



EUROPEAN UNION AGENCY
FOR CYBERSECURITY



LEO SATCOM CYBERSECURITY ASSESSMENT

February 2024

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 info@enisa.europa.eu

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

AUTHORS

Laurent Franck, Satconsult

EDITORS

Monika Adamczyk, Georgia Bafoutsou, ENISA

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), 2024

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 (). 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.

ISBN 978-92-9204-649-1 doi:10.2824/317096 TP-09-23-475-EN-N



TABLE OF CONTENTS

LIST OF ABBREVIATIONS	5
1. INTRODUCTION	7
1.1 BACKGROUND	7
1.2 SCOPE AND OBJECTIVES	7
1.3 TARGET AUDIENCE	7
1.4 STRUCTURE OF THE REPORT	7
2. LEO SATCOM OVERVIEW	9
2.1 INVENTORY OF LEO SATELLITES COMMUNICATIONS SERVICES	11
2.2 THE FINANCIAL DIMENSION OF LEO CONSTELLATIONS	13
2.3 COMPARISON TO GEOSTATIONARY SATELLITE COMMUNICATION SYSTEMS	14
3. LEO SATCOM ASSETS AND INFRASTRUCTURES	16
3.1 LEO SATCOM SYSTEM ARCHITECTURE	16
3.2 ORGANISATION OF SPACE PROJECTS	18
3.3 TECHNOLOGY AND SUPPLY CHAIN	19
4. SECURITY CHALLENGES FOR LEO SATCOM SYSTEMS AND SERVICES	22
4.1 TECHNICAL RISKS	22
4.2 FINANCIAL AND COMMERCIAL RISKS	23
4.3 MALICIOUS THREATS	23
4.4 NON-MALICIOUS THREATS	27
4.5 CYBER INCIDENTS ON LEO SATCOM SYSTEMS	29
5. STANDARDS AND RECOMMENDATIONS FOR SATCOM CYBERSECURITY	33
5.1 EUROPEAN COOPERATION FOR SPACE STANDARDIZATION	34



5.2 CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS	35
5.3 EUROPEAN TELECOMMUNICATION STANDARDS INSTITUTE	37
5.4 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY	38
5.5 EUROPEAN SPACE AGENCY AND AEROSPACE CORPORATION THREAT FRAMEWORKS	39
5.6 OTHER INITIATIVES	40
5.7 OUTLOOK ON FORTHCOMING INITIATIVES	40
6. CYBERSECURITY STRENGTHS AND WEAKNESSES OF SATCOM IN COMPARISON WITH TERRESTRIAL NETWORKS	42
7. CONCLUSIONS	48



LIST OF ABBREVIATIONS

ADC	Analogue-to-Digital Converter
AIAA	American Institute of Aeronautics and Astronautics
AOCS	Attitude and Orbit Control System
API	Application Programming Interface
BSI	German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik)
CAPEX	Capital expenditures
CCSDS	Consultative Committee for Space Data Systems
CERT	Computer Emergency Response Team
CRM	Customer Relationship Manager
DVB	Digital Video Broadcasting
ECSS	European Cooperation for Space Standardization
ETSI	European Telecommunication Standard Institute
FDIR	Fault Detection, Isolation and Recovery
FOP	Flight Operation Procedure
GMR	GEO Mobile Radio
GNC	Guidance, Navigation and Control
GNSS	Global Navigation Satellite System
GSaaS	Ground Segment as a Service
GSO	Geostationary
HEO	Highly Elliptical Orbit
HTS	High Throughput Satellite
ICT	Information and Communications Technology
IOT	Internet of things
ISL	Inter-satellite Link
IRIS²	Infrastructure for Resilience, Interconnectivity and Security by Satellite
LEO	Low-Earth Orbit
LEOP	Launch and Early Orbit Phase
MAIT	Manufacturing, Assembly, Integration and Testing
MEO	Medium-Earth Orbit
M2M	Machine-to-machine
NRA	National Regulatory Authority
NOC	Network Operation Centre
PCB	Printed Circuit Board
RF	Radio frequency
RPO	Rendezvous and Proximity Operations
SATCOM	Satellites communication
SCC	Satellite Control Centre
TC	Telecommand
TM	Telemetry
TT&C	Telemetry, Tracking & Command

EXECUTIVE SUMMARY

This report covers the topic of cybersecurity of Low Earth Orbit (LEO) constellations delivering telecommunications services (LEO satcom in short). The key specifics of an LEO satcom system may be summed up as (a) many assets forming the space and ground segments and (b) a worldwide distribution of the services delivered by those assets. These two aspects usually differentiate satcom systems from terrestrial and other space systems (such as geostationary satellites), where the service coverage under the responsibility of a single organisation/system is smaller. The global nature of LEO satcom also calls for tailored cybersecurity treatment.

When looking at different threats and incurred risks (whether technical, financial or commercial), the landscape of possible attacks is rich. It includes classic cyber threats as found in terrestrial systems that target the user and control segments (terminals, gateways, telemetry tracking and command stations, and interconnection networks). But it also extends to attacks focusing specifically on the satellites forming the space segment. For these reasons, LEO satcom systems deserve a tailored approach when it comes to their security. This situation is acknowledged by actors in the sector and has resulted in several initiatives, among them the European Space Agency (ESA) Space Attacks and Countermeasures Engineering Shield (SPACE-SHIELD).

The survey on past cyber incidents shows that most attacks fall roughly into two categories: data theft through reverse engineering of user link transmission techniques; and denial of service, targeting either the ground or space segments, possibly resulting in a service degradation or outage. The first category of incidents calls for the use of common encryption techniques. The second calls for standards and recommendations in cyber protection, which are applicable to all segments of space systems.

The report also includes a comparison of LEO satcom and broadband terrestrial cellular networks based on cyber threat exposure and impact severity. The case of cellular networks is believed to be a representative case of more generic terrestrial networks. Based on technical considerations only, the comparison reveals that the cyber risk is higher for space systems.

Concluding, the report shows that the cyber protection needs of LEO satcom systems extend beyond what exists for terrestrial systems. The advent of commercial mega-constellations is a clear call for a coordinated approach in space systems security by means of standards, recommendations, information sharing and training.

1. INTRODUCTION

1.1 BACKGROUND

Use of satellite communication for commercial purposes has been rapidly increasing in recent years, with many private companies and entrepreneurs taking advantage of this technology to support their business operations. For that reason, the rapidly growing satellite sector, particularly relying on LEO satellite infrastructure, is becoming an increasingly important part of the overall EU electronics communications market and is a focus of attention for the telecommunications National Regulatory Authorities (NRAs).

Under the European Electronic Communications Code (EECC) directive¹, the NRAs have the obligation to supervise the security of electronic communication networks and services. Satellite operators providing electronic communications services for a fee are within the scope of the EECC supervision. The NIS2 directive² includes the providers of public electronic communications networks and services as one of the critical sectors for which uniform security measures must be applied³. ENISA has identified lack of analysis and control of space-based infrastructure and objects as one of the top cybersecurity threats that are likely to emerge by 2030⁴.

1.2 SCOPE AND OBJECTIVES

With this study, ENISA wants to provide a better understanding of the LEO satcom sector from the cybersecurity perspective. However, while the report focuses on LEO satellites used for communications services, we need to acknowledge that geostationary satellites have shaped the satcom market for decades generating more than 90 % of satcom revenues. It is only recently that there has been a renewed interest and commercial activity around LEO systems. For that reason, this report will make several references to geostationary satellites to better highlights the specifics of LEO systems and their heritage as far as cybersecurity is concerned.

1.3 TARGET AUDIENCE

This document is aimed at national authorities supervising the implementation of Article 40 of the EECC and in general at national authorities that are responsible for telecom security. It may also be useful for policy experts in the European Commission, cybersecurity agencies, experts working in the telecom or satcom sectors, industry associations and other bodies with roles in standardisation and telecom security.

1.4 STRUCTURE OF THE REPORT

After the introduction, the report is structured as follows.

- Chapter 2 discusses the purpose of LEO satellite for communications services: what services they provide and what the known present and forthcoming systems are. Financial considerations are also addressed.

¹ Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) (OJ L 321, 17.12.2018, p. 36), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02018L1972-20181217>.

² 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, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80), <https://eur-lex.europa.eu/eli/dir/2022/2555>.

³ As stated in Article 43 of the NIS2 directive, Articles 40 and 41 of the EECC will be deleted in October 2024. Instead, the security measures defined in Article 21 of the NIS2 directive will apply to the telecommunication sector.

⁴ Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride!, <https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030>.



- Chapter 3 gives insights into how LEO systems are designed and the key engineering concepts.
- Chapter 4 provides an inventory of threats to which LEO telecommunications are exposed and identifies past cyber incidents affecting these systems using publicly available sources. It also includes a sample (proof of concept) attack made on an experimental satellite to illustrate how spacecraft vulnerabilities can be exploited.
- Chapter 5 describes current standardisation and recommendation initiatives published in the field of space systems security.
- Chapter 6 compares space and terrestrial systems from a cybersecurity standpoint on grounds of threat exposure and impact severity.
- Chapter 7 concludes by issuing some recommendations in the light of prior chapters.

2. LEO SATCOM OVERVIEW

Low Earth Orbit (LEO) satellites are orbiting the Earth at altitudes of several hundreds of km and provide communications services to users mostly located in remote places with no or weak connection to terrestrial infrastructures. LEO satellites are located at an altitude below 2 000 km but are generally in range from 500 km to 1 400 km above the Earth's surface, the orbital plane being often inclined with respect to the equatorial plane. Medium Earth Orbit (MEO) systems have a circular or elliptical orbit, their farthest point on orbit being located at an altitude ranging from 8 000 to 40 000 km (this is the case of Highly Elliptical Orbit (HEO)). As far as this report is concerned, no difference is made between LEO and MEO /HEO. Finally, this report also makes references to geostationary (GSO) satellites. These satellites have an altitude of around 36 000 km, their orbital plane being aligned to the Earth's equatorial plane. From the viewpoint of an on-Earth observer, they appear fixed in the sky.

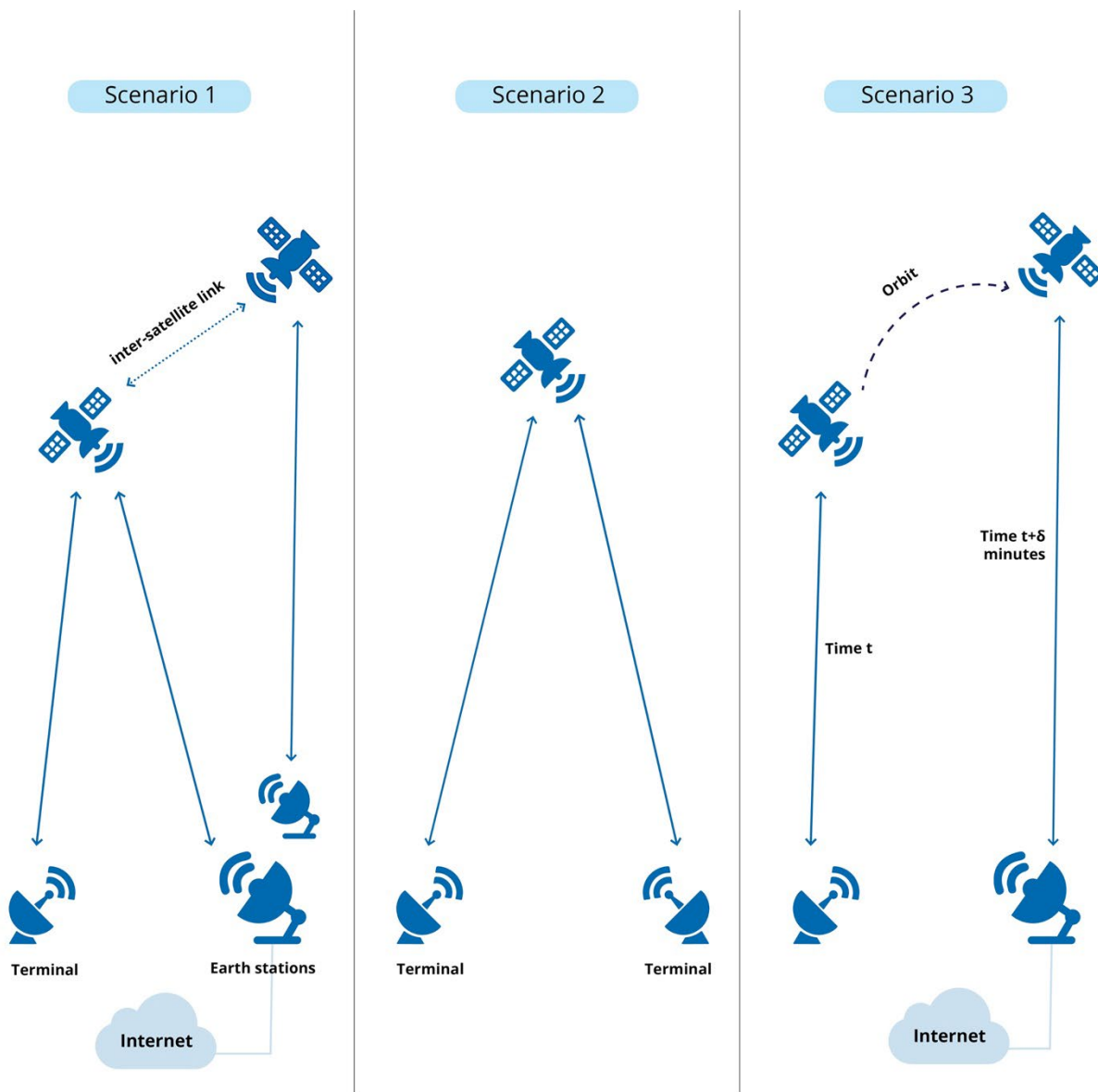
An LEO satellite sweeps the Earth's surface with a given revisit period due to the combined effect of satellite motion and the Earth's rotation. By arranging several (10+) satellites in a pattern called a constellation, it is possible to ensure that any place within the service delivery area on Earth will be covered by at least one satellite at any time. Some systems may even be composed of 'layers' of satellites arranged at different altitudes.

