures and processes for protecting intellectual property are defined and documented
	Independent review of information security	Independent review(s) of information security (auditing) are conducted
	Criticality Analysis	Criticality analysis is performed to identify critical functions, components, and data flows
	Third Party risk management	Cyber supply chain risk management processes are defined and implemented
	Cybersecurity-Safe Mode	Secure vehicle fault management functions and safe mode operations are implemented to enable a cyber-safe mode when threats are detected
	Disable Physical Ports	Physical ports are disabled prior to operations
	Access-based network segmentation	The network is segmented into subnetworks to prevent unauthorised access
	Cryptography & Crypto Key Management	Rules for the use of cryptography are defined and implemented; On-board messages are encrypted
	On-board Message Encryption	Encryption of the message and the space link
	Secret Shares	Secret shares are employed
	Satellite Unit RF Encryption	Encryption of RF link
	Data encryption	Transmitted data (bus-payload link) is encrypted
	Data Loss Prevention	Data Loss Prevention (DLP) solutions and measures are employed
	Information Lifecycle	Information assets are identified and described across their lifecycle, considering all relevant processes
	Supplier Security Management	Supplier or Third-Party compliance with relevant security standards is reviewed
	Intrusion Detection and Prevention	On-board Intrusion detection/prevention systems (IDP/IPS) are employed to detect and respond to threats and attacks
	Anomaly detection	Event data is correlated from multiple sources and communicated; Inappropriate or malicious activity within the mission's systems is detected
	Security Information and Event Management (SIEM) / Security Operations Center (SOC)	Logs of security-relevant events are integrated into a Security Information and Event Management (SIEM) system
Misuse of equipment	Secure Workload-to-Workload Authenticator	Procedures for secure authentication integration protocol are defined and documented
	Information Lifecycle	Information assets are identified and described across their lifecycle, considering all relevant processes
	Access control	Access control policies and procedures are defined and documented
	Return of assets	A procedure for asset management following termination of cooperation is defined and documented

Negligence of asset handling security requirements	Equipment maintenance	Procedures and processes for equipment maintenance are defined and implemented
	Continuous Personnel Monitoring	Personnel activity is monitored to detect anomalous behaviours
	Secure Workload-to-Workload Authenticator	Procedures for secure authentication integration protocol are defined and documented
	Anti-counterfeit Hardware	Anti-counterfeit policy and procedures are defined and implemented
	Disable Physical Ports	Physical ports are disabled prior to operations
	Access control	Access control policies and procedures are defined and documented
	Identity management	Identities are managed throughout their lifecycle
	Return of assets	A procedure for asset management following termination of cooperation is defined and documented
	Equipment maintenance	Procedures and processes for equipment maintenance are defined and implemented
	Event detection communication	Event detection is communicated to stakeholders
	Continuous Personnel Monitoring	Personnel activity is monitored to detect anomalous behaviours
	Simulation Testing	The resilience of segments is tested using attack simulations across the lifecycle
Refusal of actions	Continuous Personnel Monitoring	Personnel activity is monitored to detect anomalous behaviours
Third Party non-compliance (supply chain)	Third Party risk management	Cyber supply chain risk management processes are defined and implemented
	Anti-counterfeit Hardware	Anti-counterfeit policy and procedures are defined and implemented
	ASIC/FPGA Manufacturing	Trusted hardware development is ensured
	Supplier Security Management	Supplier or Third-Party compliance with relevant security standards is reviewed
	Cloud Cybersecurity Measures	SLAs are in place external services and cloud providers
	Outsourced development	Activities related to outsourced system development are monitor and reviewed
Unauthorised access to recycled or disposed media	Information sharing	Information is actively shared to achieve broader cybersecurity situational awareness
	Return of assets	A procedure for asset management following termination of cooperation is defined and documented
	Equipment maintenance	Procedures and processes for equipment maintenance are defined and implemented
	Secure disposal or re-use of equipment	Procedures and processes for disposal/re-use of equipment are defined and implemented
	Asset lifecycle management	Guidelines and procedures for the asset management lifecycle are defined and documented

6.1.9. Controls for addressing legacy infrastructure (LEI)

Table 12: Controls for addressing legacy infrastructure (LEI)

THREAT	CONTROL TITLE	CONTROL
Failure to maintain information systems	Asset lifecycle management	Guidelines and procedures for the asset management lifecycle are defined and documented
	Event detection communication	Event detection is communicated to stakeholders
Legacy software	Installation of software on operational systems	Procedures for software installation on operational systems are defined and implemented
	Asset lifecycle management	Guidelines and procedures for the asset management lifecycle are defined and documented

7. CONCLUSIONS AND RECOMMENDATIONS

The cybersecurity threats and vulnerabilities observed for the space solutions domain (including ground-space-user-human resources segments), pose a direct risk to the availability of essential services and industries critical to our interconnected world. Therefore, implementing a comprehensive cybersecurity strategy is essential for securing satellite infrastructure, ensuring resilience, and mitigating potential threats to the integrity and functionality of the space systems. With the commercialisation of the sector, and the range of stakeholders involved in the processes of designing, assembling, testing, launching and operating satellite infrastructure, ensuring a comprehensive approach to security becomes increasingly complex and challenging. It is therefore essential to observe and discuss the key risks and challenges related to security of the space systems, as outlined below.

- **Supply Chain Risk:** with the space sector heavily dependent on vast global supply chains, introducing potential vulnerabilities that adversaries could exploit to compromise critical systems, is an increasing risk. The risk of supply chain intrusion is two pronged: software components are vulnerable to insertion, modification, or removal of information, and corruption of the code or functionality during development, upgrade, or update of the system; hardware components are susceptible to intentional or unintentional introduction of components or electronic chips containing defects, malware, or backdoors for system sabotage or espionage.
- **Use of Commercial Off-The-Shelf (COTS) components:** in line with supply chain risks, space systems increasingly rely on off-the-shelf components for communication, launch, data reception, and control facilities. This poses as a challenge as details of some of these components are publicly available in open-source materials, which could be used by malicious actors to familiarise themselves with the targeted infrastructure. Additional hardening of COTS, as well as strict procedures for security cryptographic keys, are critical for safeguarding space systems.
- **Legacy Systems:** given the nature and the location of the space systems, many space-based assets have been designed without the security considerations needed to foresee or mitigate some of the present-day cyber challenges. Their remote nature adds another layer of complexity, making necessary updates difficult and in some instances impossible, leaving vulnerabilities that render satellite systems susceptible to cyberattacks.
- **Limited Visibility:** the remote nature of the space systems poses challenges in detecting and responding to cybersecurity incidents and addressing vulnerabilities. In contrast to legacy systems, modern satellites require regular updates through remote access, which creates another layer of risk for intrusion into the system.
- **Cryptographic Mechanism:** depending on the nature of the space system and communication infrastructure and protocols employed, there is a high potential for interception. This is particularly the case for systems relying on radio frequency signals, which may lack encryption or use a low-grade one, heightening the risk of unauthorised access and collection of transmitted information.

- **Human Error:** with space systems having a high degree of human interaction, there are increased risks of unintentional data leaks, system misconfigurations, and insider threats.
- **Sophisticated Cyber Attacks:** with space systems serving an interconnected web of services and industries, there is an increased risk of nation-state actors and APT groups, which may attempt to gain unauthorized access and exfiltrate data or disrupt critical systems.

Although threats and potential impact of risk materialisation will differ depending on the satellite's make and mission, the space threat landscape provides a baseline for considering common challenges in the space domain, to be further tailored to the given context. The recommendations listed below provide a starting point for addressing these and are widely applicable to stakeholders concerned with the cybersecurity threats related to commercial satellites and space-based technologies.

- **Information sharing and reporting:** timely awareness of the vulnerabilities, threats and threat actors' tactics, techniques, and procedures supports building resilience and enables space and relevant telecom operators to introduce adequate mitigation measures in a proactive manner. Information sharing with industrial peers, competent authorities and via relevant bodies (e.g. ISACs) is a prerequisite for situational awareness and knowledge sharing. Incident reporting is also an obligation of space and relevant telecom operators defined by the NIS2 Directive.
- **Security by default and by design:** the space and satellite technical community, as well as broader space industry players, should enforce risk-based, cybersecurity-informed engineering principles. Appropriately applied, these principles will help mitigate supply chain risks, as well as security challenges associated with the use of COTS. Finally, ensuring systems and networks are designed in adherence with security by default and by design principles, the risk of weak configuration will be reduced. The rising number of initiatives aimed at standardisation of space system cybersecurity, including also non-technical measures, will provide a useful blueprint to this end.
- **Ensuring robust supply chain security:** the NIS2 Directive will require space organisations to prioritise supply chain security and implement stricter controls throughout the supply chain lifecycle. Vetting, monitoring, and sourcing from trusted suppliers, applying diversification of the supply chains, as well as identifying counterfeit, fraudulent, and malicious equipment, are focal points for safeguarding against potential threats and effectively mitigating supply chain risks. Similar to the security by default and by design, supply chain security principles need to be cascaded down and adopted by the space and satellite technical community, as well as broader space industry players.
- **Analysis and testing before introducing components into the production environment:** the use of COTS in commercial space systems necessitates rigorous security analysis to be conducted by stakeholders in the space and satellite technical community, as well as broader space industry players involved in development, manufacturing, or testing of satellite systems. This includes, among other, black box testing mechanisms such as fuzzing, boundary value analysis, and equivalence partitioning. The same principles should be applied to the introduction of hardware and software procured through third parties (i.e. the supply chain)

Satellite industry players as well as the broader space and satellite technical community can rely on the knowledge and practice already present amongst the cybersecurity, academia and research communities and build on lessons learnt in other critical domains for the following:

- **Cryptographic mechanism:** space systems require deployment of effective, validated, and tested encryption measures designed to ensure security against current and anticipated threats throughout the entire mission lifecycle. Disruptive and emerging technologies, such as quantum computing, must be considered when selecting encryption protocols, to reduce the risks stemming from weak configuration and address the challenge of lack of encryption.
 - Future deployment of Quantum Key Distribution (QKD) via satellites will require additional robustness and availability of reliable alternative methods for communication. In the context of cryptographic technologies, a combination of quantum-resistant asymmetric cryptographic implementations (PQC) and pre-quantum asymmetric cryptographic solutions will need to be considered (hybrid), with the use of Field Programmable Gate Arrays (FPGAs) to allow reconfiguring encryption algorithms. Therefore, ensuring crypto agility will be critical, enabling systems to adapt to new cryptographic standards as they evolve, while maintaining security in the face of advancements in quantum computing. Regardless of the level of QKD maturity, Digital Signatures will still be required.
- **Segmentation:** establishing robust segmentation measures is crucial for space systems, as it enables compartmentalising sensitive components and data. This addresses the risk of weak configuration, preventing a breach in one area to compromise the entire satellite system, ensuring strengthening resilience against different cyber threats.
- **Patching:** regular and timely patching is essential for addressing vulnerabilities in space systems. Despite the challenges of limited visibility and the presence of legacies in satellite systems, ensuring that software and system is up to date with the latest security patches that are available closes potential entry points that could be exploited by different adversaries.
- **Hardening:** hardening measures involve strengthening the security posture of space systems by reducing their attack surface. This is important for addressing the challenges related to the use of COTS, and includes disabling unnecessary services, implementing strict access controls, and configuring systems to minimise potential points of vulnerability.
- **Zero trust:** Adopting a zero trust security model developed on the basis of assuming a breach, will address multiple risks across a satellite's lifecycle. This implies a multi-layered approach to access control, with access granted via continuous verification of users, devices, applications and services, and on a need-to-know basis.
- **Adoption of appropriate cybersecurity hygiene practices:** embracing effective cybersecurity hygiene practices involves enhancing capacity through awareness-building initiatives. Applicable to all stakeholders involved in the space domain, empowering the human segment of the satellite ecosystem will contribute to a reduction of risks stemming from human error.

Ultimately, as the space sector is a rapidly developing field, regulatory approaches should be designed to protect public interests without hindering performance and innovation. A risk-based approach is recommended, where oversight of risks with the greatest potential of harm are prioritised.



ANNEX A - LIST OF ACRONYMS AND ABBREVIATIONS

ACRONYMS	DESCRIPTION
ADCS	Attitude Determination and Control System
AOCS	Attitude and Orbit Control System
APT	Advance Persistent Threat
BCM	Business Continuity Management
BIA	Business Impact Analysis
BSI	German Federal Office for Information Security
CCSDS	Consultative Committee for Space Data Systems
CDHS	Command and Data Handling System
CIA	Confidentiality, Integrity, and Availability
COM	Communications Module
COTS	Commercial Off-The-Shelf
CRA	Cyber Resilience Act
DIS	Disaster
DLP	Data Loss Prevention
ECSS	European Cooperation for Space Standardization
EGSE	Electrical Ground Support Equipment
EIH	Eavesdropping/Interception/ Hijacking
ENISA	The European Union Agency for Cybersecurity
EPS	Electric Power Supply
ERP	Enterprise Resource Planning
ESA	European Space Agency
EU	European Union
EU Space ISAC	EU Space Information Sharing and Analysis Centre
EUSPA	European Union Agency for the Space Programme
FM	Failures or malfunctions
FPGA	Field Programmable Gate Array
GSaaS	Ground Stations as a Service
GSI	Geographic Information Systems
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
JAXA	Japan Aerospace Exploration Agency
LEG	Legal
LEI	Legacy infrastructure
MGSE	Mechanical Ground Support Equipment
NAA	Nefarious Activity/Abuse

NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
OBC	On-board Controller
OBSW	On-board Software
OSI	Open Systems Intercommunication
OUT	Outages
PA	Physical Attacks
PDHS	Payload Data Handling System
PESTLE	Political, Economic, Social, Technological, Legal and Environmental
PLCOM	Payload Communication Module
PNT	Positioning, Navigation, and Timing
PQC	Quantum-resistant Asymmetric Cryptographic Implementations
PKI	Public Key Infrastructure
QKD	Quantum Key Distribution
RF	Radio Frequency
RTOS	Real-Time Operating System
SDG	Sustainable Development Goals
SDL	Space Data Link
SDLS	CCSDS' Space Data Link Security protocol
SIEM	Security information and event management
SLE	Space Link Extension
SPARTA	Aerospace Corporation's Space Attack Research &Tactic Analysis
SOC	Satellite Operations Centre
SPD-5	Space Policy Directive - 5
TC	Telecommand
TL	Threat Landscape
TM	Telemetry
TTC	Telemetry, Tracking, and Command
TTPs	Tactics, Techniques, and Procedures
UD	Unintentional Damage
UDHS	Untrusted Data Handling System
UNOOSA	United Nations Office for outer Space Affairs
VSAT	Very Small Aperture Terminal

ANNEX B – DETAILED ASSET TAXONOMY

The four tables below provide detailed information on assets. Instances where the asset subdomain is self-explanatory and has not been broken down further into asset groups to maintain clarity and avoid repetition.

