2023/ISSUE 1

EUSPA Secure SATCOM

Market and User Technology Report

#EUSpace

EUSPA
European Union Agency for the Space Programme

More information on the European Union is available on the Internet (http://europa.eu).
Luxembourg: Publications Office of the European Union, 2023

Catalogue number: TS-03-23-438-EN-N
ISSN: 978-92-9206-076-3
doi: 0.2878/961897

2023/ISSUE 1

EUSPA Secure SATCOM

Market and User Technology Report

#EUSpace

EUSPA
European Union Agency for the Space Programme

Dear Reader,

The space industry is rapidly evolving as we enter a new era – also in satellite communications. New frequency bands, the demand for High-Throughput Satellite (HTS) Systems, and the rise of optical communications and quantum encryption techniques, have spurred the development of novel products, software and applications. Agile New Space players are embracing these trends to develop services benefiting diverse users in both public and private sectors.

Secure satellite communications (henceforth secure SATCOM) are essential for the resilience and strategic autonomy of the European Union and its Member States, both in space and on the ground. Secure SATCOM provide the basis for security- and safety-critical missions and operations, including crisis management, land and border surveillance and protection of the key infrastructure.

The European Union is working on the deployment of GOVSATCOM, a component already part of the EU Space Regulation (2021[1]), while preparing the ground for the ambitious IRIS[2], the new EU Secure Connectivity Programme. Those systems will complement the EU Space Programme and its components for Navigation (Galileo and EGNOS), Earth Observation (Copernicus) and Space Situational Awareness.

In this context, EUSPA produced the **first-ever Secure SATCOM Market and User Technology Report**. The report addresses the market component of the Secure SATCOM, both in terms of industrial and governmental landscape and its forecasted use in the period 2025–2040, as well as its technology component.

The **market part** offers a comprehensive review of various Secure SATCOM use cases across its three macro-families: Crisis Management, Surveillance and Key Infrastructure. We forecast that the demand for Secure SATCOM services should grow by a factor of 14 over the 2025–2040 period, to reach almost 190 Gbps in 2040. While Crisis Management accounts for almost half of the total capacity demand of secure SATCOM in 2025, we estimate that the Key Infrastructures should generate a higher level of demand during the period 2030–2040. This is driven by increased demand for institutional/diplomatic communications as well as the need for reliable, secure and guaranteed communications for a variety of other infrastructures, including energy and finance, governmental digital platforms and the overall increase of strategic data centres.

The **technology part** provides an overview of the technologies currently shaping the industry. It identifies key trends such as the introduction of software-defined satellites, the deployment of new satellite constellation systems in low Earth orbits, the increased capacity offered by High-Throughput Satellite (HTS) Systems and higher frequency bands, optical communications, the deployment of multi-orbit and multi-band terminals and 5G interoperability.

Recent geopolitical tensions at the borders of our continent have spurred demand for secured, robust and uninterrupted SATCOM. Therefore, this report underscores the added value of space-based secure connectivity for authorized governmental users in their relevant fields. It aims at assisting stakeholders in identifying business opportunities, laying the groundwork for market development, and realizing the benefits of secure communications initiatives, both in the EU and globally.

Happy reading!
Rodrigo da Costa,
EUSPA Executive Director

[1] EUR-Lex – 32021R0696 – EN – EUR-Lex (europa.eu)

How to read this report

The European Union Agency for the Space Programme (EUSPA) welcomes all readers to this first issue of the Secure SATCOM Market and User Technology Report. As the first edition, this report marks EUSPA's entry into the realm of secure SATCOM. With its diverse array of reports, EUSPA comprehensively covers all components of the EU Space Programme (GNSS, Earth Observation and now also Secure Satellite Communications), therefore providing valuable insights into the dynamic landscape of space technologies and services.

Secure SATCOM provides one or two-way reliable, accessible and guaranteed satellite capacity/service for communications (cf. definition in Annex 2). This specialized facet operates within the broader SATCOM domain, sharing similar space-based systems and involving equivalent actors along the value chain. As such, technological and economic trends that affect SATCOM also exert influence on secure SATCOM, establishing a logical correlation.

The secure SATCOM market is structured in 13 use cases, sorted into 4 categories, as follows: Surveillance (Land, Border and Maritime), Crisis Management (Maritime Emergency, Humanitarian Aid, Civil Protection, Law Enforcement Interventions, EU (European Union) External Actions and Forces Deployment), Key Infrastructure (Transport Infrastructures, Space Infrastructures, Institutional Communications and Other Critical infrastructures) and secure communications in Polar regions. Users of the EU secure SATCOM services are the governmental entities from European Union Member States, European Union agencies & organisations and are located in the European Union or deployed worldwide.

The Secure SATCOM Market and User Technology report is structured as follows:

- A general overview presents the EU Space Programme, addressing its components: Galileo, EGNOS (European Geostationary Navigation Overlay Service), Copernicus, GOVSATCOM (GOVernmental SATellite COMmunications) and SSA (Space Situational Awareness), as well as the IRIS^2 (Infrastructure for Resilience, Interconnectivity and Security by Satellite). A specific focus in this report is put on GOVSATCOM IRIS^2 and their synergies with the other components. This report specifically highlights how GOVSATCOM today and IRIS^2 tomorrow, will position themselves for the provision of secure SATCOM services to eligible governmental users.
- Delving further into the characterisation of secure SATCOM, the core of the report lies within the **Secure SATCOM Market Demand** section, which includes:
  - An overview of the SATCOM market value. Given that secure SATCOM is an integral component of the broader SATCOM domain, the aim is to underscore the primary trends shaping the value of the secure SATCOM market.
  - An estimate of the secure SATCOM capacity demand, **by eligible EU governmental users**, with a forecast covering the 2025–2040 period for the three use case categories.
  - A specific analysis to assess a set of Key Performances Parameters (KPP).
  - A presentation and characterisation of several pertinent use cases, encompassing: Key stakeholders, Interconnected units and Secure SATCOM utilization, Demand dynamics and motivators, Trends and Geographic scope.
- Following the examination of the demand aspect, the report proceeds to analyse the **Secure SATCOM Market Supply**, from both governmental and commercial entities providing insights into potential developments spanning the period 2025 to 2040.
- Finally, a detailed end-to-end secure SATCOM system containing ground, space and user segments is presented in the Secure SATCOM Technology section. The aim is to help the potential users to grasp and establish a connection between the technical characteristics of the SATCOM services and their significance. Key technological factors, as well as drivers and inhibitors and Cybersecurity elements are addressed to present the technology evolution in the near and upcoming future. It's important noting that, as the satellite communication market is in constant evolution (e.g. new entrants, evolution and consolidation of existing players, etc.) the information contained in this report is provided as-is and might not fully capture recent developments.

TABLE OF CONTENT

Executive summary

The **European Union** needs **independent, secure, resilient and high-speed space-based connectivity** to satisfy the needs of European Union institutions, bodies, agencies and Member States. **Secure SATCOM** provides one or two-way reliable, accessible and guaranteed satellite capacity/service for communications.

The first edition of the **Secure SATCOM Market and User Technology Report** provides insights into the varied contributions of secure SATCOM across a range of governmental applications. These applications are categorized into **three distinct use case categories:** Surveillance, Crisis Management, and Key Infrastructure. Collectively, the report explores a total of **13 comprehensive individual use cases**. Unless specified, the report addresses aspects related to the secure SATCOM market and user technology in the European Union (EU), though some considerations (e.g. economic and technological trends) also applyied at a global level.

Relying on those 13 use cases, the **demand for secure SATCOM for EU and its Members States is estimated to significantly increase over the 2025–2040 period**, moving from 19 Gbps in 2025 to 186 Gbps in 2040 (CAGR of 16% – Compound Annual Growth Rate). The demand will come from a variety of assets and organisations who are estimated to benefit from the provision of services and capacities from **GOVSATCOM** and in a later stage, the **EU Secure Connectivity Programme IRIS²**. Two types of satellite communication services are typically provided: MSS (Mobile Satellite Services) and FSS (Fixed Satellite Services), which use of different frequency-bands. FSS were initially designed for fixed users, while MSS were designed for mobile users. However, due to technological advancements, FSS serves effectively to cater the mobile users, resulting in blurring the boundaries between FSS and MSS. FSS satellite capacity demand is estimated to represent the largest part of the anticipated traffic, most likely addressed via Ku-band, Ka-band and X-band. Traffic for the Crisis Management use case category is estimated to represent almost 50% of the total demand over the 2025 – 2040 period, primarily driven by the demand expected to support Forces Deployment. From a geographical perspective, about two-thirds of the FSS capacity demand comes from the EU continent & waters, followed by Middle East & Africa. The future use of secure SATCOM solutions will also be contingent upon the future supply. In particular, the level of demand, and in practice consumption of secure SATCOM will depend on the capacity and solutions being **offered to end users** in the observed period. Factors such as service type, volume, cost, and the availability of suitable user terminals with appropriate interoperability, affordability and easily deployable, are pivotal in shaping consumption.

The supply of secure SATCOM capacity/services can rely on the **expertise and world-renowned excellence** of the European space industry in the satellite communications sector, integrating the know-how of leading industrial players, such as manufacturers, launch service providers, satellite distribution partners, satellite operators/service providers with the dynamism of an **emerging New Space ecosystem**. Secure SATCOM capacity can be provided to end-users via both **EU governmental systems and EU commercial companies**.

Capacity from geostationary satellites is available and forecast to remain available in all major frequency-bands being used to support voice and data streams, enabling various applications. Such capacity is limited in certain locations (especially outside European Union) and might be not sufficient to cover the whole aggregated expected demand.

Capacity from assets located in NGSO (Non-GeoStationary Orbit) is currently available from an EU company through a single constellation of satellites operating in MEO (Medium Earth Orbit), in Ka-band, whose services are planned to be enhanced in 2023. While third countries have unveiled government-backed initiatives, the **multi-orbit constellation IRIS²** shall complement and integrate the existing and future capacities of the GOVSATCOM component of the European Union Space programme for the provision of secure satellite communications.

The secure SATCOM market is impacted by **the global SATCOM technology trends**. The deployment of HTS/VHTS (Very High Throughput Satellites/Systems) and the deployment of NGSO constellations contribute to significantly increasing the volume of capacity available. This additional capacity will lead to **more cost-effective solutions for end-users**. Among key technical factors, the development of multi-orbit/multi-band terminals could facilitate further the adoption of secure SATCOM by end-users. Secure SATCOM systems need also to be protected against different types of threats (such as cyberattacks) to guarantee a reliable service.

THE EU SPACE PROGRAMME

© EUSPA

Chapter Summary

This chapter introduces the EU Space Programme and its various components in the four major domains: Navigation, Earth Observation, Satellite Communications and Space Situational Awareness. It shows how these components aim to meet the European needs and challenges in different areas, such as the economy, climate, and security. This chapter helps to understand the current and future prospects of EU Space Programme and its impact on Europe and its economy. The chapter covers the following topics:

- Three operational pillars of the EU Space Programme: Galileo & EGNOS (European Geostationary Navigation Overlay Service), Copernicus and SSA (Space Situational Awareness). It describes their benefits, challenges, and importance for monitoring and protecting the space environment.
- The GOVSATCOM programme component, which is dedicated to providing secure and cost-effective satellite communication services for governmental users, via pooling and sharing of existing space assets. It outlines its objective, scope, governance, users, and system elements.
- IRIS^2 system will boost EU satellite-based connectivity, establishing the Union Secure Connectivity programme. It will ensure reliable, secure and cost-effective global satellite communication services to government authorised users as well enable services to commercial users with the aim to remove communication dead zones and foster European competitiveness and societal progress.
- The synergies between the different components of the EU Space Programme and how they can enable innovative and integrated solutions for various applications.

Overview of the European Union Space Programme

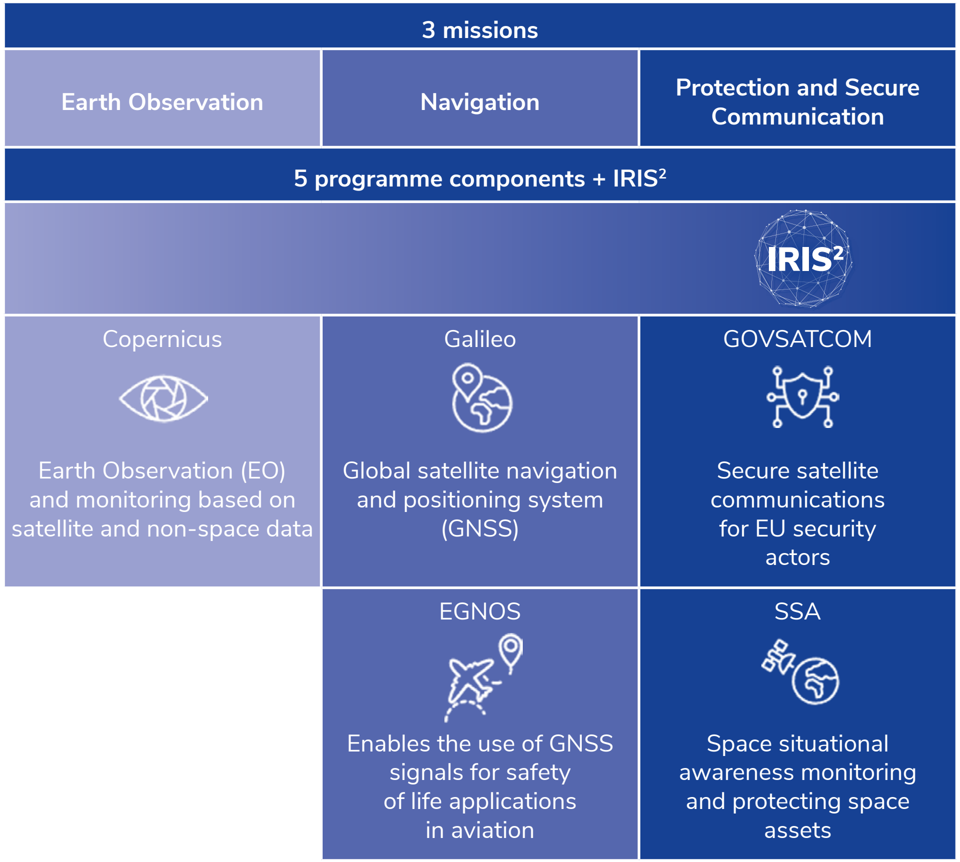
The European Union Space Programme aligns with Europe's core priorities. It contributes to achieving the European Green Deal's climate neutrality goals, advances renewable energy, and promotes a circular economy. The EU's commitment to innovation, resource efficiency, and resilience supports the digital transition, enhances competitiveness, and reinforces Europe's global standing[1].

EU Space Programme Overview[2]

The EU Space Programme embodies a multi-dimensional approach with three pivotal missions: Earth Observation, Navigation, and Protection and Secure Communication. It is composed of five integral components:

- Through **Copernicus**, it empowers comprehensive Earth Observation, and monitoring based on satellite and non-space data for environmental and societal benefits, making it the world's foremost provider of space data and information.
- **Galileo** is the European Global Satellite Navigation and Positioning System (GNSS), enhancing satellite positioning and navigation accuracy.
- **EGNOS** enhances satellite positioning and navigation accuracy by enabling GNSS signals for safety-of-life applications in aviation.
- Protection and Secure Communication are bolstered by the **GOVSATCOM** component delivering secure satellite communication services to EU authorised actors and delivers rapid support over crisis areas.
- The **Space Situational Awareness** initiative strides the European Union forward in comprehending and navigating the complex celestial environment, bolstering the EU's ability to monitor and ensure the safety and sustainability of space activities.

In addition to those five components, the **IRIS²** initiative has been recently added to complement the secured SATCOM component of the EU Space Programme. It aims to offer secure, reliable and cost-effective satellite communication services for authorized government users, and commercial services



3 missions

Earth Observation

Navigation

Protection and Secure Communication

5 programme components + IRIS²

IRIS²

Copernicus

Earth Observation (EO) and monitoring based on satellite and non-space data

Galileo

Global satellite navigation and positioning system (GNSS)

GOVSATCOM

Secure satellite communications for EU security actors

EGNOS

Enables the use of GNSS signals for safety of life applications in aviation

SSA

Space situational awareness monitoring and protecting space assets

[1] European Commission, 2022. EU Legislative Priorities for 2023 and 2024: Joint Declaration of the European Parliament, the Council of the European Union and the European Commission.

[2] European Commission, 2022. Eu Space Programme Overview.

SATCOM types and definitions[1]

SECURE SATCOM (Secure Satellite Communications)

Secure SATCOM is defined as satellite-based, one or two-way communication capacity/service that is able to provide reliable, accessible and guaranteed satellite capacity/service for communications.

It can be provided with any type of frequency band, by GOVSATCOM, COMSATCOM, MILSATCOM players.

<table>
<tr><th>GOVSATCOM
(Government Satellite Communications)</th><th>MILSATCOM
(Military Satellite Communications)</th><th>COMSATCOM
(Commercial Satellite Communications)</th></tr>
<tr><td>GOVSATCOM are highly assured SATCOM offering a certain robust security level with some resilience. GOVSATCOM systems are generally considered less protected than MILSATCOM systems, but offer a higher degree of protection with respect to COMSATCOM systems.
GOVSATCOM encompasses the communication services specifically tailored to meet the needs of governmental entities, as defined in the working document of the European External Action Service of 15/03/2017[2]. This involves the deployment of satellite communication systems to ensure reliable, secure, and resilient communication for government operations, including defence emergency response, public safety, and diplomatic communication.</td><td><b>MILSATCOM</b> is a highly protected and guaranteed SATCOM, offer, generally provided by military systems, offering highly assured and protected satellite communication capacity, both in terms of nuclear hardening, anti-jamming/dazzle capacity and highly secure Telemetry, Tracking, and Command (TT&C), supplemented by an equally robust and resilient ground segment. The security and technology are highly specific and largely sovereign in nature. Those MILSATCOM systems are primarily designed for military purposes and are under national control.</td><td><b>COMSATCOM</b> refers to SATCOM capacity and service provided on the global open market, generally with a degree of ‘on-demand’ access. These services encompass a wide range of sectors, including telecommunications, broadcasting, internet access, maritime communication, aviation, and more.
COMSATCOM systems contribute to global connectivity and information dissemination.</td></tr>
<tr><td colspan="3">These diverse categories of SATCOM collectively form a holistic satellite communication ecosystem, where secure, governmental, military, and commercial functionalities synergistically meet to address communication requirements across various domains. Public authorities, including military forces, have harnessed satellite communications from both publicly owned satellites and market-procured services.
The concept of furnishing satellite communication services for governmental purposes is commonly categorized into three tiers, each representing distinct levels of information assurance, although the precise definitions of these tiers may slightly differ. Progressing from commercial SATCOM to MILSATCOM signifies an elevated security threshold for the provided SATCOM service. This transition embodies an enhancement in security provisions.</td></tr>
</table>

[1] SATCOM categories definitions are, together with other notions, provided in Annex 2.

[2] Council of the European Union. 2017. Cover Note: High Level Civil Military User Needs for Governmental Satellite Communications, March 22nd.

EU GOVSATCOM programme

Towards the EU GOVSATCOM initiative

In 2013, following the Treaty of Lisbon's establishment of the EU Space Policy, as a shared competence between the EU and Member States, the European Council endorsed the preparation for the next generation of GOVSATCOM through collaboration among Member States, the Commission, the European Space Agency (ESA), and the European External Action Service (EEAS). Addressing the need for secure European space capabilities, the 2016 EU Global Strategy emphasized integrated conflict and crisis approaches, recognizing the critical role of satellite communications in defence, security, humanitarian aid, and emergencies.

The GOVSATCOM programme component aims to support the establishment of cutting-edge, secure satellite communication capabilities for governmental and security-related applications. This includes tailoring cost-effective solutions, enhancing market communication, and driving the growth of a competitive, innovative downstream industry. In particular, it will nurture innovation, entrepreneurship, and start-ups in line with its mission to boost technological autonomy, reinforce security, and foster a vibrant EU space ecosystem.

Objective of the EU GOVSATCOM programme

The GOVSATCOM program aims to achieve three primary objectives[1]:

- Consolidate capacities, services, and users for better geographical coverage and efficiency, capitalizing on civil-military synergies, and minimizing duplication.
- Enhance the European Union's strategic capacity for civil protection and humanitarian actions both within Europe and globally.
- Establish cost-effective solutions that ensure secure and readily available communication tools for EU governmental security and defence entities.

Secure SATCOM builds upon the groundwork set by the GOVSATCOM initiative by utilising its established framework, infrastructure, and principles to offer enhanced and reliable secure communication solutions.

GOVSATCOM users

GOVSATCOM users include Union or Member State public authorities as well as authorized individuals which are entrusted with tasks relating to the supervision and management of emergency and security-critical missions, operations and infrastructures (Art. 65 of the EU Space Regulation[1]). They require reliable, remote communication for emergencies or disrupted situations. GOVSATCOM will provide both military and civilian responders with the following usage[2]:

- **Crisis Management:**
  - Guaranteed communication services facilitating audio/video interaction.
  - Data exchange between teams in the field, with their rear bases and with their command & control centres.
- **Border and Maritime Surveillance:**
  - Near real-time distribution of sensitive information from surveillance platforms and sensors to border and maritime surveillance agencies.
  - Connectivity between EU authorities, national authorities and mobile patrols.
- **Key Infrastructure Management:**
  - EU Member States' diplomatic networks with an access to reliable and secure SATCOM independent from the hosting state, anywhere in the world.
  - Key infrastructure managers with appropriate communication services when these are critical to their activities.

GOVSATCOM is also expected to be a key enabler for the implementation of security-related services in the Polar regions, the operation of Remotely Piloted Aircraft Systems (RPAS)/ communication with their onboard sensors and Machine-to-Machine communications for applications where security is at stake.

[1] Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme

[2] European Commission, DG DEFIS. 2021. GOVSATCOM Overview.

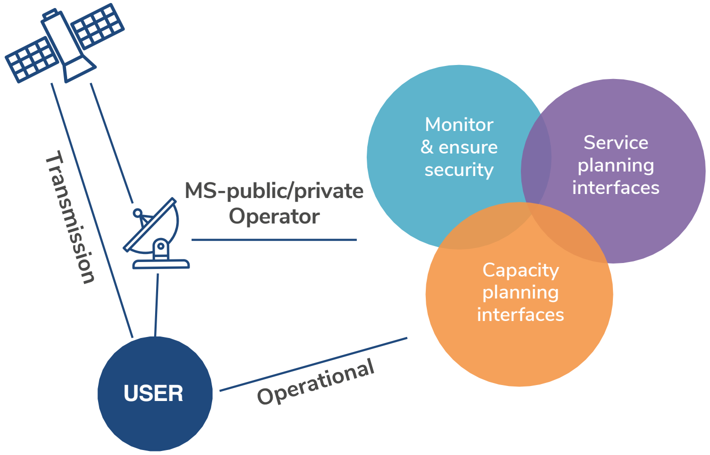
GOVSATCOM Hub and EUSPA

Security constitutes a significant facet within the GOVSATCOM Hub. The proposed long-term solution for the GOVSATCOM infrastructure prioritises robustness and relevant technology to meet stringent security requirements. This infrastructure acts as the operational interface, seamlessly connecting GOVSATCOM users with providers of secured satellite communication capacity and services. This Hub not only manages resource planning but also supports vigilant security monitoring. Its crucial role encompasses accessing resources from diverse national and commercial SATCOM sources, each possessing unique proprietary interfaces and varying security levels. This approach ensures that security considerations are integral to resource procurement and compliance with applicable provisions.

Focus on GOVSATCOM Hub[1]

GOVSATCOM services will be accessible through a Hub, which will **connect users with providers**, optimizing the available resources and guaranteeing access, even in unpredictable situations. The recent Implementing Act issued in May 2023 outlines the GOVSATCOM Hubs' functionalities and operational aspects[2]. This EU-owned Hub will incorporate all central functions to organise and manage demand and supply, and implement standardisation, security and governance. While aggregating the users' demands, it will combine and link different satellite and ground infrastructure capacities into a system-of-systems approach. Based on redundant systems located in secured and protected sites, the GOVSATCOM Hub will be in charge of monitoring and ensuring the overall capacity and service planning as well as the security of the overall system.

Secure GOVSATCOM Hub in operation


Transmission
MS-public/private Operator
Monitor & ensure security
Service planning interfaces
Capacity planning interfaces
USER
Operational

The GOVSATCOM Hub[1]

EUSPA is preparing the design and the development of the infrastructure for the GOVSATCOM Hub through a multi-stage procurement process, and, depending on the availability of a hosting facility – will proceed with its operational deployment and with an upgrade for scalability and connectivity purposes.

EUSPA is also in charge of the coordination of the GOVSATCOM network of users, with the aim to voice the user perspective and regularly assess the market trends and associated demand. **EUSPA has been leading the ENTRUSTED initiative**, which aimed to:

- Set-up a network of governmental users of secure satellite communication services.
- Foster exchange of experience, developing know-how and creating training and awareness content material.
- Establish a consolidated and prioritized set of user requirements across the addressed use cases.
- Create a long-term roadmap and coordination plan for Research & Innovation activities in the domain of user technologies.
- Prepare for the uptake of secure GOVSATCOM services.

[1] European Commission, DG DEFIS. 2021. Factsheet "How it works", April 27th.

[2] Commission Implementing Decision (EU) 2023/1053 of 30 May 2023 laying down rules for the application of Regulation (EU) 2023/588 of the European Parliament and of the Council as regards operational requirements for governmental services provided under Union Secure Connectivity Programme and its service portfolio.