The dynamics of a constellation make the end-to-end communication system more complex to engineer compared to a satellite located on the geostationary orbit. In consequence, the operating costs for large LEO satellite constellations are higher when compared with GSO satellites. However, the cost of bringing LEO satellites into orbit is significantly lower than that of launching GSO satellites. On the other hand, the smaller distance from Earth favours shorter (about 20 to 80 times smaller) radiofrequency propagation delays to the benefit of interactive communications services. Section 2.3 will cover the differences between geostationary systems in more detail.

An electronic communications service based on an LEO satellite system can follow several basic scenarios (see also Figure 1).

- **Scenario 1.** A remote person/device (called the remote terminal) uses the satellite as a relay to establish a communication link to/from an Earth station that provides interconnection to the terrestrial backbone networks. This setup can be extended if several satellites are interconnected through inter-satellite links (ISLs), relieving the need to hop to/from intermediate ground infrastructures to reach the destination.
- **Scenario 2.** Two remote terminals use a satellite as a relay to communicate with each other (possibly by going through several satellites if ISLs are present).
- **Scenario 3.** A remote terminal posts/receives messages to/from a passing satellite, these messages being transferred to/from the terrestrial backbone network when the spacecraft passes over an Earth station. This scheme is called store-and-forward operations.

Figure 1: Different scenarios of terminal–satellite–Earth station communications



The following is a summary of the key points of LEO satellite communications systems.

- LEO satellites sweep the surface of Earth on a periodic basis.
- The communication service offered is global (truly worldwide if the orbit inclination is highly aligned to North–South) thanks to Earth–spacecraft relative motion.
- The delivery of the service relies on the capability to communicate via radiofrequency and in the future via optical links to/from the satellite by means of remote terminals and ground facilities (e.g. Earth stations).
- While a remote terminal requires limited infrastructures (power-supply or none for battery-operated terminals), ground infrastructures are needed for the Earth stations that provide inter-connection to the terrestrial networks and the systems that ensure spacecraft monitoring and control.
- The combination of satellite coverage and radio frequency also enables the communication of messages from one peer to many using a single transmission.

2.1 INVENTORY OF LEO SATELLITES COMMUNICATIONS SERVICES

Table 1 lists services that are typical to LEO satcom constellations by summarising the elements examined in the previous sections.

Table 1: Types of services provided by LEO satcom systems

Service type	Service description	Applications
Short message	Uni- or bidirectional exchange of short (less than 200 bytes) messages	Internet of things (IOT), machine-to-machine (M2M), emergency alerting (when combined with satellite-based localisation)
Narrowband data	Bidirectional exchange of generic data at throughput less than 100 kilobits per second (kbit/s)	M2M, basic internet access (email, frugal web browsing)
Broadband data	Bidirectional exchange of generic data at throughput ranging from 100 kbit/s to several megabits per second (Mbit/s)	Internet access (email, web browsing), audio/video conferencing, video streaming, Voice over IP
Trunking	Bidirectional interconnection of networks at high throughput (several tens of Mbit/s)	Network interconnection, extension of cellular networks
Voice	Bidirectional, real-time voice communication	Telephony

Table 3 provides examples of how these applications can be implemented. Each example is linked to the critical sectors identified in Annex 2 and 3 of the NIS2 directive.

Table 2: Satcom applications and their relation to NIS2 directive critical sectors

Application	Example of implementation	Sector from NIS2 Annex 1
IOT	Location tracking of a container and alerting in case of anomaly (e.g. door opening)	Transport / rail
Network interconnection	Backup trans-national network for the monitoring of European power grids	Energy / electricity
Telephony	Satellite-enabled telephony for assessment teams during a disaster with potential destruction/saturation of the terrestrial cell phone networks	Public administration
M2M	Monitoring and remote operation of hydroelectric plants in remote areas	Energy / electricity
Internet access	Backup of terrestrial-based internet access for the logistics department of a hospital	Health / healthcare providers

These applications can be deployed in terrestrial, maritime and aeronautical environments, categorising the terminals either as fixed or mobile (with communication on the move or in one place).

LEO satellites are also sometimes used to deliver services such as remote sensing or Earth observation (e.g. images, infrared, radar) and location and navigation services. These services are not categorised as satellite communications services and are therefore outside the scope of this report.

Table 3 lists the main and future LEO/MEO constellations, with key characteristics and associated service types, that were on the market at the time when the study was conducted ⁽⁵⁾. The future constellations listed are those that have secured funding. The number of satellites does not include ground or in-orbit spares. For the definition of the narrowband/broadband data throughputs (in bit/s), a distinction has been made between the uplink throughput (from the user to the spacecraft) and the downlink throughput (from the spacecraft to the user). The actual performance is subject to the number of users sharing the uplink and the environmental conditions (snow and heavy rain may degrade performance).

Table 3: Key characteristics of current and future LEO/MEO constellations

Name	Owner (country)	No of satellites for full deployment	% of spacecrafts launched to achieve operational status	Service types	Coverage
Globalstar	Globalstar (United States)	24	100 %	Short message Narrowband data (10 kbit/s bidirectional) Voice	Selected areas below northern polar and above southern polar regions.
Gonets	Gonets/Leosat (Russia)	36	Unknown	Short message Narrowband data (9.6 kbit/s uplink, 20 kbit/s downlink) Voice	Russia
Iridium	Iridium (United States)	66	100 %	Short message Narrowband data (20 kbit/s uplink, 90 kbit/s downlink) Broadband data (350 kbit/s uplink, 700 kbit/s downlink) Voice	Global
Kuiper	Amazon (United States)	3 236	0 %	Broadband from 100 Mbit/s to 1 gigabit per second (Gbit/s)	Area below northern Europe and above Patagonia
OneWeb	OneWeb (United Kingdom)	648	100 %	Broadband (up to 32 Mbit/s uplink, 195 Mbit/s downlink)	Global
Starlink	SpaceX (United States)	4 408	> 74 %	Broadband (up to 250 Mbit/s bidirectional)	Selected areas below Northern polar and above Southern polar regions.
O3b mPOWER	SES (Luxembourg)	11 (MEO)	18 %	Broadband (up to 400 Mbit/s bidirectional)	Area below northern Europe and above Patagonia

⁵ Satellite company's websites in April 2023 and Euroconsult, Quarterly briefing, NGSO constellations, Q4 2022.

Looking at Table 3, it should be noted that not all constellations provide global (i.e. truly worldwide) coverage. A constellation operator devises its business model according to considerations such as (a) covering locations where the market demand is expected to be high and (b) covering locations where the market demand is low, but users are ready to pay premium prices because access to communication capabilities is critical. The service provisioning by a satellite constellation also depends on the landing rights obtained from NRAs. Some constellations provide services to residential end-user terminals while others target commercialisation of capacity towards enterprises only.

In addition to the operators listed above, there are others that deploy constellations targeting message exchange services. Because these low-price services are based on non-real-time low bit rate communications, spacecrafts can be smaller (from several kilogrammes to several tens of kilogrammes), reducing manufacturing and launching costs⁶. It should be noted that while these operators do not have the media coverage of the ones listed above, they are also very likely to be the target of cyberattacks.

Finally, it should be noted that the constellations listed in Table 3 are all commercial systems. However, some of them are also used for military applications, making them de facto dual-use systems.

2.2 THE FINANCIAL DIMENSION OF LEO CONSTELLATIONS

This section covers the financial aspects of building, launching and operating satellite constellations. This information helps to assess the value of the assets in the event of a cybersecurity incident.

The cost breakdown of building and running a satcom constellation is as follows.

- Design and manufacturing cost of the satellites.
- Launching costs.
- Ground facilities (Earth stations, infrastructures, data centres, high data rate links).
- Recurring operations costs and maintenance costs on the ground infrastructures.

The quantitative breakdown varies a lot among all constellations as it depends on the strategy chosen: a lot of small satellites offering little individual capacity or more capacitive and powerful satellites. The total manufacturing and launching costs can exceed EUR 10 billion in case of mega-constellations with several thousands of satellites.

From a business standpoint, these costs are then to be balanced by the revenues from selling the services either directly to end users and enterprises or to resellers (e.g. selling bulk communication capacity). In the case of a cybersecurity incident, the potential impact encompasses the loss of the asset and the loss of the revenues associated with the asset. Taking this perspective, Table 4 gives examples of service prices⁷ for some of the constellations listed in the previous section.

⁶ Monteiro, . and

Table 4: Estimates of service price for several satcom constellations

Name	Services prices
Globalstar	EUR 99/month for a 150-minute call plan EUR 14.95/month for 20 custom messages sent, unlimited predefined messages transmission, unlimited message reception
Iridium	EUR 153 for a 75-minute call plan per month EUR 300/month for a 300 megabyte data plan (Certus service) EUR 35.10/month for 17 kilobytes of short messages
OneWeb	EUR 200/month per connectivity data rate of 1 Mbit/s (trunking service not meant for residential users)
Starlink	USD 5000/month for 100–350 Mbit/s, unlimited data (maritime service and prosumers) Around EUR 70/month (pricing depending on country) for basic service (50–100 Mbit/s best effort, about 250 gigabytes of data volume)
O3b mPOWER	From EUR 100 to EUR 450/month per Mbit/s

To get access to the service, the end user must also procure a terminal. Depending on the form factor and capabilities (possible throughput, antenna technology), the price ranges from several hundreds of euros to tens of thousands.

Looking at the trends, it is expected that by 2031, the market value of the capacity provided by LEO satcom systems will double⁸ compared to 2021, while the market value of capacity available from geostationary High-Throughput Systems (HTS) will increase by a margin.

2.3 COMPARISON TO GEOSTATIONARY SATELLITE COMMUNICATION SYSTEMS

What differentiates LEO and GSO telecommunications systems is summarised below.

- **Lower latency.** Compared to the geostationary orbit, a lower altitude yields shortest propagation delay therefore easing the delivery of services where interactivity is key.
- **Stronger signal.** Similarly, the signal transmitted from the spacecrafts suffers less from free space loss (as a rule of thumb, doubling the travel distance cuts the signal power by four). It can either favour larger throughput or more integrated terminals.
- **More satellite diversity.** A lower altitude leads to a tighter instantaneous service coverage for single spacecraft. It calls for multiple spacecrafts and therefore a more complex space segment. However, the potential coverage of the constellation is then broader than the one of a single geostationary satellite (three geostationary satellites are needed to provide a global coverage between latitudes 80° North and South).
- **More ground infrastructure.** For a similar reason, LEO satcom systems require up to 10 times more earth stations for the ground infrastructure compared to geostationary satellite systems.
- **Smaller antennae and terminals.** When a high throughput (> 50 kbit/s) is required, the relative motion of the spacecraft calls for complex antenna designs (compared to a fixed antenna dish); on the other hand, the lower altitude of the orbit enables smaller antennae and therefore smaller terminals.
- **Lower single spacecraft capacity.** The communication capacity (in bit/s) of a single LEO spacecraft is lower than that of a geostationary satellite, therefore challenging from a financial standpoint throughput-hungry services such as multimedia

⁸ Euroconsult, *Satellite Connectivity and Video Market*, 29th edition, 2022.

broadcasting. In addition to that, the larger coverage of geostationary satellites favours broadcasting.