Given the scope and complexity of satellite solutions and purposes, the taxonomy provides a common view of satellite assets aimed at wide applicability across the commercial satellite domain. Although not completely technology agnostic, it aims for providing a common baseline which can be tailored further, depending on mission-specific requirements.

Table 13: Detailed Asset Taxonomy - Ground Segment

GROUND SEGMENT					
Category	Asset subdomain	Asset subdomain description	Asset group	Asset group description	Lifecycle Phase
Production	Design, development, and quality assurance	Methods and processes utilised during the design and development and assembly phases.	Document Management incl. Configuration Management System	A document and configuration management system that ensures efficient collaboration, while controlling access to critical design and configuration information.	1, 2
			Prototyping and software development / Integrated Design Engineering	Validating and optimising design and identifying cybersecurity vulnerabilities.	1, 2
			Enterprise Resource Planning (ERP) software	Managing project resources, such as budget, personnel, and materials.	1, 2
	Assembly	Electrical Ground Support Equipment (EGSE) and Mechanical Ground Support Equipment (MGSE) as the IT/OT infrastructure backbone, enabling data exchange and supporting simulators and satellite/mission control centres.	EGSE	EGSE includes custom hardware and an EGSE controller based on an industrial PC with Win/Linux. It includes specialised equipment that can simulate and test electrical systems on a specific satellite before it is launched into orbit.	1, 2
			MGSE	MGSE mainly consists of mechanical support devices and features electronic and, in certain cases, network controls (e.g. trolley, cranes with networked controls). It encompasses tools used for moving satellite hardware.	1, 2
	Manufacturing Systems	Systems partly based on Win/Linux, possibly supplemented by proprietary and open process control technology/commercial			2

		off-the-shelf components and subsystems.			
	Soft/Hardware Test Tools	Test tools are networkable oscilloscopes or digital multimeters			3
	Simulators	Flight dynamics software for performing orbit related computations for estimation, optimisation, and analysis of orbits for mission analysis and in-flight operations. These are commonly commercial off-the-shelf software solutions.			3
	Crypto Hardware/ Software	Hardware consisting of a crypto unit board that holds the keys and software utilised for encryption and loading keys into the satellite and satellite control centre, commonly by using symmetric encryption between the ground stations and satellites.			1, 2
	Miscellaneous (software)	Email servers, databases, operating systems, and other solutions for day-to-day business operations.			1, 2, 3
	Miscellaneous (endpoint devices)	Phones, laptops, tablets, and other devices for day-to-day business operations			1, 2, 3
Transportation	Transport Containers	Containers for transporting the satellite to its test or launch site. Specialised equipment such as the crypto unit board is also transported.	Transport Containers Software	Software controlling mobile rooms with air conditioning and alarm systems.	3, 4
	Logistics Management System	Systems utilised for logistics management and accurate (geolocation- and time-wise) delivery of the satellite infrastructure to the specified site.			3,4
Launch	Checkout systems	Systems utilised for monitoring and managing the satellite during launch.	Centralised Checkout System	The Centralised Checkout System is a software utilised for monitoring and managing satellite activity while in the pre-launch, launch, and checkout phase. It is a key part of the Mission Control System (software) which is used for managing the satellite throughout its operational lifecycle.	3, 4, 5

Satellite Operations	Satellite/ Mission Control Centres	Satellite/mission control centres include physical and digital infrastructure utilised for managing satellite	EGSE	In the context of satellite operations, EGSE comprises various electrical components and supports software such as operating systems utilised to power specific software solutions while the satellite is in orbit. Once the satellite is in orbit, EGSE is also used for troubleshooting and diagnostics, software updates, health and status monitoring.	2, 3, 4, 5, 6, 7
			Mission Control System	Software infrastructure utilised for managing different operations and control the satellite.	2, 3, 4
			Data Link (also known as Space Link Extension) ¹²¹	Data exchanges include channels in the return link (satellite to ground) and the forward link (ground to satellite). The exchange of data happens via antennas clustered as part of Telemetry, Tracking, and Command (TTC) ground stations and the Space Data Link protocol that extends on SLE.	2, 3, 4, 5, 6, 7
			Crypto Unit Ground	As per CCSDS standards, communication between satellite control centres and satellites should use symmetrical encryption where symmetrical master keys are loaded into two crypto devices - on board the satellite (usually Communication Module housing CCSDS crypto unit board) and in the satellite control centre. Given that this is only a recommendation, there are instances where the communication is not encrypted in the commercial satellite sector.	4, 5, 6, 7
			Network (WAN)	Connects control centres with TTC ground stations.	4, 5, 6, 7
			Miscellaneous (software)	Email servers, databases, operating systems, and other solutions for day-to-day business operations.	4, 5, 6, 7
			Miscellaneous (endpoint devices)	Phones, laptops, tablets, and other devices for day-to-day business operations.	2, 3, 4, 5, 6, 7
	Telemetry, Tracking, and Command (TTC) ground stations	Ground stations are the intermediary between the operations centres and satellites. Ground stations transmit and receive telemetry, tracking, and command links between satellites and operations centres. In TTC, telemetry stands for the data received	Antenna	Antenna is the essential asset of the TTC ground stations. TTC ground stations and payload data reception antenna systems frequently use radio frequency and optical techniques; transmit and receive radar and optical subsystems for ground-based space surveillance; TTC, radar and optical signal and data processing.	2, 3, 4, 5, 6, 7

¹²¹ The Consultative Committee for Space Data Systems (CCSDS) has established a Space Link Extension (SLE) which is a standardized set of services that allow control centres to connect to the ground antenna sites and to send satellite data back and forth.

		from the satellite to the ground (downlink); command stands for the data sent from the ground station to the satellite (uplink); tracking stands for the tracking of a satellite and distance measurement. These are performed utilising various antennas, and the mentioned Space Link Extension and Space Data Link protocols. Ground station services are increasingly provided on a commercial basis (GSaaS) - including downlink, uplink and data storage - whereby users only require endpoint devices to access the service.	Internet Data Link (Space Link Extension (SLE)) protocol / Space Data Link (SDL) protocol	With antenna as a physical asset, SLE serves as an internet protocol for a team of operators to communicate with the satellite through a TTC ground station. Extension on SLE is SDL, which is a protocol used to transport the satellite payload as well as telemetry and command & control. The TTC ground station/antenna is used to provide instructions to the satellite, and this link is considered as a Telecommand (TC). In turn, the satellite sends back Telemetry (TM) to the ground station, with details such as satellite's status, errors, as well as other metrics regarding satellite's payload (specific equipment such as cameras or sensors employed at the satellite platform).	4, 5, 6, 7
			Network (WAN)	Connects TTC ground stations with control centres.	4, 5, 6, 7
	Earth Station/Gateway	Similar to TTC Ground station, Earth station/gateway provides connectivity to the satellite. Earth station consists of an antenna that can receive and/or transmit signal to larger TTC ground stations, or directly to the satellite. Additionally, Earth stations usually contain modems that demodulate incoming signals from the satellite into digital data and can also modulate digital data into signals suitable for transmission over a satellite link.	Antenna	Antenna is the essential asset of the Earth stations. It provides connection to and from satellite, but it also provides connection/gateway to consumer endpoint devices.	6
			Receiver & Modem	Given the complexity of Earth stations, in terms of the components required to process the signal, modem is a clustered asset covering several other components. Modem demodulates incoming signals from satellite into digital data and can also modulate digital data into signals suitable for transmission over satellite link.	6

			Router	Although frequently separate from VSATs, routers are connected to the modems. The purpose of the router is to disperse the signal to devices on the network.	6
--	--	--	--------	--	---

Table 14: Detailed Asset Taxonomy - Space Segment

SPACE SEGMENT					
Category	Asset subdomain	Asset subdomain description	Asset group	Asset group description	Lifecycle Phase
Satellite Operations (Satellite bus)	Command and Data Handling System (CDHS)	CDHS manages the satellite and controls all functions of the spacecraft.	On-board controller (OBC)	CDHS uses an On-Board Controller (OBC) that employs a computing platform, i.e. a microcontroller and memory.	3, 4, 5, 6, 7
			On-board software (OBSW)	Executed on the OBC, the On-Board Software (OBSW) implements a remote-control server, usually based on a Real-Time Operating System (RTOS). OBSW handles TM/TC traffic, while also providing data storage, scheduling commands, performing autonomous actions, and updating the program code.	3, 4, 5, 6, 7
			Real-Time Operating System (RTOS)	RTOS is a critical part of satellite infrastructure as it usually houses a watchdog timer. The latter monitors satellite health and can reset the relevant systems, if necessary, as well as perform specific timed activities.	3, 4, 5, 6, 7
	Communications Module (COM)	COM communicates with TTC ground stations and Satellite Operations Centres via SLE/SDL protocols. It comprises an antenna, a radio, and potentially a computing setup (i.e. CCSDS crypto unit board) to handle decoding, protocol implementations, and access projection. COM is usually only dedicated to TM/TCM traffic. COM is directly coupled with the CDHS.	Antenna	Depending on the satellite setup, multiple antennas can be employed to receive/transmit information as well as different signals (radio, optical, etc).	3, 4, 5, 6, 7
			Crypto Unit Board	COM also houses the crypto unit board which contains a symmetrical master key for encryption/decryption of information from the satellite control centres. It operates based on CCSDS standards. The hardware/software is connected to CDHS.	3, 4, 5, 6, 7
			Protocols	COM utilises SLE/SDL protocols to communicate with TTC Ground and Satellite Operations Centres. Additionally, satellites also rely on Inter Satellite Link, which enables communication and pairing with other space assets.	3, 4, 5, 6, 7

Mission Execution: Satellite Payload	Attitude Determination and Control System (ADCS)	Satellites utilise ADCS to determine and adjust their attitude so that they can point antennas towards the Earth and solar panels at the Sun. ADCS is also used for managing the satellite's spinning and positioning once released from the launch vehicle.	Attitude and Orbit Control System (AOCS)	The satellite utilises thrusters to form AOCS, which is employed for minor orbit changes.	3, 4, 5, 6, 7
	Power supply (EPS)	EPS is the satellite's power supply which is usually generated by solar panels and batteries. In case when EPS fails and the batteries fully drain, it is impossible to operate the satellite.	Solar Panels	Solar cells mounted on the surface of a satellite (e.g. wings or body mounted solar arrays), generating electric currents from incoming sunlight. Power is regulated and routed to relevant satellite equipment via a Power Conditioning and Distribution Unit (PCDU).	3, 4, 5, 6, 7
			Batteries	Primary batteries contain a specified amount of usable energy determined at the time of assembly which can only be discharged. Secondary batteries can be recharged from other energy source, such as solar panels or via Radioisotope Thermoelectric Generators, and provide the satellite with power when the primary power (or its source) are not available.	3, 4, 5, 6, 7
	Payload Data Handling System (PDHS)	PDHS has a similar purpose to CDHS, it can receive data from the Payload Communication Module (PLCOM) but it can also process data directly from the payload equipment (cameras, sensors, etc.). PDHS can perform computing tasks and can also process untrusted payload user data. It is possible that PDHS and CDHS are linked, and this is known as the bus-payload link. This link is needed in cases where information relating to bus components is needed to control the payload.			3, 4, 5, 6, 7
	Payload Communication Module (PLCOM)	PLCOM has a similar purpose as COM in the bus category. It either receives structured payload data from the COM or processes raw TCs intended for the payload. Hence, PLCOM has an antenna and, optionally, a crypto unit board.			3, 4, 5, 6, 7
	Untrusted Data Handling System (UDHS)	UDHS' purpose is to run unstructured code that cannot pass through a satellite's PDHS. It is			3, 4, 5, 6, 7

		possible that PDHS contains a UDHS component and vice-versa. UDHS has previously not been part of common satellite architecture but is increasingly used in commercial satellite operations where certain satellite services are rented out to third-party users.		
--	--	---	--	--

Table 15: Detailed Asset Taxonomy - User Segment

USER SEGMENT					
Category	Asset subdomain	Asset subdomain description	Asset group	Asset group description	Lifecycle Phase
Consumer Interfaces	Very Small Aperture Terminal (VSAT)	Consumer VSATs act as a hub for end users to connect directly to the satellite or, more often, to larger ground stations which enable traffic for clusters of different hubs. Alternatively, VSATs can connect among each other using a mesh network, in which case one of the VSAT acts as a hub and facilitates connection directly to the satellite. VSATs enable other services such as GPS and consist of user antennas and modems for receiving and, in some cases, transmitting data.	Satellite dish / Antenna	Antenna or satellite dish in the case of VSAT, is a specialised receiver or transmitter device that communicates either with a ground station (hub) or directly with the satellite (in case of it being the key node in the mesh network).	6
			Modem	Given the complexity of VSAT systems, in terms of the components required to process the signal, modem is a clustered asset covering several other components. Modem demodulates incoming signals from satellite into digital data and can also modulate digital data into signals suitable for transmission over satellite link.	6
			Router	Although frequently separate from VSATs, routers are connected to the modems. The purpose of the router is to disperse the signal to devices on the network.	6

Consumer Endpoint Devices	Endpoint devices	User access content exchanged via satellites utilising endpoint devices such as satellite phones and laptops. Endpoint devices also include satellite TV, GPS receivers/devices, and weather monitoring devices. Industrial systems and aircrafts can also be listed within this asset subdomain. These assets are enabled through consumer interfaces.			6

Table 16: Detailed Asset Taxonomy – Human Resources Segment

HUMAN RESOURCES SEGMENT					
Category	Asset subdomain	Asset subdomain description	Satellite lifecycle actors	Satellite lifecycle actor description	Lifecycle Phase
Satellite Lifecycle Actors	Actors participating in development activities	Actors participating in development activities include researchers, engineers, designers, and scientists who participate in the development of satellites or their supporting elements	Aerospace engineers	Develop avionics features of the satellite	1
			Physicists	Participate in various aspects of satellite development concerning the influence of natural forces on the satellite.	1
			Cybersecurity engineers	Develop cybersecurity features of satellite software.	1
			Data Engineers / Scientists	Develop data infrastructure supporting the functioning of the satellite.	1
			Electronics engineers	Develop electronic and electrotechnical features of the satellite.	1
			Software engineers	Develop the satellite's software.	1
			Manufacturing engineers	Adjust and optimise the specific manufacturing systems in order to produce satellite components.	1
			Mechanical engineers	Develop mechanical features of the satellite.	1
			Propulsion engineers	Develop the satellite's propulsion systems.	1
			Test engineers	Plan and conduct testing of the satellite and its components.	1
			Researchers / Scientists / Engineers concerned with technical fields relevant to the nature of specific satellites	May participate in the development of various mission-specific satellite features.	1
			Astronomers	Supply other lifecycle actors with expertise on influence of	1, 7