IRIS² system will boost EU satellite-based connectivity

IRIS² background

The EU socio-economic standards are adapting to digital transformation amidst rising geopolitical and cybersecurity challenges. Global satellite communication coverage represents a **strategic infrastructure with dual-use implications**. In the EU's satellite communication sector, a landscape characterised by robust competition prevails, as global operators deploy expansive satellite constellations to cater to consumer connectivity demands. Additionally, both Russia and China have unveiled government-backed initiatives for worldwide space infrastructure, aligned with a diverse range of strategic connectivity goals. Within this context:

- The President of the European Commission (EC) emphasized secure connectivity in her 2020 State of the Union. The October 2020 European Council conclusions urged digital sovereignty and industrial alliances, including for secure networks[1].
- In 2021, a study by a consortium of prominent European space and connectivity players assessed investment options for a new secure, sovereign satellite connectivity system. This system aims also to bolster the EU‘s existing GNSS and Earth observation capacity.
- Following the Proposal for a regulation released by the European Commission in 2018, the formal initiative to establish an EU governmental satellite communications capability was approved through Regulation 2021/696[2] and funded under the 2021 – 2027 Multiannual Financial Framework (MFF). This legal framework sets common rules to all the components of the Space programme, including Galileo, EGNOS, Copernicus, GOVSATCOM and SST, setting out certain rules that are specific to each of these components.

A Call for Tender was issued by the EC in 2021, entitled ***New Space solutions for long-term availability of reliable, secure, cost-effective, and space-based connectivity***[3]. The objective was to support the definition of the system architecture of an innovative EU space-based global secure connectivity system.

On the 15th of February 2022, the European Commission proposed a Regulation of the European Parliament and of the Council establishing the Union Secure Connectivity programme for the period 2023 – 2027[4], with the objective to develop a sovereign secure space-based connectivity system for the provision of satellite communication services to governmental and commercial users.

On the 20th of March 2023, the Regulation (EU) 2023/588 entered into force, establishing the Union Secure Connectivity programme for the period. As described in the regulation, the general objectives of the Secure Connectivity Programme are to:

- **Ensure** secure, autonomous, high-quality, reliable & cost-effective satellite governmental communication services to government authorised users.
- **Enable** commercial services, or services offered to government-authorised users based on commercial infrastructure at market conditions.

[1] European Commission, 2021. Inception Impact Assessment for the Establishment of an EU Space-based Global Secure Connectivity System.

[2] Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme.

[3] European Commission, 2021. New Space Solutions for Long-term Availability of Reliable, Secure, Cost Effective Space Based Connectivity 2021/S 137-363804 Contract notice Services.

[4] European Commission, 2022. Proposal for a Regulation of the European Parliament and of the Council establishing the Union Secure Connectivity programme for the period 2023–2027.

IRIS^2 will complement and expand the GOVSATCOM service portfolio

IRIS^2 and GOVSATCOM

The release of the Regulation (EU) 2023/588, establishing the Union Secure Connectivity programme for the period 2023–2027[1], describes the relationship between GOVSATCOM programme and IRIS^2:

- The provision of the IRIS^2 governmental services shall complement and integrate the GOVSATCOM component into the secure connectivity system.
- IRIS^2 shall complement and integrate the existing and future capacities used in the framework of the GOVSATCOM component including the GOVSATCOM ground segment infrastructure, which is to be scaled up, in particular the GOVSATCOM Hub.
- IRIS^2 and GOVSATCOM capacities and services listed in the service portfolio, would be jointly pooled and shared through the GOVSATCOM Hub.

GOVSATCOM services

The GOVSATCOM service portfolio shall consist of the following categories of communication services[2]:

- **end-to-end services**, allowing the user to connect to a network capable to provide services.
- **anchored capacity services**, allowing the user to use satellite capacity and associated anchoring station facility.
- **raw capacity services**, allowing the user to use satellite capacity (bandwidth).

The GOVSATCOM services shall be provided through the GOVSATCOM hub infrastructure. Definition of GOVSATCOM services is complemented by the Sharing and Prioritisation Implementation Act[3].

IRIS^2 services

The system implementing the Union Secure Connectivity Programme shall be designed to provide or enable the following satellite communications services:

- The following services offered to **governmental users based on the governmental infrastructure:**
  - Service #1: Robust Worldwide Low-latency Service.
  - Service #2: Space Data Relay.
- The following services offered to **governmental users based on the commercial infrastructure:**
  - Service #3: Assured Worldwide Low-latency Service.
  - Service #4: Assured Worldwide Narrowband Service.

[1] Regulation (EU) 2023/588 of the European Parliament and of the Council of the 15th of March 2023, establishing the Union Secure Connectivity programme for the period 2023-2027.

[2] Commission Implementing Decision (EU) 2023/1054 of 30 May 2023 laying down rules for the application of Regulation (EU) 2021/696 of the European Parliament and of the Council as regards the service portfolio for the Governmental Satellite Communications services offered by the system established under the Union Space Programme.

[3] Commission Implementing Decision (EU) 2023/1055 of 30 May 2023 setting out the rules on the sharing and prioritisation of satellite communication capacities, services, and user equipment to fulfil the function referred to in Article 66(2) of Regulation (EU) 2021/696 of the European Parliament and of the Council

IRIS^2 missions & use cases: guarantee provision of secure SATCOM services

A reliable, secure and cost-effective governmental communication service

© Unsplash

Connecting key infrastructures

© Unsplash

Crisis Management and external actions

© Unsplash

Surveillance

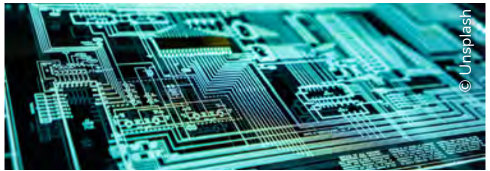
IRIS^2 is designed to enhance governmental communication services, ensuring reliability, security, and cost-effectiveness through a comprehensive set of use cases. Among these, this report primarily focuses on **three pivotal categories:** connecting key infrastructures, crisis management and external actions, as well as surveillance.

Additionally, the program addresses commercialization aspects, including a mass-market service, and gradually integrate EuroQCI (Quantum Communication Infrastructure) for encryption capabilities. This innovative initiative bridges critical infrastructures, facilitates strategic crisis responses, extends connectivity to key regions, and empowers secure communication, heralding an era of **comprehensive and adaptable governmental communication solutions**[1].

© Unsplash

Allow Mass-Market Service

- Mobile Broadband
- Fixed Broadband
- Satellite Trunking for B2B (Business to Business) services
- Satellite access for transportation – for ships, airplanes, drones, connectedcars
- Reinforcement of terrestrial networks (resilience) – asanalternative incases of disruptive events
- Cloudbased services


© Unsplash

Encryption Capability

- Government and institutional users
- Data centres
- Satellite communication networks
- Terrestrial communication networks
- Banking industries
- Other industries

IRIS^2 Infrastructure

The IRIS^2 infrastructure shall comprise a multi-orbit constellation system. The IRIS^2 infrastructure will be composed of two components to serve both governmental and commercial services[2]:

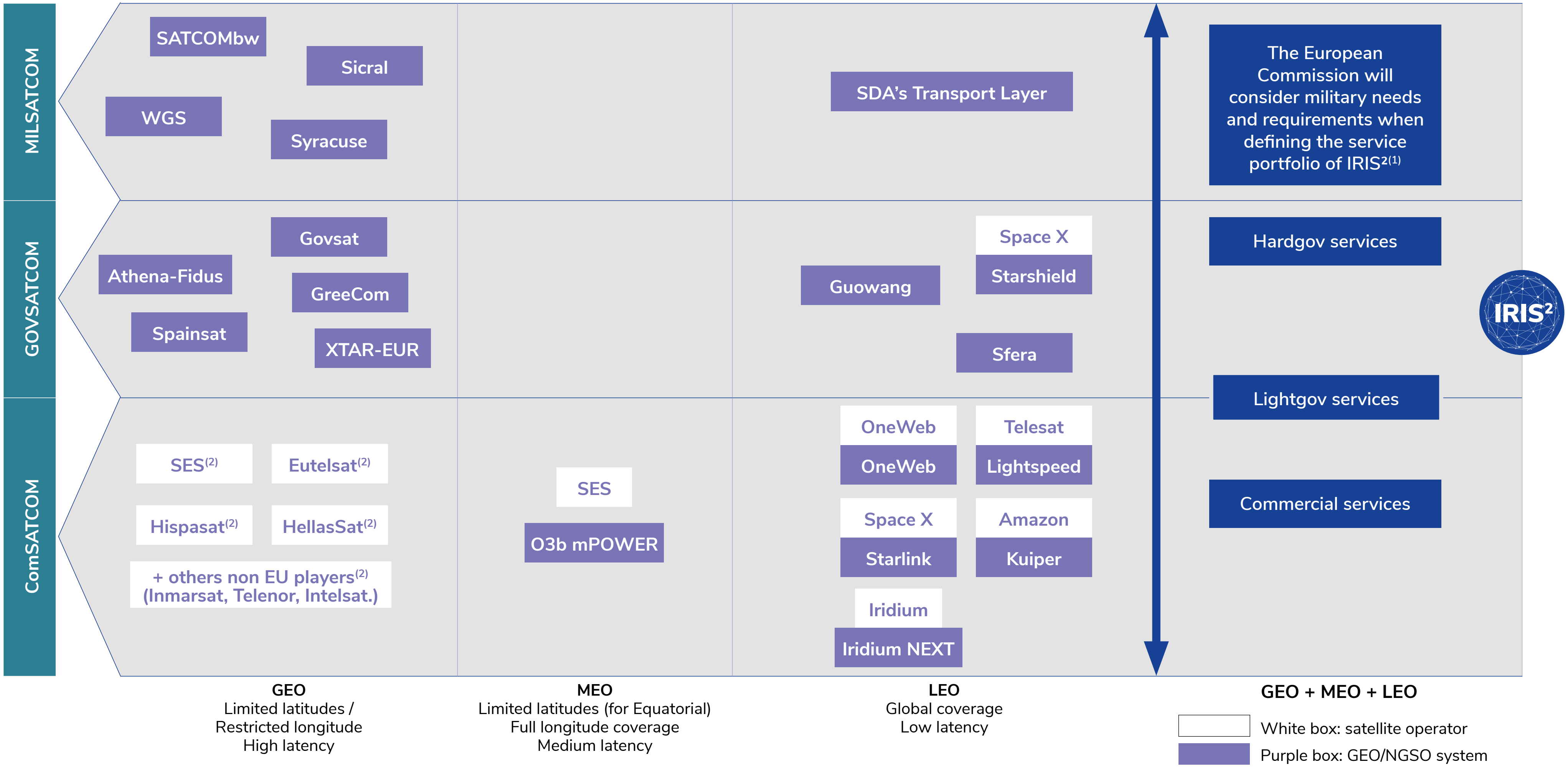
- Governmental infrastructure, called “hard gov”, (whose assets would be owned by European Union) dedicated to deliver strengthened governmental services.
- Commercial infrastructure, called “light gov”, (not owned by the European Union) able to provide services to governmental users and commercial services.

[1] European Union, 2023. Factsheet: Iris²: Infrastructure for Resilience, Interconnectivity and Security by Satellite, March.

[2] European Commission, 2023. IRIS² Industry Information Day, March 30th.

IRIS^2 SATCOM market analysis

The table below presents the positioning between IRIS^2 with respect to a selection of GEO/NGSO constellation systems. The list of GEO/NGSO constellation systems is not exhaustive and mainly focus on NGSO high-throughput for FSS systems. It is also worth mentioning that the position of the GEO/NGSO systems in each box does not illustrate a potential ranking. IRIS^2 is a multi-orbit constellation (LEO, MEO, GEO) able to serve COMSATCOM, GOVSATCOM and MILSATCOM market segments. IRIS^2 will be able to fill the gap that space powers are pursuing.



	GEO Limited latitudes / Restricted longitude High latency	MEO Limited latitudes (for Equatorial) Full longitude coverage Medium latency	LEO Global coverage Low latency	GEO + MEO + LEO
MILSATCOM	SATCOMbw Sicral WGS Syracuse		SDA's Transport Layer	The European Commission will consider military needs and requirements when defining the service portfolio of IRIS^2[1]
GOVSATCOM	Govsat Athena-Fidus GreeCom Spainsat XTAR-EUR		Space X / Starshield Guowang Sfera	Hardgov services IRIS^2 Lightgov services
ComSATCOM	SES[2] Eutelsat[2] Hispasat[2] HellasSat[2] + others non EU players[2] (Inmarsat, Telenor, Intelsat.)	SES O3b mPOWER	OneWeb / OneWeb Telesat / Lightspeed Space X / Starlink Amazon / Kuiper Iridium / Iridium NEXT	Commercial services

□ White box: satellite operator

▨ Purple box: GEO/NGSO system

■ Dark blue box: IRIS^2

[1] European Commission, 2023. European Union Space Strategy for Security and Defence, March 10th

[2] For those satellite operators, we mean that satellite fleet can be used to provide satellite communications services.

Synergies between the different components of the EU Space Programme

The establishment of EU Space Programme not only enhances the synergies combining various EU space components data and services, the potential for governmental users becomes even more significant, as it amplifies their diverse components of the EU Space Programme but also **reinforces the collective impact at both system and user level** capability to **revolutionize daily operations and processes**. This convergence of Secure Satellite Communications with Navigation and Earth Observation services and data empowers applications, making them more contextually relevant and profoundly transformative.

The upcoming pages demonstrate a selected array of applications that provide a glimpse into how the constituent parts of the EU Space Programme, coupled with their corresponding data and services, can collaboratively empower these endeavours.

Smart emergency response vehicles serve as a critical asset for first responders, such as civil protection, ambulance services, and fire & rescue teams.

The application integrates **SATCOM** to establish seamless connectivity for emergency response vehicles. Additionally, SATCOM becomes imperative when terrestrial networks are unavailable. SATCOM technology enables real-time monitoring of emergency operations, fostering effective communication among response teams and coordination centres.

Earth Observation plays a crucial role in updating maps of affected areas. When incidents cause infrastructure damage, such as collapsed bridges or inaccessible roadways, EO data provides accurate and up-to-date information for informed decision-making and navigation.

Advanced **GNSS** technology equips these vehicles with precise positioning and navigation capabilities. This dual-purpose feature enhances emergency response efficiency by ensuring accurate route guidance. GNSS facilitates fleet tracking and management functionalities, optimizing resource allocation and coordination efforts.

© Pixabay

Management of refugee camps focuses on the efficient administration of refugee camps, providing essential humanitarian support to displaced populations.

SATCOM technology empowers refugee camps with resilient broadband connectivity. This robust connectivity facilitates access to substantial data volumes, enabling camp administrators to efficiently share information.

Earth Observation data is harnessed to optimise camp management. It assists in planning camp layouts and distributing essential resources like wells and medicine. By displaying settlement concentrations and estimating population density across different areas of a camp, EO supports informed decision-making for resource allocation.

© Pixabay

Synergies between the different components of the EU Space Programme (continued)

Coordination of Health, Medicine Response, and WASH (Water, Sanitation and Hygiene) Actions addresses the coordination of health, medical responses, and Water, Sanitation and Hygiene initiatives during disasters.

SATCOM ensures consistent and reliable communication for telemedicine and telehealth services. By utilising two-way telecommunications technology, healthcare expertise can be shared remotely through multimedia and computer networks.

Earth Observation contributes by providing detailed maps of affected areas, including post-event effects. It also allows population counting.

© AdobeStock

Maritime Surveillance and Ship Detection centres: creation of a comprehensive situational overview for maritime surveillance. It involves the integration of data from diverse sources, including coastal stations, satellite imagery, specialized aircraft, and patrol vessels.

SATCOM technology addresses challenges in joint operations that arise from non-interoperable communication systems. Secure SATCOM specially allows to exchange images and videos among different types of assets (surveillance aircraft, patrolling vessels, and command centres), providing a solution to communication issues with standardised and inter-operable communications means.

Maritime surveillance utilises both EO components, radar and optical imagery for monitoring activities and ship detection. Spaceborne Synthetic Aperture Radar (SAR) is particularly valuable due to its ability to image day and night, and through cloud cover; and to identify ships (including those not utilising the AIS, Automatic Identification System).

GNSS plays a vital role in precise tracking and monitoring of maritime activities, aiding in the effective management of shipping lanes and maritime borders.

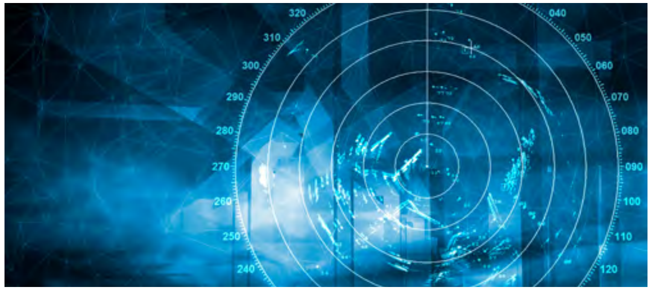
© Pixabay

Law Enforcement Assets Monitoring focuses on the management of fleets of ships, vehicles and aircrafts utilised by law enforcement and emergency services to enhance reactivity.

SATCOM is integrated with terrestrial networks and gap filler technologies. This combination establishes communication links between transports and central information centres.

Earth Observation data offers general weather information (especially when ships and aircraft are used) and infrastructure status, helping to mitigate risks of accidents and minimize impact, especially in emergency management scenarios.

GNSS is utilised for outdoor location services. These systems, combined with indoor technologies, expand location services into tunnels and ensure continuous and available positioning.



© AdobeStock

Synergies between the different components of the EU Space Programme (continued)

Reduction of Illegal Poaching of Protected Wildlife Species targets the mitigation of wildlife trafficking, encompassing the illicit trade, poaching, and collection of endangered species.

SATCOM enables the collection of data collected from distributed sensors, and networks, allowing to identify suspicious activities in sensitive areas. AI-enhanced camera networks (AI– Artificial Intelligence), connected via SATCOM to operations centres, facilitate real-time monitoring of parks and reserves. This enables rapid detection of potential illegal activities, allowing law enforcement to initiate countermeasure swiftly.

Earth Observation data, coupled with AI tools, has proven an invaluable tool for authorities combatting wildlife trafficking. Satellite imaging with AI enhancements serves as an effective method for tracking protected species, aiding in law enforcement efforts.

GNSS-enabled telemetry from animal collars contributes to species preservation. These collars, equipped with GNSS receivers, data communication radio-modems and VHF (Very High Frequency) transmitters, allow authorities to monitor and protect wildlife populations.

© Pixabay

RECOMMENDED READ: EUSPA’s EO and GNSS Market Report

EUSPA offers a collection of informative reports, available for download through the following link. The most recent addition to this series is the EO / GNSS report. The present secure SATCOM report marks a significant milestone as the first comprehensive exploration of this thematic area. With this addition, EUSPA comprehensively covers several components of the EU space programme (GNSS, Earth Observation and now also Secure Satellite Communications).

The EUSPA EO and GNSS market report is a comprehensive source of knowledge and information on the dynamic, global EO & GNSS markets. The report is published every two years, with the latest edition released in 2022. The report maintains a consistent structure while evolving from previous editions. Through the merger of EO and GNSS, the report offers insights into 15+ distinct market segments.

The report begins with an overview of the EO and GNSS market, touching on trends, size, and revenues. It delves into Copernicus and EGNSS, their global role, and policy trends. The core of the report consists of market segments, each following a uniform structure. This issue‘s Editor‘s Special highlights ‚Innovative Solutions for Health,‘ showcasing EO and GNSS‘s potential in mitigating global health challenges.

The next issue of the EO and GNSS Market report, will be published in 2024. Visit https://www.euspa.europa.eu/european-space/euspace-market/gnss-market/eo-gnss-market-report to download the most-up-to-date issue of the Report.

2022 / ISSUE 1

EUSPA
EO and GNSS
Market Report

EDITOR’S SPECIAL
Innovative Solutions for Health

SECURE SATCOM MARKET: DEMAND

© Unsplash

Chapter Summary

After presenting the different components of the EU Space Programme, paying particular attention to GOVSATCOM and IRIS2, this chapter elaborates on the forecasted demand for secure SATCOM services and their drivers. With this aim, the chapter describes how secure SATCOM networks are designed and operated, as well as the main providers and business models associated to these services. The current and future needs of the concerned users and use cases for secure SATCOM are described, as well as the key performance parameters and requirements for the envisaged secure SATCOM capacity demand. The chapter covers the following topics:

- A brief overview of the overall SATCOM market value and the drivers that are shaping the industry, creating opportunities and challenges for different services and applications. Such trends for SATCOM market value are also applicable to secure SATCOM market.
- A deep dive into the secure SATCOM market, in terms of main service provision stakeholders, value chain, business model options and factor influencing the market dynamics.
- The secure SATCOM use cases in the European Union alongside the driving elements and barriers/inhibitors that affect the demand amongst the user groups.
- The forecasted secure SATCOM capacity demand over the 2025 – 2040 period.

Key SATCOM market trends

Satellite Communications are widely used in a variety of applications, ranging from consumer TV broadcasting, maritime and plane communications, to governmental and even military use cases. The sum of all those uses represents the overall SATCOM market. Within this envelope, the secure SATCOM market is intended as the market related to three distinct use case categories (i.e. Surveillance, Crisis Management and Key Infrastructure, cf. page 30).

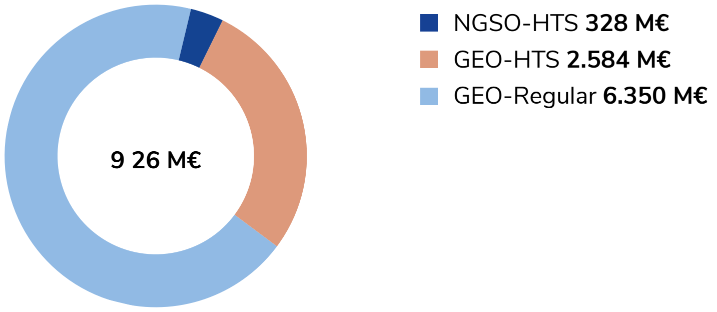
The secure SATCOM market is quite strategic even though it represents just a fraction of the overall SATCOM market. It is expected to be influenced by similar trends. Furthermore, the overall SATCOM market is conventionally split into two distinct categories: video and data. Video encompasses distribution of TV channels by satellites and professional exchanges of video content. The Data category comprises several service types, including Consumer Broadband, Enterprise Networks, Maritime, Aero, Cellular Backhaul & Trunking and MILSATCOM. The QoS (Quality of Service) would – among other parameters - be different from one service to another. The present report will first offer an overview of the overall SATCOM market, along with its economic quantification in terms of revenues (projected up to 2031). Subsequently, its ''secure'' portion is characterised in terms of capacity demand (Mbps), spanning the period 2025 – 2040, as illustrated on page 35.

The SATCOM industry has continued and accelerated its deep transformation in the 2022's increasingly competitive environment. The revenue from video capacity has been decreasing, while data revenue is on an upward trend (see next page). The move from video to data is highlighted by **the decline of GEO Regular satellite (mainly used for video) and increase of GEO-HTS/NGSO-HTS (mainly used for data)** (cf. definition of regular and HTS in Annex 2).

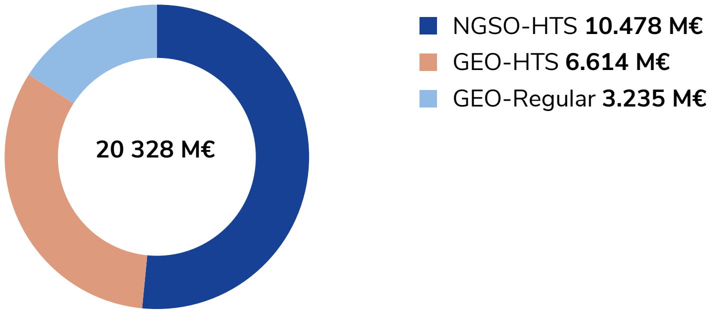
The pie chart on the right presents the revenues per capacity type (GEO-Regular, GEO-HTS and NGSO-HTS) in 2021 and a projection in 2031. The rapidly growing importance of **NGSO in connectivity markets is impacting the overall SATCOM industry** with an in-creasing number of players looking at a multi-orbit strategy to expand their business. Over the last two years, significant developments have unfolded in the NGSO sector, encompassing new constellation orders, the commencement of Starlink services, the Eutelsat's combination of activities with OneWeb, and the full deployment of OneWeb's 1st generation satellites. For the coming years, it is noteworthy to mention the planned entry of service of O3b mPOWER by the end 2023 and the services of Telesat Lightspeed scheduled to begin in late 2027. The growth of overall SATCOM revenue is mainly driven by NGSO constellation with a move from 328M€ (2021) to 10 478M€ (2031).