- **Higher system capacity.** Because multiple satellites are used, the overall capacity (in bit/s) of the constellation is usually higher than the one of a single high-throughput geostationary satellite (several terabits per second vs several tens of Gbit/s)
- **Shorter lifetime.** The lifetime of a geostationary satellite is often rated for 15 years of service. A LEO satellite lifetime can be as low as 5 years, especially if the industrial strategy favours low-cost, low-lifetime spacecrafts over more costly ones.
- **More redundancy.** LEO satcom systems often accommodate for in-orbit spares. This is one of the reasons that achieving high reliability is less costly. Redundancy in geostationary satellite networks can only be achieved through the deployment of several GSO satellites over close (or similar) orbital positions.



3. LEO SATCOM ASSETS AND INFRASTRUCTURES

This chapter covers how a LEO satcom system is organised into different segments, each segment being assigned a role in the delivery of the mission and the control of the system. The discussion will also serve as a foundation for highlighting the engineering and industrial processes supporting the development of such systems and finally highlighting the core technological blocks and the associated supply chain.

3.1 LEO SATCOM SYSTEM ARCHITECTURE

A LEO satcom system is split into three segments.

- The **space segment** includes the satellites forming the constellation. Each satellite comprises a platform and a payload. The payload is the subsystem supporting the mission, the platforms provide all services for spacecraft to behave as expected (e.g. thermal control, power supply, attitude control, etc.).
- The **user ground segment** covers all entities contributing to the delivery of the communications services: fixed and mobile terminals, and the Earth stations called gateways or hubs.
- The **control ground segment** hosts entities contributing to: (a) command and control of the space segment: the Telemetry, Tracking and Command (TT&C) station and the Satellite Control Centre (SCC) and (b) control, configuration, and monitoring of the user ground segment: the Network Operation Centre (NOC). The ground segment makes sure that the mission is conducted within the expected service level objectives.

The **launch segment** is also present, being extensively active at the very start of the system's operational lifetime. While the launch segment is not part of the LEO satcom system, its importance should not be neglected as – in addition to the initial constellation deployment – it also plays a role in placing in-orbit spare spacecrafts. For the sake of completeness, the list of technological domains provided at the end of this chapter also covers the launch segment.

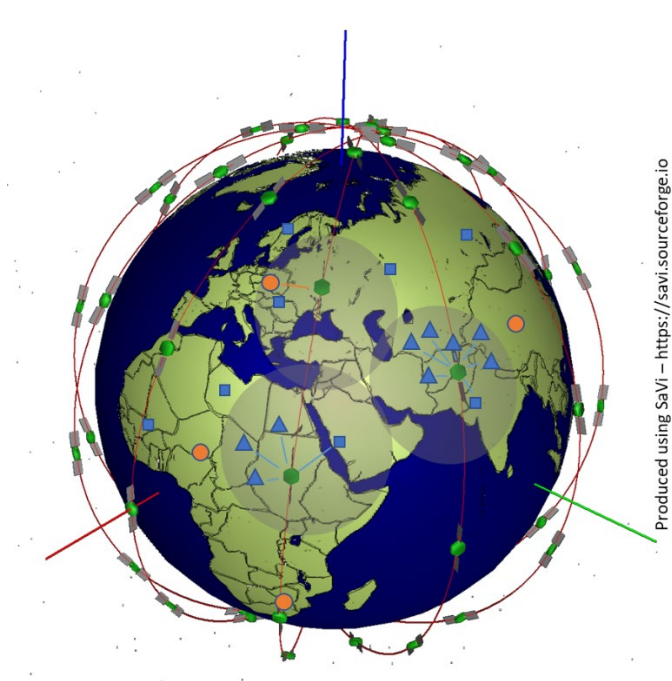
Figure 2 depicts how the space, ground and user segments constitute an end-to-end system.

- The satellites serve the associated terminals under their coverage, acting as relay with the gateway that is visible from the satellite. If inter-satellite links (ISLs) are present, mutual visibility between the terminal and the gateway is not required and ISLs are used to reach a distant gateway.
- User service requests (e.g., a new terminal logged in the network, a terminal issuing a call or data requests) are mapped to the satellite network resources by the NOC. The NOC instructs the gateways and the satellite control centre (SCC) (see below) accordingly.
- The SCC commands and monitors the fleet of satellites by means of several TT&C stations. These stations, on behalf of the SCC, receive telemetry (health information) and send telecommand (configuration and operation orders) to the satellites that are visible. They can also collect information contributing to the accurate localisation of the satellites.

Later in this chapter, the various technologies supporting all these entities will be covered.



Figure 3: Example of RF communication links involving TT&C stations



Geostationary satcom systems are also organised in three segments (space, user and control) and the roles of the different entities are similar. The difference lies in the number of satellites and user/control ground entities and in their distribution over the Earth. LEO satcom systems call for a high number of gateways (e.g. as of Q4 2022 the Starlink constellation features around 160 active gateway sites, each site hosting between 8 and 32 antennae). By comparison, a high-throughput geostationary satcom system may require up to 10 gateways. The same rule applies to the TT&C stations. A typical geostationary satcom will provision for two TT&C stations in active-passive configuration. A LEO satcom constellation should account for a larger number, finding the adequate trade-off between the cost of the ground system and the operability of the constellation. Therefore, it is not uncommon for an LEO satcom constellation to have about 50 % of the Capital Expenditures (CAPEX) dedicated to the ground system.

For remote sensing LEO systems, there is an emerging trend around the concept of Ground Segment as a Service (GSaaS). This approach makes sense when the ground segment is not permanently used (e.g. because of low density of the space segment). For LEO satcom systems that provide 'anywhere, anytime' communications services, the GSaaS concept can be revisited. Indeed, while a gateway antenna cannot be shared among different satellite operators, the upstream devices (modems, computing capabilities, storage) can be.

3.2 ORGANISATION OF SPACE PROJECTS

This section covers the engineering and industrial processes that are involved in the design, development and operations of LEO satcom systems. Because of their human and financial stakes, complexity and often non-recurring schemes, space projects are backed by well-established methodological frameworks. See for example the European Cooperation for Space Standardization (ECSS) ECSS-M-ST-10C standard⁹.

Overall, a project is split into several phases that span the major stages of the system life cycle: (a) early definition and feasibility studies, (b) definition and design, (c) production and testing and (d) utilisation and disposal. The three segments can be considered as different projects

⁹ ECSS, 'ECSS-M-ST-10C Rev.1 – Project planning and implementation (6 March 2009)', 2009.

since they are addressed by different manufacturers. This report will focus on the space segment because it is arguably the most challenging. Moreover, compared to project management for the manufacturing of consumer goods (cars, smartphones, etc.) there are major differences, as listed below.

- From the early design to the beginning of utilisation, up to 10 years can pass.
- A spacecraft is made of thousands of parts, most of these parts coming from suppliers.
- Several thousands of documents are produced during the project lifetime and stored in a document management system.
- The processes for design, production, testing and utilisation are now supported by digital tools forming a consistent and comprehensive suite relying heavily on data management and processing. For example, all satellite telemetry received from the early tests to the Launch and Early Orbit Phase (LEOP) operations and onwards is stored in a data lake.
- Today's satellite manufacturers rely heavily on subcontractors, especially for the production and testing phases.
- Customers (i.e. the operators buying the satellites) participate in most phases of the project. They are based on-premises in dedicated offices, and have access to documentation and to clean rooms hosting the manufacturing, assembly, integration and testing (MAIT) facilities. These clean rooms can also host other projects at the same time.

3.3 TECHNOLOGY AND SUPPLY CHAIN

Table 5 provides a list of technology domains that are used in LEO satcom systems (including the launch segment). The taxonomy refers to the ESA Technology Tree¹⁰ and is also used in Table 6 for the definition for each technology domain. This report only addresses the technology domains pertaining to the scope of telecommunications as defined in the Article 2 of the EEC¹¹. The ESA technology tree also includes two technology domains that are transverse to all segments: (a) system design and verification and (b) quality, dependability and safety. The latter includes aspects such as commercial off-the-shelf components and subsystems.

Table 5: ICT-related technology domains used in LEO satcom systems

Entity/segment	Technology domains
Launch segment / launch vehicle	On-board data subsystem / space system software / space system control / RF subsystems, payloads and technologies / electromagnetic technologies and techniques.
Launch segment / control centre & tracking stations	Space system software / mission operation and ground data systems / ground station systems and networks / electromagnetic technologies and techniques.
Space segment / spacecraft	On-board data subsystem / space system software / space system control / RF subsystems, payloads and technologies / electromagnetic technologies and techniques / flight dynamics and global navigation satellite system (GNSS) / optics.
Ground segment / TT&C station	Space system software / space system control / mission operation and ground data systems / ground station systems and networks / electromagnetic technologies and techniques / optics.
Ground segment / gateway	Space system software / space system control / ground station systems and networks / electromagnetic technologies and techniques / optics.
Ground segment / user terminal	

¹⁰ ESA, *ESA Technology Tree – Version 4.0*, STM-277 3rd edition, ESA Communications, 2020.

¹¹ See Directive (EU) 2018/1972.

Ground segment / network operation centre	Space system software / mission operation and ground data systems / RF systems, payloads and technologies / ground station systems and networks.
Ground segment / Satellite control centre	Space system software / mission operation and ground data systems / ground station systems and networks / flight dynamics and GNSS.

Table 6: Definition of the technology domains (reproduced from the ESA technology tree taxonomy document).

Technology domain	Definition (from the ESA Technology Tree)
On-board data subsystem	Spacecraft data management; payload data processing; hardware and software required for data acquisition, data processing, storage for both payload and spacecraft data, on-board networking and the space-link network layer and above.
Space system software	All basic techniques and technologies in the fields of software and information technology (IT) with respect to their application to space missions, for both space and ground segment.
Space system control	Design and implementation of control subsystems for space applications. Includes attitude and orbit control system (AOCS) for satellites; guidance, navigation and control (GNC) for space vehicles and launchers; and pointing acquisition and tracking systems for antennae, laser terminals, and line-of-sight stabilisation equipment.
RF subsystems, payloads and technologies	All technologies and techniques operating in the RF domain related to satellite systems and networks, spacecraft payloads, instruments and specific ground equipment, for telecommunication, TT&C, navigation, Earth observation and space science, including security aspects. (Technologies for control centres, TT&C and Earth Observation Payload Data Transmission Ground Stations and Ground Station Networks are covered in 'Ground station systems and networks')
Electromagnetic technologies and techniques	Antennas and related technologies, wave interaction and propagation, and electromagnetic compatibility.
Mission operation and ground data systems	Aspects related to the control and operations of space system elements (satellites, transfer vehicles, orbiters, landers, probes, rovers, etc.) and related ground segment, addressing the technologies associated with supporting subsystems and tools.
Ground station systems and networks	All elements and know-how required for the engineering of the facilities that connect the space segment with control centres. The application range covers everything from high-performance deep-space stations to networks of small ground stations.
Flight dynamics and GNSS	Activities related to the analysis and definition of trajectory aspects of space projects, known as mission analysis. All operational ground activities related to the measurement and control of spacecraft orbit and attitude. Provision of precise navigation services to both ground- and space-based users and also the provision of the geodetic reference frame.
Optics	Technologies and techniques for subsystems, instruments and components, as well as design, engineering and verification methods, in the field of optics.

The supply chain also plays an important role in the design, development, and operation of space systems. Here, the supply chain encompasses suppliers of hardware parts (e.g. ground

segment network appliances), subcontract workers (e.g. at the spacecraft assembly, integration, and test facilities) and service providers (e.g. leased line operators for the ground segment).

The supply chain for the space domain faces several challenges.

- As already mentioned, suppliers are extensively involved in all segments.
- Components can be highly specialised, not only because of their role, but also because of the manufacturing constraints regarding the space environment. This negatively impacts the price and reduces the number of suppliers.
- For the space segment, security risk detection or mitigation can only be consolidated while the components are on the ground.

These characteristics call for common and agreed quality and security practices among all stakeholders of the supply chain. They also raise the question of sovereignty and trust for critical components. Finally, they call for automated late testing/auditing when the components are in a controlled environment.

4. SECURITY CHALLENGES FOR LEO SATCOM SYSTEMS AND SERVICES

As described in the prior chapters, LEO satcom systems are complex and associated with high financial risks. The most dominant feature of the investment is that there is almost no exit strategy: once deployment has commenced, the complete constellation configuration needed in order to start services must be brought into use.

This chapter deals with r66 (t)-17 (h)TJ0 p11 554 Tw 0.267ss



4.2 FINANCIAL AND COMMERCIAL RISKS

These risks are related to the non-tangible assets of the organisation, such as reputation or commercial profitability. Investments in satellite communications are high yield / high risk. Securing proper and reliable debt financing is therefore challenging.