	Actors participating in supporting activities	Actors participating in supporting tasks include support technicians engaged in the physical construction and assembly of satellites or satellite components as well as the maintenance of these during all phases of the lifecycle. This also includes support scientific personnel, whose expertise on various scientific areas, such as weather, atmospheric conditions or specific systems is needed during some phases of the satellite lifecycle, such as development, launch or operations.		celestial bodies and forces on the satellite, its functioning and operations	
			Atmospheric scientists	Support other actors with expertise on atmospheric forces and their influence on the satellite and its operations.	1, 6, 7
			Data analysts	Analyses various data relevant to the satellite operations and support other actors.	6
			Manufacturing technicians	Participate in the manufacturing of the satellite components.	2
			Mechanical technicians	Install, inspect and maintain the mechanical components of the satellite during its assembly.	2
			Aerospace technicians	Install, inspect and maintain the avionic components of the satellite during its assembly, and conduct on-site control of satellite avionic features prior to its launch.	2
			Electronics technicians	Install, inspect and maintain the electronic components of the satellite during its assembly.	2
			Test technicians	Conduct tests of the satellites or their features.	3
			Launch technicians	Conduct the launch related tasks on-site.	4
			Launch engineers	Manage on-site testing and last check of the satellite and its components immediately before its launch.	3
			Launch director	Manages the overall process of the satellite launch: receives reports of other relevant actors, authorizes the process and directs the relevant actors during the process.	3, 4, 5
			Operations safety manager	Manages and enforces the safety of satellite launch operations.	3, 4, 5, 6
			Atmospheric scientists	Evaluate the weather conditions during the launch and assess the feasibility of the satellite launch.	3
			GIS Analysts	Plan the navigational patch of the satellite or its carrier during launch.	3
			Logistics and support staff	Conduct tasks related to transportation of satellite or its components on the launch site and supports other satellite actors during the launch.	3, 6
			Technicians concerned with technical fields	May participate in the installation, inspection and maintenance of various mission-	2, 3, 4, 5

			relevant to the nature of specific satellites	specific satellite features (robotics, laser technology etc.).	
Actors participating in satellite operations	Actors participating in satellite operations include actors who are directly engaged in the operations phase, once satellites are deployed in orbit. Their tasks include monitoring of satellite functions and management of mission-related tasks.	SOC operators	Remotely operate a satellite from the Satellite Operations Centre.	4, 5, 6, 7	
		SOC leader	Manages operations of the Satellite Operations Centre	4, 5, 6, 7	
		GIS analysts	Utilises data from GIS in planning of the satellite's mission and operations.	6, 7	
		Communication engineers	Establish, adjust, and maintain the communication links between satellite segments.	6	
		Mission planners	Plan a satellite mission with the assistance of other actors.	6	
		Payload operators	Operate the payload, based on the specific nature of the satellite's mission	6	
		Ground station operators	Operate and maintain the ground stations	6	
		Specialists concerned with technical fields relevant to nature of specific satellites	May participate in satellite's operations, based on its specific technical features.	6, 7	

ANNEX C – SPACE THREAT TAXONOMY

The eight tables below provide detailed information on threats, impact on CIA triad, and assets that are most likely to be affected by that particular threat.

Table 17: Detailed Threat Taxonomy

THREAT CATEGORY	THREAT	THREAT DESCRIPTION	CIA	AFFECTED ASSETS
Nefarious activity / abuse (NAA)	Abuse of leaked data	Use of previously leaked data and information for malicious purposes. Examples may include use of leaked credentials for launching subsequent phishing attacks or gaining unauthorised access using these.	C	Ground: Production Document Management which includes Configuration Management System Prototyping and software development / Integrated Design Engineering & Enterprise Resource Planning (ERP) software & miscellaneous software) Email servers, databases, operating systems, and other solutions for day-to-day business operations. Phones, laptops, tablets, and other devices for day-to-day business operations
	Abuse/ Falsification of rights	Misuse or modification of access rights and permissions to IT systems may see adversaries gain access to these systems, after which they could be able to affect multitude of processes in any segment of the satellite lifecycle. The adversaries may affect those processes to collect information, change them or incapacitate them. This threat is frequently materialised via malicious insiders trading credentials for monetary rewards.	CIA	Ground: Design, development and quality assurance Assembly Manufacturing Systems Miscellaneous (software) Miscellaneous (endpoint devices) Logistics Management System Checkout systems Mission Control System Network (WAN) User: Consumer endpoint devices
	Compromising confidential information (data breaches): Exfiltration	Exfiltration of sensitive satellite data, resulting in a data breach. Exfiltration can be conducted over alternative protocols and web services, including also automated exfiltration.	C	Ground: SLE/SDL protocols User: endpoint interfaces and devices
	Denial of Service (DoS)	DoS can pose a threat to both the satellite control centre and TTC ground stations, as well as the bus and payload of the in the space segment, affecting their availability. Given the common practice of segregation between the bus and the payload, in the case of the space segment, such threats would primarily need to be executed through the bus. DoS may be perpetrated through various kinds of techniques, such	A	Ground: all assets Space: all assets User: Consumer Interfaces devices

	as flooding of satellite with requests/commands,		
Data modification	Although a threat manifestation element of several threat clusters, modification of data as a threat category refers to the potential for adversaries to modify registers, system and authentication processes, and/or cloud compute infrastructure,	CI	Ground: Production Document Management which includes Configuration Management System Prototyping and software development / Integrated Design Engineering & Enterprise Resource Planning (ERP) software & miscellaneous software Email servers, databases, operating systems, and other solutions for day-to-day business operations. Phones, laptops, tablets, and other devices for day-to-day business operations
Electromagnetic interference	Analog interference with electromagnetic signals that are used for controlling heaters and flow valves of the propulsion subsystem. Attacks aimed at these signals could cause freezing of propellant lines, valves locking, lead to unstable spinning of the satellite or put it in de-orbit.	IA	Space: EPS, RTOS and AOCS
Firmware corruption	Threats against firmware include the potential of adversaries overwriting or corrupting firmware devices (e.g. flash memory contents of system OS) making them inoperable or unable to boot.	A	Ground: all assets Space: all assets
Identity Theft	Targeted take-over of an identity of certain satellite lifecycle actors, by acquiring their personal items, information or other artifacts which would allow adversaries to pose as those actors. This may grant adversaries access to processes, information or even facilities where they could perpetrate multitude of actions whose results can compromise each aspect of CIA triad of satellite lifecycle.	CIA	Human resources: all assets
Jamming	Overpowering the frequency of a legitimate RF signal in order to disrupt communications between the ground station and the satellite, or vice versa. Jamming can result in unauthorised commands for guidance and control being sent to the satellite, injection of malicious code, and/or overall Denial of Service. It is one of the most common threats to space infrastructure targeting both ground and space segments as well as space-link communication and has been increasingly employed by a wide range of threat actors.	A	Ground: TTC Ground (Antenna) Space: BUS (COM) & Payload (PLCOM) User: VSAT
Malicious code/ software/activity: Cryptographic exploit	Exploitation of weak communications protocols, commonly due to a lack of encryption, or malicious use of compromised master keys or any encryption key. This threat may result in adversary gaining access to any communication/information in the satellite lifecycle.	C	Ground: Crypto Hardware/Software & Transport Container (Crypto Unit Board) & Satellite Control Centre (Crypto Unit Ground) Space: Crypto Unit Board

	Malicious code/ software/activity: Malicious injection	Injection of malicious software (e.g. rootkits, bootkits, backdoors) into space operations control systems and/or satellite data receivers and transmitters. Malicious code could also be injected into software updates, affecting for example on-orbit software updates, upgrades, patches, or direct memory writes. Malicious injection could enable satellite data extraction and/or manipulation targeting the bus or payload.	I A	Ground: Production (Manufacturing systems & Simulators & Crypto hardware/software) & Centralised Checkout Systems & Satellite Operations Centre (Mission Control System) Space: BUS (CDHS/COM/) & Payload (PDHS/PLCOM)
	Malicious code/ software/activity: Network exploit	Exploitation of misconfigurations and software vulnerabilities to gain unauthorized access to critical systems and networks. Exploitation of the computer network (CNE) in ground control stations as a result of poor configuration could, for example, lead to unauthorised access to and hence compromise of satellite lifecycle assets.	A	Ground: Satellite Control Centre & Centralised Checkout Systems & TTC Ground (Antenna) Space: BUS (CDHS, COM) & Payload (PDHS, PLCOM) User: VSAT
	Malicious code/ software/activity: Software and vulnerabilities' exploit	Exploitation of security weaknesses in satellite infrastructure resulting from poor configuration and/or logic or implementation errors. These may result in systemic vulnerabilities and affect the satellites' reliability and overall stability. Threat actors may exploit such weaknesses by injecting instructions to manipulate control functions, cause resource exhaustion or introduce flaws in satellite components via the supply chain, enabling them to launch subsequent attacks. This threat may encompass time synchronization executions, compromise of boot memory, exploiting faults in geofencing, software defined assets and others.	C I	Ground: Production (Manufacturing systems & Simulators) & Centralised Checkout Systems & Satellite Operations Centre (Mission Control System) Space: Satellite Bus, Satellite payload
	Manipulation of hardware and software: Zero-Day exploit	Exploitation of software vulnerabilities that are at the time of the exploitation unknown to the user. Presenting the so-called "unknown unknown" phenomenon, the Zero-Day exploits are especially threatening, since the users are not aware of the fact that they should be remediating them. Because of the exploitation window, limited detection and response, and significant risk and impact, zero-day vulnerabilities are treated with heightened urgency and specialized approaches in cybersecurity compared to regular software exploits. The Zero-Day exploit may be present in any segment of the satellite lifecycle.	CIA	Ground: all assets Space: all assets User: all assets
	Preventing services	Intentional deactivation of security safeguards such as firewalls, virus scans, log monitoring, etc. This may manifest as a modification of the internal values of the satellite lifecycle assets and may include modification of internal tables, registers, algorithms, cryptographic standards and other software components, as well as inhibiting system recovery.	CIA	Ground: Production (Design, development, and quality assurance & Assembly) & Satellite Control Centre

	Resource exhaustion	Threats of resource exhaustion affect the space segment and can be targeted both at the satellite bus and payload (incl. overall satellite operations, logical storage, and communications). In the case of satellite operations, components such as the payload receive commands to sense, emit, or run whatever mission the satellite has - constantly, to the point that the battery is fully drained/depleted. In the case of logical storage, this includes utilisation of storage capacity until the full limit is reached. Finally, communications are affected by the amount of traffic sent.	A	Space: BUS (CDHS/COM) & Payload (PLCOM/PDHS) - satellite ops; BUS (CDHS, OBSW) - logical storage; BUS (COM, antenna) - communications
	Seizure of control: Satellite bus	Threats to the availability of the satellite bus as a result of adversaries taking control of space assets by exploiting existing vulnerabilities. Such hostile takeovers can result in overtaking control of the management segment to execute malicious commands, as well as complete lockout of legitimate satellite users by overtaking access control.	A	Ground: TTC Ground (SLE/SDL protocol) Space: BUS (CDHS/COM)
	Social Engineering	Deliberate deception regarding the identity and intention of the perpetrator in order to manipulate the victim to perform specific actions that the adversary wants them to do. The threat is mainly materialised through the launch of phishing or spear phishing. This way, all segments of the satellite lifecycle can be affected, since the adversary can achieve anything from gathering sensitive information.	CIA	Ground: Design, development, and quality assurance & Satellite Control Centre & Miscellaneous Software/Hardware
	Spoofing	Also known as "malicious misdirection". Threats aimed at deceiving the receiver, seeing adversaries transmitting erroneous data for malicious purposes via what appears to be a legitimate signal. Attacks involving spoofing can be launched on sensor data and/or guidance control, that is, on both the receiver and the transmitter end. Spoofing threats can result in malicious commands being sent to the satellite or erroneous data to the ground stations.	A I	Ground: TTC Ground (Antenna, SLE/SDL protocol) Space: BUS (COM) User: VSAT
	Supply Chain Compromise	Threats to and from the supply chain including potential leaks of software/tools/data sheets, malicious use of open-source materials on satellite components provided by third parties, the use of common components in satellites running different missions, as well as the potential of introducing malicious software or backdoors through third parties' components. These threats often materialize from the compromise of suppliers' facilities/sites.	CIA	Ground: Production (Manufacturing systems & Assembly & Simulators) & Centralised Checkout Systems & Satellite Operations Centre (Mission Control System) & TTC Ground Space: all assets
	Theft of authentication information	Threats of physical or logical theft (e.g. via keylogger) with potential impact on assets that are connected to the crypto unit board or the crypto unit ground. Such threats can materialise in different phases of a	CIA	Ground: Crypto Hardware/Software & Transport Container (Crypto Unit Board) & Satellite Control Centre (Crypto Unit Ground) & Satellite Control