Such trend would also impact secure SATCOM Market. Consequently, **NGSO constellation are assessed to be also from a market value point of view- the major growth driver for secure SATCOM.**

Revenue breakdown by capacity type, million €, 2021 (1)(2)



Revenue breakdown by capacity type, million €, 2031 (1)(2)

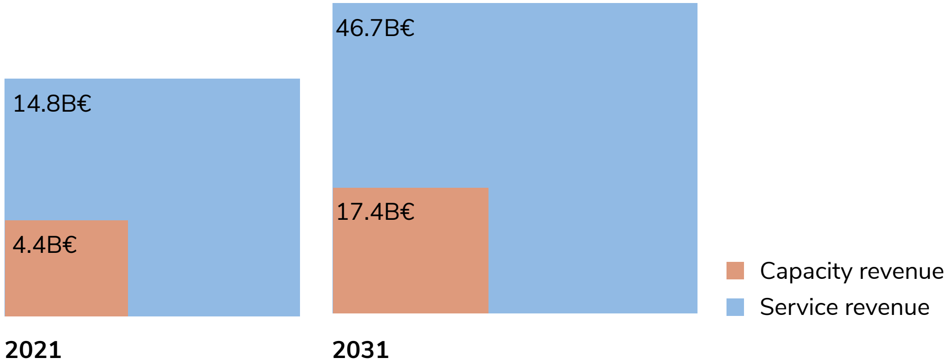


[1] "Satellite Connectivity and Video Market, 29th Edition, Euroconsult" © Euroconsult

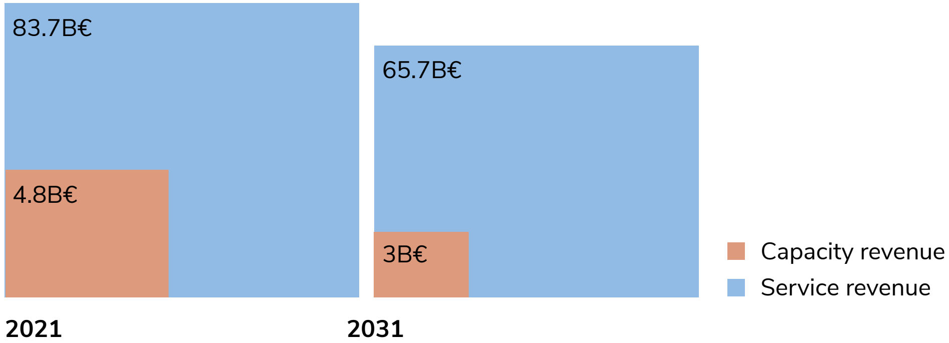
[2] Original data is in U.S.$. Converted in €, using a conversion rate of 1,10$/€ (average value from European Central Bank over July 2023)

SATCOM market growth is driven by services & data

Revenues for Data segments, billion € (2021 – 2031) [1][2]



Revenues for Video segments, billion € (2021 – 2031) [1][2]



The introduction of cost-effective systems (such as HTS (High Throughput Satellites) payloads, NGSO constellations) and a fiercely competitive market have contributed to changes in strategies, with operators pushed to look for extra revenues to avoid the commodity price trap. Operators have increasingly set their sights on a **new revenue stream: services**. The latter have been on a downward trend since 2017, mainly due to the negative impact of video services and the impact of COVID-19 in 2020-21 on mobility markets. However, FSS service revenues are poised to experience a resurgence in growth which in 2022. Revenues are projected to escalate from €98.5 billion to €112.4 billion between 2021 and 2031, culminating in cumulative earnings of €1.1 trillion over the decade.

The decline in capacity demand for video services is expected to persist, primarily affecting mature TV markets. On the other hand, all data markets, are projected to experience substantial growth. Among others, direct-to-device (D2D) data revenues are also estimated to grow, but is not included in our market value assessment. The data services are expected to grow from €14.8 billion in 2021 to €46.7 billion in 2031 (10-year CAGR: 12%), with all data segments contributing to revenue growth by 2031. Overall, the share of data applications is set to jump from 15% of total service revenues in 2021 to 42% by 2031. Drivers will include growth in subscribers/sites and ARPUs (Average Revenue Per User, the amount of money received from each user on average), supported by the improving abilities of satellite technology to support **higher quality broadband connectivity**. Additional factors contributing to this trend will involve the expansion of communication demands driven by data-intensive applications, alongside broader movements aimed at achieving universal access and closing the digital divide. Furthermore, the utilization of satellite connectivity for mobile applications plays a role in this trajectory.

Capacity revenues will follow a similar trend as service revenues for both data and video segments. On the data side, capacity revenues is estimated to be multiplied by four to more than €17.4 billion in 2031. Further drops in the pricing levels are expected with the entry into service of new VHTS (Very High Throughput Satellites) and NGSO constellations, which is estimated to drive demand for data services and contribute to revenue growth.

Data and services would create value for secure SATCOM

Service (and not capacity) and data are also estimated to be the growth driver – from a market value point of view – for secure SATCOM.

[1] "Satellite Connectivity and Video Market, 29th Edition, Euroconsult" © Euroconsult
[2] Conversion rate of 1,10$/€ (average value from European Central Bank over July 2023)

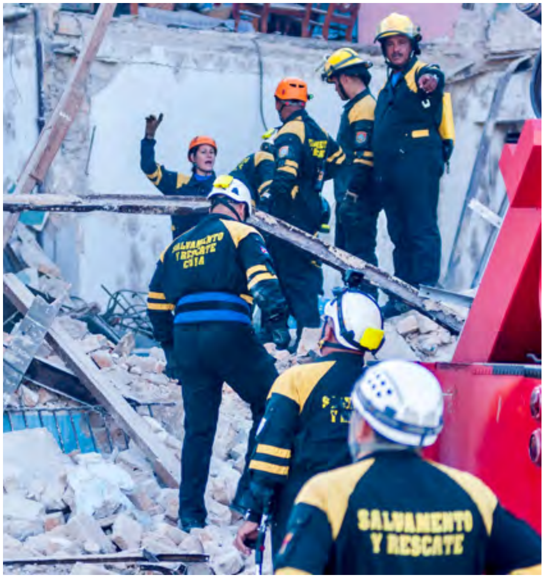
Focus on secure SATCOM

From now onwards, the report will specifically focus on the secure SATCOM market, in terms of secure satellite connectivity value chain, service provision, business models, users, use cases and forecasted secure SATCOM capacity demand, over the 2025 – 2040 period.

Each use case is presented individually, focusing on the actors, the connected units and their use of secure SATCOM, the dynamics and drivers of the use case' demand and the required geographical coverage as well.

Regarding the secure SATCOM capacity demand forecast, the analysis mainly focuses on FSS, as the vast majority of the satellite capacity demand arises from FSS. In addition, the analysis is provided over the 2025 – 2040 period, characterising the demand through Key Performance Parameters (KPP). A set of 5 Key Performance Parameters are introduced to identify future demand patterns across the estimated demand, regarding, for instance, the latency or the geographical coverage.

© Unsplash

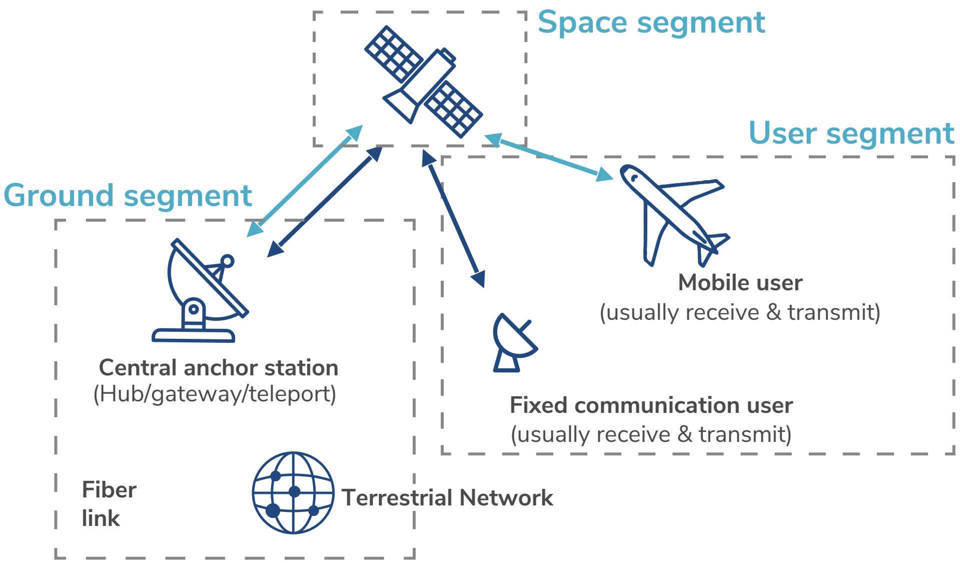


© Unsplash

© EUSPA

Typical System Architecture

Organisation of a satellite communication network structure



To establish a SATCOM link between two or multiple users and/or user networks, three essential components are necessary for both SATCOM and secure SATCOM, in conjunction with transmission networks. The figure provides a schematic representation of these distinct elements (more in-depth technical insights are given in section secure SATCOM technology, from page 80).

Space segment: A satellite (or a set of satellites for constellation) with different existing designs. Satellites can operate in different orbits and be part of different constellation concepts. Satellites are composed of a platform (also called bus) and one or several payloads. The payload(s) is/are really tailored to the mission(s) of the system. Space segment is manufactured by satellite manufacturers, purchased and operated by satellite operators.

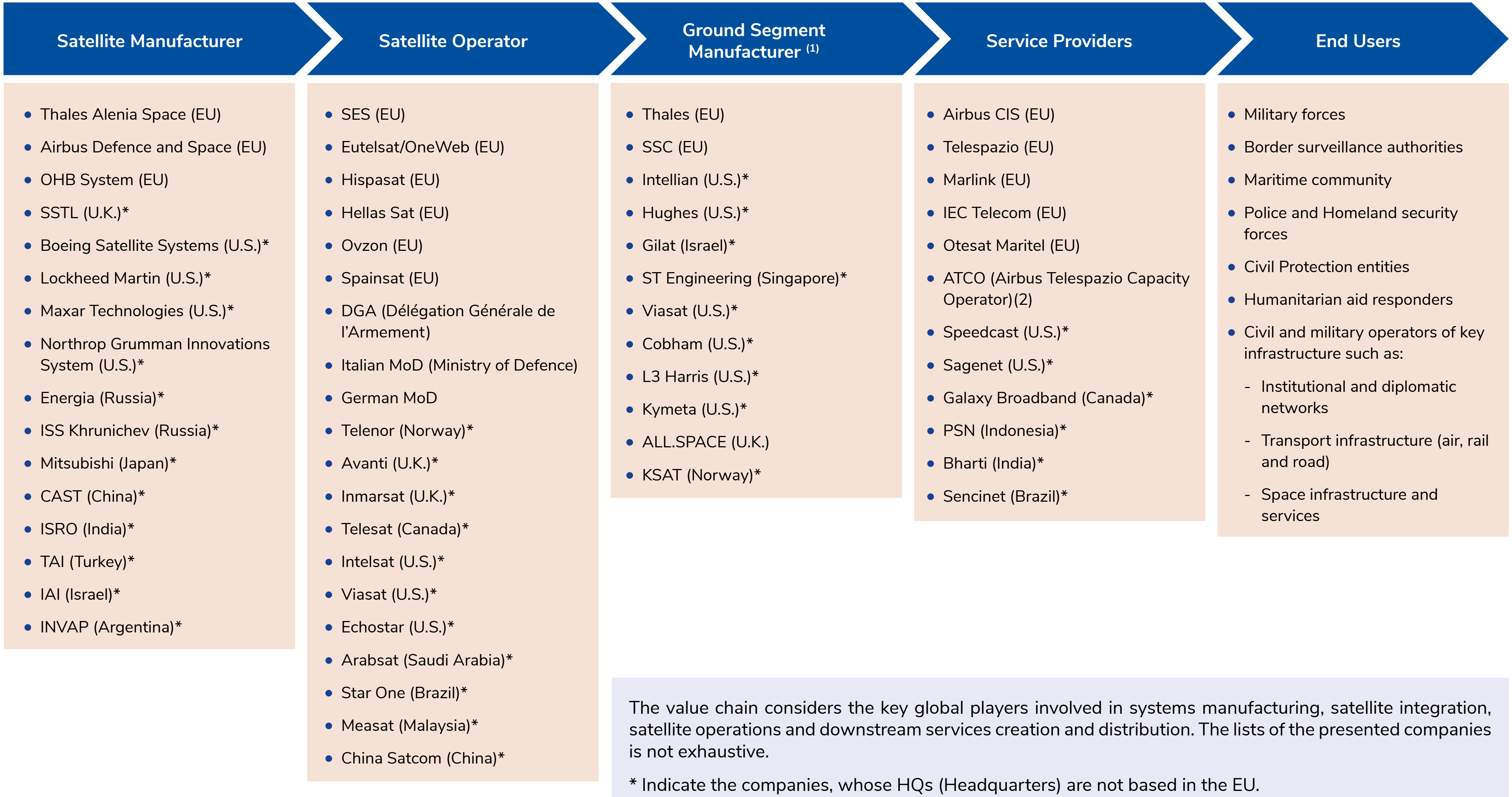
Ground segment: It consists of all the ground-based elements of a space-based system required to operate the satellite(s) and distribute the payload(s) data among interested parties on the ground, via a dedicated network.

Ground segment is mainly made of several ground stations, called Hub or gateway. Those ground stations can be grouped in a ground site called teleport.

User segment: User segment is made of various satellite communication terminals that usually support voice and data transmissions (both in reception and transmission). The user terminal includes the RF (Radio Frequency) equipment and the modem as well as the interfaces to the user networks and the user himself. It also includes the management aspects to sufficiently interact with the overall SATCOM system. The user terminal itself can be furnished as part of the SATCOM service or it can be a terminal provided by the end-user. Terminals which are provided by a satellite operator/service provider will generally lock the end-user into the SATCOM platform provided by that provider only; whereas a terminal provided by an end-user can be used on a wide variety of SATCOM platforms.

However, the space segment, the ground segment and the user segment alone do not suffice. Provision of secure SATCOM requires additional entities who design services in line with user requirements, define technical requirements to satisfy user needs (aiming at an optimized use of the available resources) and assess the economic viability of service provision. Such entities are called service providers, and the characteristics of the service provision are defined in a contract between the service provider and the end users.

As a result, the provision of SATCOM/secure SATCOM services necessitates a cohesive set of actors operating within a value chain structure. Within this framework, the role of each entity is precisely delineated. The subsequent page outlines the pivotal contributors in the value chain responsible for providing secure SATCOM services. Notably, it is important to reiterate that both SATCOM and secure SATCOM share the same satellite communication networks and value chain, as highlighted at the beginning of this page.



Satellite Manufacturer

- Thales Alenia Space (EU)
- Airbus Defence and Space (EU)
- OHB System (EU)
- SSTL (U.K.)*
- Boeing Satellite Systems (U.S.)*
- Lockheed Martin (U.S.)*
- Maxar Technologies (U.S.)*
- Northrop Grumman Innovations System (U.S.)*
- Energia (Russia)*
- ISS Khrunichev (Russia)*
- Mitsubishi (Japan)*
- CAST (China)*
- ISRO (India)*
- TAI (Turkey)*
- IAI (Israel)*
- INVAP (Argentina)*

Satellite Operator

- SES (EU)
- Eutelsat/OneWeb (EU)
- Hispasat (EU)
- Hellas Sat (EU)
- Ovzon (EU)
- Spainsat (EU)
- DGA (Délégation Générale de l'Armement)
- Italian MoD (Ministry of Defence)
- German MoD
- Telenor (Norway)*
- Avanti (U.K.)*
- Inmarsat (U.K.)*
- Telesat (Canada)*
- Intelsat (U.S.)*
- Viasat (U.S.)*
- Echostar (U.S.)*
- Arabsat (Saudi Arabia)*
- Star One (Brazil)*
- Measat (Malaysia)*
- China Satcom (China)*

Ground Segment Manufacturer [(1)]

- Thales (EU)
- SSC (EU)
- Intellian (U.S.)*
- Hughes (U.S.)*
- Gilat (Israel)*
- ST Engineering (Singapore)*
- Viasat (U.S.)*
- Cobham (U.S.)*
- L3 Harris (U.S.)*
- Kymeta (U.S.)*
- ALL.SPACE (U.K.)
- KSAT (Norway)*

Service Providers

- Airbus CIS (EU)
- Telespazio (EU)
- Marlink (EU)
- IEC Telecom (EU)
- Otesat Maritel (EU)
- ATCO (Airbus Telespazio Capacity Operator)(2)
- Speedcast (U.S.)*
- Sagenet (U.S.)*
- Galaxy Broadband (Canada)*
- PSN (Indonesia)*
- Bharti (India)*
- Sencinet (Brazil)*

End Users

- Military forces
- Border surveillance authorities
- Maritime community
- Police and Homeland security forces
- Civil Protection entities
- Humanitarian aid responders
- Civil and military operators of key infrastructure such as:
  - Institutional and diplomatic networks
  - Transport infrastructure (air, rail and road)
  - Space infrastructure and services

The value chain considers the key global players involved in systems manufacturing, satellite integration, satellite operations and downstream services creation and distribution. The lists of the presented companies is not exhaustive.

* Indicate the companies, whose HQs (Headquarters) are not based in the EU.

(1) Including User Terminal

(2) ATCO is a Joint-Venture between Airbus and Telespazio to provide military communication services using SYRACUSE IV (French military satellite)

Service provision for secure SATCOM services

Secure SATCOM services can be provided by two types of companies: the commercial satellite operators and the service providers. Indeed, commercial satellite operators can also offer directly secure SATCOM services to users (cf. page 60 for more details on the vertical integration trend for the satellite operators).

Commercial satellite operators

Established satellite operators, whether operating GEO satellites or NGSO satellites systems, are usually the owners of their ground infrastructure. Each GEO satellite usually has its own ground infrastructure. Satellite operators might lease/manage capacity or network solutions (including equipment) either directly to the end consumer or through a service provider. It is noteworthy that equipment can be located in a proprietary site or hosted in third-party owned site.

Examples of European Union companies [1]: SES, Eutelsat, Hellas Sat, Hispasat/Hisdesat, Ovzon

Service providers

Service providers link the satellite operators to the end users. Providers exist in a wide variety of forms, ranging from teleport operators to local resellers, and develop value-added services. The frontiers between activities are partly blurred because, depending on the market they serve and, on their activities, service providers can operate in SATCOM only or on other domains at the same time (Earth observation and Navigation). Some companies own and operate their own ground segment, buying wholesale capacity from satellite operators and tailoring their own offering before reselling it to end users. Providers can also deliver services directly to certain customers.

Examples of European Union companies[1]: Telespazio, Airbus, Marlink

Type of ownership

A company's type of ownership can have an impact on its provided service. For example, a decision can be taken amongst the ownership and the administration of a country to withdraw services or to take full control of its facilities in order for a hostile entity not to be able to act and infringe upon the sovereign status of the company. The following three types of ownership are observed:

- **Privately held company:** A registered company that is held in private ownership and is not quoted on a public stock exchange. This type of company is likely to have a reason to change in ownership profiles, but a change of ownership could occur without warning.
- **Publicly listed company:** A publicly listed company is a registered company with shares traded on a public stock exchange. Share can be bought and sold, and there are normally several large shareholders controlling the majority of the shares.
- **Government owned:** An organisation that is government owned or controlled, either as sovereign entity or an Intergovernmental organisation.

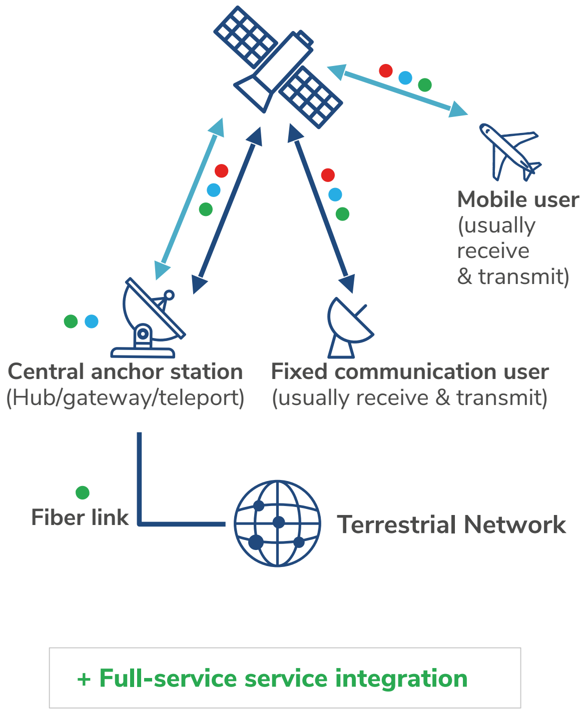
[1] *List is not exhaustive and intends to present a selection of the most relevant companies for the provision of secure SATCOM services.*

Business models for satellites operators

The GOVSATCOM service portfolio shall consist of three different categories of communication services: end-to-end services (allowing the user to connect to a network capable to provide services), anchored capacity services (allowing the user to use satellite capacity and associated anchoring station facility) and raw capacity services (allowing the user to use satellite capacity/bandwidth)[1] .

Following the GOVSATCOM service portfolio taxonomy, the following table presents the different items that will compose the provision of the services by a satellite operator (as mentioned in the previous page, secure SATCOM services can be provided by satellite operators and service providers). The part of the services that are not included in the red dot line, are provided by the service provider[2].

	END-TO-END SERVICES	ANCHORED CAPACITY SERVICES	RAW CAPACITY SERVICES
SATELLITE BANDWITH / CAPACITY	• Capacity managed by the operator/provider from/ to router/switch of anchor station	• Raw capacity packaged and sold to Service Providers or directly to the end user	• Raw capacity sold (in MHz) to Service Providers or directly to the end user.
GROUND INFRA	• Owned and managed by satellite operator. • Vendor specific	• Owned and managed by satellite operator. • Maybe co-located with the feeder link	• Can be produced or leased by third parties
NETWORK OPERATIONS	• Smart routing and network optimization managed by satellite operator, together with the integration with terrestrial network	• Routing and integration with terrestrial network to be arranged with third parties	• Smart routing, network optimization and integration with terrestrial network to be arranged with third parties
SERVICE PROVISION	• Operator/Provider responsible for full connectivity service integration and performance (QoS).	• Includes the provision of capacity as well as a central anchor station and customer support	• Satellite raw capacity only • A third party Service Provider designs the desired services (i.e. SLA and CIR – Committed Information Rate)



[1] Commission Implementing Decision (EU) 2023/1054 of 30 May 20223 laying down rules for the application of Regulation (EU) 2021/696 of the European Parliament and of the Council as regards the service portfolio for the Governmental Satellite Communications services offered by the system established under the Union Space Programme.

[2] In case of GOVSATCOM service provision, service provider includes also GOVSATCOM participant. Regulation (EU) 2021/696 of the European Parliament and of the council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU

Business models for satellites operators (continued)

Historically, the satellite operator industry was structured around fixed prices that were applicable to a contract for several years. As such, pricing was often expressed in €/MHz/year. Since several years ago, pricing contracts have been using **Mbps** instead of **MHz**; this trend has developed in parallel with the growth of data services and the services provided by HTS systems. In addition, and in correlation with a marked decrease in satellite capacity, an increasing number of operators have started to **move down in the value chain** by offering managed capacity directly using Mbps or GB (GigaByte) as opposed to using raw capacity (in MHz).

Beyond those trends, several factors have affected the price of satellite capacity including **frequency-band, power, back up duration** and **volume of the lease**. Other operator-specific factors (a unique beam or interconnectivity scheme, exclusive coverage/power level, teleport service, backhaul service) have come into play. These factors help differentiate satellite bandwidth from a commodity and highlight satellites' ability to provide services that could not exist without them (aero/maritime connectivity) or that alternative terrestrial solutions would not provide as efficiently from a financial point of view.

While all customers of capacity expect a high-quality service, different types of customers have different priorities, and this can greatly affect **capacity pricing**.

The red box on the right provides a sample of the criteria that certain user segments consider to be highly important for them. **Four major factors** contribute to the definition of capacity pricing in the various regions and segments:

- The **purchasing power** of the targeted customers.
- The **cost-efficiency** of satellite assets (i.e., the price level required to generate a return).
- The balance between supply and demand/the level of **competitive pressure**.
- The **nature of the operator** (fully commercial, government owned).

Sample of basic requirements for secure SATCOM provisions

Depending on regulatory obligations & the criticality of communications these may be the basic requirements:

- A high availability rate for the network.
- A cost-effective solution for users (with varied levels of sensitivity).

For mobile and/or occasional requirements (such as defence users), there may be:

- The ability to provide seamless connections to different locations.
- A single contact point for capacity management.
- Strong back-up options in case of satellite failure.

Role and impact of newcomers

New entrants refer to non-incumbent/non-legacy secure SATCOM providers (for instance, SES, Eutelsat, Marlink... are incumbent players). They have to face high **barriers to entry** such as the finite resource of orbital positions/frequencies, need for high upfront CAPEX (Capital Expenditure) before operations and high technical expertise throughout the satellite lifecycle.

Their impact is twofold: Firstly, they provide **innovative solutions** which open the door to new applications or unlock some barriers to entry. For instance, new technologies have enabled the production of low-cost, low-power, small size antennas for fixed and mobile terminals. More generally, newcomers **disrupt** the traditional way of doing things. In addition. New entrants reinforce the competition between the market players and lead them to develop innovative and cost-effective solutions providing benefits for the end-users. For instance, Starlink (SpaceX) could have a significant impact on the satellite capacity pricing in a short-term perspective by leading incumbent satellite operators/service providers to **adapt to new market conditions.**

Major features of secure SATCOM services defined by contractual agreements

Focus on the Service Level Agreement (SLA)

A Service-Level Agreement (SLA) is a contract between the provider of the services and its customers that documents what services the provider will furnish and defines the service standards the provider is obligated to meet. Service providers need SLAs to help them manage customer expectations and define the severity levels and circumstances under which they are not liable for outages or performance issues. Customers can also benefit from SLAs because the contract describes the performance characteristics of the service – which can be compared with other vendors' SLAs – and sets forth the means for redressing service issues.