Table 8: Financial and commercial risks

Financial and commercial risk	Details	Main associated technical risks
Harm to the company reputation	Satcom services are often considered as 'premium services' either because of their price or because of their positioning on the market. Satellite operations require careful coordination between all space stakeholders (orbits, frequency). Having a reputation for being serious in business often helps the business itself run smoothly.	User service degradation/outage Monitoring and control degradation/outage Data theft, data leak Extraneous asset or service damage/destruction/outage Capability hijacking
Loss of commercial capabilities	Chapter 2 indicates that, to offer a global service, a constellation of satellites is required as well as a set of earth stations. Any impairment to these elements can compromise the delivery of the communication service, leading to financial loss, among other things.	User service degradation/outage Capability hijacking Monitoring and control degradation/outage Asset damage/destruction
Financial loss because of penalties	The provision of satellite communications services is often associated with service-level agreements (SLA). This is especially enforced if the satellite communication service is established as a backup of a terrestrial service. Non-compliance with SLA leads to financial penalties.	User service degradation/outage Extraneous asset or service damage/destruction/outage
Loss/degradation of competitive advantage	The recent developments in New Space have led to an increase in competition between LEO satcom operators. The competition spans from the technical to commercial fields. Therefore, any delay in the time to market or leak of industrial property may lead to the degradation of competitive advantage.	Data theft, data leak Asset damage/destruction Capability hijacking

4.3 MALICIOUS THREATS

All systems are exposed to threats. A threat will resolve into a successful attack when an existing vulnerability is exploited. It is therefore important to know the threats targeting LEO satcom systems and to devise adequate prevention and recovery plans. Table 9 shows a list of malicious threats, which are associated with the technology domains described in an earlier chapter.

This list is inspired by attack matrices such as the European Space Agency (ESA) space attacks and countermeasures engineering shield (SPACE-SHIELD)¹², space attack research

¹² ESA, 'SPACE-SHIELD', ESA website, retrieved May 2023, <https://spaceshield.esa.int/>.

and tactic analysis (SPARTA)¹³ and MITRE ATT&CK¹⁴. Work on the threat landscape has been conducted by various organisations, including academics¹⁵ and the Center for Strategic and International Studies (CSIS)¹⁶. According to the published findings, attack campaigns use the weakest spot as an entry point in the system and exploit (e.g. through lateral movements) a sequence of threats to achieve their goal. Therefore, several threats can be involved in a single attack.

Table 9: Threats of malicious origin

Threats	Short definition and example	Technology domains
Signal/information level threats		
Signal jamming/interference	Transmission of a stronger signal to degrade the quality of a legitimate signal and disrupt its effect (e.g. jamming the telecommand TC uplink) ¹⁷ .	RF subsystems, payloads and technologies, space system control, ground station systems and networks, optics.
Signal spoofing	Forgery of a signal bearing wrong information (e.g. spoofing of GNSS signals to misroute a spacecraft) ¹⁸ .	RF subsystems, payloads and technologies, ground station systems and networks.
Signal replay	Replay of a previous valid signal to trick the receiving entity (e.g. replay of a telecommand) ¹⁹ .	RF subsystems, payloads and technologies, ground station systems and networks.
Signal intelligence	Study of signal characteristics to derive additional knowledge (e.g. reverse engineering of the user downlink signal) ²⁰ .	RF subsystems, payloads and technologies, ground station systems and networks.
Information eavesdropping	Illegitimate interception of information to gain knowledge (e.g. capture of login/passwords when using unsecured remote-access/web protocols) ²¹ .	On-board data subsystems, space system software, ground station systems and networks, mission operation and

¹³ The Aerospace Corporation, 'SPARTA: Space Attack Research and Tactics Analysis', Aerospace website, retrieved May 2023, <https://aerospace.org/sparta>.

¹⁴ MITRE, 'MITRE ATT&CK', MITRE website, retrieved May 2023, <https://attack.mitre.org/>.

¹⁵ Pavur, J., 'Securing New Space: On Satellite Cyber-Security, A thesis submitted for the degree of Doctor of Philosophy, University of Oxford, 2021; Plotnek, J., 'A threat-driven resilience assessment framework and security ontology for space systems', thesis submitted for the degree of Doctor of Philosophy, The University of South Australia, 2022.

¹⁶ CSIS, Bingen, K. A., Johnson, K. and Young, M., *Space Threat Assessment 2023*, Center for Strategic and International Studies, Washington DC, 2023.

¹⁷ Some states have army corps dedicated to electronic warfare including mobile transmitting stations for jamming satellites.

¹⁸ Some LEO satellites rely on GNSS signals for orbit determination.

¹⁹ Signal replay can be used to fool a system protected with authentication if no anti-replay protection is embedded. A TC can then be issued twice (the first time being legitimate), with expected harmful consequences.

²⁰ Characterising an unknown signal (frequency, modulation, and coding schemes) is the first step in gathering intelligence from its source or developing a signal spoofing strategy.

²¹ Information eavesdropping is the first technique used on clear (not encrypted) communication channels to capture sensitive information (e.g. passwords).

		ground data systems.
Information spoofing	Forgery of fake information to fool a user or system (e.g. forgery of an illegitimate command packet to gain access to a spacecraft subsystem). This threat can be part of the subsequent stages of an attack based on an initial threat.	On-board data subsystems, space system software, ground station systems and networks, mission operation and ground data systems.
System/subsystem level threats		
Payload hijacking	Illegitimate use of the satellite (communication) ²² .	On-board data subsystems, space system software, space system control, RF subsystems, payloads and technologies, mission operation and ground data systems.
Platform hijacking	Illegitimate control of the spacecraft platform (e.g. modifying the spacecraft attitude to create service outage)	On-board data subsystems, space system software, space system control, RF subsystems, payloads and technologies, ground station systems and networks, mission operation and ground data systems.
System/subsystem impairment	Interaction with a system/subsystem to create disruption (e.g. blinding of spacecraft star tracker with a laser during a manoeuvre) ²³ .	All
Hardware-/software-level threats		
Physical tampering	Physical interaction with a component to gain an advantage (e.g. physical connection to a spacecraft bus probe point to collect information). This is an example of insider threat. However, physical tampering is not restricted to phases where the spacecraft is on the ground (e.g. in clean room). Some states have developed spacecrafts meant for illegitimate interaction with / inspection of other spacecrafts called rendezvous and proximity operations (RPO)	All
Hardware backdoor	Modification of a hardware component to add/modify functionalities (e.g. a modified	All

²² Some satellites work as transparent RF relays, taking the signal that comes in, amplifying it and sending it back to Earth. With that respect, there is no check as to whether or not the signal is legitimate.

²³ In the most extreme form, it includes the use of anti-satellite kinetic weapons such as missiles. Such destruction will generate additional space debris. The Kessler syndrome depicts a phenomenon where a sudden increase of debris on an orbit may damage other spacecrafts, triggering a chain reaction of destruction.

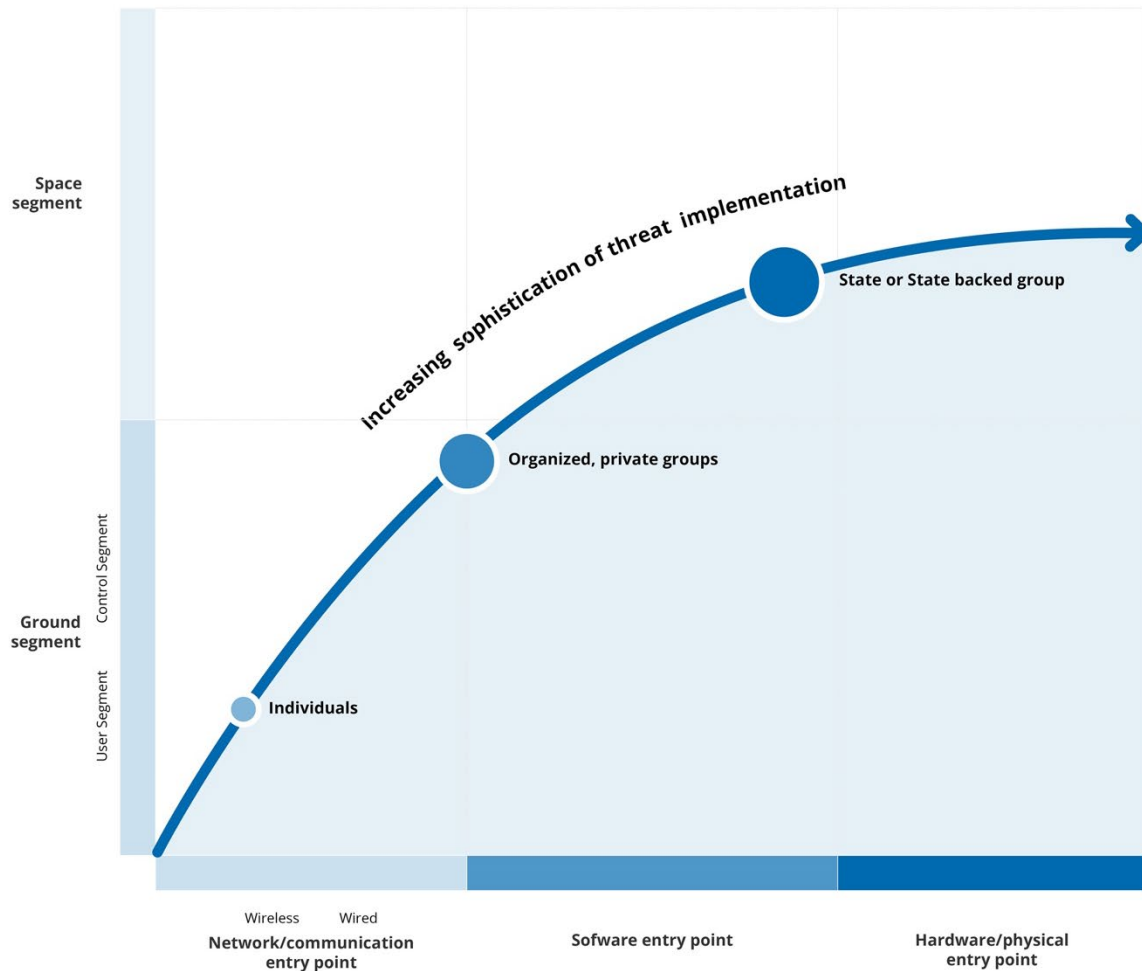
	chipset in a computer to bypass memory read protection). This is an example of insider threat.	
Software backdoor	Modification of a software component to add/modify functionalities (e.g. a network server that receives a specific illegitimate packet will trigger the execution of unwanted code). This is an example of insider threat.	On-board data subsystems, space system software, space system control, ground station systems and networks, mission operation and ground data systems.
Malware injection	Injection of rogue software to conduct illegitimate activities (e.g. injecting a key logger on a control centre computer).	On-board data subsystems, space system software, ground station systems and networks, mission operation and ground data systems.
Privilege escalation	Exploit of a software/hardware weakness to gain undue privileges (e.g. hacking of a modem to bypass transmit power limitations) ²⁴ .	On-board data subsystems, space system software, ground station systems and networks, mission operation and ground data systems.
User-level threats		
Social engineering	Taking advantage of human weakness/credulity/fears to gain information knowledge (e.g. phishing to gain access to remote access credentials).	Ground station systems and networks, space system software, mission operation and ground data systems.
Weak cybersecurity practices by users	Taking advantage of security protections being impaired by users not applying best security practices (weak passwords, sensitive information written out on post-its, etc.).	All.

These threats cover a whole spectrum of attacks that can be conducted against the user/control ground or space segments. Additionally, depending on the threat or the entry point in the asset that is targeted, the level of sophistication required for conducting the attack varies. It also depends on whether best practices of cyber protection have been applied.

Some general trends can be identified. For example, it is easier to attack a ground asset connected to the internet than to get physical access to a spacecraft bus in space. Figure 4 depicts these coarse-grained relations.

²⁴ Privilege escalation (i.e. undue granting of software execution rights) is a threat that also applies to on-board software such as a spacecraft real-time operating system.

Figure 4: Sophistication level of an attack versus entry point



As mentioned in the introduction of this chapter, risks relate to threats through vulnerabilities. There is also a link between the risk exposure and engineering practices, especially in relation to system reliability. For example, if the power supply of a ground system is not guaranteed by means of an Uninterruptible Power Supply (UPS), basic attacks to the power distribution network are likely to result in a denial of service. This is also true in the case of failure of the power grid, showing how reliability engineering and cybersecurity protection share common grounds. These aspects cover all phases of the space project: from design to operations and decommissioning.

Finally, physical security was also not addressed here but has a direct relation to the mitigation of cybersecurity risks. For example, manufacturing facilities with poor physical security are exposed to threats from outsiders and insiders. Launchpads are exposed to sabotage if not physically secured.

4.4 NON-MALICIOUS THREATS

The following figure describes non-malicious threats from the harshness of the space environment, system failures or human error. Such errors can be either operators' mistakes or misconfiguration/bugs in the spacecraft/ground control software, especially for situations that do not happen often or software execution branches that are special or uncommon (e.g. during anomalies). Regardless of their unintentional nature, they yield similar risks as malicious threats.