Eavesdropping / Interception / Hijacking (EIH)		satellite's lifecycle, including while the satellite is manufactured, being transported to its launch site, or via attacks on the satellite control centre once the satellite is in orbit.		Centre (Mission Control System) Space: BUS (COM, Crypto Unit Board)
	Unauthorised modification: Parameters	Deliberate or incorrect modification of a satellite's parameters or test procedures which could enable further tampering with satellite reset and update procedures and result in infinite restarts of the satellite (manipulating RTOS components).	CIA	Space: CDHS (RTOS)
	Unauthorised use of equipment	Unauthorised access to physical devices in scope of the satellite lifecycle, such as physical workstations, machinery in production/assembly facilities or launch facility, may allow the adversary to conduct multitude of nefarious activities with far reaching consequences for the satellite lifecycle.	CIA	Ground: Production (Manufacturing & Assembly) & Satellite Control Centre (group: EGSE/MGSE)
	Hijacking	Malicious alteration or complete replacement of a satellite's legitimate signals with the aim to reuse it for another purpose. Hijacking and unauthorised commands to guidance control are a threat to both ground and space segments, primarily impacting the satellite control centre and TTC ground stations, as well as the satellite bus in the space segment. This type of threats can be materialised by compromising the SLE and SDL protocols.	IA	Ground: Satellite Control Centre & TTC Ground (SLE/SDL protocol) Space: BUS (CDHS & COM) & Payload (PDHS & PLCOM)
	Interception of communication	Interception of data over a communication channel. This may concern any existing communication link in the satellite lifecycle, inside of specific segments - ground, space, user and human resources - as well as between the segments. It concerns both primary and secondary communication channels (e.g. used as backup). This threat is commonly employed for cyber espionage, as it may compromise any information in the satellite lifecycle. For example, the threat of interception of communication can manifest itself as interception of Multi-Factor Authentication.	C	Ground: TTC Ground (Antenna, SLE/SDL protocol) Space: BUS (COM) & Payload (PLCOM) User: VSAT
	Man-in-the-Middle	Threats stemming from Man-in-the-Middle attacks can be materialised by bypassing access control on the COM/PLCOM parts of the satellite, as well as SLE protocol on the ground segment. Similar to DoS, Man-in-the-Middle attacks target the same group of assets satellite control centres and TTC ground stations in the ground segment, as well as the bus and payload in the satellite segment. Additionally, this type of threat can impact VSAT in the user segment.	CIA	Ground: Satellite Control Centre & TTC Ground (SLE/SDL protocol) Space: BUS & Payload User: VSAT
	Network manipulation (Bus-Payload Link)	Threats to the link between connected payload components, in instances where more than one PDHS or UDHS exists (i.e. denial of the link's availability by one to the others). The materialisation of such threat may result in compromise of multiple services hosted by the satellite. This may	CI	Space: BUS (CDHS & COM) & Payload (PLCOM & PHDS & UDHS)

		potentially lead to payload data leaks from all hosted payload components.		
	Network traffic manipulation (TC)	Threats targeting the ability of a satellite to handle traffic coming from the ground station (telecommand) through TC suppression. This type of threats can impact SLE and SDL protocols.	A	Ground: Satellite Control Centre & TTC Ground (Antenna & SLE/SDL protocol) Space: BUS (COM)
	Position detection (telemetry)	Adversaries obtaining information on the orientation of the satellite enabling them to draw conclusions on its function/mission, orbit, etc. and possibly launch subsequent targeted attacks.	C	Ground & Space: SLE/SDL protocols Space: CDHS (OBSW, OBC) / ADCS (group: AOCS)
	Replay of recorded authentic communication traffic	Replay of previous legitimate messages (communication traffic) at a later time to trigger a system response or to enable access to data. An examples of replay attacks may include attacking the scheduling table to affect tasking.	C I	Ground & Space: SLE / SDL protocols
	Unauthorised access	Threat actors gaining and maintaining unauthorised access to a network, which enables them to pre-position themselves for reconnaissance, espionage and/or launch of potential subsequent attacks. The threat can be materialised via web page attacks, cross-site scripting, cross-site request forgery, drive-by hacking, phishing, or attacks on air gapped solutions (i.e. intranet), or through brute force password cracking. Additionally, via masquerading techniques, threat actors presenting themselves as legitimate entities/users can gain unauthorised access.	C I	Ground: all assets (including SLE/SDL protocol)
Physical access (PA)	Coercion, extortion or corruption	The threat of violence, other harms in order to gain access to desired premises or information, or manipulating the victim to perform other actions that the adversary wants them to do. This threat may impact any segment of satellite lifecycle, where human activity or interaction is present.	CIA	Human resources: all assets
	Damage/ Destruction of segment assets	Intentional damage or destruction of satellite infrastructure (hardware and/or software) as a result of intentional adversary action can negatively impact availability of each segment of satellite lifecycle.	A	Ground: Production & Assembly & Transport & Launch & Satellite Control Centre & TTC Ground Space: all assets
	Damage/ Destruction of the satellite via the use of ASAT / Proximity operations	Deliberate physical damage to the satellite or some of its segments. This threat can negatively impact any aspect of satellite operations, depending on the specific satellite asset that has been damaged. Physical damage to the satellite can be caused by a deliberate attack via an ASAT weapon. ASAT includes space or ground based directed energy weapons or kinetic weapons intended to physically destroy satellites, namely: high-powered microwave (HPM) weapons, electromagnetic pulse (EMP), high-powered laser weapons, laser dazzling and blinding, and high-altitude nuclear detonation. This also entails proximity operations where rogue space objects	A	Ground: TTC Ground Space: all assets

		approach space assets for the purpose of assessing their capabilities (spying), making physical contact (ramming), or conducting aforementioned attacks.		
	Loss during shipping	Any satellite lifecycle asset component may be required to be shipped from one location to other, for multitude of reasons, such as calibration/verification, use, or repair. These transfers may be both internal and external to the satellite lifecycle. During the transfer, the asset may be lost, which would strip any segment of the lifecycle of any capability supplied by this asset.	CIA	Ground: Transport Container - Crypto Unit & Logistics Management Systems
	Sabotage through hardware/software	Threats resulting from connection of unauthorised rogue hardware and software, such as USB sticks, unauthorised applications, etc. may endanger the integrity, confidentiality and availability of satellite components. They can be perpetrated as a result of intentional, targeted human intervention or even on the orbit itself (docking of another satellite).	CIA	Ground: Design, development, and quality assurance & Assembly & Satellite Control Centre
	Unauthorised physical access	Unauthorised access/intrusion into buildings, premises and sites. This may result into various types of threats, including compromise, modification, damage to or even theft of the satellite lifecycle assets (ground or space, if they are located on the ground).	CIA	Ground: all assets
Unintentional damage (UD)	Lack of Segregation	Although uncommon, it is possible that a satellite does not have built-in bus-payload segregation, or that segregation is implemented improperly. If these two asset subdomains are not segregated, potential materialisation of threats to the satellite bus can impact a wider set of assets, including the satellite payload.	A	Space: BUS (CDHS/COM) & Payload (PDHS/PLCOM/UDHS)
	Operating errors	Improper handling of systems or applications of satellite lifecycle assets can negatively impact each aspect of satellite lifecycle operations. It can lead to limitation, degradation or outright disruption of function of these assets.	CIA	Human Resources: all assets
	Software misconfiguration	Improper configuration of software resulting in vulnerabilities such as unsecure code and/or logic errors. These may lead to unauthorised access enabling data corruption/modification (intentional or non-intentional) by threat actors, and cause further software or hardware failure, enable use of unauthorised software, or impact the confidentiality, integrity or availability of data.	CIA	Ground: Design, development, and quality assurance & Manufacturing systems & Assembly & Simulators & Satellite Control Centre Ground & Space: SLE/SDL protocols
	Inadequate security planning / management	Lack of appropriate security planning in the Planning/Design phases of the lifecycle, resulting in a lack of testing, for example. Lack of adequate security management once the satellite infrastructure is in the operation phase may lead to unidentified or exposed critical assets, which results in a lack of relevant security measures due to	CIA	Space: all assets Ground: all assets User: all assets Human Resources: all assets

		limited visibility of the infrastructure in its entirety.		
--	--	---	--	--

Failures / malfunction (FM)	Failure of air conditioning or water supply	Threat of basic services malfunctions which can result in unfavourable conditions for people and infrastructure/systems such as heat or frost, due to malfunctions of air conditioning and water supply, etc. Apart from the production and assembly phases of the satellite's lifecycle, these threats can also impact subsequent phases if affecting the ground stations (e.g. server rooms overheating due to air conditioning malfunction)	A	Ground: Production (Design, development, and quality assurance (MGSE) & Assembly & Soft/Hardware Test Tools & Simulators) & Transport Container & Launch
	Failure of Cloud infrastructure	With the proliferation of Cloud solutions and the rise of Ground Stations as a Service (GSaaS), threats to Cloud infrastructure can deny availability of satellite receivers in the ground segment, affecting ground stations as especially impacting users of GSaaS. This will be more pronounced with the introduction of Satellite Operations as a Service (SOaaS) ¹²² . Furthermore, the multi-tenant nature of SOaaS introduces distinct threats to data privacy and service availability in orbit.	A	Ground: Satellite Control Centre & TTC Ground & VSAT Space: BUS (CDHS) & Payload (PDHS, PLCOM, UDHS)
	Failure of communication networks	Failure of communication networks may be caused by malfunction of either hardware or software supporting this network's function or attack directed at them. The satellite lifecycle is dependent on connectivity and so this threat may disrupt functioning of any of its segments.	A	Ground: TTC Ground (Antenna, SLE/SDL protocol) Space: BUS (COM) User: VSAT
	Failure of power supply	Disruption or failure of the satellite's power supply, resulting in satellite becoming unresponsive due to a shut down. This can happen several times as a result of, for example, faulty batteries, damage to, or malfunction of other power sources, such as solar panels, are also possible.	A	Ground: Production & Assembly & Transport & Checkout systems Space: BUS (EPS)
	Rogue hardware	Tainted hardware components may be built into both space and ground segments, ultimately resulting in hardware failure. Failure or malfunction may occur as a result of hidden, malicious capabilities that are built in during the design and development and assembly stages of a satellite's lifecycle. Apart from built-in malicious capabilities, the hardware may simply not be produced according to the specification provided by the manufacturer, or it may be counterfeit.	A	Ground: Assembly (EGSE/MEGSE) & Crypto Hardware/Software & Satellite Control Centre
Outages (OUT)	Personnel Absence	Threats pertaining to limited availability of critical staff, or lack thereof, at any of the satellite lifecycle phases. Personnel absence may result in loss/unavailability of relevant information and inability to complete tasks, comply with prescribed roles and responsibilities, or enforce the four-eyes principle for risk and quality assurance.	C A	Human Resources: all assets

¹²² SOaaS - Satellite Operations as a Service: <https://connectivity.esa.int/projects/soaas>

Disaster (DIS)	Security services failure	Unavailability of security safeguards such as firewalls, virus scans, log monitoring, etc. due to either system failure or malicious action of an adversary. Security services are key for ensuring confidentiality, integrity and availability of satellite lifecycle processes, their disruption may hence compromise each satellite lifecycle asset.	CIA	Ground: Production (Design, development, and quality assurance & Manufacturing) & Satellite Control Centre
	Atmospheric hazards	Disruption or damage of satellite infrastructure as a result of atmospheric events such as electromagnetic pulses, geomagnetic disturbance, or thermal radiation, as well as man-made space debris. Such developments can affect satellite systems both in the test environment and in orbit.	A	Ground: Simulators & Checkout systems (group: Centralised Checkout System) Space: BUS (CDHS, group: OBSW & RTOS; & COM; & ADCS, group: AOCS)
	Environmental hazards	Disruption, damage, or destruction of satellite infrastructure (hardware and/or software) from natural hazards such as fire, floods, environmental pollution, dust, corrosion, frost, etc. Such developments are mainly focused on the satellite lifecycle phases related to the ground and user segment but can have cascading effects on links and the space segment, especially at check-out.	A	Ground: Design, development, and quality assurance & Manufacturing system & Assembly & Soft/Hardware Test Tools & Transport & Launch & Satellite Control Centre & TTC Ground Space: EPS (group: Solar Wings & Batteries) User: VSAT
Legal (LEG)	Data leaks	Threat of potentially disclosing sensitive information to external third parties or stakeholders who do not have the need and/or permission to view/access it. Leaked information can subsequently be abused for launching attacks on the entity the data originates from, as well as its partners, suppliers, etc. depending on the content of the data.	C	Ground: Production (Document Management incl. Configuration Management System Prototyping and software development / Integrated Design Engineering & Enterprise Resource Planning (ERP) software & Crypto hardware/software & Simulators & Soft/Hardware Test Tools)
	Misuse of equipment	Misuse of device(s) and tools.	CIA	Ground: Satellite Control Centre (group: EGSE/MGSE)
	Negligence of asset handling security requirements	Threats stemming from irrational or improper behaviour of actors involved in a satellites' lifecycle. These may include instances of, for example, non-conformity to security requirements during the design, configuration, and operation phases of software and/or hardware components, etc. which could be a source of vulnerabilities and open the doors for subsequent threats and attacks.	CIA	Human Resources: all assets
	Refusal of actions	Postponing or ignoring security requirements (e.g. reporting, updates, patches) by satellite lifecycle actors, due to negligence or purposeful refusal, may affect any segment of satellite lifecycle, due to inherent presence of satellite lifecycle actors in them.	CIA	Ground: all assets Space: all assets User: all assets Human resources: all assets
	Third Party non-compliance (supply chain)	Threats from unvetted, of insufficiently monitored third parties a satellite's the supply chain which may result in the development and delivery of specific	CIA	Ground: Production (Manufacturing & Assembly & Crypto hardware/software & Simulators) & Centralised

		components that fail to comply or live up to the security specifications and requirements that have access to sensitive data or are intended to support critical satellite functions. Examples include use of counterfeit or copied software (e.g. pirated software) that may contain malware, such as disk wiper malware, or the provision of hardware components that contain back doors.		Checkout Systems & Satellite Operations Centre (Mission Control System)
	Unauthorised access to recycled or disposed media	Third parties get access to information from disposed/recycled media or decommissioned infrastructure.	C	Space: Payload (PLCOM & PDHS & UDHS)
Legacy infrastructure (LEI)	Failure to maintain information systems	Disruption or damage to satellite infrastructure due to a lack of maintenance or hardware regeneration at the asset's End of Life.	CIA	Ground: Production (Design, development, and quality assurance) & Assembly & Simulators & Satellite Control Centre
	Legacy Software	Unpatched/Outdated/Legacy COTS software deployed among the platform	C I	Ground: Production (Manufacturing systems & Assembly & Simulators) & Satellite Operations Centre (Mission Control System) & TTC Ground Space: Bus & Payload User: VSAT

ANNEX D – CYBERSECURITY CONTROL FRAMEWORK

Table 18: Policies and Procedures control cluster

#	Control title	Control	Control description	Reference framework	Lifecycle phase	Segment
1	Information Security Policies	An Information Security Policy (ISP) and other relevant cybersecurity policies and guidelines are defined and documented (e.g. change management policy, remote access policy, incident response, and other)	ISP and topic-specific policies, procedures and other types of documentation are defined, approved by management, published, communicated to, and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur. Although primarily focused on management aspects of cybersecurity, the control has wide applicability across the Threat Taxonomy.	ISO27k NIST IR 8401 NIST IR 8411 SPARTA	All	Ground Space User Human Resources
2	Information security roles and responsibilities	Information security roles and responsibilities are defined	Information security roles and responsibilities are defined, allocated and communicated according to the organization needs and the ISP. These are also coordinated with third party roles and responsibilities, as applicable. Roles and responsibilities are defined in contractual agreements, which include information security responsibilities that remain valid after termination or change of employment and confidentiality and/or non-disclosure agreements aligned with the organization's information protection requirements The allocation of roles and responsibilities specifies segregation of duties and responsibilities involves separating conflicting duties and areas of responsibility to prevent conflicts of interest or potential misuse of authority, ensuring transparency, accountability, and integrity within the organizational structure. Management requires that all personnel apply information security measures in accordance with the established information security policy, topic-specific policies and procedures of the organization. Although primarily focused on management aspects of cybersecurity, the control has wide applicability across the Threat Taxonomy.	BSI TR-03184 ISO27k NIST IR 8323r1 NIST IR 8401 NIST IR 8411	All	Ground Space User Human Resources
3	Resource allocation	Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies.	Sufficient resources are assigned appropriately in alignment with the cybersecurity risk strategy, encompassing the designated roles, responsibilities, and policies, thereby ensuring adequate support and funding for effective risk management and mitigation efforts. Although primarily focused on management aspects of cybersecurity, the control has wide applicability across the Threat Taxonomy.	NIST CSF 2.0	All	Ground Space User Human Resources