For secure SATCOM, the SLA is usually more demanding than for SATCOM as it generally includes a **higher level of guarantee for the provision of the services**. SLAs can be classified in different types, from the less to the more demanding. An SLA includes generally the following items:

- **Guarantee of access to the service:** Commitment from the service provider to provide the service according to the agreed contractual performances (generally greater than 99%). In general, the more demanding are SLAs regarding service continuity and availability, the greater the impact on the price of its provision.
- **Reporting processes:** Definition of the process for reporting some information on a periodic basis or on request when an incident happens.
- **Customer support:** Provision of a dedicated service manager and 24/7/365 customer service. Agreement for restoration times or reaction times to respond to an incident, warehouses (for maintenance and repair of the hardware equipment), training.
- **Potential additional value-added services** such as Cloud connectivity, End-to-end managed services using SD-WAN (Software-Defined Wide Area Network) orchestration, Bandwidth on demand, Data management (web compression, filtering and firewalling), IT services.

Business model for terminals

The customer for secure SATCOM services can have different approach to the **procurement and operation of terminals:**

- **Build:** The customer procures bespoke terminals developed according to their specification.
- **Buy:** The customer procures the terminal according to dedicated catalogues.
- **Lease:** The customer procures access to terminal through lease agreements with suppliers.
- **Gov2Gov:** The governmental user gains access to terminals through agreements with other governments or institutions (European Commission, European Defence Agency, NATO (North Atlantic Treaty Organisation)). For instance, as a part of EU SATCOM market (led by EDA), Airbus delivers SATCOM services to EU member States, EU military and civilian missions, as well as EU bodies. The contract covers the provision of satellite communication (C-, Ku-, Ka- and L-band), the sale and rental of terminals, as well as the provision of turnkey solutions, particularly in theatres of operations outside of the EU. In the frame of this contract, Marlink supply some of the terminals and specific L- and Ku-band services. As of April 2022, the EU SATCOM market had 33 members and, on average, a new SATCOM order is coming in every 1.5 days.

The chosen approach by the customer may depend on the characteristics of the use case/mission. As of today, most of the terminals used for the provision of secure SATCOM services are bought. Indeed, in addition to the ownership (which guarantee access to terminal availability), “buy” choice has an advantage from a financial point of view: customers request the relevant budget only at the purchase period, and not on a yearly basis to pay the lease. It is noteworthy, that in case of lease, the terminal has to be returned in good working condition at the end of the lease agreement while some working conditions and environment can be harsh for some mission/use cases.

Secure SATCOM use cases in the EU

The secure SATCOM market is shaped according to the list of the use cases categories envisaged for GOVSATCOM as identified below and considered the GOVSATCOM component of the EU Space Programme (cf. page 11). In addition to the three use case categories (surveillance, crisis management and key infrastructure), another use case category exists, named Specific Use Case. In the frame of the present satellite capacity demand analysis, it includes one use case ("Polar regions") which has been identified as users or potential users of satellite communications in Polar regions (i.e. Arctic region) for EU Member States and EU Institutional entities. Some user needs may apply to more than one category, for instance the satellite communication demand from the Specific Use Case "RPAS C&C" is included in all the use cases where RPAS (i.e. UAV (Unmanned Aerial Vehicle)) is concerned. Similarly, the demand for the Specific Use Case "M2M (Machine to Machine)/IoT (Internet of Things)" is included in several use cases such as Transport Infrastructures and Other Critical Infrastructures.

The different use case categories include both missions currently using SATCOM to a large extent and missions which are not yet SATCOM users or are only to a limited extent.

Surveillance	Crisis Management	Key Infrastructure	Specific Use Case
Land Border Surveillance (i.e the surveillance of sea and land border)	**Maritime Emergency** (i.e Search & Rescue missions and response to maritime disasters)	**Transport Infrastructures** (i.e Air, Road, Rail and Maritime traffic management)	**Polar regions** (i.e SATCOM for government, public and scientific research institutions in Arctic region)
Maritime Surveillance (i.e the surveillance of illegal activities)	**Humanitarian Aid** (i.e the assistance in case of disasters/conflicts, to refugees and telemedicine)	**Space Infrastructures** (i.e support to GNSS, EO and SSA activities)	
	Civil Protection (i.e activation of the related forces such as ambulance, fire rescue in case of disasters)	**Institutional Communications** (i.e SATCOM for embassies, EU representations offices)	
	Law Enforcement Interventions (i.e national police misions and fight against international organized crime groups)	**Land Border Surveillance** (i.e the surveillance of sea and land border)	
	EU External Actions (i.e CSDP missions, election observation and contribution to UN missions)	**Other Critical Infrastructures** (i.e SATCOM link for critical infrastructure such as energy grid and financial ones)	
	Forces Deployment (i.e the deployment of EU Member States forces as part of national/European missions)		

Factors influencing the demand of secure SATCOM

The following table presents key driving elements, barriers and inhibitors for the use of secure SATCOM by National and European user communities. They apply to different use cases/use case categories with different levels of impacts. For each use case, a presentation of the dynamics and drivers of the demand will be provided in the next pages.

DRIVERS

Geopolitical trends & evolution of threat environment	Geopolitical tensions increase the needs for border and maritime surveillance, security of the key infrastructure, diplomatic activities and crisis management missions.
Climate change & global warming	Changing climatic conditions have two types of major consequence, leading to a growing needs for secure SATCOM. Firstly, global warming will lead to more humanitarian crises and secondly, it will also increase shifts in population, requiring more border surveillance and humanitarian activities.
Economic growth & rise of digital economy	Economic growth (or slowdown) may have a major impact on world trade and commercial exchanges, especially for aircrafts and merchant ships. Since the middle of 20th century, the GDP (Gross Domestic Product) has continuously grown with a temporary decrease in 2008 (financial crisis) and 2020 (COVID-19)[1]. The World Bank's short term forecasts point to continued growth in the global economy[2].
National and International regulations/EU policy	Regulations and EU Policies are major growth drivers for secure SATCOM. An example is the European Security Strategy and the Internal Security Strategy efforts to make Europe more secure by fighting terrorism and serious crime, and strengthening cooperation on law enforcement, border management, civil protection and disaster management[3].

BARRIERS & INHIBITORS

Fragmentation of the demand	The so-called "fragmentation of the demand" refers to the diversity of the users' needs and requirements. Differences can vary from the applications being used, to the nature of traffic(permanent links to on-demand/occasional requirement), to the location of the users (fixed location, transportable, mobile) etc..
Affordable and interoperable equipment	The end-users need to have access to equipment suitable and adequate to perform their missions. Among all the elements of the satellite communication value chain, the terminals are a major point. Terminals must be fit for the purpose and need to be available at an affordable price.
Need for significant awareness and expertise of the users	Awareness of the actual benefits and the key advantages of secure satellite communications solutions is a key driver for the user demand. In addition, the end-users must be trained to exploit the secure satellite communication capabilities during the missions.

[1] Banque Mondiale. Croissance du PIB (% annuel].
[2] World Bank Blogs. 2023. Sowing the seeds of change to solve the water crisis, August 18
[3] European Commission. What the Commission is doing. Borders and security.

Methodology used to assess secure SATCOM capacity demand for the European Union users

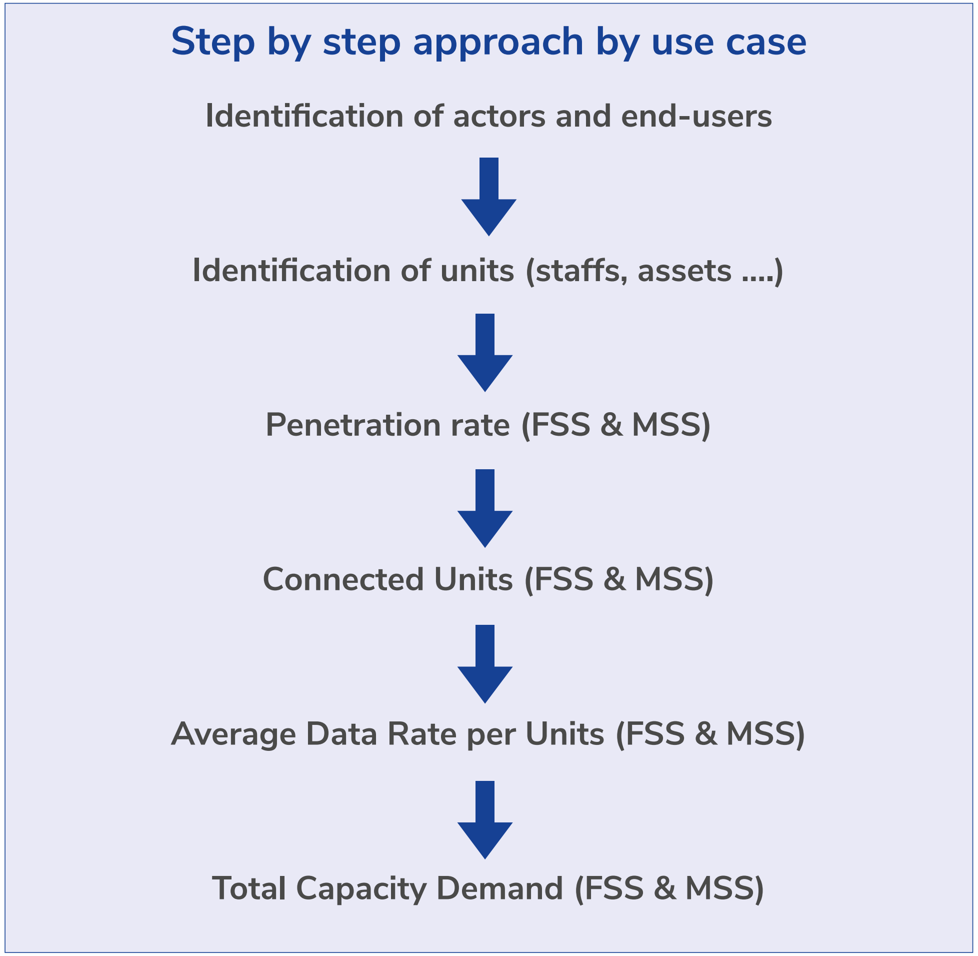
Users of secure SATCOM are civil and military entities supervising or managing security-critical missions or infrastructures, including Union and Member State public authorities; they can be located in European Union or deployed worldwide. The quantified demand presented in the next pages concerns users belonging to each EU Member States, as well as EU Institutional entities, located in the European mainland and worldwide[1], across the identified secure SATCOM use cases[1].

A bottom-up approach was followed, assessing each use case and end-users' requirements as well. The analysis also takes into account the dynamics and drivers of every type of missions and applications. The analysis starts with the identification of all actors, end-users and the assets, and the staff needed to be deployed in order to comply with the missions. The analysis also includes the estimated number of units and assets deployed taking into account both:

- the geographical distribution.
- the needs or actual use that may be different for EU Member States and for EU Institutional entities as well as by types of mission.

In the frame of satellite capacity forecast, the vast majority of the satellite capacity demand arises from FSS. However, MSS data would be important for the future secure SATCOM offering. MSS terminals operate in lower frequency-band (such as L-band or S-band), with limited data rate but have smaller size and are provided at lower cost in comparison to FSS terminals.

Finally, the analysis provides the information on the amount of satellite capacity forecast to be used per use case category. The analysis does not include the user demand which might be possibly satisfied by optical links.



Step by step approach by use case

Identification of actors and end-users

Identification of units (staffs, assets ….)

Penetration rate (FSS & MSS)

Connected Units (FSS & MSS)

Average Data Rate per Units (FSS & MSS)

Total Capacity Demand (FSS & MSS)

[1] Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme, Article 65.

Key Performance Parameters

Several Key Performance Parameters (KPP) have been introduced to facilitate the computation of different traffic distribution and to illustrate certain future demand patterns across the use cases.

The following table presents the different KPPs and give a few examples of the use of KPP to different terminals.

Notes: Low latency is typically required for (near-) real time applications. Since one specific terminal might be used to serve more than one application needed in a specific use case, the notion of 'low latency' would only correspond to part of the traffic associated to the concerned use case.

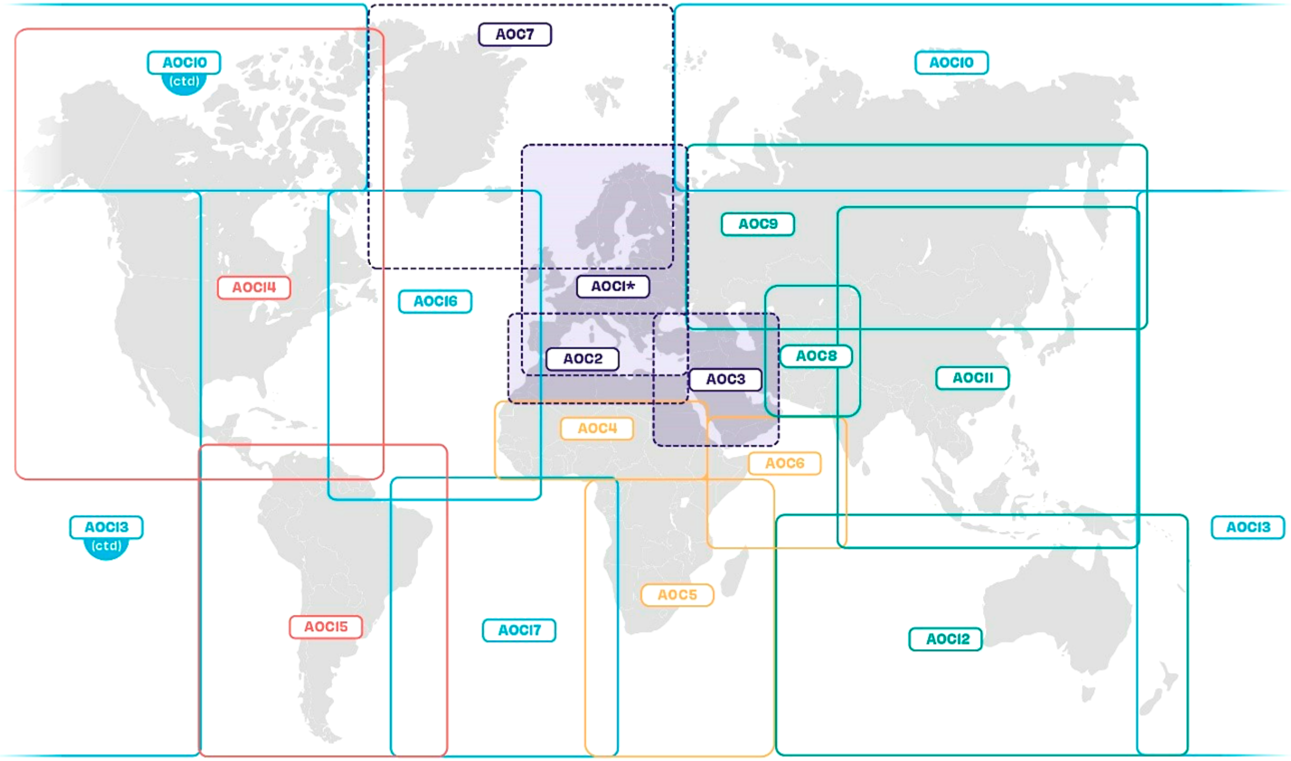
KPP	Definition	Status
Link Purpose	Allows qualifying the anticipated role in satellite. This shall also commenting on the impact of requirement for new network.	- Primary (for primary connection) - Backup (for backup role)
Mobility	Enables to qualify the type of traffic, potential changes in the patterns over time.	- Fixed - Deployable - COTM (Communication On The Move)
Bandwidth level	Distribution of assets by level of data rates, in order to highlight some transverse trends through the different use cases.	- Below 10 Mbps - 10 – 25 Mbps - 25 – 50 Mbps - 50 – 100 Mbps - Greater than 100 Mbps
Geographic distribution	Allow to assess the traffic per different geographical areas.	- EU continent & waters - Middle East & Africa - Asia Pacific - Polar - Americas - Atlantic
Latency	Allow to assess the share of traffic which may need (or not) low latency. Low latency is considered below 250 ms.	Level 1: Low latency estimated to be critical for up to the majority of the traffic (>65%) Level 2: Low latency estimated to be critical/having a high added value for a significant part of the traffic (> 20%) Level 3: Low latency not to be critical, although it could be beneficial

KPP – definition of geographic distribution

Secure SATCOM user demand can vary from a geographical area to another. A potential overlap exists between certain areas (e.g. the need in mobile assets) and subsequently the consolidated value coming from the whole distribution by region may exceed the total estimated demand as provided by different use cases.

The table below presents the distribution matrix between the geographical areas as defined in the ENTRUSTED project[1].

Geographical distribution (as defined in ENTRUSTED project)

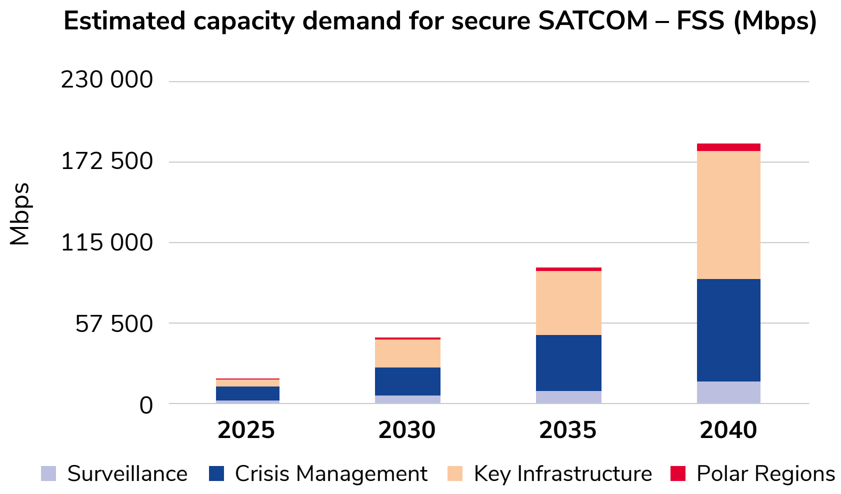


*See: EU & outermost regions – Regional Policy – European Commission (europa.eu)

Ref.	Name	In the report
AOC1	Continental Europe and EU outermost regions	Europe
AOC2	Mediterranean sea and North Africa	Europe
AOC3	Turkey & Middle East	Middle East & Africa
AOC4	Central Africa	Middle East & Africa
AOC5	Southern Africa	Middle East & Africa
AOC6	Arabian Sea and Gulf of Aden	Middle East & Africa
AOC7	Greenland and North Europe	No pricing available
AOC8	South-West Asia	Asia Pacific
AOC9	Russia and Central Asia	Asia Pacific
AOC10	Rest of the Arctic	Polar
AOC11	China and South-East Asia	Asia Pacific
AOC12	Oceania and Indian Ocean	Asia Pacific
AOC13	Pacific Ocean	Asia Pacific
AOC14	North and Central America	Americas
AOC15	South of America	Americas
AOC16	North Atlantic	Atlantic
AOC17	South Atlantic	Atlantic

[1] ENTRUSTED project (H2020 Grant Agreement No. 870330) https://entrusted.eu/

Synthesis of the FSS capacity demand forecast 2025 – 2040



Both FSS and MSS capacity demand for secure SATCOM have been estimated; The FSS capacity demand will be presented first FSS type (from page 35 to 39) and MSS later (page 40). The figure on the top presents the estimated capacity demand for secure SATCOM (FSS) and for each of the three different use case categories. It is estimated that user demand with FSS solutions will **increase by a factor of 14 over the 2025 – 2040 period** to reach around 186 Gbps in 2040.

In 2025, the FSS capacity demand for Crisis Management is expected to count for around half of the total FSS capacity demand, with Crisis Management representing be-tween 40% and 50% of the anticipated demand over the forecast period. Within this appli-cation field, **Forces Deployment is estimated to represent the highest level of demand**, followed by Civil Protection and Law Enforcement interventions. For Forces Deployment , the Strategic Compass and the future threats are by themselves a key driver for future secure SATCOM demand. A trend towards an increasing number of units equipped with a communication on the move capability, the spread of more sensors, the sharing of data richer information, has been assessed to contribute to higher secure SATCOM needs for military users.

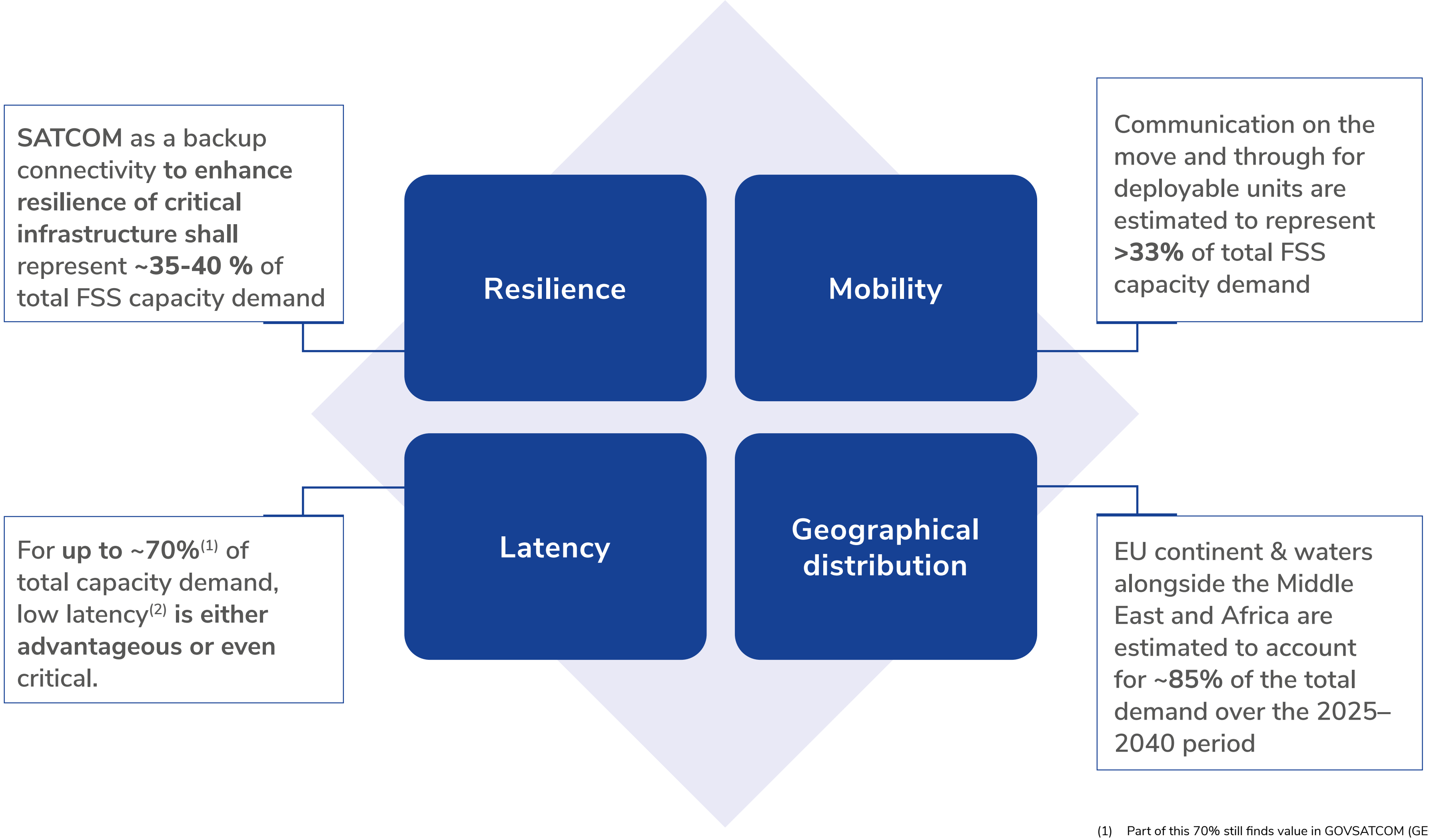
From around 2030, the Key Infrastructure category will generate the highest level of demand to represent around 50% of the total capacity demand in 2040. The two largest uses cases within the segment are **Institutional Communications and Other Critical Infrastructures.**

When it comes to **Institutional Communications**, several European Union entities (EU Delegation,EU embassies) and national entities (national embassies) are located worldwide where reliable terrestrial communications means are not always available. It is esti-mated they would need more satellite capacity, relying on global higher satellite capacity demand. Moreover, the geopolitical context, cyber and hybrid threats further prompt secu-rity and resilience concern. It significantly increases the need of a guaranteed and secure access to communication means for any type of Institutional Communications. As regards **Other Critical Infrastructures**, such as the banking and energy sector as well as specific European and National infrastructures are strategic assets for European Union. The numbers of those entities are not expected to substantially increase in the coming decade, but only their need for reliable, secure and guaranteed communication means. Digital transformation of both the EU economy and so-ciety is accelerating and the digital information of the infrastructures as well. Such infrastructures are key for, among others, the development of e-government services, the simplification of administrative procedures/formalities and the increasing digitalization of public ser-vices. Among them, data centres are key for resilience and EU data protection and confidentiality standards. Their use is expected to rise in the coming decade with important required data rate (several hundreds of Gbps). An illustration of their ex-pected increasing use is the European Union investigations to improve the energy efficiency and circular economy performance in cloud computing and data centres[1].