Table 10: Threats of non-malicious origin

Non-malicious threats	Details	Technology domains
Solar radiation	During high-energy periods of Sun cycles, on-board electronics may get damaged or disrupted. Satellite lifetime may decrease because the Earth atmosphere envelope 'swells' causing unwanted drag on the spacecraft (in some extreme cases, the spacecraft burns in the atmosphere).	On-board data subsystem, RF subsystems, payloads and technologies, electromagnetic technologies and techniques, space system control, mission operation and ground data systems, ground station systems and networks.
Collisions with debris and other space bodies	Debris is the result of former activities in space (launches, collisions, or intentional destruction of satellites). Considering the travel speed of debris and orbiting objects, even the smallest object (e.g. a bolt) has enough kinetic energy to pierce through the wall of a satellite and cause damage. Debris is tracked by several governmental agencies.	Space system control, flight dynamics and GNSS, mission operation and ground data systems.
Collisions with other satellites	Unintentional collision between two spacecrafts can occur (and has occurred) either because one of the spacecrafts is not under control or simply as the result of a human mistake. In addition to the damage it causes, it creates additional debris. The European Space Surveillance and Tracking (EU-SST) ²⁵ cooperation implements a collision warning service dedicated to operators of spacecrafts. Collision avoidance manoeuvres can then be conducted.	Space system control, flight dynamics and GNSS, mission operation and ground data systems.
Miscomputed manoeuvre	Manoeuvres are meant to maintain the spacecraft on its intended orbit. The associated parameters (e.g. thruster activation) are computed on ground before being uploaded on board. A miscomputed manoeuvre (e.g. because it is unusual) may for example cause a service outage because of payload antenna de-pointing.	Space system control, flight dynamics and GNSS, mission operation and ground data systems.
Misconfiguration of the platform	The spacecraft is 'driven' through TCs and flight operation procedures (FOPs). The satellite user manual provides guidance regarding what sort of TCs is allowed based on the current operating state of the satellite. Executing a flight operation procedure that is not compatible with the satellite state may trigger a Fault Detection, Isolation and Recovery (FDIR) mechanism that will autonomously put the spacecraft in safe mode. This often corresponds to a temporary interruption of the current mission and therefore to a service outage.	On-board data subsystem, space system software, RF subsystems, payloads and technologies, space system control, mission operation and ground data systems.
Misconfiguration of the payload	Like the platform, the payload is configured through TCs and flight operations procedures. Payloads with on-board processing are complex (as often found in LEO satcom systems), a misconfiguration can translate into service outage.	On-board data subsystem, space system software, RF subsystems, payloads and technologies, space system control, mission operation and ground data systems.
Non-compliance with radio regulations	Space systems rely a lot on wireless transmissions (often RF). For that reason, international radio regulations enforce a fair share and use of the RF spectrum among all users. Although signal jamming is an example of malicious non-compliance, there are also cases of non-malevolent infringements, such as a	RF subsystems, payloads and technologies, electromagnetic technologies and techniques, mission operation and ground data systems, ground station systems and networks.

²⁵ See <https://www.eusst.eu/>

	malfunctioning device or an incorrect understanding of the radio regulations.	
Launcher failures	Launch failures translate either to the destruction of the spacecraft or to a wrong injection into orbit. In the latter case, the outcome depends on how far the injection orbit is from the planned one. If the difference is too significant, the spacecraft must be decommissioned, otherwise the spacecraft uses its own propulsion subsystem to reach the intended orbit, at the expense of a reduced lifetime (due to reduced propellant available for conducting the mission).	Space system control, mission operation and ground data systems.
Unspecified failures	Spacecrafts are also subject to unexpected failures. The spacecraft design is resilient to some failures using redundant units. In some cases, redundancy cannot help (so-called single point failures without any redundancy), and the failure translates to degraded performance of the platform or the payload (e.g. parts of a solar panel may fail, impairing the overall power budget available to the payload) or a total loss of the spacecraft.	All.

4.5 CYBER INCIDENTS ON LEO SATCOM SYSTEMS

This section describes known cyber incidents that affected LEO satcom constellations. It should be noted that the list of incidents is not long. Because of the very nature of these incidents, not all of them were reported publicly. Providers of public electronic communications networks or of publicly available electronic communications services have the obligation to report cyber incidents to national or European authorities (see the Article 40 of the EEC²⁶). ENISA runs the Cybersecurity Incident Reporting and Analysis System platform (CIRAS)²⁷, where competent authorities submit annual incident reports.

This chapter ends with the description of an attack made on an experimental satellite operated by ESA. The attack – although real – was legitimate and conducted within the frame of research work. For that reason, it is extensively documented and constitutes a good reference for how (illegitimate) attacks could be conducted.

Table 11 lists cyber incidents disclosed publicly that target LEO satcom constellations. Regarding the term ‘incident’, some of these incidents cover actual attacks, while others are public disclosures of weaknesses or engineering details that may be exploited by a malicious third party.

²⁶ As of October 2024, security requirements from ECCC will be replaced by security requirements from the NIS2 directive, which also include mandatory incident reporting.

²⁷ ENISA, ‘Incident reporting – CIRAS’, ENISA website, retrieved June 2023, <https://ciras.enisa.europa.eu/>.

Table 11: Cyber incidents affecting LEO satcom systems, gathered from public sources

Year	Affected system	Threat and risk	Description
2014	Iridium ²⁸	Software backdoor, privilege escalation	Terminal contains hardcoded and undocumented credentials for accessing the terminal management interface. No known attack, could be used to render terminal useless (service outage) or for illicit terminal usage (capacity hijacking).
2015	Globalstar ²⁹	Signal spoofing, information spoofing	Reverse engineering of the uplink waveform to spoof the signal. No known attack, demonstrated application for spoofing an asset tracking signal, obfuscating the ongoing asset theft (extraneous asset theft).
2015	Iridium ³⁰	Information eavesdropping leading to data theft	Reverse engineering of the clear pager channel leading to the ability to eavesdrop on customer messages.
2022	Starlink ³¹	Signal jamming leading to service outage	Repeated jamming of Starlink downlink signals and GNSS signals used by the terminal during set-up.
2022	Starlink ³²	Subsystem denial of service leading to service outage	Denial-of-service attack on an application programming interface (API) taking part in service delivery and leading to service outage.
2022	Starlink ³³	Privilege escalation	Injection of hardware fault on the terminal printed circuit board to gain privileged access to the terminal software. No known attack, could be used to render terminal useless (service outage) or for illicit terminal usage (capability hijacking).
2022	Gonets-M ³⁴	Privilege escalation, leading to subsystem denial of service leading to service outage	Privilege escalation exploit on the ground CRM system, enabling the deletion of a key database used for service delivery.

²⁸ Santamarta, R., 'SATCOM terminals: Hacking by air, sea, and land', Proceedings of the BlackHat US 2014 conference, retrieved June 2023, <https://www.blackhat.com/docs/us-14/materials/us-14-Santamarta-SATCOM-Terminals-Hacking-By-Air-Sea-And-Land-WP.pdf>.

²⁹ Moore, C., 'Spread spectrum satcom hacking: Attacking the Globalstar simplex data service', Proceedings of the Blackhat US 2015 conference, retrieved June 2023, <https://www.blackhat.com/docs/us-15/materials/us-15-Moore-Spread-Spectrum-Satcom-Hacking-Attacking-The-GlobalStar-Simplex-Data-Service-wp.pdf>.

³⁰ Sec and Schneider, 'Iridium hacking – Please don't sue us', Proceedings of the 2015 Chaos Communication Camp, retrieved June 2023, <https://www.youtube.com/watch?v=ahZOGhV8qnc>.

³¹ Laursen, L., 'Satellite signal jamming reaches new lows', IEEE Spectrum website, May 2023, retrieved June 2023, <https://spectrum.ieee.org/satellite-jamming>.

³² Trustwave, SpiderLabs blog, 'Killnet claims attacks against Starlink, Whitehouse.gov, and United Kingdom websites', Trustwave website, November 2022, retrieved June 2023, <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/killnet-claims-attacks-against-starlink-whitehousegov-and-united-kingdom-websites/>.

³³ Wouters, L., 'Glitched on Earth by humans: A black-box security evaluation of the SpaceX Starlink user terminal', Proceedings of the Blackhat US 2022 conference, retrieved June 2023, <https://i.blackhat.com/USA-22/Wednesday/US-22-Wouters-Glitched-On-Earth.pdf>.

³⁴ Bussoletti, F., 'Cyber warfare, Team OneFist hits Russia in space again', Difesa & Sicurezza website, October 2022, retrieved June 2023, <https://www.difesaesicurezza.com/en/defence-and-security/cyber-warfare-team-onefist-hits-russia-in-space-again/>.

2023	OPS-SAT ³⁵	Privilege escalation, leading to hijacking of capabilities	Demonstration from a research team of taking control of the spacecraft by exploiting a bug in the data handler through the sending of specially craft TCs.
------	-----------------------	--	--

The war in Ukraine has caused a surge of attacks on satellite communication systems. Readers interested in space electronic warfare may refer to these sources ³⁶. They cover topics such as: destruction of space assets by means of kinetic or non-kinetic weapons and use of spacecrafts to inspect or malevolently interact with other spacecrafts (RPO: rendezvous and proximity operations).

Case study: an attack on the OPS-SAT experimental satellite

This case study is based on the work from Willbold et al. ³⁷ on on-board software security. One of the case studies addresses the OPS-SAT experimental satellite.

OPS-SAT is a satellite demonstrator based on a 3U-CubeSat platform developed by Graz University of Technology under the auspices of ESA. It was launched in 2019 on low-earth orbit. It takes on board various payloads for Earth observation, RF and optical communications meant to host experiments. Its on-board software is open source and based on commercial off-the-shelf products. In that respect, it is representative of the majority of CubeSats that are launched either by academic institutions or by New Space companies as part of their product development roadmap.

As such, OPS-SAT does not match the scope of this report (i.e., LEO constellations offering communications services). However, its experimental and scientific purpose yields well-documented studies that are illustrative and relevant to the topic of satellite cybersecurity.

By combining experiments and study of the on-board software source code, Willbold et al. followed the steps listed below to take over control of the spacecraft.

1. Search for an entry point in the commanding subsystem of the spacecraft. It turned out that one of the TC channels was configured in clear mode, i.e. not implementing encryption and authentication. The other TC channels were protected.
2. Search for specific TCs that give access to critical functions, such as updating the on-board software or modifying the internal file structure. A weakness was found that combines two elements: (a) such critical TCs bear a special flag, however no extra protection is implemented; and (b) protected and unprotected TC channels ended in the same on-board computer, the latter not checking against the origin of the TC (e.g. protected, or unprotected TC channels).
3. Search for weaknesses in on-board functions that can be invoked from TC. Several weaknesses were found, one of them allowing arbitrary code execution. Such weaknesses are often linked to the lack of protection for memory write operations (e.g. buffer overflow attacks).

³⁵ This entry is not a malicious attack. It is a demonstration from a team of academics. OPS-SAT is a single satellite, not a constellation.

³⁶ CSIS, Bingen, K. A., Johnson, K. and Young, M., *Space Threat Assessment 2023*, Center for Strategic and International Studies, Washington DC, 2023

4. Craft special TC packets that exploit the weaknesses exposed in the previous points and allow the execution of a piece of code that takes control of the spacecraft.

Having a clear TC channel may seem non-representative of real (i.e. commercial) spacecrafts. Surprisingly, it is still common practice for some satellite manufacturers to enable TC channel encryption and authentication only at the end of launch and early orbit phase (LEOP) operations. For geostationary satellites with electrical propulsion, these operations may last for up to 6 months.

One may also object that having open-source software is a major weakness. It triggers the traditional debate about the effectiveness of 'security through obscurity', where not publishing the software sources is thought to increase the product's inherent security. Considering that satellite manufacturing (a) relies on a network of suppliers and sub-contractors and (b) tends to increase the use of off-the-shelf (i.e. not space specific) components, it can be stated that the so-called 'obscurity' is not guaranteed. A safe approach is therefore to not rely on 'security through obscurity' and to implement all required safeguards and best practices. This is the subject of the next chapter.