4	Secure Workload-to-Workload Authenticator	Procedures for secure authentication integration protocol are defined and documented	Policies and procedures to ensure that the developed or delivered systems do not embed unencrypted static authenticators in applications, access scripts, configuration files, nor store unencrypted static authenticators on function keys are defined and documented. These also include digital document signatures that ensure authentication of all documents.	NASA BPG	1	Ground Space User Human Resources
---	---	--	---	----------	---	-----------------------------------

Table 19: Compliance control cluster

#	Control title	Control	Control description	Reference framework	Lifecycle phase	Segment
5	Legal, statutory, regulatory, and contractual requirements	Legal, statutory, regulatory, and contractual requirements relevant to information security and the organization's approach to meet these requirements are identified, documented, and kept up to date.	Legal, statutory, regulatory, and contractual requirements relevant to information security and the organization's approach to meet these requirements are identified, documented, and kept up to date. This encompasses, but is not confined to, regulations stemming from the organization's industry and its role within or connection to critical infrastructure, privacy regulations, and regulations concerning cybersecurity incident reporting, and extra-territorial jurisdiction.	BSI Profile for Space ISO27k NIST CSF 2.0 NIST IR 8401 NIST IR 8411 METI	All	Ground Space User
6	Intellectual property rights	Procedures and processes for protecting intellectual property are defined and documented	Suitable measures to safeguarding intellectual property rights are defined and implemented. This includes developing comprehensive protocols to prevent unauthorized access, use, or disclosure of proprietary information, as well as instituting procedures for promptly identifying and addressing any potential infringements or breaches. All employees and relevant stakeholders are educated about the importance of protecting intellectual property and are provided with clear guidelines and training on how to uphold these rights effectively.	ISO27k	1, 6	Space User
7	Independent review of information security	Independent review(s) of information security (auditing) are conducted	The organization's strategy for overseeing information security and its execution, encompassing personnel, procedures, and technologies, is subjected to periodic independent reviews, scheduled at regular intervals or following notable changes or incidents. Assessments encompass both internal and external cybersecurity audits, along with forensic audits, and extend to suppliers, partners, or other third parties involved.	ISO27k NIST IR 8270 NIST IR 8411	All	Ground Space User
8	Assessment & Authorization concept	Assessment & Authorization (A&A) procedures and processes are defined and documented	The assessment and authorization (A&A) process delineates how thoroughly a specific design and implementation adhere to a predefined set of security requisites outlined by the organisation and relevant regulatory frameworks and is documented within a formal authorisation package.	SPARTA	1	Ground

Table 20: Risk Management control cluster

#	Control title	Control	Control description	Reference framework	Lifecycle phase	Segment
9	Threat modelling	Threat modelling is employed to identify and reduce the attack surface	Threat modelling, attack surface analysis, and vulnerability assessment are employed to guide the development process, drawing on analysis from similar systems, components, or services when relevant. Leveraging identified threats, organisation can work towards minimising the attack surface where feasible. For the space segment, threat modelling considers the lifetime of the system that can be over 15 years and includes analysis of emerging threats stemming for nascent technologies (quantum).	SPARTA	1	Ground Space User Human Resources

10	Criticality Analysis	Criticality analysis is performed to identify critical functions, components and data flows	A criticality analysis is performed to identify mission critical functions, critical components, and data flows and reduce the vulnerability of such functions and components through secure system design. Identification of critical components/functions enables focusing measures for supply chain protection, access management or network security on those most critical. As in control #9, the criticality analysis considers the lifetime of the system that can be over 15 years.	SPARTA	1	Ground Space User Human Resources
11	Adaptive Risk Response and Resource Allocation Function	Continuous process of qualitative and quantitative mission security risk analysis and risk response is conducted for the duration of the mission	A continuous process for qualitative and quantitative mission security risk analysis and risk response is established and implemented, spanning the entire duration of the mission. The process includes regular assessments to identify potential security threats and vulnerabilities, evaluate their potential impact and likelihood, and prioritize them based on their severity. Effective risk response strategies are defined and implemented to mitigate identified risks, monitor the effectiveness of these strategies, and make necessary adjustments in response to new threats or changes in the mission environment. Continuous training and awareness programs are conducted to ensure all mission personnel are equipped to recognize and address security risks. Regular audits and reviews are performed to ensure compliance with security policies and procedures, and to incorporate lessons learned from past incidents and emerging best practices.	NASA BPG	All	Ground Space User Human Resources
12	Third Party risk management	Cyber supply chain risk management processes are defined and implemented	Cyber supply chain risk management (SCRM) processes are identified, established, assessed, managed and agreed to by organizational stakeholders. These ensure that supply chain risks are identified, assessed, and managed. The SCRM process includes third parties, such as suppliers or partners, who provide information systems, components and/or services. It enables considering and defining multi-supplier strategies (supporting supplier diversification).	METI NIST CSF 2.0, NIST IR 8401 NIST IR 8411	All	Ground Space User
13	Risk management	Risk management processes and procedures are defined and implemented	Risk management processes and procedures are defined and implemented, including risk management objectives, risk appetite and tolerance thresholds, and appropriate risk response options, considering internal and external stakeholders' needs and expectations. Identified threats and vulnerabilities are assessed using a standardised method for calculating, documenting, categorising, and prioritising cybersecurity risks. Processes and procedures for reporting on the current levels of risks are in place.	METI NIST CSF 2.0 NIST IR 8323r1 NIST IR 8411	All	Ground Space User Human Resources
14	Business Impact Analysis (BIA)	Business Impact Analysis is conducted during the design and development phase to prevent any future vulnerabilities.	Business Impact Analysis (BIA) is conducted to identify and assess potential impacts of threats and the likelihood of their occurrence. It is a crucial process for BCM that identifies and evaluates the potential effects of disruptions on critical business operations. BIA informs the BCM strategy, ensuring that roles and responsibilities are clearly defined, with teams assigned to mitigate risks and	ISO27k NIST IR 8401 NIST IR 8411	1	Ground

			implement effective recovery measures in the event of a disruption.			
--	--	--	---	--	--	--

Table 21: Security by Design control cluster

#	Control title	Control	Control description	Reference framework	Lifecycle phase	Segment
15	Configuration Management	Configurations, including security configurations, are defined, documented, implemented, monitored, and reviewed.	Configurations, including security configurations, of hardware, software, services, and networks are established, documented, implemented, monitored, and reviewed. A baseline configuration of information technology/industrial control systems that incorporates security principles (e.g. concept of least functionality) is created and maintained. The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	ISO 27k NIST IR 8270	1, 2, 6	Ground Space
16	Coding Standard	Secure coding principles for software development are defined and implemented to ensure proper security constructs are in place	Acceptable coding standards to be used by the software developers are defined, including acceptable software development language. The language should consider security requirements, scalability of the application, the complexity of the application, development budget, development time limit, application security, available resources, etc. The coding standard and language choice must ensure proper security constructs are in place. Automated means to evaluate adherence to coding standards should be employed. The principles also take into account on-board software in terms of code size/computing power required (e.g.; safe memory access/allocation) and potential trade-offs and constraints due to the software's capabilities and runtimes needed to support the language choice.	ISO27k SPARTA	1	Ground
17	Secure Development Lifecycle	Rules for the secure development of software and systems should be established and applied.	Principles for engineering secure systems should be established, documented, maintained, and applied to any information system development activities	BSI TR-03184 ISO 27k NIST IR 8270	1, 6	Ground Space
18	Cybersecurity-Safe Mode	Secure vehicle fault management functions and safe mode operations are implemented to enable a cyber-safe mode when threats are detected	The capability to enter the spacecraft into a configuration-controlled and integrity-protected state representing a known, operational cyber-safe state (e.g. cyber-safe mode) is provided. The spacecraft should be able to enter a cyber-safe mode when conditions that threaten the platform are detected. The cyber-safe mode ensures all nonessential systems are shut down and the spacecraft is placed in a known good state using validated software and configuration settings. Within cyber-safe mode, authentication and encryption should still be enabled. The spacecraft should be capable of reconstituting firmware and software functions to pre-attack levels to allow for the recovery of functional capabilities (by self-healing or supported from the ground). If not possible, a reduced level of mission capability should be achieved. Cyber-safe mode software/configuration should be stored onboard the spacecraft in memory with hardware-based controls and should not be modifiable.	NASA SPARTA	1, 5, 6, 7	Ground Space

19	Secure Command Mode(s)	Spacecraft protection is enhanced by additional protection modes	Additional protection modes for commanding the spacecraft are in place. These may include the spacecraft restricting command lock based on geographic location of ground stations, special operational modes within the flight software, or temporal controls where the spacecraft will only accept commands during certain times.	SPARTA	5, 6, 7	Space
20	Security of Power Systems	Power randomization and power consumption obfuscation techniques are employed	Hardware circuits are designed to ensure that the hardware module is built into the chip that adds noise to the power consumption to mask changes in power consumption. This increases the cost/difficulty of a power analysis attack. Alternatively, obfuscation is performed but it should not degrade operability of the system. These come at an increased cost for manufacturing sensor nodes. Power randomization is not energy efficient and could be impactful for size, weight, and power which is limited on spacecraft as it adds to the fabrication cost of the device.	SPARTA	5, 6	Space
21	Separation of Environments	The development, testing and production environments are separated and secured	Development, testing, and production environments are separated and secured to prevent unauthorized access and mitigate the risk of cross-environment contamination. This ensures that changes in development and testing do not impact production systems and maintains the integrity and confidentiality of each environment. Backup systems are equally secured.	ISO 27k	1, 2	Ground
22	Change Management	Change management procedures are defined and documented	Changes to information processing facilities and information systems are subject to defined and documented change management procedures. Configuration change control processes are in place.	ISO 27k NIST IR 8270	6, 7	Ground Space

Table 22: Environmental and Physical Security control cluster

#	Control title	Control	Control description	Reference framework	Lifecycle phase	Segment
23	Transport Security	Transport from the integration hall to the test stations, between different facilities, and to the start facility is secured	The date, the route, the shipping company, and the personnel involved is kept as secret as possible. Staff should be instructed and obligated to maintain secrecy. Use of trustworthy personnel for transport is ensured, accounting for time and security-related conditions for transport. Electronic document exchanges are conducted using protected communication channels or encryption of the information for transmission via open communication channels. Separation of important elements of the satellite during transport should be examined if this is still possible at this stage of integration. It should also be examined whether the selection of suitable tamper measures for individual components or for the transport container is necessary and useful. This also includes ensuring that the containers used for transport are properly secured from different environmental and atmospheric hazards. The services offered by the transport companies, the means of transport provided, or the courier services commissioned are assessed with regards	BSI TR-03184	2, 3	Ground

			to their scope of services and execution - measured against contractually specified requirements. For further information on supplier reviews, refer to the Supply Chain Management controls.			
24	Tamper Protection	Physical inspection of hardware is performed to identify potential tampering	Tamper proof protection is employed where possible when shipping/receiving equipment, with physical inspection of hardware performed. Cybersecurity measures for satellite operation and data utilisation facilities – tracking and control station, receiving station, network operation system, and mission control system – are in place (including satellite control system and orbit control system).	SPARTA METI	1, 2, 3	Ground

Table 23: Network Security control cluster

#	Control title	Control	Control description	Reference framework	Lifecycle phase	Segment
25	Communications Security	Secure communication protocols are employed to prevent unauthorized disclosure of, and detect changes to information	Secure communication protocols with strong cryptographic mechanisms are employed to prevent unauthorized disclosure of, and detect changes to, information during transmission. Confidentiality and integrity of information during preparation for transmission and during reception is maintained. The spacecraft mode of operations prevents disabling cryptography on the TT&C link (i.e. crypto-bypass mode). Wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters are identified and rejected. Value and relevance of data/information is determined at specific time intervals to ensure that varying levels of encryption complexity are applied.	METI NIST IR 8323r1 SPARTA	6	Space User
26	Anti-counterfeit Hardware	Anti-counterfeit policy and procedures are defined and implemented	Anti-counterfeit policies and procedures designed to detect and prevent counterfeit components from entering the information system are documented and implemented. These includes tamper resistance and protection against the introduction of malicious code or hardware.	SPARTA	1	Ground
27	Transmission security	Transmission security solutions and measures are employed to protect communication transmission	Transmission security solutions and measures are employed to prevent interception, disruption of reception, communications deception, and/or derivation of intelligence by analysis of transmission characteristics such as signal parameters or message externals. For example, jam-resistant waveforms are utilised to improve the resistance of radio frequency signals to jamming and spoofing.	SPARTA	4, 5, 6	Space