As previously stated, the estimated level of demand is contingent, among other factors, upon the availability of a secure SATCOM service in the different time periods, with technical/operational features and prices (for both connectivity services and terminals) allowing and favouring a large adoption. For certain use cases, accelerated deployment may also come from the presence of regulatory mandates (it is assessed such regulatory factor would arise over the 2025–2040 period). Taking a concrete example, the ability of certain military forces to use new secure solutions by 2025 may also depend on the deployment of new terminals or in the ability to use their existing terminals (or ones already under procurement) to receive secure SATCOM services.

[1] European Commission. Green cloud and green data centres. Shaping Europe's digital future.

KPP synthesis for future FSS secure SATCOM capacity demand



SATCOM as a backup connectivity **to enhance resilience of critical infrastructure shall** represent **~35-40 %** of total FSS capacity demand

Resilience

Mobility

Communication on the move and through for deployable units are estimated to represent **>33%** of total FSS capacity demand

For **up to ~70%**[1] of total capacity demand, low latency[2] **is either advantageous or even** critical.

Latency

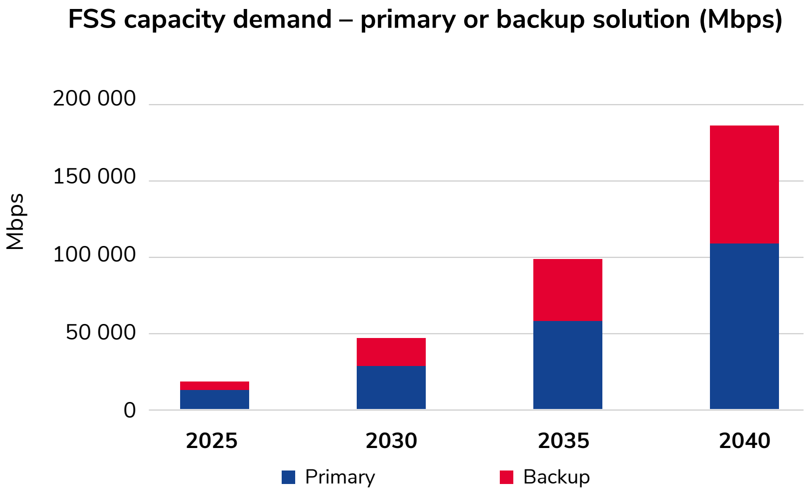
Geographical distribution

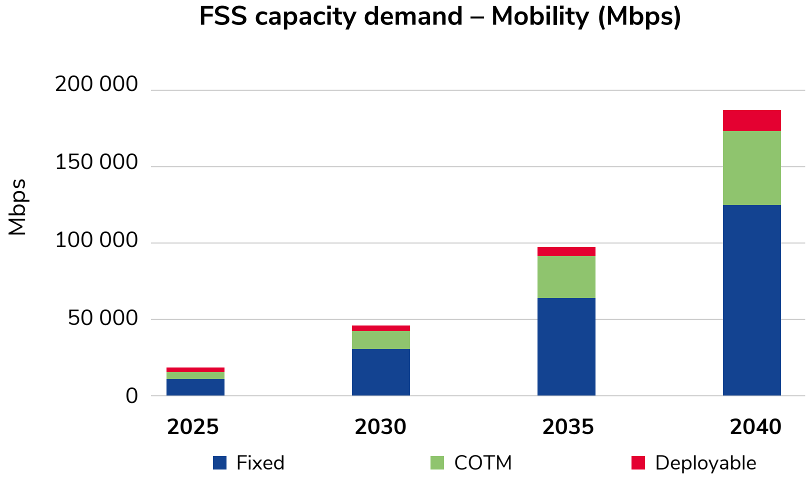
EU continent & waters alongside the Middle East and Africa are estimated to account for ~**85%** of the total demand over the 2025–2040 period

[1] Part of this 70% still finds value in GOVSATCOM (GEO-only)

[2] Low latency (below 250 ms) is defined on page 33

Growing mobility demand for both primary and backup solutions





Secure satellite connectivity is projected to serve as **the primary means of communication for users (partially or totally) out of reach of terrestrial networks or with specific needs.** That is the case for users operating at sea or in remote locations, as well as in cases where terrestrial services are disrupted (e.g. after natural disasters), or for users with stringent requirements in need of secured/dedicated network (such as Institutional communications).

However, satellite connectivity can be used as a backup solution, offering both redundancy and enhanced availability to cope with outages. Such demand is estimated to mainly come from fixed sites established in the European Union territory. Most of those sites,from certain headquarters to data centres and special operation sites including for space missions, will predominately rely on fibre connectivity. Nevertheless,a backup solution will likely often in the meantime require a high level of satellite capacity(up to hundreds of Mbps) to guarantee a sufficient resilience for critical data exchanges.

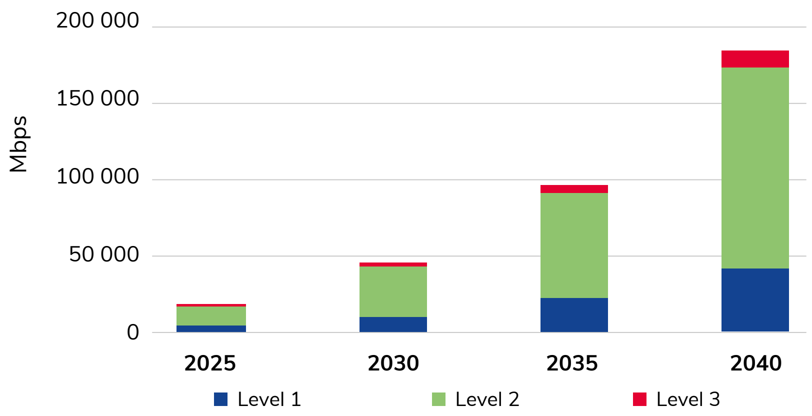
Capacity demand from fixed users is estimated to represent 62% of the total FSS capacity demand all over the 2025 – 2040 period. For fixed users, most of the demand is estimated to come from Civil Protection, Forces Deployment, (Crisis Management), Space infrastructure , Institutional Communications and Other Critical infrastructures (Key Infrastructure) use cases. It should be noted that we considered as fixed locations, terminals that would remain deployed for a long time, even if the installation is not permanent (example: case of certain refugee camps).

Capacity demand for COTM (Communications on the Move) users is estimated to represent about 25% of the total FSS capacity demand all over the 2025 – 2040 period. Increasing equipment of mobile units (aircraft, vessels, land vehicles and UAVs), together with increasing data transmissions per unit is estimated to support demand.

In comparison, **capacity demand for deployable** units is estimated to also increase but at a slower pace.

Low latency is important for the majority of the FSS secure SATCOM demand

FSS capacity demand – Estimated importance of latency by user terminal (Mbps)



Definition of the different levels for low-latency

- **Level 1:** Low latency estimated to be critical for up to the majority of the traffic (>65%)
- **Level 2:** Low latency estimated to be critical/having a high added value for a significant part of the traffic (>20%)
- **Level 3:** Low latency not to be critical, although it could be beneficial

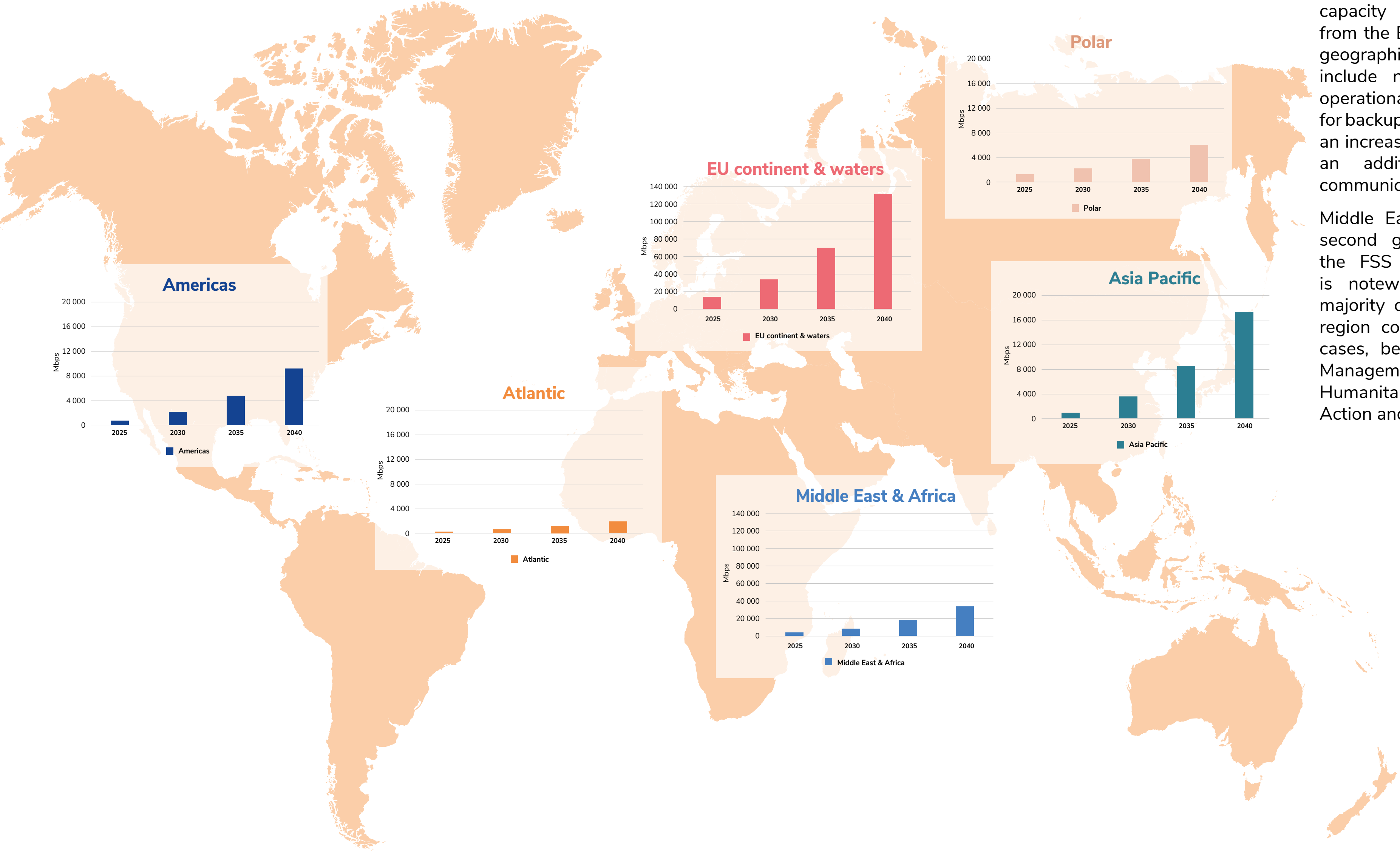
Estimating the criticality of latency in future capacity demand is subject to several considerations and assumptions for several reasons. Firstly, a user might use a single terminal for multiple applications, some of which mandatorily require low latency, while others may find it advantageous but not critical (and others not require it at all). Futhermore, future satellite communication terminals may be able to **communicate with different satellite networks** (i.e. in different orbits and frequency bands). While such terminals may not be widespread in the short term, they are estimated to become increasingly available over the forecast period.

When a terminal carries substantial traffic that requires a low latency (or in case some data links are critical even if requiring low capacity), it is assumed that the end user would primarily choose a satellite terminal and network meeting its requirement for low latency. **Terminals considered as corresponding to Level 1 shall generate around 25% of the total FSS capacity demand that was estimated between 2025 and 2040**. It includes Hospitals for telemedicine, Central command sites, Nuclear Power Plants, Financial infrastructure and Data Centres. Terminals that we considered as corresponding to **Level 2 shall generate more than two thirds of the total FSS capacity demand that was estimated between 2025 and 2040.** Terminals that we considered as corresponding to **Level 3 shall generate less than 10% of the total FSS capacity over the 2025 – 2040 period** and mainly comes from Humanitarian Aid and certain use cases related to Space Infrastructures.

It is noteworthy that even for terminals/traffic that could benefit from a lower latency, a migration may only occur when an appropriate network is available. For legacy networks, it can also be dependent on the lifecycle of current terminals. It remains noteworthy that it is anticipated that a majority of the users could give priority to a network with a low latency (pending adequate technical, operational and pricing features). **Availability of flexible terminals enabling access to several networks (and tentatively several frequency bands) is estimated to represent an important enabler in the middle term, also favoring the traffic capacity optimisation.**

Geographical coverage need for secure SATCOM

Geographical distribution of the FSS capacity demand

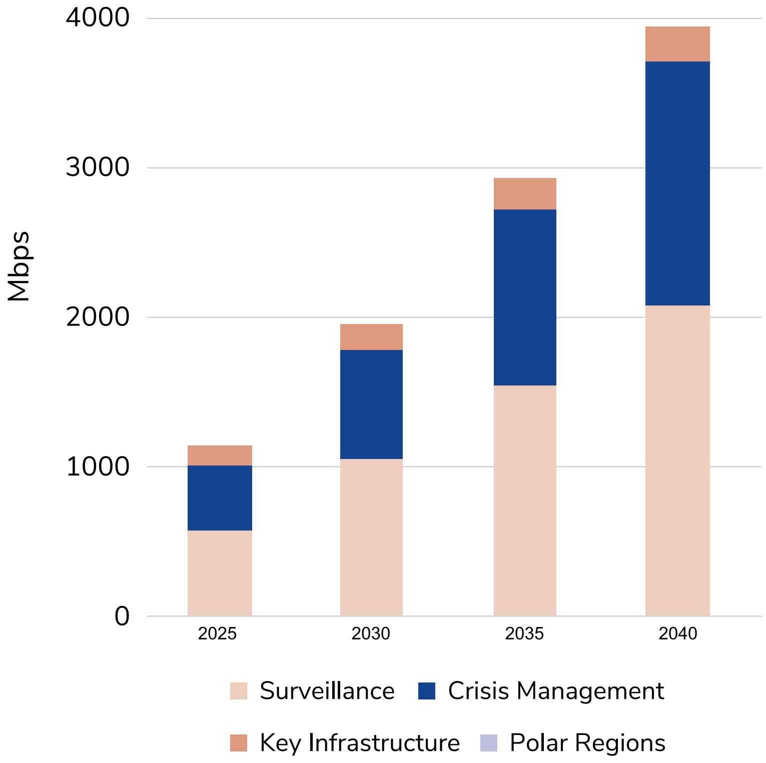


About two-thirds of the FSS capacity demand will come from the EU continent & waters geographical area. It would include needs for permanent operational missions and needs for backup communications, with an increasing need to guarantee an additional resilience to communication networks.

Middle East and Africa is the second geographical area for the FSS capacity demand. It is noteworthy that the vast majority of the demand in this region comes from three uses cases, belonging to the Crisis Management use cases family: Humanitarian Aid, EU External Action and Forces Deployment.

Synthesis of the MSS capacity demand forecast 2025 – 2040

Estimated capacity demand for secure SATCOM – MSS (Mbps)[1]



As mentioned earlier in the report, the vast majority of the satellite capacity demand arises from FSS type. However, it is noteworthy to mention that MSS data will be important for the future secure SATCOM offering. MSS terminals operate in lower frequency-band (such as L-band or S-band), with limited data rate but have smaller size and are provided at lower cost in comparison to FSS terminals.

User demand for secure SATCOM from MSS satellite networks/capacity is expected to increase **from around 1.2 Gbps (2025) to 3.9 Gbps (2040)**.

It is noteworthy that MSS spectrum is also used to support IoT services. While these terminals may represent large volumes, the actual related capacity remains limited as it primarily corresponds to data bursts representing in each case a few kilobits. Exceptions may however correspond to services where IoT/data collection comes together with a return link or includes more data transmissions (such as sending images or video material).

We estimate that most of the user demand for **MSS capacity will come from the maritime surveillance missions and operations.** Indeed, the majority of the maritime surveillance units will likely rely on MSS either as a primary or backup solution.

[1] The data does not include satellite capacity for AIS, ADS-B (Automatic Dependent Surveillance-broadcast) (Aircraft), LRIT (Long Range Identification And Tracking) /VMS (Vehicle Monitoring System) (Vessels) and IoT for cars and trains (IoT for cars and trains are assessed below 10 Mbps in 2040)

Use cases presentation

Following the analysis of the overall secure SATCOM capacity demand, each use case belonging to the three use case categories (Surveillance, Crisis Management and Key Infrastructure) and the use case Polar regions, is presented.

For each addressed use case the specific different actors (i.e. EU National and/or European organizations) which use secure SATCOM are first presented. Secondly, **the connected units** (i.e. the assets which are operationally connected to space-based systems to communicate) are detailed. Thirdly, **the dynamics and drivers** of the secure SATCOM demand are assessed. Finally, the **geographical coverage** paragraph provides an indication where secure SATCOM is needed to answer the operational needs of the use case. To be noted that, although the use cases may refer to missions beyond EU territory, they are always intended for EU Member States and/or European Union users.

© Unsplash

© Unsplash

© Unsplash

© Unsplash

Land border surveillance use case

Actors

Frontex (European Border and Coast Guard Agency) together with Member States ensure safe and well-functioning external borders providing security. Its main tasks is to protect borders, to fight cross-border crime, to monitor borders, perform risk analysis, seek international and EU cooperation, provide training, conduct research and innovation, provide return and reintegration and ensure safer Schengen and smoother travels.

At national level, national police and customs agency are also part of the land border surveillance use case users.

Connected units and their use of secure SATCOM

A diversity of assets can take advantage of secure SATCOM. Frontex works in coordination with EU member states. A headquarter for centralised communication of assets, institutions and governments can be used for information sharing, real-time monitoring and control.

Aircraft, helicopters, vessels, road vehicles and UAVs can also rely on secure SATCOM to exchange information/data in the frame of the Land Surveillance use case. Aircrafts are used for surveillance, rescue and joint return operations. Secure SATCOM can enable real-time information sharing through video surveillance and communication. Helicopters are used to transport people, equipment and supplies. Secure SATCOM can aid communication through for a more targeted approach towards an operation. Vessels are used for surveillance, illegal migrants' control and search and rescue missions. Having satellite connectivity can enable **centralised video surveillance and quick response for search and rescue missions.**

Frontex rolled out its own patrol vehicles in 2019. Surveillance on land and having satellite connectivity on-board road vehicles can ensure better information gathering, video surveillance and quick response in case of border breach. Patrol officers **can use secure SATCOM to alert headquarters of any disturbance at border** and for an active communication link in case of land border breach or equipment malfunction.

Large UAVs are used for surveillance covering a large area and can reach an altitude of 15.24 kilometres with speeds up to 444 km/h staying aloft up to 30 hours. Small UAVs can be used at a shorter range for imaging and movement detection through radars and have altitudes up to 450 m, speed up to 50 km/h and endurance of 30 – 50 min.

Dynamics and drivers of the demand

Irregular and illegal migration have been a strong concern for European Union countries. Climate change, geopolitical tensions, international conflicts and wars lead people to migrate. As those factors are set to increase, need for land border surveillance is expected to grow in the coming years. Migration flows evolve, based on economic opportunities and border regimes in different countries. Thus, **innovative solutions need to be implemented** to prevent not only illegal migration, but also any type of entities which plan to threaten peace at all land borders.

Geographical coverage	Primarily European Union (including the overseas territories) focused on land and sea borders.

Maritime surveillance use case

Actors

The maritime surveillance is usually conducted by the Navy and Coast Guards which ensure the safety and security of national marine borders and the territorial waters. These agencies also provide safe waters for the sea-borne trade in the waters controlled by them by counteracting against piracy and other illegal activities. Apart from national agencies and Frontex, European Union has EMSA (European Maritime Safety Agency). Europe also has a common body called European Fisheries Control Agency (EFCA) to regulate the fishing activities within European waters. Within the European Union, there are at least 25 Members States with a functional navy as a part of the country's defence forces. Some of the countries even have active coast guards in addition to the navy to secure the country's marine borders.

More often, coast guards act in unison with the naval forces and even sometimes are part of the navy itself. Most of the European countries are also a part of the North Atlantic Treaty Organisation (NATO) agreement and often deploy their navy vessels in regions covered under the agreement.

Connected units and their use of secure SATCOM

Maritime surveillance activities require marine vessels to establish control over national territorial waters. We have assumed that vessels with sizes greater than 20 m will require at least one means of satellite communication. Smaller vessels (sizes less than 20 m) usually conduct nearshore operations and spend most of the time in the terrestrial network coverage, communication is mainly served by the terrestrial means. Bigger naval vessels, such as aircraft carriers, frigates, ocean-going patrol vessels, etc. normally host larger onboard crew and participate in the missions globally, are already fitted with FSS and MSS as a backup.

The maritime surveillance from the air is comprised of aircrafts (fixed wing) and helicopters possesses an onboard satellite connectivity terminals that can be used to establish mission-critical communication and to acquire crucial communication during maritime surveillance. The business aircrafts that are used for transporting important persons are possibly equipped with FSS as well as MSS terminals. Helicopters were more difficult to equip with satellite connection due to their constantly rotating rotors. The new terminal technology is able to overcome this problem and as a result, make it possible to equip a helicopter with satellite connectivity. UAVs are more reliant on satellite connectivity, but it depends on the size and operational range of the UAV. Smaller UAVs are not able to support the weight of the FSS equipment hence they are addressed by either MSS or terrestrial means of communications.

Satellite connectivity is estimated to be used as primary connectivity as the operational areas of connected units are out of reach of terrestrial networks.

Dynamics and drivers of the demand

Maritime surveillance is a major activity for defence forces and coast guards and their respective vessels use secure SATCOM for both crew welfare and operational needs.

For aircraft, helicopters and UAVs, the demand is purely from their operational applications.

The continuous efforts to develop smart ships, unmanned vessels and UAV's that will increasingly be deployed for maritime surveillance activities will escalate the demand for higher, faster and more reliable bandwidth.

Geographical coverage	• Very large to medium vessels: worldwide. • Small vessels, aircraft, helicopters and UAVs: European Union.

Maritime emergency use case

Actors

The actors involved in Maritime Emergency missions depend on the location of the vessel and on the type of emergency considered. Coastal states have adopted the IMSO (International Mobile Satellite Organisation) convention requiring ships to be equipped with GMDSS (Global Maritime Distress and Safety System). This system allows vessels in danger to send a distress call alerting other ships in the area which can help as well as the closest Maritime Rescue Coordination Centre (MRCC). This coordination centre will then send the information to local coast guards or Navy entities and ships to provide rescue as fast as possible.

In the case of a piracy or terrorist attack, ships can activate either their Ship Security Alert System (SSAS) or Ship Security Reporting System (SSRS). SSRS being the upgraded version of the SSAS. The signal emitted by the endangered vessel will be sent to Naval Operation Centres which will inform the closest Navy forces to provide military support. Furthermore, SSAS and SSRS calls can be answered by EU organisations in some specific areas of the world, even if they are not located in a Member State's waters. Indeed, most SSAS and SSRS registered calls are in the Gulf of Aden. To protect ships in this strategic corridor, the Maritime Security Centre – Horn of Africa (MSCHOA) and United Kingdom Maritime Trade Operations (UKMTO) monitoring centres are in charge of collecting such calls and coordinating international efforts. They will inform an alliance of naval forces, the EU NAVFOR (EU Naval Forces) Somalia – Operation Atalanta, which takes action in the region against attackers.

Connected units and their use of secure SATCOM

A majority of the vessels spend most of their traveling time close to shore and thus remain in range of VHF communications. However, some of them engaged on international voyages or going farther from the shore **need to be able to send emergency messages at all times**, which includes when they are out of reach from those communications means. In that case, satellites provide a reliable connectivity solution allowing distress calls from ships to be sent.

Several types of vessels are connected through satellites, mainly due to national and international regulations. Usually, large and commercial ships are more subject to international regulations having them connected through satellites.

Merchant, cruise and offshore Oil & Gas vessels above 300 Gross Tonnage need to be equipped with GMDSS (Global Maritime Distress and Safety System). Required equipment for GMDSS includes a VHF radio, a Search & Rescue transponder, a NAVTEX receiver, an EPIRB (Emergency Position Indicating Radio Beacon) as well as DSC (Digital Selective Calling) and Inmarsat-C terminals.

In addition, all types of vessels above than 500 Gross Tonnage are required to be equipped with either SSAS (Ship Security Alert System) or its upgraded version, the SSRS (Ship Security Reporting System). SSAS and SSRS include a messaging service for security alerts in case of piracy or terrorist attack as well as two alarm buttons with no sound and no flashing lights so that they are not obvious to intruders. Finally, vessels can also rely on satellite **communications for onboard reporting (e.g. emergencies, telemedicine)**.

Dynamics and drivers of the demand

Each of the Maritime Emergency related assets considered are mainly connected to comply with regulations. Consequently, the primary growth driver of secure SATCOM connectivity is the implementation of new regulations either by national or international bodies overseeing traffic of vessels. It can come as a totally new regulation or an enlargement of the scope of existing ones, thus affecting more assets. Moreover, the **increasing importance of safety and control over the vehicles** is estimated to further increase the demand in the coming years. For example, a modernisation of the GMDSS standards is expected to enter in service in 2024.

Another driver is the growth in the number of assets to be regulated due to an increase in the overall number of merchant ships, fishing vessels, cruise ships, yachts and offshore support vessels.

Geographical coverage	Global

Humanitarian aid use case

Actors

EU humanitarian action stands for the principle of solidarity, which indicates that the European Union will provide assistance, relief and protection for victims of disasters. Humanitarian aid missions include civil protection and humanitarian assistance in Europe but also outside of the region.