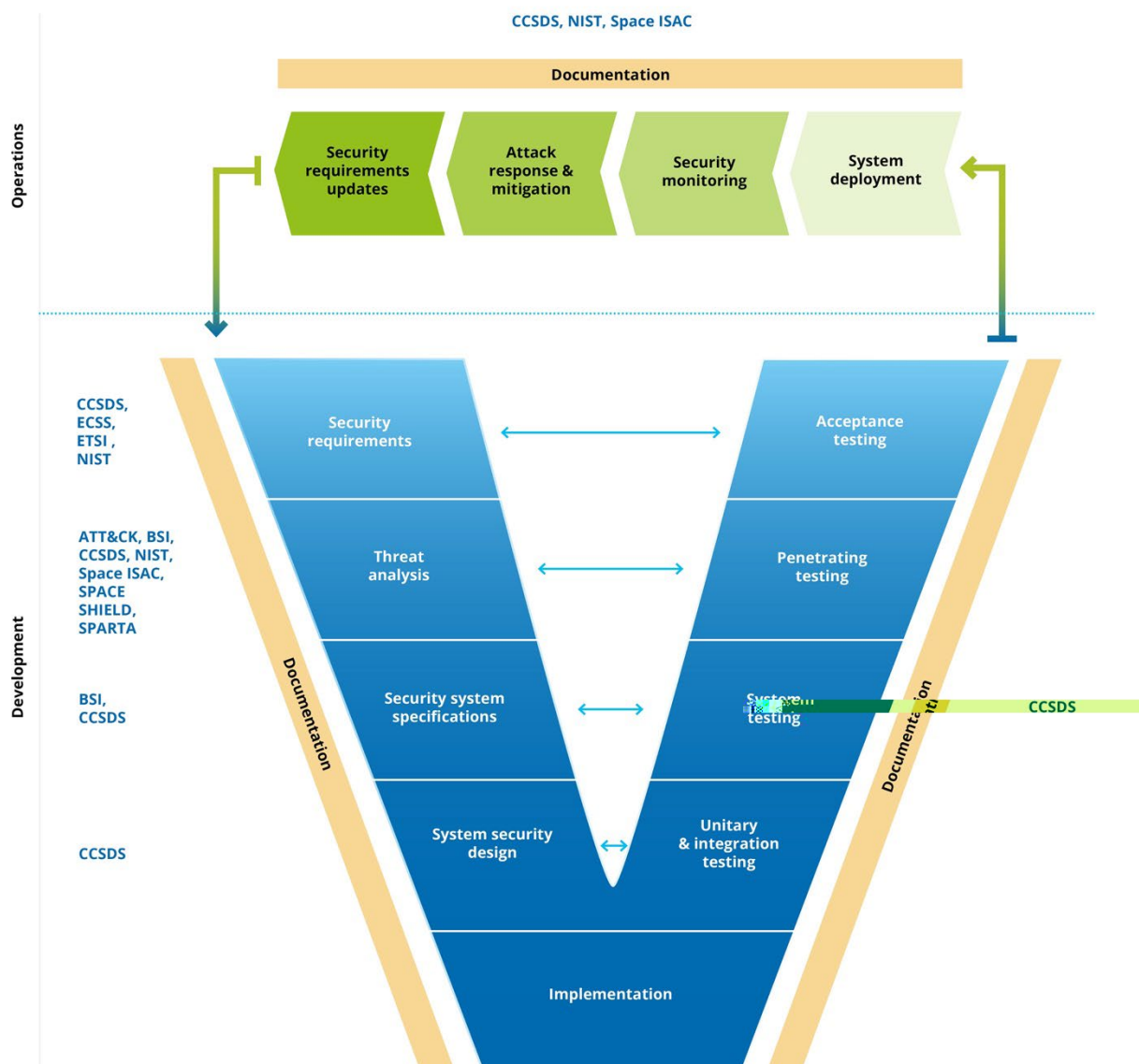
5. STANDARDS AND RECOMMENDATIONS FOR SATCOM CYBERSECURITY

This chapter discusses published standards and existing recommendations for securing satellite systems. Some of these initiatives deal with threat landscape, while others describe best practices for securing a satellite link by means of cryptography. In order to illustrate these different scopes, this report adopts a conceptual view of ‘cybersecurity engineering’ loosely inspired by the well-known ‘V-model’ development life cycle, augmented with operations (Figure 5).

The left part of the V shape depicts the requirements–specification–design trilogy while the right part addresses all the equivalent verification and validation activities. Standards and recommendations identified in the following sections of the chapter are positioned on the figure with respect to their scope.

The chapter ends with an outlook on forthcoming initiatives.

Figure 5: Framework for cybersecurity development and operations



5.1 EUROPEAN COOPERATION FOR SPACE STANDARDIZATION

ECSS standards and handbooks, when applied to commercial satcom systems, mostly refer to project management, manufacturing, testing, launch activities and communications for the control segment. The ECSS documents do not address cybersecurity in a dedicated standard or recommendation, however the topic is mentioned in several documents (see Table 13).

Furthermore, for communications engineering, ECSS relies on the suite of Consultative Committee for Space Data Systems (CCSDS) standards (see the CCSDS section later in this chapter), sometimes further detailing adaptations of a CCSDS standard through an Adoption Notice. See for example ECSS-E-AS-50-25 covering the adoption of the CCSDS TC Space Data Link Protocol, including the use of SDLS (Space Data Link Security) for providing confidentiality, authentication, and integrity.

Table 13: ECCS documents covering security aspects

Document	Document type	Asset and risk addressed	Positioning on system development and operations framework
ECSS-E-ST-10 'System engineering general requirements' ³⁸	Standard	All assets, no specific impact addressed.	Development (testing is cited in the document).
ECSS-E-ST-40 'Software' ³⁹	Standard	All assets, no specific impact addressed.	Development (requirement, specifications, testing). Operations (from security monitoring to security requirements update). Documentation.
ECSS-E-ST-50 'Communications' ⁴⁰	Standard	Assets: control and user segments (links). Risk: capability hijacking and data theft (loss of link confidentiality, integrity and authentication).	Development (requirement, design).
ECSS-E-AS-50-25 'Adoption Notice of CCSDS 232.0-B-4, TC Space Data Link Protocol' ⁴¹	Adoption notice	Asset: control segment (links). Risk: capability hijacking and data theft (loss of link confidentiality, integrity and authentication).	Development (design).

5.2 CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS

The CCSDS is an international forum publishing various documents, including recommended standards ('blue books'), recommended practices ('magenta books') and informational reports ('green books').

Books are identified by a series number, a volume number, a letter code depending on the colour of the book and a version number. Books in the 350, 351, 352, 355, 356 and 357 series cover various aspects of space system security: from threat assessment through security architecture to management of keys for securing data links (Table 14). CCSDS standards have been implemented on hundreds of missions ranging from space probes to experimental CubeSats. Because of this, there are several commercial off-the-shelf products supporting the CCSDS protocols, for both the space segment and the ground segment.

While most commercial satcom system use CCSDS protocols for the command-and-control part of the spacecraft, the user segment often relies on proprietary solutions, and is therefore outside of the scope of standardisation.

³⁸ ECSS, 'ECSS-E-ST-10C Rev.1 – System engineering general requirements (15 February 2017)', 2017.

³⁹ ECSS, 'ECSS-E-ST-40C – Software (6 March 2009)', 2009.

⁴⁰ ECSS, 'ECSS-E-ST-50C Rev.1 – Communications (1 March 2021)', 2021.

⁴¹ ECSS, 'ECSS-E-AS-50-25C Rev.1 – Adoption Notice of CCSDS 232.0-B-4, TC Space Data Link Protocol (13 January 2023)', January 2023.

Table 14: CCSDS documents related to security

Document	Document type	Asset and threat addressed	Positioning on system development & operations framework
CCSDS 350.0-G-3 'The application of security to CCSDS protocols' ⁴²	Informational report	Assets: control and user segment (communication links). Risk: capability hijacking, information forgery and data theft (loss of link confidentiality, integrity, and authentication).	Development (design).
CCSDS 350.1-G-3 'Security threats against space missions' ⁴³	Informational report	All assets. All risks, mostly coming from threats with malicious origin.	Development (threat analysis).
CCSDS 350.4-G-2 'CCSDS guide for secure system interconnection' ⁴⁴	Informational report	Assets: control and user ground segments (IT network interconnections). All risks.	Development (requirements, specifications, design and testing). Operations (all phases).
CCSDS 350.5-G-1 'Space data link security protocol—summary of concept and rationale' ⁴⁵	Informational report	Assets: control and user segment (communication links). Risk: capability hijacking, information forgery and data theft (loss of link confidentiality, integrity, and authentication).	Development (design).
CCSDS 350.6-G-1 'Space missions key management concept' ⁴⁶	Informational report	Assets: all segments. Risks: all risks protected by crypto systems (data theft, capability hijacking and information forgery).	Development (requirements, specifications, design).
CCSDS 350.7-G-2 'Security guide for mission planners' ⁴⁷	Informational report	Assets: all segments. Risks: all risks.	Development (requirements, threat analysis).
CCSDS 350.8-M-2 'Information security glossary of terms' ⁴⁸	Recommended practice	Not applicable.	Not applicable.
CCSDS 350.9-G-1 'CCSDS cryptographic algorithms' ⁴⁹	Informational report ⁵⁰	Assets: all segments. Risks: all risks protected by crypto systems (data theft, capability hijacking and information forgery).	Development (design).
CCSDS 351.0-M-1 'Security architecture for	Recommended practice	Assets: all segments (communication links).	Development (design).

⁴² CCSDS, 'The application of security to CCSDS protocols', *Informational Report*, No 3, CCSDS 350.0-G-3, 2019.

⁴³ CCSDS, 'Security threats against space missions', *Informational Report*, No 3, CCSDS 350.1-G-3, 2022.

⁴⁴ CCSDS, 'CCSDS guide(006 Tc 0.006 Tw Tc 0 Tw 2.433 0 Td04 Tc 0.004 Tw 0.507 0 Td4.0CSurit

space data systems ⁵¹		Risk: capability hijacking, information forgery and data theft (loss of link confidentiality, integrity, and authentication).	
CCSDS 352.0-B-2 'CCSDS cryptographic algorithms' ⁵²	Recommended standard	Assets: all segments. Risks: all risks protected by crypto systems (data theft, capability hijacking and information forgery).	Development (design).
CCSDS 355.0-B-2 'Space data link security protocol' ⁵³	Recommended standard	Assets: control and user segment (links). Risk: capability hijacking, information forgery and data theft (loss of link confidentiality, integrity, and authentication).	Development (design).
CCSDS 355.1-B-1 'Space data link security protocol–Extended procedures' ⁵⁴	Recommended standard	Assets: control and user segment (links). Risk: capability hijacking, information forgery and data theft (loss of link confidentiality, integrity, and authentication).	Development (design).
CCSDS 356.0-B-1 'Network layer security adaptation profile' ⁵⁵	Recommended standard	Assets: control and user segment (links). Risk: capability hijacking, information forgery and data theft (loss of link confidentiality, integrity, and authentication).	Development (design).
CCSDS 357.0-B-1 'CCSDS authentication credentials' ⁵⁶	Recommended standard	Assets: all segments. Risks: capability hijacking, information forgery and data theft (breach of authentication).	Development (design).

5.3 EUROPEAN TELECOMMUNICATION STANDARDS INSTITUTE

The European Telecommunication Standards Institute (ETSI) hosts a technical committee, called Satellite Earth Station, addressing standardisation for space communication systems. ETSI Satellite Earth Station has issued a set of standards for satellite phones (phone handsets communicating by means of satellites) under the common denomination of GEO-mobile radio interface (GMR). The GMR standards (they are called GMR-1 and GMR-2, but are different standards addressing different systems) are used by some geostationary system operators and include provision for encryption at the air interface (i.e. the transmission scheme that is used between the user terminal and the satellite). However, the standards do not specify what encryption algorithm or what authentication scheme to use, leaving it up to vendors. By applying reverse engineering on the firmware of two satellite phones, in 2012 researchers were able to

⁵¹ CCSDS, 'Security architecture for space data systems', *Recommended Practice*, No 1, CCSDS 351.0-M-1, 2012.

⁵² CCSDS, 'CCSDS cryptographic algorithms', *Recommended Standard*, No 2, CCSDS 352.0-B-2, 2019.

⁵³ CCSDS, 'Space data link security protocol', *Recommended Standard*, No 2, CCSDS 355.0-B-2, 2022.

⁵⁴ CCSDS, 'Space data link security protocol–Extended procedures', *Recommended Standard*, No 1, CCSDS 355.1-B-1, 2020.

⁵⁵ CCSDS, 'Network layer security adaptation profile', *Recommended Standard*, No 1, CCSDS 356.0-B-1, 2018.

⁵⁶ CCSDS, 'CCSDS authentication credentials', *Recommended Standard*, No 1, CCSDS 357.0-B-1, 2019.

reveal weaknesses in the implemented encryption algorithms⁵⁷, potentially compromising the confidentiality of voice calls.

Table 15: ETSI GMR-1 and GMR-2 documents related to the security of user data traffic

Document	Document type	Asset and threat addressed	Positioning on system development and operations framework
GMR-1 (ETSI TS 101 376-3-9 V1.1.1) 'GEO-Mobile Radio Interface Specifications; Part 3: Network specifications; Sub-part 9: Security related Network Functions; GMR-1 03.020' ⁵⁸	Standard	Asset: user segment (links). Risks: capability hijacking, information forgery and data theft.	Development (requirement).
GMR-2 (ETSI TS 101 377-2-3 V1.1.1) 'GEO-Mobile Radio Interface Specifications; Part 2: Service specifications; Sub-part 3: Security Aspects; GMR-2 02.009' ⁵⁹	Standard	Asset: user segment (links). Risks: capability hijacking, information forgery and data theft.	Development (implementation).