			This is applied to space-space (i.e.: inter-satellite links) systems if these space systems have such capability. For the encryption of the group-space communication via RF, please refer to control #39.			
28	Disable Physical Ports	Physical ports are disabled prior to operations	Data connection ports or input/output devices (e.g. JTAG) are disabled or removed prior to spacecraft operations.	SPARTA	1, 2	Ground
29	Backdoor Commands	Non-critical backdoor commands are disabled	An analysis of critical (backdoor/hardware) commands that could adversely affect mission success if used maliciously is performed. All viable commands are identified and documented. Only critical commands for the purpose of providing emergency access where commanding authority is appropriately restricted are employed.	SPARTA	1, 2	Ground
30	Resilient Position, Navigation, and Timing	Authentication mechanisms to verify GNSS information sources are in place	Authentication mechanisms that allow GNSS receivers to verify the authenticity of the GNSS information and of the transmitting entity are utilised where possible, to verify trusted sources. Fault-tolerant authoritative time sourcing is in place for the spacecraft to synchronize internal system clocks for each processor when the time difference is greater than the FSW-defined interval. Where the SpaceWire data communication protocol is employed, the spacecraft adheres to mission-defined time synchronization standard/protocol to synchronize time across a SpaceWire network with an accuracy around 1 microsecond.	SPARTA	6	Ground Space User
31	Smart Contracts	Smart contracts are used to enforce security protocols	Smart contracts are used to mitigate harm when an attacker is attempting to compromise a hosted payload. Smart contracts stipulate security protocols required across a bus and, if violated, the violator is barred from exchanges across the system after consensus achieved across the network.	SPARTA	6	Space
32	Communication Physical Medium	Alternate physical mediums for networking are in place to mitigate network security concerns	Alternate physical mediums for networking based on the threat model/environment are in place. For example, fibreoptic cabling is commonly perceived as a better choice in lieu of copper for mitigating network security concerns (e.g. eavesdropping/traffic flow analysis) because optical connections transmit data using light and don't radiate signals that can be intercepted.	SPARTA	6	Ground
33	Traffic Flow Security	Traffic flow security and confidentiality measures are in place to mitigate traffic analysis attacks	Techniques to assure traffic flow security and confidentiality are applied to links that carry TT&C and/or data transmissions (to include on-board the spacecraft) to mitigate or defeat traffic analysis attacks or reduce the value of any indicators or adversary inferences. These may include methods to pad or otherwise obfuscate traffic volumes/duration and/or periodicity, concealment of routing information and/or endpoints, or methods to frustrate statistical analysis.	SPARTA	6	Ground
34	Access-based network segmentation	The network is segmented into subnetworks to prevent unauthorised access	Network segmentation is based on the specifications for network architecture and design. Information should not be allowed to flow between partitioned applications unless explicitly permitted by security policy. Isolate mission critical functionality	BSI TR-03184 ISO27k NIST IR 8323r1 NIST IR 8411 SPARTA	5, 6	Ground Space User

			from non-mission critical functionality by means of an isolation boundary (implemented via partitions) that controls access to and protects the integrity of, the hardware, software, and firmware that provides that functionality. Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices and is managed consistent with the assessed risk. Enforce approved authorizations for controlling the flow of information within the spacecraft and between interconnected systems based on the defined security policy that information does not leave the spacecraft boundary unless it is encrypted. Implement boundary protections to separate bus, communications, and payload components supporting their respective functions. Relevant assets include antennas, receivers, servers, and subscriptions, as well as radio frequency emanations.			
35	Cryptography & Crypto Key Management	Rules for the use of cryptography are defined and implemented; On-board messages are encrypted	Rules for the effective use of cryptography, including cryptographic key management, are defined, and implemented. Only approved cryptographic algorithms, cryptographic key generation algorithms or key distribution techniques, authentication techniques, or evaluation criteria are employed. Encryption key handling is performed outside of the onboard software and is protected using cryptography. Encryption keys are restricted and cannot be read via any telecommands. In future deployment of Quantum Key Distribution (QKD) via satellites, consider public key infrastructure (PKI), a combination of quantum-resistant asymmetric cryptographic implementations (PQC) and pre-quantum asymmetric cryptographic solutions, with the use of Field Programmable Gate Arrays (FPGAs) which will allow to reconfigure the encryption algorithms. Frequency of key update and key length/complexity is determined based on the importance/relevance of data being secured - see control #25. In case of detected attacks, or other forms of anomalies and events, existing communication encryption and other measures such as the change of crypto hardware and software, algorithms and keys should be reviewed. In addition to authentication on-board the spacecraft bus, as well as all the network connections, authenticated encryption is also recommended to protect the confidentiality of the data traversing the bus. Ensure basic protections like encryption are still being used on the uplink/downlink to prevent eavesdropping. Lastly, the Inter-Satellite-Link (ISL) which enables satellite to connect to each other and communicate is protected via encryption.	BSI TR-03184 BSI Profile for Space ISO27k SPARTA	1, 2, 6	Ground Space
36	On-board Message Encryption	Encryption of the message and the space link	In addition to authenticating the on-board the spacecraft bus, encryption is also recommended to protect the confidentiality of the data traversing the bus. Basic protections like encryption are still being used on the uplink/downlink to prevent	SPARTA	6	Space User

			eavesdropping. CCSDS defines and recommends specific protocols, which could be applied in ensuring secure linking; modularity between the existing implementations of the SDL protocols (Telemetry, Telecommand, and Advanced Orbiting Services) and the Space Data Link Security Protocol (SDLS) protocol is envisaged. The latter protects the services offered by the SDL protocols and supports the three security services of Authentication, Encryption, and Authenticated Encryption.			
37	Power Masking	Power masking is used to protect secret keys	Masking is a scheme in which the intermediate variable is not dependent on an easily accessible subset of secret key. This results in making it impossible to deduce the secret key with partial information gathered through electromagnetic leakage.	SPARTA	6	Space User
38	Satellite Unit RF Encryption	Encryption of RF link	Implement cybersecurity measures in the satellite system (main satellite unit and RF communication).	SPARTA	1, 6	Space
39	Data encryption	Transmitted data (bus-payload link) is encrypted	Encryption and transmission security is employed in accordance with availability, integrity, and confidentiality requirements. Time protocols may need integrity, authentication, and— for certain use cases — confidentiality protections. Data encryption and decryption practices should be discussed with external organizations. Measures such as error detection, error correction, bulk link encryption and other transport layer protections should be considered. The link between bus and payload is also encrypted / segmented depending on the purpose of the space system (with keys/algorithms used for specific segments).	NIST IR 8323r1 NIST IR 8411	6	User

Table 24: Data Security control cluster

#	Control title	Control	Control description	Reference framework	Lifecycle phase	Segment
40	Information classification and labelling	Information is classified according to the assessed risk level and confidentiality, integrity, and availability needs (CIA), and labelled accordingly	Information is classified according to its risk rating from risk assessments, labelled accordingly, and stored in a regularly maintained data inventory. The assigned classification levels are used to determine access rights, acceptable use, and protection requirements.	BSI TR-03184 ISO27k	6	User
41	Data Management	Data is protected in all states (rest, transit, use)	The confidentiality, integrity, and availability of data at rest, in transit, and in use are safeguarded according to the risk and classification level. Integrity checks for transferred data utilize checksum or hash-based methods. Data at rest, such as backups, is stored securely and separately from the operational system. Procedures for handling data in all states include considerations and requirements for third parties.	ISO27k NIST CSF 2.0 NIST IR 8323r1 NIST IR 8401 NIST IR 8411 SPARTA	All	Space User
42	Data Loss Prevention	Data Loss Prevention (DLP) solutions and measures are employed	DLP solutions are implemented to safeguard information assets from unauthorized access, disclosure, and modification, employing methods such as authentication, information flow isolation, access control, and encryption. Physical locations housing critical assets are secured against data leakage.	ISO27k NIST IR 8323r1 NIST IR 8401 NIST IR 8411 SPARTA	All	Ground Space User

			Additionally, shared system resources like registers, main memory, and secondary storage are sanitized to remove any information previously stored from prior use.			
43	Backup	There is a defined and implemented process for conducting, maintaining, and testing backup of information	Information and data are backed up regularly following established procedures that dictate the frequency, methods, responsibilities, and access. These backups are tested periodically to check for errors and verify integrity, ensuring that critical data can be restored after a disruption or incident.	BSI TR-03184 ISO27k NIST CSF 2.0 NIST IR 8411 SPARTA	6	Space User
44	Information Lifecycle	Information assets are identified and described across their lifecycle, considering all relevant processes	The lifecycle of information assets is explicitly outlined, encompassing all relevant processes. Data is retained only as long as needed to achieve its intended purposes, even by third parties. Once the data lifecycle ends, it is destroyed following established procedures to ensure proper sanitization and disposal.	BSI TR-03184 ISO27k NIST IR 8401 NIST IR 8411	All	Ground Space User
45	Data masking	Data masking is employed to obfuscate original, sensitive data	Techniques of data masking, both dynamic and static, are used in accordance with the existing policies and procedures, the business environment and legislative obligations (e.g. related to personal identifiable information (PII) of satellite lifecycle actors). Data masking techniques may include pseudonymization, anonymization, redaction, and substitution.	ISO27k	6	Space User
46	Real-time physics model-based system verification	Real-time physics model-based system is used to verify data input and control sequence changes	Real-time physics model-based system is used to verify data inputs to satellite bus and payload.	SPARTA	6	Space
47	Process ID whitelisting	Process ID whitelisting is employed in the satellite	Only a limited list of IDs is allowed to communicate with and issue commands to the satellite bus and payload firmware.	SPARTA	5, 6	Space
48	A tamper resistant body	A tamper resistant body is used when producing a sensor node	Sensor nodes are encased in bodies made from tamper-resistant material.	SPARTA	6	Space User

Table 25: Vulnerability Management control cluster

#	Control title	Control	Control description	Reference framework	Lifecycle phase	Segment
49	Malware Protection	Mission operated systems employ malicious code protection mechanisms to detect and eradicate malicious code	Mission operated systems employ malicious code protection mechanisms at information system entry and exit points and on system components. These enable real-time scans of files from external sources on endpoints devices and at network entry/exit points as files are downloaded, opened, or executed to detect and eradicate malicious code, including those inserted through the exploitation of information system vulnerabilities. Mission system software updates are validated as free from malware prior to deployment, launch, and at defined regular intervals while the mission is in operation. Results from malicious code analysis is incorporated into organizational incident response and flaw remediation processes.	BSI TR-03184 ISO 27k NASA BPG	1, 2, 6	Ground Space User

50	Vulnerability Management	Vulnerability management processes and procedures are defined and implemented	Information about technical vulnerabilities of information systems in use is collected and exposure to such vulnerabilities is evaluated. Asset vulnerabilities are identified, validated, and recorded. There is a defined and implemented process for receiving, analysing, and responding to vulnerability disclosures. A vulnerability management plan is in place covering also vulnerabilities that are potentially inherited from external organisations and assets.	ISO 27k NIST CSF 2.0 NIST IR 8270 NIST IR 8323r1	1, 6	Ground Space User
51	Installation of software on operational systems	Procedures for software installation on operational systems are defined and implemented	Procedures and measures for securely managing software installations on operational systems are established. These include installing solely tested and authorized software, ensuring releases and installations adhere to specified permissions and procedures, conducted exclusively by authorized personnel, such as within a controlled test environment. Information security needs should be identified, defined, and sanctioned during the development or procurement of applications.	ISO 27k NIST CSF 2.0 NASA BPG BSI TR-03184	1, 2, 3	Ground Human Resources
52	Vulnerability scanning	Vulnerability scanning is used to identify vulnerabilities	Vulnerability scanning activities are defined and implemented, ensuring they do not impact operations. Vulnerability scanning is used to identify known software vulnerabilities (excluding custom-developed software - ex: COTS and Open-Source), and vulnerabilities in dependencies and outdated software (i.e. software composition analysis). Vulnerability scanning tools and techniques facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: (1) enumerating platforms, custom software flaws, and improper configurations; (2) formatting checklists and test procedures; and (3) measuring vulnerability impact. Ground segment technologies and measures may be employed to perform vulnerability analysis of the space segment. Scans may be performed on test systems rather than the space segment itself.	BSI Profile for Space BSI TR-03184 NIST IR 8270 NIST IR 8401 SPARTA	All	Ground Space User
53	Security Testing Results	Results of penetration testing and vulnerability scanning are used to build report and vulnerability repositories	Penetration testing and vulnerability scanning results are used to support identification of detailed vulnerabilities and insight on how to exploit them.	BSI TR-03184 SPARTA	1, 6	Ground Space
54	Software Updates	Regular software updates are performed to mitigate exploitation risk	Software updates are regularly performed. Updated versions of the software/firmware systems incorporating security-relevant updates are released after suitable regression testing, at a frequency no greater than mission-defined frequency. Old versions of software are removed after upgrading but restoration states (i.e. gold images) are recommended to remain on the system. This control also includes the on-board software, and workarounds for maintaining security are to be found at times when it cannot be updated (while in orbit) - see control #19 for potential solutions.	BSI TR-03184 SPARTA	All	Ground Space

55	Protocol Update / Refactoring	Protocols are updated based on emerging threats and vulnerabilities	A protocol is a set of rules (i.e. formats and procedures) to implement and control some type of association (e.g. communication) between systems. Protocols can have vulnerabilities within their specification and may require updating or refactoring based on vulnerabilities or emerging threats (i.e. quantum computing). These apply for space/ground protocols and on-board protocols.	SPARTA	5, 6, 7	Ground Space
56	Software Source Control	The use of binary or machine-executable code is controlled	The use of binary or machine-executable code from sources that do not offer a warranty or provide source code is prohibited to ensure ability to verify, maintain, and secure the software against potential vulnerabilities.	SPARTA	1	Ground
57	ASIC/FPGA Manufacturing	Trusted hardware development is ensured	Application-Specific Integrated Circuit (ASIC) / Field Programmable Gate Arrays are developed by accredited trusted foundries to limit potential hardware-based trojan injections.	SPARTA	1, 2	Ground
58	Integrity Checking and Assurance	Integrity checking mechanisms are used to verify software, firmware and information integrity	Integrity checking mechanisms are used to validate the integrity of mission software, programmable logic devices, and firmware, as well as proper management of information and records, aligning with the risk strategy and the requirements for protecting information confidentiality, integrity, and availability.	NASA BPG NIST IR 8323r1 NIST IR 8411	1, 2, 5, 6	Ground Space User