To avoid duplication of relief efforts, a response at European level is prioritised with the Emergency Response Coordination Centre (ERCC) at the heart of the EU Civil Protection Mechanism (EUCPM) created in 2001 by the European Commission to improve prevention, preparedness and response to disasters. Emergency relief provided by ERCC can take several forms including in-kind assistance such as the deployment of specially-equipped teams and assessment coordination of aid by experts sent to the impacted area. The EUCPM was activated 114 times in 2021 (1), with 61% of activations linked to COVID-19. For humanitarian aid, the ECHO department shares responsibilities with EU Member States. It has provided humanitarian assistance since 1992.

Other actors not managed directly by ECHO that are involved in humanitarian aid missions include the UN and other national government aid agencies. The UN is involved in peacekeeping missions whose mandate is to protect civilians under threat of physical harm. The protection of civilians is done in cooperation with humanitarian actors. The UN (via UNHCR (United Nations High Commissioner for Refugees) also offers shelter, food, water, and medical care to refugees. The UN usually assumes refugee camp coordination in refugee emergencies while NGO (Non-Governmental Organisation) partners or national authorities manage the camps. NGOs are also frequently involved in medical actions.

Connected units and their use of secure SATCOM

Secure SATCOM can act as the main option for some humanitarian aid missions (including the humanitarian teams and the hospitals/mobile clinics) in areas with no terrestrial connectivity (usually outside of Europe) or where terrestrial connectivity was cut due to a disaster. **The need for telemedicine in these situations often occurs** in a context of a lack of terrestrial infrastructure, calling for access to secure SATCOM. In this case, **assured access to communications is critical for the preservation of life**. The use of secure SATCOM is also key to assist different mobile units such as aircraft, helicopters and UAVs when EUCPM support is activated. SATCOM also often acts as back-up option (e.g. refugee camps). Crisis management missions are characterised by the need for back-up links for which secure SATCOM are well suited (e.g. civil protection after natural disasters or for humanitarian aid).

Dynamics and drivers of the demand

The number of forcibly displaced people including refugees has increased significantly in recent years. In the 2010s alone, the number of refugees has increased by 75%. Reasons for the growth trend include increasing global insecurity, geopolitical tensions and impact of climate change. The EU is increasingly impacted by the overall situation as displaced populations often end up in refugee camps, some of them based in the region (e.g. Greece, Spain). This regularly pushes the EU to assist countries in dealing with the challenge of hosting refugees (e.g. Greece) based on the principle of solidarity.

Due to the non-scheduled nature of disasters and armed conflicts, the EU must be able to rely on relevant communications network when needed to undertake relief efforts. **In many cases, terrestrial networks are not sufficient to guarantee the success of EU interventions**. The need for secure SATCOM in this segment is estimated to observe strong growth in the coming decades, notably due to the continued increase in refugees, many of them expected to seek asylum in the EU, which will likely push the region to increase refugee-related investments. In parallel, the growing expected number of disasters (natural and man-made) will lead to an increasing number of requests for EUCPM assistance with the EU expected to remain at the forefront of international relief actions.

Geographical coverage	Global with main focus on European Union and MEA (Middle East and Africa)

[1] European Commission. Emergency Response Coordination Centre (ERCC).

Civil protection use case

Actors

Civil protection shares boundaries with humanitarian aid with both verticals complementing each other. In the frame of this report, the civil protection vertical considers needs of EU civilians with respect to disasters prevention and preparedness. Disasters can occur anywhere and at any time. For better readiness, it is important to ensure that existing infrastructure is capable enough to mitigate the repercussions of these disasters. At European level, there are different mechanism tools allowing the deployment of civil protection means.

EU Civil protection mechanism is a mechanism where in the occurrence of a natural or man-made disaster, the affected country can request assistance from the mechanism through the Emergency Response Coordination Centre (ERCC). After the affected country accepts the offer, member states help and ERCC coordinates the deployment and delivery of assistance. In some cases, EU civil protection teams are also deployed and are returned at the end of the emergence response. **European Civil Protection Pool** was established to advance European coordination in civil protection through bringing together 25 member states that are capable to deploy to a disaster zone (man-made or natural) at short notice. Said resources include rescue and medical teams, experts, specialized equipment, mobile laboratories, water purification equipment and transportation. Finally, **rescEU** is the latest element of civil protection introduced with the objective of enhancing the protection of citizens from disasters and the wider management of emerging risks. It also establishes a separate reserve of resources including firefighting planes, helicopters, medical evacuation planes, medical equipment and field hospitals. Said resources can help respond to health emergencies, chemical, biological, radiological and nuclear incidents.

Connected units and their use of secure SATCOM

With advancements in technology, it is now possible to not only detect and predict some disaster occurrences but also improve post-disaster management. Hospitals, ambulances and fire stations can be equipped with secure SATCOM technology enabling them to communicate in real-time developing effective and efficient emergency response programmes and provide support even in areas where there is limited availability of communication networks. Considering communication needs of citizens, mobile units to restore connectivity through secure SATCOM can be introduced. These units can provide connectivity in a large area to the effected population.

Firefighting planes are primarily used in case of large-scale forest fires and would require connectivity primarily for communication and image sharing. For firefighters, secure SATCOM is also key to offer guaranteed and resilient connectivity. Helicopters can be used to transport people, equipment and supplies and in this scenario, secure SATCOM can aid communication for a more targeted approach towards search and rescue.

Mobile Laboratories can be sent to an affected area prone to infectious viral and bacterial disease specially where there is a risk of spread. Secure SATCOM connectivity can give better access to necessary communication. Test samples results can even be sent over secure SATCOM link for more detailed research to find cures to disease. With specific medicals needs, such use case needs mostly low-latency satellite capacity.

Dynamics and drivers of the demand

Disasters are not limited to forest fires, health emergencies or hurricanes. As reported by GHSL (Global Human Settlement Layer), the populations exposed to earthquakes as well as built-up areas exposed to earthquakes has historically been increasing and similar trends apply to population and built-up areas within 100 Km of volcanoes, tsunami hazards, flood hazards and cyclone storm surges[1]. Since limitations exist for traditional terrestrial communication infrastructure in these situations, having deployable units connected to satellites capable of restoring communication in such areas can be crucial. Connectivity, communication and information sharing through live video streams will not only be used by mobile units but also by the people they support leading to higher demand and growth of data utilisation in the civil protection use case.

Geographical coverage	Prime focus on European Union, worldwide to assist other countries

[1] European Commission. 2021. Overview of natural and man-made disaster risks the European Union may face.

Law enforcement interventions use case

Actors

In the EU, law enforcement interventions are led at both a national and regional level. Each state has its own police force and law enforcement bodies that mainly conduct missions at a national or local level. Missions typically include policing, investigations, emergency measures and support services, the goal being to enforce the law, prevent and control crimes, maintain peace and order and ensure public safety. The number of bodies varies depending on the country (for instance, Germany has 16 state police forces and 3 federal law enforcement agencies).

EMPACT (European Multidisciplinary Platform Against Criminal Threats) is a cooperation platform of EU members created in 2010. It is the EU's flagship instrument to tackle organized and serious international crime. EMPACT is supported by all EU institutions, bodies and agencies that are involved in international law enforcement activities. They include EUROPOL (European Union Agency for Law Enforcement Cooperation), EUROJUST (European Union Agency for Criminal Justice Cooperation), CEPOL (European Union Agency for Law Enforcement Training), OLAF (European Anti-Fraud Office), EU-LISA (European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice) and EFCA (European Fisheries Control Agency). Other non-EU countries, international organisations, and other public and private partners are also associated. EMPACT became a permanent instrument in 2021. EUROPOL brings together hundreds of EU police organisations to fight crime as one player. The agency's goal is to provide safety to EU citizens. Main areas of focus include terrorism, international drug trafficking, money laundering, organized fraud, trafficking in human beings and the counterfeiting of euros.

Each of the other EU agencies involved in international law enforcement activities has a specific focus. EUROJUST works with national authorities to combat cross-border crimes, OLAF investigates fraud within the EU, EU-LISA ensures the operation of large-scale IT systems, and Frontex is tasked with border control.

Connected units and their use of secure SATCOM

In the law enforcement interventions use case, both fixed and mobile assets require connectivity. Police communications include data, pictures and videos from surveillance units that must be exchanged promptly and seamlessly between HQ (Headquarters) and the Member's law enforcement organisations while using highly secure links. Connectivity can frequently be used by these agencies for **centralised communications, real-time monitoring of an event, information sharing and communication links** between HQ and the Member's law enforcement units.

For mobile assets, having access to connectivity is key for numerous reasons including to stay in touch with other assets or ground control, and to acquire crucial communication during surveillance, search & rescue and other emergency situations. Law enforcement agencies frequently deploy various mobile assets (Police vehicles, aircrafts, helicopters and UAVs) depending on the nature and area of activity.

Dynamics and drivers of the demand

In the EU, most of the law enforcement communications are provided via terrestrial links (radio and fixed), with secure SATCOM understood to mainly be used as a backup. TETRA (Trans European Trunked Radio), an alternative to the use of cell phones for two-way communication (limited to 7.2 kbps channels), was designed for use by emergency services and is widely used by police forces. In coming years, the use of secure SATCOM is expected to grow with the question of **communications anywhere and at any time** represents a factor which is crucial for this segment to address ongoing threats (e.g. terrorism).

Geographical coverage	European Union

EU external action use case

Actors

Based in Brussels, the EEAS relies on an extensive network of EU diplomatic presence worldwide and brings together European civil servants, diplomats from the foreign services of the EU Member States and local staff in countries around the world. The EEAS is specially in charge of the CSDP (Common Security and Defence Policy), which is an integral part of EU foreign policy. Since its implementation in 2003 and through its military operations and civilian missions, the CSDP has contributed to both global and regional security challenges.

In the frame of this report, UN Peacekeeping missions are included in this use case, while they are not directly managed by EEAS. UN Peacekeeping missions help countries navigate the difficult path from conflict to peace. European Member States provide military and government/administration personnel of their own national services to UN Peacekeeping missions.

Connected units and their use of secure SATCOM

A diversity of assets can take advantage of secure SATCOM. For every type of missions (election observation, UN, CSDP (Common Security and Defence Policy)), secure SATCOM can be used to connect EEAS mission HQ to Brussels and to staff in missions for centralised communications, information sharing and real-time monitoring.

In addition to HQs, different type of staff can also rely on secure SATCOM to exchange information/data in the frame of the EU External Action use case. Firstly, short-term observers (about two-thirds of the observers) and the long-term observers (about one-third of the observers) for election are the two types of observers deployed for every election observation missions. Satellite communication can definitively provide a reliable solution for collection of data, relevant on-time monitoring of the electoral process. Secure SATCOM can be used fixed for the stationary teams or mobile for the mobile observation teams. Secondly, the 18 CSDP missions and operations involve the deployment of around 5000 people. Regarding the scope of CSDP missions, and in addition to HQ connectivity, deployed staff can rely on secure SATCOM to have continuous communication means at any time throughout the duration of the operation's length.

Thirdly, the staff for UN Missions can be mentioned. Indeed, UN Peacekeeping missions is composed of military staff (staff officer and troops) from supporting national countries, but not only. Indeed, some UN Peacekeeping missions also include Formed Police units and Individual Police members.

Specially for UN and CSDP Missions, and based on national military forces, several types of other units can be connected. Can be quoted armoured personnel carrier (to transport troops), logistic vehicles, vessels, aircraft, helicopters, UAVs and mobile BGAN (Broadband Global Area Network) units to provide connectivity in case of emergencies.)

Satellite connectivity is estimated to be used as the primary connectivity as the operational areas of connected units can suffer a lack of relevant and secure terrestrial networks.

Dynamics and drivers of the demand

One key objective of EEAS, via the Common Security and Defence Policy (CSDP), is to work towards strengthening the EU's capacity to respond to security challenges and to consolidate its role as a global player. The global geopolitical stability has worsened in recent years, and as such EEAS promotes peaceful and democratic outcomes to longstanding crises. The 18 CSDP missions and operations which are currently running continues to be an emblematic high visibility EU foreign policy tool to address crises around the world.

Geographical coverage	Worldwide with a focus on Africa and Middle East

Forces deployment use case

Actors

Some of the EU Member States have deployed forces in external theatres over the last decade as part of national missions or international missions (such as under a NATO). Those operations usually involve the use of satellite communications (based on FSS or MSS capacity) either based on proprietary government satellites or third-party assets (such as systems managed by private commercial operators). EU Member States can also deploy forces in the future as part of European missions, such as the EU Rapid Deployment Capacity (EU RDC), as highlighted below.

In March 2022, the EU Member States have agreed on a common strategic course of action for security and defence towards a stronger and more capable European Union: the Strategic Compass [1]. It is a guide for action and its unique value proposition is to act more quickly and decisively when facing crisis with the following commitments (1) Up to 5,000 strong EU RDC; (2) Live exercises on land and at sea; (3) Enhance military mobility and (4) Reinforce CSDP missions and operations (CSDP missions and operations are part of EU external action use case, cf. page 48).

Connected units and their use of secure SATCOM

Different military units can use secure SATCOM and each one uses different types of terminals.

Land units: Based in the EU, the central command units (for every mission) are the central controlling entity which manage the missions from Europe. Satellite connectivity contributes by providing an **independent, secure and autonomous link with the military deployment, wherever it is deployed**. Theatre hubs provide HQ operations and connection in the operating area. Certain hubs can also correspond to long term, fixed installations of military bases outside Europe.

In addition, deployed troops and staff can use Flyaway/manpack terminals. Any type of land vehicles (armoured or logistics ones) required by military forces are also equipped with secure SATCOM terminals. It is noteworthy to mention that MSS terminals also provide connectivity to troops and staff but with a lower data rate than the flyaway and manpack (the MSS terminal has a smaller size, too) (cf. page 32).

Piloted aero units: Different types of aircraft such as transport aircraft, combat aircraft, aircraft dedicated to special missions (such as ISR (intelligence, surveillance and reconnaissance)) and helicopters are needed to support the forces missions.

Maritime units: The Maritime assets are partly the same as the ones used in the frame of the Maritime Surveillance use case (the profile of assets are similar).

Finally, this report is primarily focused on the future requirement for MALE (Medium Altitude Long Endurance) type UAVs, although other types of UAVs, tactical to HALE (High Altitude Long Endurance) type could be deployed and require satellite connectivity over the forecast period.

Dynamics and drivers of the demand

Different elements will lead to feed secure SATCOM demand. Firstly, the Strategic Compass is by itself a key driver for future demand. It estimated to lead to new investment, modernisation of forces, and new operations. Secondly, an increase in the data transmission requirement for essentially all of the terminals used by military forces is anticipated. Thirdly, Sensitivity to new and/or increasing threats, i.e. contested operations, jamming, cybersecurity (etc.) is estimated to result in a demand for more "secure" capabilities compared to traditional commercial satellite communication solutions.

Finally, the location of future threats, crises and operations is difficult to anticipate, as exemplified by the situation in Ukraine in 2022. As such, the ability to rapidly adapt, with an increasing level of flexibility and mobility is estimated to represent an important driver. The trend towards an increasing number of units equipped with a communication on the move capability is estimated to increase.

Geographical coverage	Worldwide with a focus on Africa and Middle East

[1] European Commission. 2022. A Strategic Compass for Security and Defence.

Transport infrastructures use case

Actors

EU Member States have various types of transport infrastructure on their territories and various entities manage transport infrastructure depending on the type of asset considered:

The European Organisation for the Safety of Air Navigation (Eurocontrol) manages air traffic and oversees collision avoidance between aircraft and all subjects related to Search and Rescue in case of an accident. In addition, Air Navigation Service Providers (ANSPs) manage traffic on a national level and can be either public or private.

The European Fisheries Control Agency (EFCA) consolidates information collected by Member States and regional organisations on the localization of fishing vessels to avoid illegal fishing. This information is then used by national fisheries inspection services to enforce regulations. On the other hand, the European Maritime Safety Agency (EMSA) collects data on vessels to provide them with continuous position and navigational safety information for safety purposes such as collision avoidance.

When it comes to private and commercial land vehicles, some manufacturers will use secure SATCOM IoT in the coming years to monitor their clients' assets in order to conduct predictive maintenance and improve the quality of their products. Lastly, railway operators will increasingly use information generated by their assets for optimization and management of traffic. ERA (EU Agency for Railways) will primarily devise the technical and legal framework to enable the removing technical barriers to this adoption.

Connected units and their use of secure SATCOM

Commercial and business aircraft must remain connected for navigation purposes during their whole flight time. Airplanes doing international or long flights will be more likely to be connected through satellite at some point.

Several types of vessels are connected through satellites, mainly due to national and international regulations. Usually, large and commercial ships are more subject to international regulations having them connected through satellites. On the other hand, fishing vessels of any size must be equipped with a VMS (Vessel Monitoring System), but it depends on the country they are registered in.

Trains and rail related assets such as railcars, passenger railway vehicles and locomotives mostly use terrestrial means of communication but some of them may be connected in the future as operation management and optimization will need a continuous connectivity. This can be achieved only through satellites for trains crossing unpopulated regions.

Same as for trains, every land vehicle can possibly be connected through satellite for predictive maintenance and optimization. However, only the high-end of the market is expected to be connected through IoT in the coming years due to the price of the equipment.

Dynamics and drivers of the demand

Each of the transport infrastructure related assets considered are mainly connected in order to comply with regulations. Consequently, the primary growth driver of secure SATCOM connectivity is the **implementation of new regulations** either by national or international bodies overseeing traffic of vehicles and assets. It can come as a totally new regulation or an enlargement of the scope of existing ones, thus affecting more assets of a segment. Moreover, the increasing importance of safety and control over the vehicles will further increase the demand in the coming years. Another driver is the growth in the number of assets to be regulated due to an increase in the number of land vehicles, trains or aircraft travelling through the EU.

Geographical coverage	Depending on the type of assets: Global for vessels and aircraft, regional for trains and land vehicles.

Space infrastructures use case (Copernicus)

Actors

The Space Infrastructure use case consists of four sub use-cases linked to the relevant program component: i) Copernicus, ii) Galileo & EGNOS, iii) SSA, and iv) a transversal use case concerning Ground Segment. Most of the data and information provided by **Copernicus** are made available to any citizens and organizations free of charge. Governmental users, such as Union institutions and bodies, European, national, regional or local authorities entrusted with the definition, implementation, enforcement or monitoring of a public service or policy, are core usesrs of the Copernicus.

The EDRS (European Data Relay System) represents the backbone infrastructure for the data transfer of Copernicus.

The authorities that use the derived services are usually the ones responsible for the definition, implementation of a public service / policy in the following areas: Atmospheric monitoring, Marine environment monitoring, Land monitoring, Climate change, Emergency management (e.g. civil protection) and security (e.g. border guards).

Finally, staff of the research sectors (universities or any other research and education establishment), charities, non-governmental organizations and international organizations are also interested in using COPERNICUS data for their various applications.

Connected units and their use of secure SATCOM

Secure SATCOM can be used to retrieve directly data from the satellites to the ground.

Six Sentinel satellites were in service as of May 2022. Sentinel-1A and 1B provides all-weather, day and night radar imagery for land and ocean services. Sentinel-1A was launched in 2014 and Sentinel-1B was launched in 2016. Sentinel-2A and 2B provides high-resolution optical imagery for land and emergency services. Sentinel-2A was launched in 2015 and Sentinel-2B was launched in 2017. Sentinel-3A and 3B provides high-accuracy optical, radar and altimetry data for marine and land services. Sentinel-3A was launched in 2016 and Sentinel-3B was launched in 2018. Sentinel-5 Precursor is dedicated to atmospheric composition monitoring, Sentinel-5P is a payload embarked on a MetOp Second Generation satellite. Sentinel-5P was launched in 2017.

Sentinel-6A provides data about surface of the oceans (waves, surface winds, sea level) used for short-term marine meteorology forecasts and measurements of evolution of the height of the oceans. Sentinel-6A was launched in 2020.

Dynamics and drivers of the demand

Six high-priority additional Sentinel missions are under development to address EU policy and gaps in Copernicus user needs and to expand the current capabilities of the Copernicus space component:

- CHIME: Copernicus Hyperspectral Imaging Mission.
- CIMR: Copernicus Imaging Microwave Radiometer.
- CO2M: Copernicus Anthropogenic Carbon Dioxide Monitoring.
- CRISTAL: Copernicus Polar Ice and Snow Topography Altimeter.
- LSTM: Copernicus Land Surface Temperature Monitoring.
- ROSE-L: Copernicus L-band Synthetic Aperture Radar.

They will help to address challenges such as urbanisation, food security, rising sea levels, diminishing polar ice, natural disasters and, of course, climate change[1]. Such additional satellites and missions will reinforce the **need for high volume of data to transfer in real-time**.

Geographical coverage	Worldwide

[1] ESA. Copernicus Sentinel Expansion missions.

Space infrastructures use case (EGNOS & Galileo)

Actors

Galileo and EGNOS are the EU system components part of the European Global Navigation Satellite System (GNSS).

Both programmes are managed by the European Commission with the support of EUSPA in specific aspects related to the operational management, security monitoring and accreditation as well as the development of the downstream market and integrated applications leveraging the components and their synergies.

Galileo and EGNOS offer accurate and reliable Positioning, Timing and Velocity via the provision of several services to a broad range of users, from Consumer solutions, Mobility and Governmental applications as well.

Connected units and their use of secure SATCOM

In both architectures of Galileo and EGNOS systems, three types of links exist:

- **Internal links.** For instance, between the Reference Monitoring Stations and the Central Facility of the system.
- **External links** serving as interface to other system providers (e.g. Galileo satellites host a SAR payload, which receives signals from users in an emergency situation).
- **User links** which includes ranging signals and data dissemination.

The use of secure SATCOM might contribute to the availability and reliability of the GNSS infrastructure and service provision, when it comes to transferring within the ground segment, with external providers and when disseminating data to the end-users.

EGNOS: The Reference Monitoring Stations are named RIMS (Remote Integrity Monitoring Stations) and the Central Facility is named CPF (Central Processing Facility). The CPF is a module of the MCC (Mission Control Centre) that uses the data received from the network of RIMS to compute the corrections and integrity of the message.

Galileo: The Reference Monitoring Stations are named GSS (Galileo Sensor Stations) and the Central Facility is named GMS (Galileo Mission Segment). The GMS is responsible for the determination and uplink of navigation data messages.

Dynamics and drivers of the demand

The number of ground stations (both RIMS and GSS) are forecast to increase in order to provide enhanced accuracy or higher reactivity for Safety of Life applications. This increase is the main driver of the demand growth, for both EGNOS and Galileo.

Geographical coverage	Worldwide

Space infrastructures use case (SSA & ground segment)

Actors

SSA (Space Situation Awareness) is the EU Space programme component dealing with detection, tracking and cataloguing of space objects to determine their orbits and predict future collisions, fragmentations and re-entry events of satellites and/or debris.

Space debris is one of the principal threats to satellites and it is estimated that 750,000 debris objects larger than 1 cm orbit around the Earth. After launch and deployment into orbit, space debris is often the next highest risk to a satellite mission. Space sustainability – and by extension, SSA/STM- are topics which are garnering increasing attention worldwide by both government and private sector actors.

European national governments have developed communication programmes for both military and governmental needs. As most of those space systems are linked to sovereign needs, satellite communications could be used as a backup solutions to exchange data in the frame of the ground segment infrastructure.

Connected units and their use of secure SATCOM

In the frame of SSA, satellite communications could be used:

- as a backup connection for the users.
- to transmit data from and interconnect the ground-based sensors.
- for access to the space-based sensors (deployed on space assets) for the TCR (Telemetry, Command and Ranging).

For miliary/governmental satellite system, secure SATCOM could provide the sovereignty, level and guarantee needed to exchange data in the frame of the Ground Segment infrastructure.

Dynamics and drivers of the demand

The EU SST network is comprising of sensors to survey and track objects in all orbital regimes (LEO, MEO, HEO and GEO). The network relies on different types of sensors such as radars, telescopes and laser ranging stations. As part of the EUS Space Pogramme , EU SST will continue to provide operational services related to surveillance and tracking of space objects that orbit the Earth, while expanding its user base and developing additional services aimed at improving the safety and sustainability of space activities in the frame of the Space Traffic Management (STM) initiative. Currently more than 130 organizations are receiving these services and more than 240 European satellites are safeguarded from the risk of collision.[1]

Several European countries have long-standing national communications programmes managed by their armed forces. While France was the first European country to operate such dedicated assets, Luxembourg, Italy, Spain and Germany have also deployed their first-generation systems during the last decade. Those systems currently offer a combination of frequency bands to serve military requirements.

Certain systems also support certain civil requirements, and/or have agreed to make capacity available to partner countries and organisations. Considering the current status, three countries in the EU have either recently launched new generation systems (France with Syracuse-4A and Syracuse-4B) or plan to launch these in the next three to four years (Italy, Spain). The German government's current satellites (COMSATbw-2A and COMSATbw-2B) is estimated to reach their end of life before the end of this decade, and they plan to invest in successor programmes.

Geographical coverage	Worldwide

[1] https://www.eusst.eu/wp-content/uploads/2021/12/eu-sst-leaflet.pdf.