ETSI also hosts standardisation activities related to the digital video broadcasting (DVB) project. DVB standards (such as DVB/S2) are popular transmission schemes used in commercial satcom systems. Despite the name, DVB standards are also applicable to data-based satcom systems. However, these standards do not specify security mechanisms (e.g. encryption schemes). They are left to the higher layers of the communication stack (e.g. at IP or application level).

5.4 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

The National Institute of Standards and Technology (NIST) is a US agency, originally founded to provide accurate time reference. Nowadays, NIST is involved in standard publications and is the home of the Cybersecurity Framework⁶⁰: 'a methodology to protect individual privacy and civil liberties when critical infrastructure organizations conduct cybersecurity activities'. Using this framework as a baseline, NIST has developed a few cybersecurity guidelines for satellite systems.

⁵⁷ Driessen, B., Hund, R., Willems, C. et al., 'Don't trust satellite phones: A security analysis of two satphone standards', 2012 *IEEE Symposium on Security and Privacy*, 2012, pp. 128–142.

⁵⁸ ETSI, 'ETSI TS 101 376-3-9 V1.1.1 – GMR-1 GEO-Mobile Radio Interface Specifications; Part 3: Network specifications; Sub-part 9: Security related Network Functions; GMR-1 03.020', 2001.

⁵⁹ ETSI, 'ETSI TS 101 377-2-3 V1.1.1 – GMR-2 GEO-Mobile Radio Interface Specifications; Part 2: Service specifications; Sub-part 3: Security Aspects; GMR-2 02.009', 2001.

⁶⁰ NIST, Barrett, M. P., *Framework for Improving Critical Infrastructure Cybersecurity*, 2018.

Table 16: NIST reports addressing security in satellites

Document	Document type	Asset and threat addressed	Positioning on system development and operations framework
NIST IR 8401 Satellite Ground Segment Applying the Cybersecurity Framework, to Satellite Command and Control ⁶¹	NIST Interagency report	Asset: ground segment. Risks: all risks.	Development (from requirements to specifications) and operations covered by five 'functions': identify (assets, threats), protect, detect (attacks), respond, and recover.
NIST IR 8270 Introduction to Cybersecurity for Commercial Satellite Operations (2nd Draft) ⁶²	Draft of NIST Interagency report	Asset: space segment. Risks: all risks.	Development (from requirements to specifications) and operations covered by five 'functions': identify (assets, threats), protect, detect (attacks), respond, and recover.
NIST IR 8441 Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN) – Initial public draft ⁶³	Draft of NIST interagency report	Assets: all segments. Risks: all risks. <i>NB: hybrid satellite networks cover spacecraft that hosts different payload for different missions and virtualised (e.g. cloud-based) ground segments.</i>	Development (from requirements to specifications) and operations covered by five 'functions': identify (assets, threats), protect, detect (attacks), respond, and recover.

5.5 EUROPEAN SPACE AGENCY AND AEROSPACE CORPORATION THREAT FRAMEWORKS

Threat and attack frameworks have already been referenced in Chapter 4 when listing risks and threats. They are recapped in Table 17 and are both derived from the MITRE ATT&CK⁶⁴ framework with elements focusing specifically on space systems.

Table 17: Threat and attack frameworks for space systems

Framework	Comments
Aerospace corporation SPARTA ⁶⁵	Applicable to all space segments. Covers attacks and countermeasures. Has a similar structure to ESA SPACE-SHIELD. Attacks are categorised according to techniques (e.g. reconnaissance, initial access, defence evasion).and the framework also covers risks such as data manipulation, jamming and loss of spacecraft commanding. Initially released in 2022.
ESA SPACE-SHIELD ⁶⁶	Applicable to all space segments. Covers attacks and countermeasures. Has strong links with the work of the Aerospace corporation with SPARTA. Initially released in 2023.

⁶¹ NIST, 'Satellite ground segment – Applying the cybersecurity framework to satellite command and control', *NIST Interagency Report*, NIST IR 8401, 2022.

⁶² NIST, 'Introduction to cybersecurity for commercial satellite operations', *NIST Interagency Report Draft (2nd)*, NIST IR 8270, 2022.

⁶³ NIST, 'Cybersecurity framework profile for hybrid satellite networks (HSN)', NIST IR 8441 (initial public draft), 2023.

⁶⁴ MITRE, 'MITRE ATT&CK', MITRE website, retrieved May 2023, <https://attack.mitre.org/>.

⁶⁵ The Aerospace Corporation, 'SPARTA: Space attack research and tactic analysis', Aerospace website, retrieved May 2023, <https://aerospace.org/sparta>.

⁶⁶ ESA, 'SPACE-SHIELD', ESA website, retrieved May 2023, <https://spaceshield.esa.int/>.

The primary use of these frameworks is to make a systematic inventory of possible threats and attacks during a threat analysis (as shown in Figure 5). However, thanks to the rich underlying information model of these frameworks, they reveal their full power when navigating downstream (from threats to mitigation techniques), upstream or sideways (e.g. among threats sharing a common mitigation). They are fully applicable to commercial satcom systems.

5.6 OTHER INITIATIVES

The German Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* (BSI)) has published two documents that address cybersecurity in satellite systems.

Table 18: BSI guidelines on satellite security

Document	Comments
IT-Grundschutz Profile for Space Infrastructures – Minimum Protection for Satellites Covering their Entire Life Cycle ⁶⁷	The IT-Grundschutz is a methodology for information security management systems. It is compatible with ISO/IEC 27001. This document aims at easing the listing of security requirements during all phases of satellite design, manufacturing and operations (including decommissioning).
Technical Guideline BSI TR-03184 Information Security for Space Systems, Part 1: Space segment ⁶⁸	This document is focused on the space segment. It provides a mapping between business processes (e.g. manufacturing, launch), applications (e.g. software and hardware tools, transport containers), threats and security measures.

5.7 OUTLOOK ON FORTHCOMING INITIATIVES

EU Space Strategy for Security and Defence

In March 2023, the European Commission published the EU Space Strategy for Security and Defence. The topic of resilience and protection of EU space systems and services is addressed notably through the intention to ‘set up an Information Sharing and Analysis Centre (ISAC) to raise awareness and facilitate exchange of best practices among commercial and relevant public entities on resilience measures for space capabilities’⁶⁹.

The implementation of an EU Space ISAC will be backed by the ‘ISAC in Box’ initiative developed by ENISA, aiming to provide ‘as a kit’ all tools, documents and processes needed to set up an ISAC⁷⁰. US-based Space ISAC, founded in 2019 to establish a forum ‘to enhance our ability to prepare for and respond to vulnerabilities, incidents, and threats; to disseminate timely and actionable information among member entities’⁷¹, is also used as an example for the creation of the EU Space ISAC.

The strategy also states that the Commission will consider proposing the creation of an EU

Space Law. The EU recognises space as a 0 Td(US)Tj0 1-2.7 (e2)13.3 (i)-0.7 (S)Tj0 Tc Tw 3.96 0 is.7 (S)Tjt-0.7 (nf)2 e i6 (,)2 ()13.

upcoming Cyber Resilience Act, as well as other existing cybersecurity frameworks, will incentivise the uptake of cybersecurity requirements for critical digital products that are used in space. Specific cybersecurity standards and procedures in the space domain could be considered as part of the EU Space Law where relevant.

A call for space security standardisation

In 2022, a group of space professionals (academics and members of the industry) took the opportunity of the American Institute of Aeronautics and Astronautics Ascend conference to publish a call to action for the standardisation of cybersecurity practices for commercial space systems ('An International Technical Standard for Commercial Space System Cybersecurity – A Call to Action'⁷²). The authors anticipate a move to mass production, driven by a growing demand for space missions, not always from companies that are well established or well acquainted with the space environment. For that reason, the scope of the foreseen technical standard targets modular and commercial off-the-shelf space systems (whatever the segment), including the supply chain.

In February 2023, the Institute of Electrical and Electronics Engineers' (IEEE) Space System Cybersecurity Working Group was created with the following project scope: 'This standard defines cybersecurity controls for space systems including subcommittees for the space/ground/user/link segments and the integration layer.'⁷³

⁷² Falco, G., Henry, W., Aliberti, M. et al., 'An international technical standard for commercial space system cybersecurity – A call to action', American Institute of Aeronautics and Astronautics Ascend conference, 24–26 October 2022, 2022.

⁷³ IEEE, 'P3349 – Standard for space system cybersecurity', IEEE website, retrieved September 2023, <https://standards.ieee.org/ieee/3349/11182/>.

6. CYBERSECURITY STRENGTHS AND WEAKNESSES OF SATCOM IN COMPARISON TO TERRESTRIAL NETWORKS

This chapter elaborates on the commonalities and differences between LEO satcom and terrestrial networks as far as cybersecurity is concerned. It is important to state that – as mentioned later – the comparison is based on a high level of comparable architecture threat and impact analysis and does not consider the actual cyber protection put in place in concrete implementation scenarios. Therefore, this chapter should not be considered as a definitive assessment as to whether one or the other sector is more or less secure.

Before focusing further on cyber aspects, Table 19 describes key differences between space systems and terrestrial systems.

Table 19: Key characteristics of LEO satcom systems compared to terrestrial systems

Key characteristics	Description
Large service coverage	A single satellite at an altitude of 500 km sweeps an area of 2 372 000 km ² (assuming it is visible at least 25 degrees above the horizon). In similar conditions, a telecommunication device placed at an altitude of 100 m 'sees' 4 000 km ² . This has two consequences: (a) terrestrial communication systems require denser infrastructures; and (b) terrestrial communication systems are more dependent on the geopolitical context.
Direct information broadcasting	Because of the large service coverage and the use of RF transmission, the broadcasting of information is easily affordable. While LEO satcom systems are not the best choice for multimedia broadcasting, other use cases exist, such as distribution of network management information. In terrestrial networks, such information broadcasting either requires complex routing strategies or is inefficient from a resource usage standpoint.
High throughput transmission	LEO satcom systems can provide the service throughput they were designed for on every part of the service area at any time. A single satellite has a capacity of at least several Gbit/s, often several tens of Gbit/s that directly connect the service area to the corresponding Earth station. This combination of ubiquity and very high throughput is unique.
High system resilience	Satcom systems display a high level of resilience for three reasons: spacecrafts are less exposed to terrestrial incidents or catastrophes; they are designed to survive failures (see the next paragraphs); and the ground infrastructure is less complex and less distributed. This helps reliability engineering.

These key characteristics are essential in order to tackle the challenges of launching and operating assets in space. These challenges are listed in Table 20.