Table 26: Access Management control cluster

#	Control title	Control	Control description	Reference framework	Lifecycle phase	Segment
59	Computing Device Authentication	Computing devices are authenticated before network connections are established	Computing devices, including mobile devices and network connected endpoint devices (e.g. workstations, printers, servers, VoIP Phones, VTC CODECs) are uniquely identified and authenticated before establishing a network connection.	NASA BPG	All	Ground Space User Human Resources
60	Access control	Access control policies and procedures are defined and documented	Rules to control physical and logical access to information and other associated assets are established and implemented based on business and information security requirements. The rules incorporate security best practice such as least privilege, separation of duties and the four-eyes principle and target all relevant systems and subsystems in the satellite lifecycle. Additionally measures to implement physical access control include badge with pins, guards, gates, etc.	ISO27k NASA BPG NIST CSF 2.0 NIST IR 8323r1 NIST IR 8401 NIST IR 8411 SPARTA	All	Human Resources
61	Identity management	Identities are managed throughout their lifecycle	Identities and credentials are issued, managed, verified, revoked and audited for authorized devices, users and processes. Identities are proofed and bound to credentials and asserted in interactions. Each identity is verified prior to provisioning authenticators. For long term project all historical records are kept, and in cases of users being involved in several phases of the lifecycle, at different time points with different level of credentials, the identities and credentials are recorded and managed.	ISO27k NASA BPG NIST CSF 2.0 NIST IR 8270 NIST IR 8323r1 NIST IR 8401 NIST IR 8411	All	Human Resources
62	Authentication information management	Allocation and management of authentication information governed by a management process,	Allocation and management of authentication information is governed by a management process, including advising personnel on the appropriate handling of authentication information	ISO27k	All	Human Resources

		including guidance for personnel on proper handling.				
63	Access rights	Access control policies and procedure determining access rights to information and associated assets are defined and implemented	Access control policies and procedure determining access rights to information and associated assets are defined and implemented. Access rights to information and other associated assets is provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control. Privileged access rights are restricted and managed, including privileged utility programmes. Read and write access to source code, development tools and software libraries should be appropriately managed.	ISO27k	All	Human Resources
64	Authentication	Authentication procedures are defined and documented	Users, devices, and other assets are authenticated (e.g. single-factor, multi-factor) commensurate with the risk of the transaction (e.g. individuals' security and privacy risks and other organizational risks). Communication sessions (crosslink and ground stations) are authenticated for all commands before establishing remote connections using bidirectional authentication that is cryptographically based. Adding authentication on the spacecraft bus and communications on-board the spacecraft is also recommended.	ISO27k NASA BPG NIST CSF 2.0 NIST IR 8270 NIST IR 8323r1 NIST IR 8401 NIST IR 8411 SPARTA	All	Human Resources
65	Remote access management	Remote access management procedure and processes are defined and documented	Remote access is managed, including the possible remote deletion function.	BSI TR-03184 NIST IR 8270 NIST IR 8323r1 NIST IR 8401 NIST IR 8411	All	User
66	Multi factor authentication	The zero-trust concept is applied to access management	Multi-Factor Authentication is employed. Zero-trust access controls to the code repositories are employed where possible. For example, the main branches in repositories are protected from injecting malicious code.	NASA BPG SPARTA	All	Human Resources
67	Relay Protection	Relay and replay-resistant authentication mechanisms and employed	Relay and replay-resistant authentication mechanisms for establishing a remote connection or connections on the spacecraft bus are employed.	SPARTA	1, 6	Space
68	Session Termination	Procedures for session termination are established	User sessions are defined and implemented. Connections associated with a communications session are terminated at the end of the defined session or after an acceptable amount of inactivity which is established via the concept of operations.	SPARTA	6	Space
69	Insider Threat Protection	Insider Threat procedures and guidelines are defined and documented	Policies and procedures to prevent individuals (i.e. insiders) from masquerading as individuals with valid access to areas where commanding of the spacecraft is possible are defined and documented. An Insider Threat Programme is established to aid in the prevention of people with authorised access performing malicious activities.	SPARTA	All	Human Resources
70	Restricted zones access	Informal meeting places within restricted zones are defined	Meeting places within the restricted zone (coffee, smoking corners, etc.) are defined, minimising access e.g. to avoid tailgating.	BSI TR-03184	All	Human Resources
71	Password security	A password policy and guidelines are defined and documented	A clear password policy is defined and documented.	BSI TR-03184	All	Human Resources

Table 27: Asset Management control cluster

#	Control title	Control	Control description	Reference framework	Lifecycle phase	Segment
72	Asset Inventory	An asset inventory if established and maintained	An inventory of information and other associated assets (hardware and software) is developed and maintained, including asset owners and dependencies between assets. The inventory should also include assets provided or managed by third parties, including tools used for project management and day-to-day business operations.	BSI TR-03184 ISO27k NIST CSF 2.0 NIST IR 8401 NIST IR 8411 SPARTA	1	Ground Space User Human Resources
73	Return of assets	A procedure for asset management following termination of cooperation is defined and documented	A procedure for asset management following termination of cooperation is defined and documented, including requirements for personnel and other interested parties to return all the organizational assets in their possession upon change or termination of their employment, contract, or agreement	ISO27k	All	Ground Space User Human Resources
74	Equipment maintenance	Procedures and processes for equipment maintenance are defined and implemented	Procedures and processes for equipment maintenance are defined and implemented ensuring equipment is maintained correctly to ensure availability, integrity, and confidentiality of information.	ISO27k	All	Ground Space User Human Resources
75	Secure disposal or re-use of equipment	Procedures and processes for disposal/re-use of equipment are defined and implemented	Procedures and processes for disposal/re-use of equipment are defined and implemented ensuring items of equipment containing storage media are verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. This also includes the use of a "kill switch" that prevents hijacking of assets that have been disposed.	ISO27k	7	Space User
76	Asset prioritisation	Guidelines for asset prioritisation are defined	Guidelines for asset prioritisation are defined and documented. Assets are prioritised and protected based on their classification, criticality, resources, and impact on the mission.	BSI TR-03184 ISO27k NIST CSF 2.0 NIST IR 8323r1 NIST IR 8411	All	Ground Space User
77	Asset lifecycle management	Guidelines and procedures for the asset management lifecycle are defined and documented	Assets (systems, hardware, software, services, and data) are managed throughout their life cycles. Management takes into account cybersecurity best practice and implications of other activities, such as risk management and others as well as the asset classification. Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.	NIST CSF 2.0 NIST IR 8323r1 NIST IR 8401 NIST IR 8411	6, 7	Ground Space User

Table 28: Supply Chain Management control cluster

#	Control title	Control	Control description	Reference framework	Lifecycle phase	Segment
78	Supplier Security Management	Supplier or Third-Party compliance with relevant security standards is reviewed	Subcontractors and participating companies are required to provide evidence of security management or established security standards. If required, a review of compliance with the applicable rules and standards is conducted via an ISMS self-assessment or an audit. The scope of the security standard should be examined in the relevant areas.	BSI Profile for Space METI	1, 2, 3, 4	Ground
79	Software Version Numbers	Version numbers of COTS or Open-Source are protected	The version numbers of deployed COTS or Open-Source are adequately protected. These numbers can be cross referenced against public repos to identify Common Vulnerability Exposures (CVEs) and exploits available.	SPARTA	1, 2	Ground
80	Software Bill of Materials	The Software Bill of Materials (SBOM) is generated to identify known vulnerabilities	The Software Bill of Materials (SBOM) is generated against the entire software supply chain and cross correlated with known vulnerabilities (e.g. Common Vulnerabilities and Exposures) to mitigate known vulnerabilities.	SPARTA	1	Ground
81	Software Supply Chain Integrity	Technical measures are in place to ensure integrity of the supply chain	Integrity of the supply chain is ensured through various means including technical measures (e.g. hash sum), organisational measures (e.g. sealed letters, personal handover) as well as auditing of suppliers. Response and recovery planning and testing are conducted with suppliers and Third-Party providers.	BSI TR-03184 NIST IR 8401	1, 2	Ground
82	Cloud Cybersecurity Measures	SLAs are in place external services and cloud providers	Selection of external and Cloud-related services is based on the level to which security requirements and service level agreements (SLAs) are met, in relation to applicable laws, regulations and the mission itself.	ISO 27k METI	1, 2, 6	Ground Space User
83	Outsourced development	Activities related to outsourced system development are monitored and reviewed	All activities related to outsourced system development are directed, monitored, and reviewed to ensure compliance with security, quality, and performance standards. This includes overseeing the development process, evaluating the adherence to contractual obligations, and conducting regular audits to mitigate risks associated with outsourcing. Conduct supplier review prior to entering into a contractual agreement with a contractor (or sub-contractor) to acquire systems, system components, or system services. Their role in the supply chain is identified and communicated. Providers of information systems, components and services are identified, prioritised, and continuously assessed using a cyber supply chain risk assessment process. If components/software cannot be procured from the original component manufacturer or their authorized franchised distribution, the contract is approved by the supply chain board or equivalent to prevent and detect counterfeit and fraudulent parts, materials, and software. Note that the supply chain risk management (SCRM) is typically an intra-organization function.	ISO 27k NIST IR 8270 NIST IR 8323r1 NIST IR 8411 SPARTA	All	Ground Space User

Table 29: Monitoring and Alerting control cluster

#	Control title	Control	Control description	Reference framework	Lifecycle phase	Segment
84	Network and Communications Monitoring Function	Communications are monitored to identify cybersecurity events and verify the effectiveness of protective measures	Communications are monitored at the external boundary of the system and at mission critical internal boundaries within the system. The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. The granularity of the monitoring and the depth of the analysis is consistent with the findings of the risk assessment. Monitoring is performed on the interface to the bus or payload; the receivers that process and form the commands; responses and telemetry; the processed telemetry; and state of health information from the space segment. Additionally, cyber-related events spanning over multiple work shifts should be detected and communicated effectively across all shifts and potentially varying time-zones.	NASA NIST IR 8323r1 NIST IR 8401	6	Ground Space
85	Intrusion Detection and Prevention	On-board intrusion detection/prevention systems (IDP/IPS) are employed to detect and respond to threats and attacks	Normal activities on the network for accessing and controlling mission applications and capabilities are identified and documented. On-board intrusion detection/prevention systems (IDP/IPS) that monitor the mission critical components or systems and audit/logs actions are employed. The IDS/IPS have the capability to respond to threats (initial access, execution, persistence, evasion, exfiltration, etc.) and it to address signature-based attacks. The IDS/IPS are integrated traditional fault management to provide a holistic approach to faults on-board the spacecraft. The spacecraft should have capacity to select and execute countermeasures that are compatible with the system's fault management system to avoid unintended effects or fratricide on the system (i.e. 'safe countermeasures'). At minimum, the response should ensure vehicle safety and continued operations. Ideally, the goal is to trap the threat, convince the threat that it is successful, and trace and track the attacker — with or without ground support. This would support successful attribution and evolving countermeasures to mitigate the threat in the future. For further information on monitoring and alerting, refer to the Monitoring & Alerting controls.	BSI Profile for Space BSI TR-03184 NASA BPG SPARTA	4, 5, 6	Ground Space
86	Event detection communication	Event detection is communicated to stakeholders	Detected events are communicated to personnel, partners, analytics, and downstream application users. For example, ground antenna data anomalies are communicated together with the current best estimate of data quality. When the cause of a service disruption event is suspected to be external, event detection is shared with appropriate external stakeholders for further investigation.	NIST IR 8323r1	6	Ground

87	Anomaly detection	Event data is correlated from multiple sources and communicated; Inappropriate or malicious activity within the mission's systems is detected	Audit/log records are determined, documented, implemented, and reviewed in accordance with documented policies and procedures. A baseline of network operations and expected data flows for users and systems is established and managed. Event data are collected and correlated from multiple sources and sensors. The network is monitored to detect potential cybersecurity events, including malicious code. Capabilities are in place to enable detection of inappropriate or malicious activity within the mission's systems and provide alerts upon detection. Automated mechanisms are employed to maintain and validate baseline configuration to ensure the spacecraft's configuration is up-to-date, complete, accurate, and readily available.	NIST IR 8323r1 NIST IR 8270 NASA BPG SPARTA	4, 5, 6	Ground
88	Mission Cyber Actor Actions Detection	An on-board cyber actor actions detection function is in place	An on-board cyber actor actions detection function is included in the mission's defined requirements and the resulting system.	NASA BPG	6	Space
89	Critical Telemetry Points Monitoring	Critical telemetry points are monitored for malicious activities	Defined critical telemetry points are monitored for malicious activities (e.g. jamming attempts, commanding attempts – command modes, counters, etc.). This includes valid/processed commands as well as commands that were rejected. Telemetry monitoring is synchronised with ground-based Defensive Cyber Operations (i.e. SIEM/auditing) to create a full space system situational awareness from a cybersecurity perspective.	BSI Profile for Space BSI TR-03184 SPARTA	5, 6	Space
90	Reinforcement Learning	A reinforcement learning agent is deployed to detect anomalous events	A reinforcement learning agent is deployed to detect anomalous events and redirect processes to proceed by ignoring malicious data/input.	BSI Profile for Space BSI TR-03184 SPARTA	5, 6	Space
91	Space-Based Radio Frequency Mapping	Space-based RF mapping is in place to monitor and analyse the RF environment	Space-based RF mapping is deployed to monitor and analyse the RF environment that affects space systems both in space and on Earth. The space-based RF mapping provides space operators with a more complete picture of the space environment, the ability to quickly distinguish between intentional and unintentional interference, and the ability to detect and geolocate electronic attacks. RF mapping allows better characterisation of jamming and spoofing attacks from Earth or from other satellites so that other defences can be more effectively employed.	BSI Profile for Space BSI TR-03184 SPARTA	5, 6	Space
92	Continuous Personnel Monitoring	Personnel activity is monitored to detect anomalous behaviours	Personnel activity and technology usage are monitored to detect potentially adverse events.	NIST CSF 2.0	All	Human Resources
93	Dependency Confusion	Protections are in place for mitigating dependency confusion	Proper protections are in place for ensuring dependency confusion is mitigated. This includes assurance that internal dependencies are pulled from private repositories vice public repositories, that the CI/CD/development environment is secure and validation of dependency integrity by ensuring checksums match official packages.	SPARTA	6	User
94	Security Information and Event Management (SIEM) / Security Operations Center (SOC)	Logs of security-relevant events are integrated into a Security Information and Event Management (SIEM) system	Security-related events within system management are systematically recorded and integrated into a Security Information and Event Management (SIEM) system, allowing for real-time monitoring and analysis of potential security threats or breaches. Timely detection and response	BSI TR-03184 NIST IR 8323r1	6	Space User

			to identified security incidents within the infrastructure is enabled.			
--	--	--	--	--	--	--

Table 30: Incident Response control cluster

#	Control title	Control	Control description	Reference framework	Lifecycle phase	Segment
95	Public relations management during incidents	Information distribution during an incident is centralised and coordinated.	Information distribution during an incident is centralised and coordinated and the public-facing representation of the organisation is managed. This includes, but is not limited to: - media interactions - handling and 'triaging' phone calls and email requests - matching media requests with appropriate and available internal experts - screening all of the information provided to the media	NIST IR 8323r1 NIST IR 8401	6	User
96	Incident Response Plan	Procedures and processes for Incident Response are defined and documented	Incident response procedures and processes are defined and documented in an Incident Response Plan. The Incident Response Plan describes in detail the process of recovery after a cybersecurity incident, including the specific actions which need to be taken and the roles and responsibilities of stakeholders involved. This includes: - Incident identification - Conditions for activation and communication of incident response plan - Incident analysis - Categorization of incidents - Incident containment - Incident mitigation - Information collection and post-mortem (forensic) analysis, including incident categorization The Incident Response Plan is regularly reviewed and updated, based on current trends and developments in technology and threat landscape, regulatory requirements and lessons learned from the materialized incidents. Additionally, adding Security Information and Event Management (SIEM) measure could enhance threat visibility and response times. SIEM can help centralise logs, identify patterns, and trigger alerts, giving the incident response team immediate insights.	BSI Profile for Space BSI TR-03184 ISO27k NIST IR 8270 NIST IR 8323r1 NIST IR 8401	6	User
97	Incident Thresholds	Incident thresholds are defined and documented based on an understanding of potential impact	Incident thresholds are defined and documented based on an understanding of potential impact to the mission enabling proper reporting, alerting thresholds, and the development of adequate incident alert procedures. Required notification or alarm communication time upon nearing and exceeding thresholds is defined and documented.	NIST IR 8323r1	6	Ground