Institutional communications use case

Actors

EU Representations Offices: EU Delegations are a huge strategic asset for the European Union and the achievement of a more coherent, visible and effective external action. Indeed, EU Delegations are reportedly the primary source of political information on a given country context for European Commission (Brussels). They are hybrid administrative constructs that combine diplomatic tasks and operational tasks (as development cooperation and trade). EU Delegations are also responsible for coordinating and chairing EU working groups and meeting in third countries.[1]

National diplomacy: In addition to their national duties, the diplomatic missions of European member states work in a close relationship with EU Delegations. Indeed, both diplomatic representations have to coordinate to ensure the external representation of EU foreign policy with third countries and multilateral organisations. Moreover, EU Delegations can provide complementary support to Member States in their role to provide protection to EU citizens.

ECHO field offices: The EU Civil Protection and Humanitarian Aid Operations department has been providing assistance to people in need (both Civil protection and Humanitarian Aid) since 1992. The presence of field humanitarian staff across the world enables the Commission to have an up-to-date overview of humanitarian needs in a given country or region, which enables the better development of intervention strategies and policy.

Connected units and their use of secure SATCOM

European Institutional organisations mainly use terrestrial networks. However, satellite communications are generally used by institutional organisations either as a back-up solution (when terrestrial means cannot provide the relevant level of Quality of Service) or when security of the communication cannot be guaranteed due to the dependency to any local (or any third-party) entity. The European Union, its organisations and the Member States, are in charge of critical missions requiring guaranteed, secured and resilient communications means. Some of the regions of strategic interest to the EU (as the Polar, the Atlantic and Africa regions) lack connectivity infrastructure. Moreover, embassies, consulates (or any diplomatic representations) are at the forefront of any crisis to lead and manage the required actions. **Satellite connectivity is estimated to then be used as the primary connectivity option.**

Secure SATCOM represents a vital technology for various institutions that need to maintain reliable and confidential communication channels in different scenarios. Some examples of such entities are:

- EU Representations Offices: secure SATCOM can be used to provide a secure and autonomous communication means between Brussels HQ to the EU Delegations; even if many responsibilities have been transferred from Brussels HQ to the EU Delegation over the last 20 years.
- National Embassies: Similar to the EU Representations Offices, national embassies also need secure and autonomous connectivity system. Not only to interact with their national country but also to interact with EU Delegations.
- ECHO Field Office: Connectivity is not only needed for the ECHO Field Office. ECHO has also to rely on both international experts and national staff members to carry out their mission dedicated to providing governmental aid in preparation for or immediate aftermath of a disaster in Europe and worldwide.

Institutional communications use case is estimated to be one of the three major contributors for the secure SATCOM capacity demand.

Dynamics and drivers of the demand

The trend for Institutional Communications use case is similar to the one observed for the EU External Actions use case (cf. page 48). The EU Delegation, national embassies and ECHO are all at the heart of the EU external action. The geopolitical context, cyber and hybrid threats further prompt security and resilience concerns. It significantly increases the need for a guaranteed and secure access to communications means for all diplomatic activities in an unrestricted manner.

Geographical coverage	Worldwide

[1] ECDPM. 2014. A closer look into EU's external action frontline: framing the challenges ahead for EU Delegations, March 14th.

Other Critical Infrastructures use case

Actors

The other critical infrastructures use case includes the sites which – due to the nature of their activities (both industrial and financial) – require a guaranteed, reliable and secured communication link as a back-up.

There are many critical infrastructure/industrial sites operated by European private and public entities which require secure and resilient communication links. In the frame of the report, we decided to focus on key sites of:

- **Industry & Energy infrastructure:** SEVESO Sites, Nuclear power plants and coal-fired power stations.
- **Financial infrastructure:** European Central Bank and National central banks.
- **Data Centre:** Data Centres with high data rate required. Satellite communications can be used as a backup solution to increase the resilience of the data transmission to and from the site where it is located.

Connected units and their use of secure SATCOM

Whatever the connected unit, satellites are able to offer **a reliable and guaranteed continuous communications** in case of a major accident.

A SEVESO site is defined as an industrial site which pose major risks due to their activity which include the handling, the manufacturing, the use or the storage of hazardous substances such as oil depots for instance. SEVESO is the name of an Italian city where a major industrial accident happened in 1976. SEVESO name was given to a European directive in 1982 which aims to limit the risks of industrial accidents and their consequences. The second element considered in the frame of Industry & Energy infrastructure are nuclear power plants. Here, we refer to the ones used for electricity generation but definitively exclude the nuclear elements covered by relevant nuclear legislation (treaties and Community Law).

Thirdly, the coal-fired power stations which burn coal to produce electricity. Even if their number in Europe is forecast to decrease over the coming decade, they pose a major industrial risk and need to have reliable and guaranteed means of communication whenever is necessary.

At a financial infrastructure level, the European Central Bank is the central bank of the 19 European Union countries which use the Euro. We also include the Central Bank of every European Member state.

Finally, Data Centre covers a diversity of needs such as State institutions and energy undertaking or General Healthcare System. They require data rates greater than 100 Mpbs.

Such critical elements mostly need low-latency satellite capacity **through secure SATCOM**.

Dynamics and drivers of the demand

Industrial risks are more and more taken into account at legislation level (cf. the rise of SEVESO sites during the past decade). In December 2021, the European Commission is preparing to classify nuclear as a green energy, paving the way to a continual use of nuclear energy[1].

Banking sector – and especially the European and National infrastructure – are strategic assets for the European Union. It is not expected the number of those entities increase in the coming decade but their need for reliable, secure and guaranteed communication means would increase.

Digital transformation of both the EU economy and society is accelerating and the digital information infrastructure as well. Among them, data centres are key for their contribution to resilience, to EU data protection and confidentiality standards. Their use is expected to rise in the coming decade. An illustration of which is the European Union investigation to improve the energy efficiency and circular economy performance in cloud computing and data centres[2].

Geographical coverage	European Union

[1] Toute l'Europe. 2023. Energie nucléaire: quells sontles principaux pays producteurs en Europe, June 15th.

[2] European Commission. Green cloud and green data centres. Shaping Europe's digital future.

Polar regions use case

Actors

In Polar Regions use case, we consider Arctic regions (for what it may concerns in the report, Polar regions means Arctic). We refer to Polar as the territories located above 60°N in the EU. This includes Finland and Sweden. Denmark is not included, except Greenland and the Faroe Islands (as their latitude is above 60°N). When part of the territory is located below 60°N (true for both countries), secure SATCOM connected units and total demand are for areas located above 60°N.

National players in Finland, Sweden (plus Greenland and Faroe Islands):

- Government organisations: Includes government offices, first responders (firefighter stations and police stations) and coast guards.
- Public institutions: Includes hospitals staff, dentist, physician offices, nursing/residential care facilities, teachers and students.
- Scientific research institutes: Includes wildlife observation, climate research and community studies in the Polar regions.

EU players: This includes commission representations and offices of the European Union External Action in the Polar member states, and decentralised agencies that aim to contribute to the implementation of EU policies. EU players also include EU agencies with activities in the Polar including FRONTEX (for border control), EFCA (fisheries regulations) and EU-PolarNet (European Polar research programme). The EU's updated Arctic policy (published on October 13, 2021) aims to help preserve the Polar areas as regions of peaceful cooperation, to slow the effects of climate change, and to support the sustainable development of Polar regions to the benefit of Polar communities, not least Indigenous Peoples, and future generations.

Connected units and their use of secure SATCOM

Terrestrial telecommunications infrastructure in the Polar regions remains sparse or inexistent in some areas. Considering the small addressable market and high operational costs, service providers and telecom operators are generally reticent to provide broadband services in Polar regions. Moreover, the existing networks are heterogeneous, seldom meeting the required speed and latency of today's operational needs. Satellite communications are a relevant way to provide a **minimum level of communications**, notably for highly sensitive activities (e.g. medicine, law enforcement, coast guards).

The Healthcare institutions (hospitals, dentist and physician offices, nursing and residential care facilities as well as medical and diagnostic labs) can benefit from the advantages of secure SATCOM. Connectivity requirements for telemedicine, complete Internet access and backups to terrestrial links. For schools, secure SATCOM can be used for e-learning, intranets and complete Internet access. For Government offices, secure SATCOM can be used as a backup solution to a terrestrial network in case of a failure or to divert over extended terrestrial networks during peak hours. Border and Coast guards have a wide variety of assets deployed including Aircraft carriers, Submarines, Amphibious, Frigate/Destroyer, Mine countermeasures, Patrol, and Auxiliary vessels. All those assets can be equipped with relevant terminals for satellite connectivity. Finally, secure SATCOM can also be the unique connectivity mean for EU offices (including offices of decentralised agencies, of commission representations, and of the EU External Action) and staff involved in EU missions in the Polar regions to support activities such as research, border control.

Dynamics and drivers of the demand

In addition to the increasing demand for high bandwidth applications (such as video conferencing and video streaming) by the Polar population, secure SATCOM is needed to connect the governmental actors to fulfil EU and National policies. The national policies are not only fulfilled by countries in Polar regions but also by other EU players.

More generally, Polar regions has been a region of growing environmental, commercial, military and strategic interest for many nations (U.S., Russia, China …). Secure SATCOM can provide **resilient communication system** capable of supporting the interests in those geographical areas.

Geographical coverage	Polar

SECURE SATCOM MARKET: SUPPLY

© wirestock.com

Chapter Summary

After having presented the secure SATCOM market in terms of use cases, demand capacity forecast (Mbps) and business models, this chapter introduces the supply of secure SATCOM services and the factors that influence it. It helps to understand how the satellite-based connectivity market is changing and growing from a supply point of view, as well as the main technologies, actors, and dynamics that are transforming it. It also helps to understand the existing and planned governmental and commercial satellite systems that would provide secure SATCOM services. The chapter covers the following topics:

- The selected dynamics and drivers of secure SATCOM supply that are shaping the market. It identifies several technology drivers that are transforming the satellite-based connectivity ecosystem and the estimated impacts of these changes for secure SATCOM in the EU.
- The supply by geographical areas for secure SATCOM services. It is presented with two categories of countries: Category I (EU member states) and Category II (non-EU countries with strategic interest or partnership with EU). It also discusses some additional key drivers for governmental supply of secure SATCOM services.
- The trends for the capacity supply from Category I and Category II countries for governmental satellite systems and commercial GEO and NGSO systems over the 2025–2040 period. It presents some potential dynamics over 2025–2040 while providing some key players and case studies that will be instrumental to the future supply of secure SATCOM.

Introduction

When it comes to secure SATCOM capacity and assets owned by organisations based within the EU, the landscape can be summarised by GEO and MEO/LEO orbits.

The capacity from assets located in geostationary orbit:

- is estimated to be available in essentially all of the major frequency bands being used to support voice and data streams, with the possibility to support various activities. It is noteworthy that those assets belong to either national government or private organisations with a different ability to access to such capacity.
- is available depending on the location. Most systems offer capacity covering all of European Union and/or a larger part (or at least all of Europe by combining several of them). Coverage can then vary depending on the locations outside the European Union.

The capacity from assets located in MEO and LEO orbit:

- is currently available through a single constellation of satellites, such as SES's O3b, operating in the MEO orbit, and in a single frequency band. The new spacecraft for the second generation of the system have started to be launched from December 2022 and the enhanced service is estimated to be available from Q4 2023.
- is not available from LEO orbit yet. Additional LEO systems are currently planned and/or under development, at least for the supply of IoT capabilities.

A single constellation consisting of 3 GEO spacecraft, or less than 10 MEO spacecraft, or at least several hundreds LEO spacecraft, can provide a sufficient worldwide coverage and services (except for Polar areas in case of GEOs and MEOs).

Finally, it is noteworthy to mention that the necessary secure SATCOM capacity is highly dependent on use cases and associated specific operation/mission. For example, Data Center (in the frame of Other Critical Infrastructures use case) would require high data links of more than 100 Mbps, potentially increasing to 500 Mbps over the forecast period to 2040.

Note: C-, Ku- and Ka-band are the most common frequency-band used in SATCOM, including secure SATCOM, by now. Higher frequency bands (such as Q/V-band) tend to favour broadband connectivity due to the larger spectrum available, leading to higher throughputs. In the meantime, higher frequency bands tend to be more sensitive to weather conditions such as rain, clouds and fog.

Overview of SATCOM frequency bands

	Frequency band	Frequencies	Applications
Possible "Broadband Connectivity"	Protected EHF (Extremely High Frequency)	30 GHz to 300 GHz	For military applications.
	V band	40 GHz to 75 GHz	Video and data. Inter-satellite links.
	Q band	33 GHz to 50 GHz	Video and data. Inter-satellite links.
	Ka band	27 GHz to 40 GHz	Video and data. (Military applications for part of the spectrum named Mil Ka band).
	Ku band	12 GHz to 18 GHz	Video and data.
	X band	8 GHz to 12 GHz	Mainly used for military applications.
	C band	4 GHz to 8 GHz	Video and data.
"Narrowband"	S band	2 GHz to 4 GHz	S-band supports applications such as deep space communications, weather radar and ship radar.
	L band	1.2 GHz to 1.8 GHz	L-band supports GNSS as well as satellite mobile phones enabling sea, land and air communications.
	UHF (Ultra High Frequency) band	0.300 GHz to 1 GHz	UHF is used for mobile communication and meteorological satellites.

Technological drivers transforming the secure satellite-based connectivity

Several structural drivers have started to transform and largely increase the volume of capacity offered through satellite assets. These will likely also impact the capacity and services available for secured connectivity. Overall, digital technologies are at the heart of this transformation alongside the use of higher frequency bands and other features. Ultimately, the benefits will likely go in three directions:

- An increase in the **volume of available capacity**.
- A **higher flexibility** in the ability to dynamically allocate the capacity and design of services.
- A **higher cost efficiency** of satellite assets.

While several drivers are estimated to apply in the coming decade, it is important to keep in mind that the visibility on several impacts, including on the implementation of current and emerging technologies in operational networks, is significantly higher for the next three to five years and tentatively to the end of this decade. It is important to bear in mind that most programmes can require a **minimum of three to five years to become operational** networks (including GEO and NGSO assets) with potential longer development time for complex systems and/or complex infrastructure. Examples of these would be:

- The development time for government (in particular military) satellite systems will often take a longer time due to the complexity of the system and the need to develop unique security features.
- The development of at least the first generation of NGSO constellations have to date required more than five years, from the inception of the programmes to the start of commercial services. This currently applies to projects (outside European Union) such as Starlink and OneWeb that already started their commercial operations. The reasons for the development time includes the need to develop new manufacturing process (including new factories for the mentioned projects), the time to raise the required financing, the manufacturing and deployment time and other aspects.

Some future innovation and deployment cycles already identified

As for any technology, new space-based connectivity solutions can be subjects to certain limits and/or require cycles of adoptions. For instance, the need to deploy new terminals, either because the new networks make use of new frequency bands, or because their design (e.g. a NGSO network) requires a fast-tracking antenna.

The specific requirements of secure connectivity should also be considered, with the need to either validate existing solutions or to adapt them to the user requirement. One example can be found in the observed trends associated with the **use of software defined and/or cloud solutions**.

The existing and future secure connectivity programmes will have to meet the user requirements while also trying to take profit from the existing and upcoming solutions. As mentioned before, the use of software defined and/or cloud solutions is a clear technological trend which will increasingly impact space-based connectivity.

An adaptation of the worldwide SATCOM ecosystem

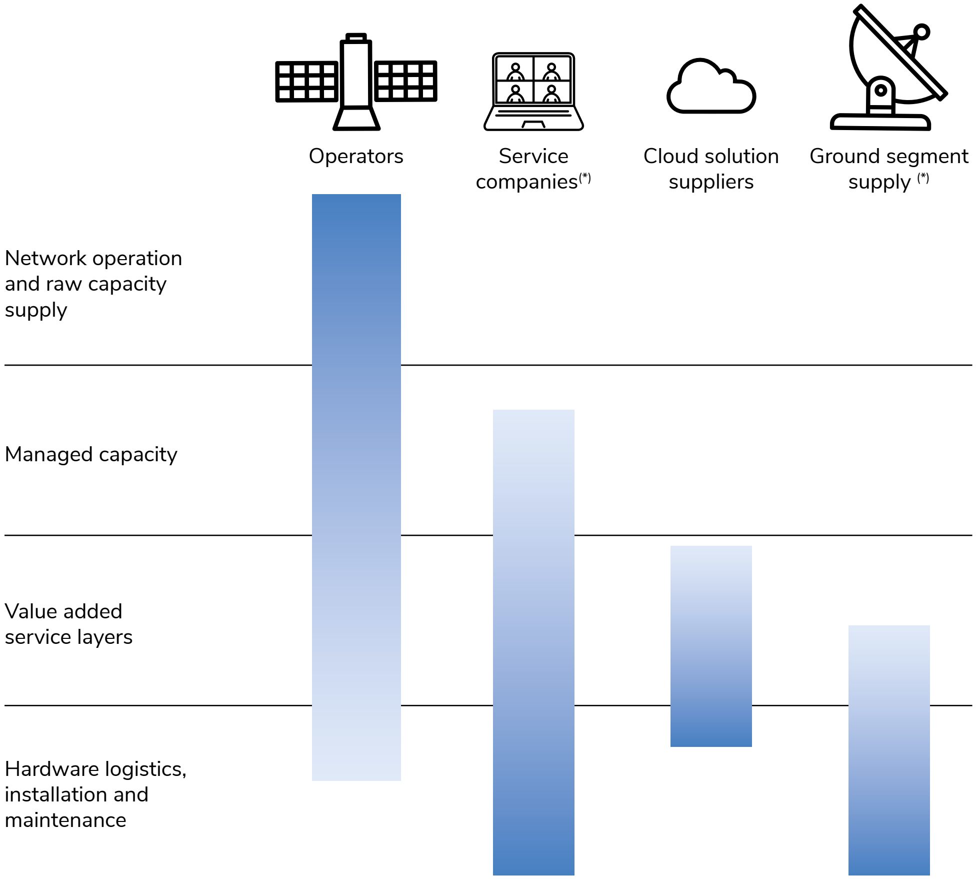
Satellite connectivity ecosystem is changing

The worldwide satellite connectivity market is subject to significant future changes, triggered by the ongoing technology advances and their impact on industry operations and economics. It is useful to summarize the most important global changes impacting the commercial satellite ecosystem, including vertical integration, presence of new entrants and a potential consolidation. Secure SATCOM, as a part of SATCOM, is logically impacted by such evolution.

A trend toward **vertical integration** exists, where satellite network operators get more involved into the management of capacity and the delivery of satellite services. This vertical integration can go in two directions: Firstly, certain service companies can progressively acquire satellite systems in order to provide an end-to-end capability. Examples of such organisations include Hughes Network Systems (U.S.), Viasat (U.S.), and more recently Anuvu (Canada). The graph on the right illustrates the vertical integration trend, where different players - rather than occupying a single segment begin to move up and/or down the value chain-. Secondly, wholesale operators develop managed capacity and service capabilities. Examples include SES, Eutelsat, Intelsat, Telenor, Hispasat etc. These can be either based on organic investments, and/or involve the acquisition of third-party companies. This vertical integration tends to be organized in a tactical way, and the level of integration can vary depending on the vertical segment.

More than half of the operators of NGSO satellite broadband constellations correspond to new entrants in the satellite connectivity ecosystem. While the EU operators have made an early move to launch their NGSO (SES + Eutelsat/OneWeb), upcoming NGSO projects seem to occur outside of the EU. The new projects have also branched out into innovative space and ground solutions.

Satellite connectivity ecosystem – dynamics



(*) Excluding fully vertically integrated companies

Note: Defence users often act as the secured SATCOM operators and provide the secured SATCOM services to the armed forces directly "in house", rather than outsourcing this to commercial entities.

An adaptation of the worldwide SATCOM ecosystem (continued)

Several large tech companies offering cloud solutions have started to take position in the satellite data and connectivity market, as there is an expected increased use of cloud solutions in SATCOM service provision. Such companies include the Amazon Group and AWS, Microsoft, and Google, with several partnership announcements since 2021. We anticipate that those groups (whose HQs are not based in the EU) will significantly increase their involvement in the coming years. An ongoing trend is the installation of satellite antennas in data centre sites in order to provide direct access to the resources of the associated data centres to data and/or connectivity clients.

A potential consolidation led by historical market leaders is likely to be reinforced. In order to benefit from economies of scale and/or to acquire new capabilities, several incumbent operators and service companies have either been involved in transactions or announced publicly that an industry consolidation could make sense. As examples of recent transactions:

- Eutelsat and OneWeb decided to combine their activities; the transaction was closed in Q3 2023.
- The service provider Marlink acquired in 2020-2021 ITC Global, a subsidiary of Panasonic, as well as the land service activities of Anuvu.
- Viasat (U.S.) finalized the acquisition Inmarsat (U.K.) on the 31st of May 2023. This transaction will significantly impact the operations of the two organisations.
- In December 2020, Intelsat (U.S.) completed its acquisition of the Commercial Aviation business of Gogo (U.S.). On the 13th of July 2021, the Gogo name was dropped.
- Ground segment supplier ST Engineering iDirect (Singapore) acquired Newtec (Belgium) in 2019.
- In December 2018, the service provider Speedcast (U.S.) acquired Globcomm (U.S.).

Key impacts for secure SATCOM in the EU

EU based space companies could be acquired by non-EU organisations	In view of the ongoing consolidation dynamics, the possibility to see **certain EU suppliers being acquired by non-European organisations** seems likely. In this case, it will be more sensitive when considering large network operators and/or technology companies.
Involvement of cloud suppliers is estimated to increase	**Cloud solution suppliers will take an increasing role in the connectivity ecosystem**. Their role, either in the management of satellite network, and/or for the management of end user data will have to be considered within secure SATCOM solutions, especially if such cloud suppliers are non-EU companies.
A living ecosystem to support secure SATCOM	Technology disruption will result in the presence of new entrants as well as in the adaptation of existing organisations. As such, **any programme for secure SATCOM would have to enable the participation of new organisations** over time.
Digitalisation of the SATCOM network	Digital disruption impacts of the space ecosystem: space and ground segment, ground station and satellite communication services. Coping with such a digital revolution will require a **significant and continuous R&D effort** from European Industry.

Considered geographical areas

As mentioned on page 58, secure SATCOM capacity/services can be provided from assets belonging to either national government organisations (Governmental supply) or to private organisations (Commercial supply).

Geographical distribution for Governmental supply

The geographical distribution used (in order to categorise the origin of the capacity, relying on the system owner), can be separated into three primary categories :

- **Category I**: Countries which are a European Union Member States.
- **Category II**: Countries which are not part of Category I countries, but which have extended relationship with European Union : United Kingdom, Norway, Canada and Switzerland.
- **Category III**: Countries with are neither part of Category I, nor part of Category II. Category III countries are shared into the following sub-categories: Sub-category III.1: North America – Sub-category III.2: Latin America and Caribbean – Sub-category III.3: Middle East and Africa – Sub-category III.4: Asia.

The definition of geographical distribution for Governmental supply is used from page 64 to page 68.

Geographical coverage for Commercial supply

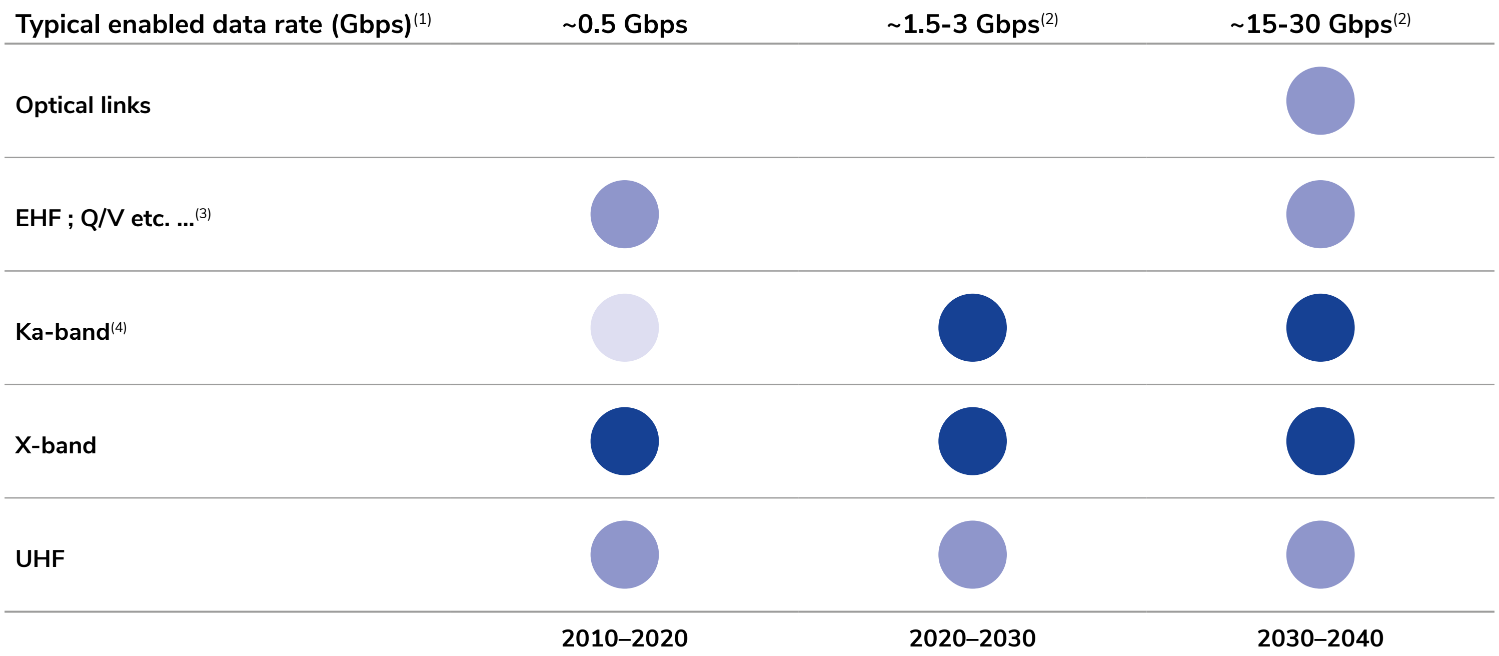
The geographical distribution for the analysis has been grouped into three categories:

- **Category I**: Satellite Commercial Operators which have their Tax residence, Management and Operational Facilities in a European Union Member State.
- **Category II**: Satellite Commercial Operators which are not part of Category I countries, but which have their Tax residence, Management and Operational Facilities in a country which has extended relationship with European Union: United Kingdom, Norway, Canada and Switzerland.
- **Category III**: Satellites which are neither part of Category I, nor part of Category II.