Table 20: Challenges that satcom systems face

Challenge	Description
Launching capabilities	Satellites rely on launching capabilities to put spacecrafts in orbit. Currently, the most visible New Space ⁷⁴ developments are related to launcher technology, showcasing a decrease in price per mass to launch, reusability of launcher elements, new propulsion systems and new structure material. The Russian war of aggression against Ukraine and the associated ban on some launch services providers has also raised the case of access to space sovereignty.
No servicing possible	Once launched, servicing a spacecraft is (currently) not possible. This has a lot of implications: space-proven technology is usually more costly than the terrestrial equivalent or the performance/price ratio is less favourable. Designs often make use of redundant components, impairing the weight and power consumption. Finally, assembly, integration and testing activities are costly to ensure the required quality. Taking these into account, cost-effective mass production is a challenge.
Harsh space environment	Vacuum, cosmic radiations, 300+ °Celsius thermal variations, vibrations during launch and limited power supply make the space environment hard to reach and harsh to stay in. Spacecraft must be designed

Figure 6: Components making the architectures of LEO and cellular networks

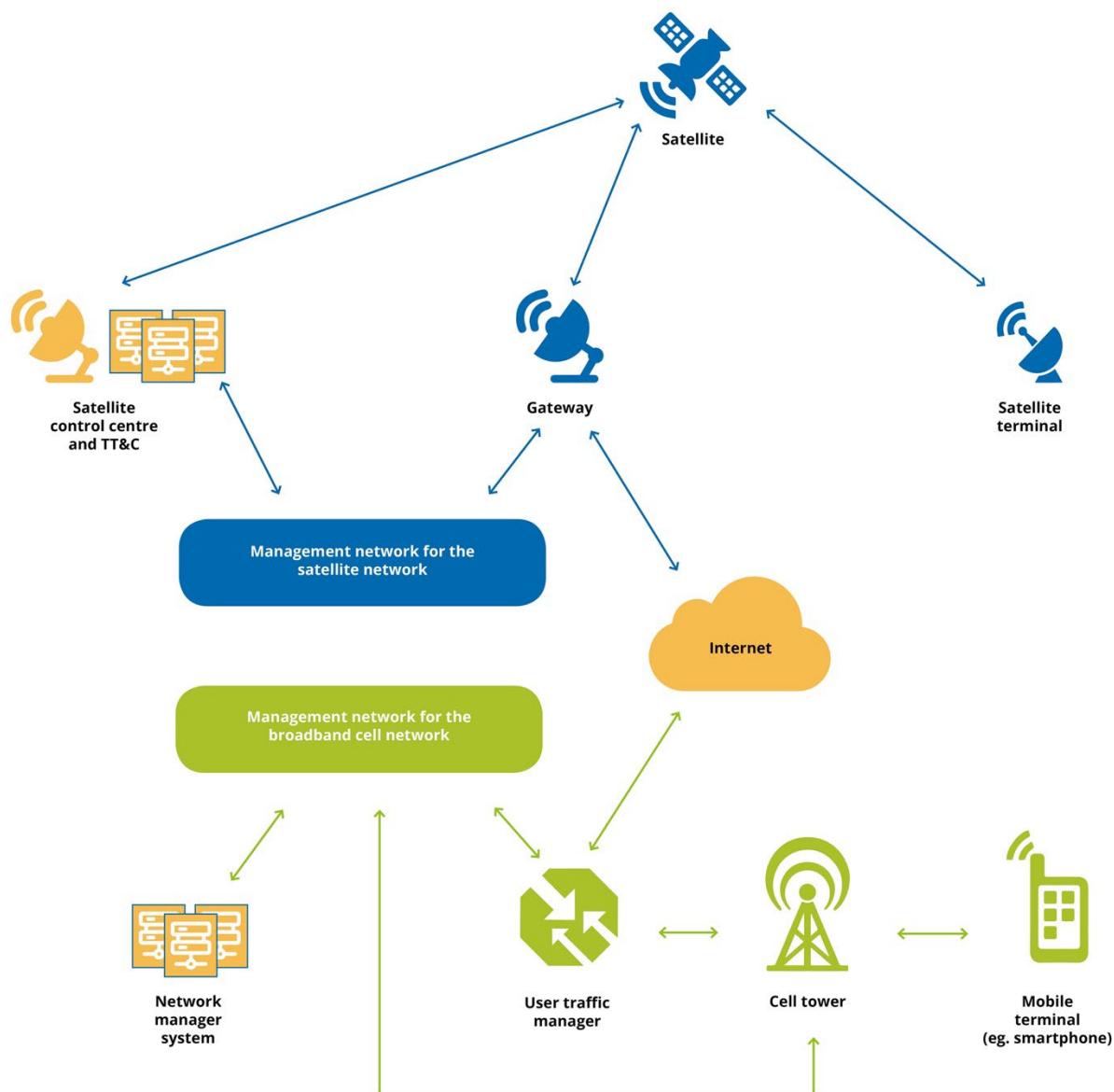


Table 21 details the correspondence between components of the LEO and cellular network architectures. The mapping is based on the coarse-grain functions of each component.

Table 21: Mapping of LEO and cellular networks components based on their function

LEO satcom system	Cellular networks	Coarse-grain function
Satellite terminal	Mobile terminal (e.g. cell phone)	Provisioning of the service to the user
Satellite	Cell tower (e.g. eNodeB in the 4G architecture)	Relay between the terminal and operator's network
Satellite Gateway	User traffic manager (e.g. the Evolved Packet Core in the 4G architecture)	Management of the user traffic within the operator's network and interconnection

		with the internet or other backbones
SCC and TT&C stations	Network management system	Monitoring and control of the network components

The cybersecurity comparison will be built on the concepts of threat and impact. Note that this chapter is not meant to provide an extensive comparison. Rather, the objective is to identify general strengths and weaknesses applicable to LEO satcom systems, keeping in mind the generalisation towards terrestrial systems. For this reason, the following considerations apply when referring to threats and impacts.

- The exposure to threats: is a LEO satcom system more exposed to threats than a cellular broadband network?
- The severity of the impacts: if a threat turns into a successful attack, is a LEO satcom system likely to be more severely impacted than a cellular broadband network?

These elements are covered in Table 22 and Table 23.

Table 22: Comparison of the exposure to threats for components of LEO satcom systems vs cellular broadband networks

Component	Exposure to threats
Satellite terminal vs mobile phone	<p>Both a satellite terminal and a mobile phone are exposed to threats coming from their carrier network (satellite or cellular) or the terrestrial connectivity they are using/offering (e.g. Wi-Fi, Bluetooth or wired LAN).</p> <p>However, compared to a satellite terminal, a mobile phone also hosts third-party applications and offers email and web browsing directly from the phone. For that reason, the surface of exposure to threats is larger. Another consideration is the fierce competition in the phone consumer market leading to frequent product lines renewal. This often impairs the availability of security updates (firmware, operating systems or even the applications) for the older versions of mobile phones.</p> <p>Finally, because of their carry-everywhere nature, phones are much more exposed to risks deriving from crowded places (airports, hotels, train stations), such as physical theft, data theft and capability hijacking. At a more basic level, smartphone users may not follow basic cybersecurity hygiene practices.</p> <p>Satellite terminals, on the other hand, only serve as communication bridges between a local network and the satellite network. End users have few – if any – interactions with terminals apart from the physical connection of cables. The exposed surface is therefore smaller. Software updates for satellite terminals are often pushed ‘over the air’ from the system operator’s facilities.</p>
Satellite vs cell tower	<p>A satellite, because of its location in space, is less exposed to ‘cheap’ attacks (such a destruction through brute force). On the other hand, its design is more complex, increasing the threat surface for attackers that can afford access to satcom transmission technology.</p> <p>Unlike a cell tower, LEO satellites are exposed to a fixed ground attacker for a limited amount of time, during the pass. Attacks requiring longer times (i.e. more than 10 minutes) are therefore less straightforward to conduct or require coordination among multiple attackers.</p>
Satellite gateway vs user traffic manager	<p>Both entities serve the same role: connecting the terminals to backbone networks such as internet (see Figure 6) indirectly through the satellite or the cell tower. For that reason, the surface of exposure is almost similar.</p> <p>There is a disadvantage to the satellite gateway. Satellite links are wireless, so all threats based on signal jamming/spoofing or eavesdropping apply. User traffic managers, on the other hand, are connected to cell towers by means of wired technology.</p>

SCC and TT&C vs network management system	<p>Both entities implement monitoring and control of the system. They are therefore exposed to similar threats, especially those targeting software systems, networks and human operators, all of these being core elements of such systems. It should be noted that, in both cases, the software update policy should be considered as early as during the system design. The objective is to balance the difficulty of software maintenance on mission-critical systems and the need to have up-to-date software.</p> <p>In addition, because monitoring and controlling the satellite is done through TM/TC wireless links, it opens the door to additional signal threats (jamming, spoofing, eavesdropping), like the ones of the satellite gateway.</p>
---	---

Table 23: Comparison of the impact severity for components of LEO satcom systems vs cellular broadband networks

Component	Severity of the impacts
Satellite terminal vs mobile phone	<p>In the case of a successful attack on a satellite terminal, the impact is likely to be more severe than for a mobile phone for two reasons:</p> <ul style="list-style-type: none"> satellite communications are often used for critical missions requiring a high availability figure; satellite terminals are deployed in remote areas, possibly making servicing or replacement more complicated.
Satellite vs cell tower	<p>If a satellite is compromised (vs a cell tower), the impact will be much higher. The two major reasons are:</p> <ul style="list-style-type: none"> the value of the asset (millions of euros); the inherent difficulty of diagnosing and fixing a satellite located thousands of kilometres away.
Satellite gateway vs user traffic manager	<p>As with the prior element, the disadvantage is on the space system side. Having a failed gateway decreases – at least temporarily – the overall system capacity. There are several reasons for this.</p> <ul style="list-style-type: none"> The redundancy factor (how many spares for a working unit) of gateways is less than the cellular broadband networks, mostly for cost reasons. Less redundancy means less resilience to outages. Recovery operations on the space system are more complex and possibly not automated. They may require reconfiguration of the satellites' payload and processing strategy. <p>On the other hand, satcom systems that feature ISLs can rely on the ISL to divert the traffic from the failed gateway to another one. While this improves failure resiliency, it also increases the load on the ISLs, possibly at the expense of low-priority users.</p>
SCC and TT&C vs network management system	<p>Both components for space and terrestrial networks are based on software, IT and communication networks. They also share commonalities in terms of location, implementation, and resilience strategies.</p> <p>An SCC also relies on TT&C stations for transmitting commands and receiving telemetry to/from the satellites. It raises the question of what the impact of losing a TT&C station is. Contrary to gateway antennae, bringing down a TT&C station has less impact on the overall command and control capabilities. Other TT&C stations can take over without compromising the global command and control capabilities.</p> <p>For this reason, there is no significant difference in terms of impact on the SCC and the network management system.</p>

Summarising these two tables, one can say the following.

- Since LEO satcom systems rely heavily on wireless links (terminal to spacecraft, spacecraft to gateway and uplink and downlink of command and control), their threat exposure is generally higher than that of cellular broadcast networks. Regarding the terminal, mobile phones also run third-party applications, e.g. web browsing or email services; therefore, their surface exposure to attacks is expected to be higher.
- The impact of a successful attack on a LEO satcom system is more severe than what can be observed on a cellular broadcast network. This statement relies on two facts: first, the price of a satcom assets is higher; second, spacecrafts or remote terminals, because of their isolated location, are more difficult to diagnose or fix.

Note that the presented analysis does not infer the actual security of a specific real-world system, space or terrestrial. The actual security of each system depends on a wide range of aspects, including but not limited to the risk factors and implemented cyber protection measures. Therefore, this report is not making a judgment as to whether one type of system is more secure than another, but only points out where possible larger security issues exist in satcom in comparison to terrestrial networks.

7. CONCLUSIONS

This report addresses the topic of cybersecurity for constellations of LEO satellites delivering publicly available electronic communications services. To some extent, it also covers space communications systems in general.

The in-depth and extensive study of cyber protection for space systems is a recent concern despite decades of computer crime and countermeasures having been observed on terrestrial systems. One of the reasons for this is the assumption that space is less exposed to cybersecurity threats because it is demanding to reach (both technically and financially) and usually reserved to governments and specialised companies.

Several trends prove that this assumption is wrong, the following among them.

- Access to space is now easier and cheaper than before, with the strong development of new and more affordable launch services.
- The strong development of the New Space transforms space into a business market for private companies (including startups) delivering new and innovative services.
- Commercial off-the-shelf components are now favoured – when possible – over custom or specifically developed components for space. Retro-engineering and in-depth technical analysis is then easier to conduct.
- The development of some large space systems calls for extensive supply chains: the wider the supply chain, the more difficult it is to secure.
- Industrial engineering and operations must be optimised to sustain the pressure of competition: time and cost to market work against long engineering cycles (including extensive testing).
- Cybercriminals now have easy access to advanced technology (e.g. software defined radio) and information: this increases the number of potential threat actors and attack vectors.
- Rendezvous and proximity operations (RPO) ⁽⁷⁵⁾ are now a reality, compromising the simple belief that space is a safe place.

The need for a coordinated approach in space systems security is clear and calls for standards, recommendations, information sharing and training.

- When devising space systems, security requirements must be integrated into the early phase of the project and be subject to the same processing as other requirements, assessing the cost vs benefit of cyber protection. It calls for a comprehensive risk analysis also covering the potential impact on other, neighbouring systems.
- From an industrialisation perspective, the former point would benefit from the organisation of integrated (manufacturer and customer) teams to handle the topic of cybersecurity. Because devising cybersecurity is a matter of trade-off and lacks a truly integrated approach, this will lead to over-specification of the cybersecurity features, severely impairing the cost-effectiveness and operability of the system. The actual implementation of such integrated teams could be the subject of standard and recommended practices.

⁷⁵ A spacecraft approaches another spacecraft for inspection or more aggressive behaviour.

- On the topic of standards and recommendations, there is a need to further develop this activity across two dimensions.
 - A system dimension, encompassing the space segment but also the variety of missions (Earth observation, broadband telecommunications, IoT connectivity, etc.), considering how specific these missions are.
 - A European dimension. Because cybersecurity has strong links with sovereignty and state-specific regulatory aspects, these standardisation activities must be conducted as close as possible to the states where they are applicable. This will guarantee the best match and applicability.
- Finally, there is a need to ensure an overlap between cybersecurity and space engineering skills. There must be enough practitioners knowledgeable in both fields to ensure that cybersecurity requirements are properly taken into account during the early phases of space product development and beyond.



ABOUT ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at 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 978-92-9204-649
doi:10.2824/317096