Table 31: BCM/Disaster Recovery control cluster

#	Control title	Control	Control description	Reference framework	Lifecycle phase	Segment
98	Emergency power sources	Emergency power generators and UPS systems are in place - power chain is available and dimensioned properly	The function of security equipment and the availability of critical installations are guaranteed in the event of power failures to avoid damage due to uncontrolled power failures. In addition to the general solutions such as UPS & generators, the whole power chain (power grid lines, transformers, UPS, generators) are available and dimensioned properly.	BSI TR-03184	All	Ground Space User
99	Incident Recovery Plan	Procedures and processes for Incident Recovery are defined and documented	Incident Recovery procedures and processes are defined and documented in an Incident Recovery Plan. It Incident Recovery Plan describes in detail the recovery after a cybersecurity incident, including the specific actions which need to be taken and the roles and responsibilities of stakeholders involved. These Incident Recovery Plan is regularly reviewed and updated, based on current trends and developments in technology and threat landscape, regulatory requirements and lessons learned from the materialized incidents. Additionally, global drills are performed to assess the staff's capability to respond to incident, as well as drills for specific categories of staff.	BSI TR-03184 NIST IR 8270, NIST IR 8323r1 NIST IR 8401	6	Space User
100	Cabling security	A secure cabling protocol is defined	Cables carrying power, data or supporting information services are protected from interception, interference, or damage.	ISO27k	3, 4, 5, 6	Ground User
101	Critical Services Delivery Requirements	Resilience requirements to support delivery of critical services are established for all operating states	Resilience requirements supporting the delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations). Resilience requirements are defined based on the ability for the space segment to function autonomously, the criticality of the services provided by the payload, the system's architecture, and procedural considerations (e.g. recovery time, periods of outage).	NIST IR 8401	6	User
102	Capacity to ensure availability	The required level of availability and capacity for the ground segment is maintained and established	Command, response, and telemetry tend to be low-bandwidth operations and the command link is sensitive to delay and jitter. All services and communications pathways to and from the spacecraft are examined to ensure they have adequate capacity to handle peak throughput requirements. Cyber/counterspace-relevant cases are considered when determining peak command and telemetry throughput for system sizing. Cyber-relevant cases may include downtime at one site shifting additional throughput to another site or provider. Contingency cases may require high-volume interaction with the vehicle for activities such as root cause analysis or anomaly response. Measures for addressing such cases may encompass high-availability networks, additional power sources, air-conditioning systems, redundant frequencies, load balancers, hot-swaps, and others.	BSI TR-03184 ISO27k NIST IR 8270 NIST IR 8323r1 NIST IR 8401	6	Ground Space User

103	System redundancy	Redundancy is introduced for critical infrastructure and data is backed up	Due to the sensitivity of space communication ground segment organizations employ one or more redundant facilities which include transmitters, receivers, and servers that are fully backed up (with critical databases, reference software, gold codes, keys etc.). These facilities need to be subject to the same level of cybersecurity protection as primary ones. In a disastrous event, the redundant infrastructure and the backed-up data can generate commands, process telemetry, and other critical operations. Additionally, redundancy can be achieved through interoperability across different systems and solutions used by different providers. For data-related backup please refer to control #44.	NIST IR 8401	6	Ground Space User
-----	-------------------	--	--	--------------	---	-------------------

Table 32: Capacity Building control cluster

#	Control title	Control	Control description	Reference framework	Lifecycle phase	Segment
104	Information sharing	Information is actively shared to achieve broader cybersecurity situational awareness	Information on suspected intentional interference is shared with stakeholders and relevant organisation in the respective region where the operator is located through appropriate channels and procedures to support broader cybersecurity situational awareness. If agreed upon between stakeholders, common data formats are employed for information sharing to strengthen the protection of the user community.	ISO 27k NIST IR 8270 NIST IR 8401	All	Ground Space User
105	Cybersecurity awareness and training	Cybersecurity is included in human resources practices and personnel are provided with awareness and training	Specialized cybersecurity personnel, including privileged users, receive ongoing awareness and training to equip them with the necessary knowledge and skills to undertake their duties with cybersecurity risks in consideration. The content of these training materials is regularly refreshed to reflect current trends and advancements in technology and the threat landscape, updated regulatory standards, and insights gleaned from past incidents.	BSI TR-03184 NIST CSF 2.0 NIST IR 8323r1 NIST IR 8401 NIST IR 8411 SPARTA	All	Human Resources
106	Cyber threat intelligence	Cyber threat intelligence is collected and analysed	Cyber threat intelligence is collected to enhance the organization's cybersecurity posture continually. This intelligence is commonly sourced from various outlets, including information-sharing forums, and analysed to discern attack targets and methodologies.	BSI TR-03184 NIST IR 8270 NIST IR 8323r1 NIST IR 8401 NIST IR 8411	All	Ground Space User

Table 33: Testing control cluster

#	Control title	Control	Control description	Reference framework	Lifecycle phase	Segment
107	Software Mission Assurance	Assurance activities are performed according to documented procedures	Procedures and technical methods for performing software assurance are documented and implemented. Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and the mission's management.	ISO 27k	All	Ground Space User
108	Software and Hardware Testing Function	End to end testing is performed according to documented procedures	Procedures and technical methods for conducting end to end testing are documented and implemented. These include negative testing (i.e. abuse cases) of the mission hardware and software as it	NASA BPG	5, 6	Space

			would be in an operating state ('test as you fly').			
109	Dynamic Code Analysis	Dynamic Code Analysis is performed to identify software/firmware weaknesses and vulnerabilities	Dynamic code analysis is performed to identify software/firmware weaknesses and vulnerabilities in developed and incorporated code (open source, commercial, or third-party developed code). Testing may include simulation, penetration testing, and fuzzing, among other. Testing should be conducted (1) on potential system elements before acceptance; (2) as a realistic simulation of known adversary tactics, techniques, procedures (TTPs), and tools; and (3) throughout the lifecycle on physical and logical systems, elements, and processes. Lab-based learning boards (FLATSATS) as well as digital twins can be used to perform the dynamic analysis depending on the TTPs being executed. Digital twins via instruction set simulation (i.e. emulation) provide a robust environment for dynamic analysis and TTP execution.	SPARTA	All	Ground Space User
110	Static Code Analysis	Static Code Analysis is performed to identify system-relevant weaknesses	Static source code analysis is performed for all available source code looking for system-relevant weaknesses using no less than two static code analysis tools. A prioritised list of software weakness classes (e.g. Common Weakness Enumerations, CWE) is defined and documented based on system-specific considerations and used during static code analysis for prioritisation of static analysis results.	SPARTA	1, 2, 3	Ground
111	Long Duration Testing	Long Duration Testing is performed to identify race conditions and time-based attacks	Testing is performed using hardware or simulation/emulation where the test executes over a long period of time (30+ days). This testing is aimed at identifying race conditions and time-based attacks.	SPARTA	6	Space & User
112	Machine Learning Data Integrity	Data integrity testing is performed on AI/ML training datasets	The integrity of training data sets for AI/ML is used for mission critical operations is tested to ensure there is no data poisoning. Countermeasures that could either block attack attempts or detect malicious inputs before the training cycle occurs are identified and implemented. Regression testing over time, validity checking on data sets, manual analysis, and/or statistical analysis to find potential injects are employed to detect anomalies.	SPARTA	6	User
113	OSAM Dual Authorization	Multi-factor authentication is employed for OSAM servicers	Before engaging in a On-orbit Servicing, Assembly, and Manufacturing (OSAM) mission, verification of servicer should be multi-factor authenticated/authorized by both the serviced ground station and the serviced asset.	SPARTA	1, 6, 7	Ground
114	Simulation Testing	The resilience of segments is tested using attack simulations across the lifecycle	The simulation of information security related attacks (e.g. penetration testing & threat simulations) should be carried out during various segments, the integration, and the operational phase taking into account the ground segment. In the case of particularly vulnerable missions, an attack simulation should also be considered on the check-out system, transport, launch setup, and the phase of the launch campaign. Existing simulators include SPARTA Cyber Exploiter (SPACE) Invader, and from ESA: Ground to Space Threat Simulator (GSTS).	BSI Profile for Space	All	Ground Space User Human Resources

115	Detection processes are tested	Event detection processes are tested to ensure they are operating as intended	Periodic testing is performed to verify the performance of detection processes against the most current threat profiles and vulnerabilities. Devices and components that are upgraded are re-validated with end-to-end user testing.	NIST IR 8323r1	3, 4, 5, 6	Ground Space
-----	--------------------------------	---	--	----------------	------------	--------------

Table 34: Continuous Improvement control cluster

#	Control title	Control	Control description	Reference framework	Lifecycle phase	Segment
116	Detection Processes	Detection processes are continuously improved	Detection processes are continuously improved and are maintained and tested to promote awareness of anomalous events. This includes maintenance, testing and updating of relevant processes and procedures deployed on information systems and assets as well as analytic processes.	NIST IR 8323r1 NIST IR 8411	All	Ground Space User
117	Oversight and governance	Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy.	Cybersecurity risk assessment results are reviewed to inform and adjust the organisation's risk strategy and direction. Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all security capabilities.	NIST CSF 2.0	All	Ground Space User

Table 35: Defence Capabilities control cluster

#	Control title	Control	Control description	Reference framework	Lifecycle phase	Segment
118	Manoeuvrability	Satellite evasive manoeuvre protocols are implemented	Satellite manoeuvre is an operational tactic that can be used by satellites fitted with chemical thrusters to avoid kinetic and some directed energy ASAT weapons. For unguided projectiles, a satellite can be commanded to move out of their trajectory to avoid impact. If the threat is a guided projectile, like most direct-ascent ASAT and co-orbital ASAT weapons, manoeuvre becomes more difficult and is only likely to be effective if the satellite can move beyond the view of the onboard sensors on the guided warhead.	SPARTA	6	Space
119	Defensive Jamming and Spoofing	Jammers and spoofers are employed for defensive operations	A jammer or spoofer can interfere with sensors on an approaching kinetic ASAT weapon, impairing its ability to navigate accurately during the terminal phase of flight. When combined with manoeuvring, this tactic enables a satellite to evade a kinetic attack effectively. Such systems could also deceive SDA sensors by manipulating the reflected radar signal, altering the perceived location, velocity, and quantity of detected satellites, resembling digital radio frequency memory (DRFM) jammers utilized in numerous military aircraft. Additionally, a space-based jammer might disrupt an adversary's communication capabilities.	SPARTA	6	Space

120	Deception and Decoys	Deception and decoys are employed for defensive capabilities	Deception tactics can be utilized to hide or mislead regarding a satellite's location, capability, operational status, mission type, and/or robustness. Public messaging, like launch announcements, might restrict information or actively spread misinformation about satellite capabilities, and operational techniques can obscure certain capabilities. Another tactic could involve altering satellite capabilities or payloads while in orbit. Satellites with interchangeable payload modules could deploy on-orbit servicing vehicles to periodically transfer payloads between satellites, complicating adversaries' targeting calculations by obscuring which payload is on which satellite. Additionally, satellites may employ tactical decoys to confuse ASAT weapon sensors and SDA systems. These decoys, such as inflatable devices mimicking satellite characteristics or electromagnetic decoys simulating RF signatures, are akin to aircraft using airborne decoys like the ADM-160 Miniature Air-launched Decoy (MALD).	SPARTA	6	Space
121	Antenna Nulling and Adaptive Filtering	Antenna nulling and adaptive filtering are employed for defensive operations	Satellites can incorporate antennas designed to suppress signals from specific regions on the Earth's surface or areas in space where jamming is detected, a technique known as 'nulling'. While nulling can effectively counter jamming from identifiable locations, it may inadvertently block transmissions from friendly users within the nullified area. Conversely, adaptive filtering is employed to suppress particular frequency bands irrespective of their source. This method proves advantageous when jamming consistently occurs within certain frequency ranges, allowing satellite transmissions to proceed uninterrupted. However, the efficacy of adaptive filtering may diminish if a wideband jammer disrupts a significant portion of the utilized spectrum, potentially compromising overall system performance.	SPARTA	6	Space
122	Physical Seizure	Space traffic control and debris mitigation protocols are established	A spacecraft equipped for docking, manipulating, or manoeuvring other satellites or debris can be deployed to prevent space-based attacks or alleviate their aftermath. This system could seize a threatening satellite used for hostile actions or rescue a disabled or hijacked satellite. It could also gather and eliminate harmful orbital debris generated by an attack. However, a key constraint is that each satellite's capability is limited by time and propellant, particularly depending on its orbit. For instance, a satellite stationed in GEO might not be well-suited to capture an object in LEO due to the substantial propellant required for repositioning. Therefore, physical seizure satellites might need to be stationed on Earth and dispatched to a specific orbit when required to counter a particular threat.	SPARTA	6	Space
123	Filtering and Shuttering	Filters and shutters are employed to protect sensors from laser dazzling and blinding	On remote sensing satellites, filters and shutters serve to safeguard sensors from laser interference. Filters shield sensors by permitting only specific wavelengths of light to pass through, but they are less effective against lasers operating at the same wavelengths the sensors are	SPARTA	6	Space

			designed to detect. Shutters, on the other hand, rapidly obstruct or redirect all light to a sensor when an anomaly is detected or a threshold is reached, mitigating potential damage but temporarily interrupting data collection.			
124	Defensive Dazzling/Blinding	Laser systems are employed to dazzle or blind the optical or infrared sensors of ASAT weapons.	Laser systems can be employed to impair or incapacitate the optical or infrared sensors of an approaching ASAT weapon during its terminal phase. This tactic resembles the use of laser infrared countermeasures on aircraft to counter heat-seeking missiles. By disabling the guidance system of an ASAT weapon and potentially manoeuvring to a different position, a satellite could evade a kinetic attack effectively. Additionally, such systems could hinder inspector satellites' ability to image a satellite seeking to conceal its capabilities or disrupt adversary space domain awareness efforts.	SPARTA	6	Space
125	Protective Technology	Mechanisms to ensure resilience requirements are defined and employed	Mechanisms such as failsafe systems, load balancing, and hot swapping are implemented to meet resilience requirements under both normal and adverse conditions.	NIST 8401 NIST 8411	6	Space



ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA

European Union Agency for Cybersecurity

Athens Office

Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office

95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office

Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu



ISBN 978-92-9204-696-5
DOI: 10.2824/8841206