The definition of geographical distribution for Commercial supply is used from page 69 to page 74.

Typical GEO government payload profile and enabled data rate

For GEO government owned systems, various types of payloads are expected to be deployed up to 2040. If Ka-band is expected to represent a significant share of the payloads, the move to high-frequency-band is estimated to lead to the deployment of payloads in Q/V-band and optical payloads. Such payloads are mainly expected in the next decade.



Typical enabled data rate (Gbps)[1]	~0.5 Gbps	~1.5-3 Gbps[2]	~15-30 Gbps[2]
Optical links			●
EHF ; Q/V etc. ...[3]	●		●
Ka-band[4]	●	●	●
X-band	●	●	●
UHF	●	●	●
	2010–2020	2020–2030	2030–2040

Legend: The darker the blue, the higher the quantity of payloads are estimated to be deployed.

[1] Typical enabled total data rate for a GEO government owned system. Data relay is not included here.
[2] Based on satellites under procurement for which information is available.
[3] Includes several types of high frequency-band.
[4] Primarily "military" Ka-band. One satellite launched in the last decade (Athena-Fidus) also makes use of the "civilian/commercial" Ka-band spectrum.

Overview of the governmental satellite systems in Cat I and Cat II

European national government will likely continue to increase their capacity through modernisation programmes

Several European countries have long-standing national communication programmes managed by their armed forces. While France was the first country to operate such dedicated assets, other European Member States including Luxembourg, Italy, Spain and Germany deployed their first-generation systems during the last decade.

Those systems currently offer a combination of frequency bands, to serve military requirements from their respective countries. Certain categories of them also support some civil requirements, and/or have agreed to make capacity available to partner countries and organisations.

While two joint satellite programmes were developed between France and Italy (Athena-Fidus and Sicral), the difficulties of aligning programme priorities and schedules amongst other factors, has resulted in all countries investing to date in proprietary assets for their next generation programmes. Since 2019, Greece has an operational Governmental Satellite Communication system ("GreeCom") connecting Ministries, Parliament, Embassies and civil protection authorities.

Considering the current status, three countries in the EU have either recently launched new generation systems (such as France with Syracuse-4A and -4B) or plan to launch these in the short term (Italy, Spain). Others, whose current satellites are estimated to reach their end of life before the end of this decade, will likely invest in a successor program.

Overall, we observe that new generation assets have come with new capabilities, going in the direction of more broadband capability and in more flexible assets. Overall, information available on new generation assets suggest that they will have at least three times more capacity, as estimated for the Syracuse-4 satellites (at least the 4A and 4B)(1).

Capacity sharing mechanisms to support government requirements

National governments have been long term users of commercial satellite capacity to support their operations.

At the European level, the European Defence Agency (EDA) established the EU SATCOM Market mechanism, now supported by 34 contributing members. Total orders in the pool have reached +675 SATCOM orders and €80.2 million over the 2012–2022 period. In 2022, the second framework contracts for communication and information system services were awarded to Airbus Defence and Space and Thales SIX(2).

More recent initiatives have included work on the design of **GOVSATCOM Hubs**, that will be in charge of monitoring and ensuring the overall capacity and service planning as well as the security of the overall system (cf. page 12).

Other mechanisms found internationally can include partner countries in a government programme, in particular the WGS (Wideband Global SATCOM) programme in the U.S., and the procurement of capacity by NATO to support the operations of the Alliance.

As mentioned in the Regulation (EU) 2023/588 of the European Parliament and of the Council of the 15th of March 2023, IRIS^2 shall complement and expand the existing and future capacities of the GOVSATCOM component of the Union Space programme.(3)

(1) Opex360.com, February 2023: Télécommunications par satellite : La Marine nationale a reçu ses premières stations navales Syracuse IV

(2) EDA, 2022: EU SATCOM Market Factsheet

(3) Regulation (EU) 2023/588 of the European Parliament and of the Council of the 15th of March 2023, establishing the Union Secure Connectivity programme for the period 2023-2027, OJ L 79, 17.3.2023, p. 1–39.

Additional trends for governmental supply

The following table provides a selection of key drivers for the supply of secure SATCOM capacity by government satellite systems. This comes as an addition to the generic technology drivers presented at the beginning of this chapter.

New generation governemental systems under development for several European countries	Most governments in the EU that currently own and/or operate government communication satellite systems, including France, Germany, Italy and Spain, are currently investing in new generation programmes. Those new generation systems are estimated to have extended capabilities, while offering continuity in the ability to use the frequency bands available on the previous generation. Target launch dates are spanning through this decade. Those assets are primarily in the GEO orbit and make use of the "military" frequency bands. Based on programme cycles, where new generation systems have been deployed on a ten to fifteen-year basis, a successor generation is estimated to be deployed in the 2030–2040 time period to replace and augment the current assets.

Investment in new capabilities observed internationally	On a global scale, investments in new generation capabilities are being observed in most parts of the world: • In the U.S., new confirmed satellite programmes for the U.S. defence sector include for example the WGS-11 satellite[1]. The ESS (Evolved Strategic Satellite) programme will also commence in the next decade and will eventually replace the AEHF (Advanced Extreme High Frequency Satellite) network[2]. In addition, a numąber of maintenance and modernisation programmes are being organized in order to both maintain current user terminals in operating conditions but also to develop new networks. • A number of other countries have recently procured, and/or have announced their intention to work on new generation systems. a non-exhaustive list includes the Australia, Brazil, Egypt, Japan, Korea, Qatar, the UAE, U.K.

[1] USSF, February 2022: Wideband Global Satellite Communications Program completes major milestone in development of WGS-11+ Satellite }and Ground System

[2] Northrop Grumman, September 2020: ESS program will interoperate with and eventually replace the Space Force's AEHF system

Additional trends for governmental supply (continued)

Certain European countries are partners and/or users of government programmes

While Luxembourg was the only one country in the EU to launch its first national government communication in the last decade (i.e. Luxembourg) and while no concrete plan has been announced to date for the remaining countries that do not own such satellites, it is noteworthy that a number of countries have either invested and/or make use of international programmes to support their government communication requirement.

- A first example is the U.S. WGS satellite programme, which includes a set of international partners. Partner countries in the EU include Denmark, Luxembourg and the Netherlands[1].
- Initiatives have been started at the EU level. The current operational mechanism is mainly the procurement of the assets by the governmental entity, while other mechanisms have been explored such as through a service contract or Pooling & Sharing (cf. page 12 with the GOVSTCOM Hubs).

Change in user requirement playing part in new asset deployment

Operations conducted by civil and defence forces have changed significantly in just the past decade. Taking several examples:

- Defence missions conducted in external theatres have required a higher focus on mobility and flexibility, in view of the large operation theatres, and of the nature of the threats.
- In the EU, activities related to border surveillance have significantly increased, requiring a more active monitoring of both the maritime and land areas.
- The increasing use of certain new assets, such as RPAS (Remotely Piloted Aircraft System), have resulted in new and/or changing requirements.

Those changes have had (and will continue to have) an impact on the design on new government satellite assets, with for example a stronger focus on mobile communications enabled by the upcoming satellite systems.

[1] NSR, February 2023: it is official, WGS 12 is on its way

Governmental supply from Cat I countries (2025–2040)

Situation up to 2025

The governmental supply for secured SATCOM from Category I countries mainly relies on GEO satellites until 2025. Overall, the total government satellites operated are estimated to remain relatively stable at around 9.

New generation systems will also offer continuity and/or an increase in the supply of frequency bands including Ka-, Mil Ka-, UHF and X-band. The capacity additions up to 2025 are estimated to primarily result from the launch of Syracuse-4A (launched in October 2021) and Syracuse-4B (launched in July 2023) by France. The Italian Sicral 3A satellite is estimated to enter into service around 2026[1]. The Spanish satellites Spainsat-NG1 and Spainsat-NG2, to be operated by Hisdesat for the Spanish government, are estimated to be launched in 2024–2025[2].

KEY UNDERLYING ASSUMPTIONS for 2025–2040

- Owners of the major Government and Defence systems will renew their assets in the two coming decades.
- Relying on technological upgrades to counter new threats, new space assets will offer more capacity per asset.
- Part of the capacity needs can move to lower orbits (advantages of NGSO vs. GEO).
- None or only a few new countries from Category I would invest in a dedicated Government and Defence Systems.

Evolution over the 2025–2040 period

Over the 2025–2030 time period, four satellites are estimated to reach their theoretical End Of Life (EOL): COMSATbw-2A and COMSATbw-2B, Athena-Fidus and Sicral-2. In the meantime, four satellites are under procurement, including Spainsat-NG2, Sicral-3A, Sicral-3B. In addition, the Italian Space Agency announced in 2019 the procurement of an Ital-GOVSATCOM satellite as a contribution to the EU GOVSATCOM initiative[3]. We also anticipate the procurement of at least replacement capacity for the two German COMSAT bw satellites. The new satellites are estimated to offer more capacity than their predecessors, largely through the addition of Ka-band capacity. Capacity is estimated to typically be up to several Gbps.

Over the following decade, a new generation of assets is estimated to be deployed to replace and augment the capacity deployed in the early 2020s, as it is anticipated that the connectivity requirement of the national governments will increase. While new countries may consider the launch of national systems, the probability is considered as relatively limited. While completely new architectures shall be considered, including the use of smaller assets in different orbits, we currently consider that the investment in anchor large capacity GEO systems is likely to stay, in view also of the orbital positions and spectrum available. With regards to NGSO, the cost to benefit from proprietary global broadband connectivity seems excessive against the requirement of individual countries.

New generation assets are estimated to have more capacity, either due to the use of new frequency bands, of higher power and/or of new optimization techniques, to an increase in the number of beams etc. We also would like to highlight the widespread introduction of optical payloads over the next decade. They will be dedicated to specific applications, but will bring broadband capacity as well.

It is noteworthy to mention that New Space actors bring innovative and cost-effective solutions at a high pace, which could contribute to a potential move of Governmental/Defence entities to purchase services from commercial entities instead of relying solely on their own, custom-designed space infrastructure.

[1] Telespazio, June 2022: Thales Alenia Space and Telespazio sign follow-on contract with Italian Ministry of Defence to develop the SICRAL 3 SATCOM system
[2] SpaceRef, July 2023: Hisdesat will launch the first satellite of the SPAINSAT NG programme next summer
[3] Thales, July 20119: Thales Alenia Space and Telespazio win contract from Italian Space Agency

Governmental supply from Cat II countries (2025–2040)

Situation up to 2025

National government satellite capacity supplied from Category II countries will include two networks in the 2020–2025 time period:

- The U.K. Skynet-5 GEO satellite network. Those assets, procured through a PFI (Private Finance Initiative) programme, is estimated to be nearing their end of life. They offer both UHF and X-band capacity.
- New Highly Elliptical Orbit (HEO) satellites procured in Norway. (HEO satellites provide a better and permanent coverage in Northern latitudes, cf. pages 79).

The U.K. government ordered in the interim communication GEO satellite Skynet-6A in 2020 with a launch planned for the year 2025[1]. This new satellite will likely replace existing capacity and potentially include additional supply in the Ka-band.

From 2024[2], capacity supply in X-band is estimated to increase following the launch of the ASBM 1 and 2 satellites (Arctic Satellite Broadband Mission). ASBM satellites are procured by Space Norway HEOSAT AS, a subsidiary company of Space Norway[3]. The two satellites include X-band payload for the Norwegian MoD (Ministry of Defence) that will provide polar coverage from 65° North as well as an interoperability with the U.S. WGS constellation.

KEY UNDERLYING ASSUMPTIONS

- U.K. is likely expected to pursue the Skynet programme, through GEO “proprietary”capacity, and potentially through the addition of capacity from third party networks.
- Strategic interest for the Polar regions would increase, likely leading Norway to add more capacity between 2035 and 2040 for mobile broadband applications, covering both civilian and military needs in the area.

Evolution over the 2025–2040 period

No satellite is yet formally planned for the 2025–2040 period, though the U.K. government is expected to increase its satellite communication capacity beyond the interim Skynet-6A satellite. Norway’s ASBM 1 and 2 satellites are assessed to reach their theoretical EOL in 2039, while Skynet-6A is expected to do so in 2040.

We anticipate that new government programmes will be procured in Category II countries between 2030 and 2040. The need to continuously support military operations, and the increasing activity in Northern latitudes, is estimated to result in decisions to maintain and expand capabilities.

In line with the assumptions that were applied for the government of the Category I countries, it was assumed:

- The launch of at least one additional GEO system of approximately less than 5 Gbps in the second part of the decade.
- The potential replacement and expansion of the HEO capacity in the second part of the next decade.

The forecast for secure SATCOM for 2040 is influenced by the introduction of optical payloads which will be reserved for specific applications alongside broadband capacity as well.

[1] Airbus, July 2022: SKYNET 6A satellite passes Critical Design Review
[2] Space SYSTEMS Command, July 2023: Space Systems Command and Space Norway Complete Enhanced Polar System Recapitalization Flight One Payload Thermal Vacuum Test
[3] SpaceNews, July 2019: Northrop Grumman to build two triple-payload satellites for Space Norway, SpaceX to launch

Macro trends impacting the GEO commercial supply

Uncertain dynamics from the middle to long-term regarding the addition of commercial GEO capacity over the European Union

Assessing the long-term supply dynamics for commercial satellite capacity from GEO systems presents several challenges. Among these:

- Competition from NGSO systems will be strong and get more competitive over time, especially in all the segments where low latency is considered as a strong added value, and if/when the user terminals are competitive in terms of performance and price. The IRIS² initiative for a satellite constellation would also address European needs[1]. This will be beneficial and support with addressing part of the market gap for GEO satellite platforms. It is worth noting that several European operators have already invested in NGSO capabilities, including SES and more recently Eutelsat with its combination of activities with OneWeb.
- In Europe, considering the open commercial market, capacity from non-European operators, in particular from Viasat in the Ka-band, is estimated to increase significantly with the forecast launch of Viasat-3 EMEA (Europe, Middle East and Africa)[2][3]. This may make the decision to invest in new GEO broadband systems for the European market more challenging in the next few years.

It is noteworthy to mention that the decision to invest in the Konnect VHTS satellite (ordered in 2018) came together with the announcement of significant presales to the Orange and Thales group[4]. It is likely that a new decision to invest could depend on the reach of a high level of use of the Konnect VHTS system, and on the willingness of a set of clients in large European countries to commit to new GEO capacity.

In the near term and at a global level, commercial operators are increasingly opting for flexible GEO satellite systems with medium to large size payloads. The balance between decisions to invest in GEO vs. NGSO capacity in the middle term presents a large level of uncertainty. Our scenario in the frame of this report, assumes the launch of a mid-sized satellite before the end of this decade, and a limited increase over the next decade.constellation.

GEO capacity supply: potential dynamics over the EU

Regarding the different timelines (up to 2040), the potential dynamics are the following:

Near term (before 2025)

- Large GEO HTS capacity addition. As an example from Eutelsat (Konnect VHTS, launched in 2022) and Viasat satellite operators.
- Several operators invest in flexible GEO systems, with some supply possibly over the EU[5].
- Entry into service of several commercial NGSO broadband constellations[6][7].

Middle term to 2030

- Potential slowdown in capacity additions, including from operators in Category I. Possible to have one mid-sized system with targeted coverage.
- Expected deployment of an EU procured NGSO constellation (IRIS²).

Long-term to 2040

- Limited visibility, with dependence on the balance in the use of NGSO and GEO platforms, and on the integration with terrestrial networks.

[1] European Union, March 2023. Factsheet: "Iris²: Infrastructure for Resilience, Interconnectivity and Security by Satellite", March.

[2] Capacity of each Viasat-3 satellite is 1Tbps, The Viasat-3 satellite constellation

[3] The two first Viasat-3 satellites are planned to be launched before 2024: Viasat Q3FY23 sgareholder letter

[4] Orange and Thales secured as distribution partners,Thales, March 2018: Eutelsat commande Konnect VHTS,

[5] Astra 1Q is expected to provide capacity over Europe from 2024, SES H1 2023 results, the 03rd of August 2023, available here: SES financial results

[6] OneWeb plans global coverage for Q3 2023, Eutelsat, August 2023: Eutelsat Investor Presentation

[7] O3b mPOWER to enter into service in Q3 2023, SES H1 2023 results, the 03rd of August 2023, available here: SES financial results

Commercial GEO supply from Cat I countries (2025–2040)

Situation up to 2025

Approximately 30 GEO satellites owned by operators from Category I cover partially or entirely the EU territory. Among them, the vast majority currently carry regular payloads with widebeam coverage. The vast majority of that capacity is used to support video distribution services, while part of them also support data services for different applications, such as inflight connectivity.

In comparison, four satellites had HTS payloads onboard in the second part of 2021, with one from Hispasat 30W-6, Hellas Sat-4, the new Konnect and Quantum satellites of Eutelsat.

Following a period of relative stability, the supply capacity dramatically increased with the launch of the Konnect VHTS satellite of Eutelsat in September 2022. Konnect VHTS is a GEO satellite, offering capacity in the Ka-band to end-users (with Q/V band for gateway links).

The satellite operators SES and Hispasat are estimated to be able to offer together more than 10 Gbps of capacity over Europe via GEO systems. It is noteworthy that SES also operates the MEO constellation O3b, with the deployment of the new generation mPOWER which started in December 2022.

Currently using Intelsat capacity, the Ovzon company plans to launch its first satellite (Ovzon-3) in late 2023 or early 2024[1].

KEY UNDERLYING ASSUMPTIONS

- One or a few commercial satellite operators from Category I would provide new GEO HTS satellites to ensure growing needs for broadband and mobile applications but with balance and relevant investments between GEO and NGSO assets.
- Broadcast satellites reaching EOL before 2030 would be replaced with new types of assets fitting the SATCOM market shift from broadcast video to data.

Evolution over the 2025–2040 period

In the near term, we do not anticipate the procurement of large GEO HTS systems by operators in the Category I, in view of the capacity already being planned. It is noteworthy that the capacity increase is primarily related to the Konnect VHTS satellite. We still anticipate that at least one GEO satellite platform (typically flexible) could be procured to address a set of requirements (from mobility to broadband) in the second part of this decade.

While more capacity could be available, situations could exist where the entire capacity over a certain territory would have been leased by one to several clients. This could for example be the case for the capacity of Konnect VHTS in certain countries in the EU.

For the 203–2040 time period, the current scenario assumes that:

- The requirement of certain users, and/or the ability to combine the use of GEO and NGSO supply efficiently results in a continuous use of the two orbits.
- Large operators currently in the Category I remain in that category (under the definitions that would be considered as relevant in 2030 and after).
- Consequently, capacity is being replaced, and partially extended, however at a slower pace than the potential growth of satellite traffic (thus corresponding to a relatively lower share in the supply and use of GEO platforms).

[1] Ovzon, June 2023 : Ovzon provides update on launch and progress of the Ovzon 3 satellite

Macro trends impacting the NGSO commercial supply

Future Cat I commercial NGSO supply dependent on multiple factors

It is noteworthy that a single European Union operator currently fully owns a NGSO (MEO) constellation that is estimated to cover at least part of Europe. Several considerations shall be taken into account with regards to future prospects:

- The operator Eutelsat has combined its activities with OneWeb. This is likely to represent its focus in NGSO broadband assets in at least the near term. The operator SES, in addition to its MEO constellation, may consider investments in the LEO orbit, as suggested in an interview with SES's CEO in January 2022[(1)]. The size and profile of such an investment is unknown. No plan has been announced by other satellite operators in Category I.
- In addition to the most prominent NGSO satellite programmes, it is noteworthy that several dozens of companies have submitted filings for spectrum in the NGSO orbit, including the last quarter of 2021. Those organisations, for the ones identified, were not in Category I.
- For most commercial operators, an NGSO broadband constellation is a global infrastructure, with the ability to generate a return being dependent on the ability to generate large revenues from a large number of national markets. Europe would only represent a share of the addressable market to that target.
- The **IRIS² initiative for a constellation for secured communication shall also have an impact on the perceived addressable market in Europe**, and on the strategy for investments in NGSO assets by commercial operators, although the impact may highly depend on the design of that programme.

Understanding that NGSO constellations of the next decade would involve completely new generations of assets, any forecast can only be conservative. It could involve both new technology designs, as well as potential changes in the corporate ownership of the programmes.

Commercial NGSO capacity supply: potential dynamics over the EU

Regarding the different timelines (up to 2040), the potential dynamics are the following:

Near term (before 2025)

- Capacity from the upcoming O3b mPOWER constellation will become available over part of Europe (commercial service to start by the of end of 2023)[(2)].

Middle term to 2030

- Potential extension of the NGSO assets of SES[(3)].
- Expected deployment of IRIS2 programme providing additional NGSO supply and impacting the strategy for and/or availability of commercial NGSO supply.
- Probability of a deployment of another new commercial broadband constellation of Category I considered as having a low probability.

Long-term to 2040

- It is estimated that at least one constellation from category I will have coverage over Europe.

[(1)] Via Satellite, January 2022: SES Will 'Likely' Leverage LEO in Multi-Orbit Future, by Mark Holmes, 20 January 2022

[(2)] SES H1 2023 results, the 03rd of August 2023, available here: SES financial results

[(3)] Projet de loi autorisant le Gouvernment, à financer le programme "Medium Earth Orbit Global Services (MGS) Luxembourg", 21st of February 2023

Commercial NGSO supply from Cat I countries (2025–2040)

SES' O3b mPOWER : currently the only NGSO constellation in Cat I [5]

SES currently operates the MEO O3b constellation of 20 satellites in the Ka-band. O3b's current coverage of Europe is very limited. However, SES started launching in 2022 its new generation "O3b mPOWER" constellation. With an announced coverage going up to 52°N[1], the constellation is estimated to cover up to the North of France, i.e. covering part of central to southern Europe.

SES has reportedly been working on proposing a more integrated network capability, with the possibility to combine use of its MEO and GEO assets[2]. The O3b mPOWER constellation is also operating in the Ka-band. The initial deployment is estimated to include 11 satellites, of which 4 were launched as of May 2023 and the remaining are planned to be launched in 2023 and 2024. O3b mPOWER satellites are estimated to have flexibility features, thanks to dynamic beam-forming, steering and sizing[3].

KEY UNDERLYING ASSUMPTIONS

- O3b mPOWER constellation would expand in the 2020's decade in relationship with the SES request to the FCC (MEO/LEO) on May 2020. The coverage of Europe may only be partial for most, if not all, of the current decade.
- There is no assumption of another NGSO constellation in Category I countries until at least 2030; this is excluding a potential commercial service from the EU constellation initiative.
- At least one constellation would be available from a category I country in NGSO, with capacity increase over the period.
- High level of uncertainty applies in view of the limited number of constellations.

Evolution over the 2025–2040 period

Following the planned launch of the 11 O3b mPOWER spacecraft, SES has expansion plans for its NGSO system. In May 2020, SES asked the FCC (Federal Communications Commission) to grant U.S. market access for a constellation of 36 LEO satellites that would provide high data rate communications for internet-of-things devices and serve as a relay network for other digital traffic. SES also asked for market access rights for an additional 34 satellites that it would add to the O3b broadband constellation it has already deployed in MEO. SES told the FCC the purpose of its new MEO filing is to prepare for a third generation of O3b satellites, which would follow the first eleven O3b mPOWER satellites. For its third-generation O3b network, SES said it wants to operate 10 satellites in an equatorial MEO orbit. Another 24 satellites would operate in inclined MEO orbits and would use a smaller platform that allows for more satellites to fit within available launchers[4].

It is estimated that at least one NGSO constellation could be operated by an operator included in Category I, and that capacity would be increased, either by adding more satellites and/or by using new technical capabilities (such as the use of higher frequencies etc.).

[1] Projet de loi autorisant le Gouvernment, à financer le programme "Medium Earth Orbit Global Services (MGS) Luxembourg", 21st of February 2023
[2] SES, MEO and GEO, our multi-orbit strategy
[3] SES H1 2023 results, the 03rd of August 2023, available here: SES financial results
[4] SpaceNews, 29th of May 2020, SES details LEO constellation and expanded MEO constellation to FCC
[5] To be noted that OneWeb has become part of the Eutelsat group during the report production, thus complementing the NGSO supply within Category I countries

Commercial GEO supply from Cat II countries (2025–2040)

Situation up to 2025

Most of the GEO satellite capacity supplied by satellite commercial operators belonging to Category II currently belongs to Inmarsat[1], the U.K.-based satellite operator. In particular, most of the capacity is associated with the Inmarsat-5 F5 that got launched in 2019 and covers a corridor from Europe to the Middle East. In addition to its current fleet of HTS satellites (Inmarsat-5/GX family), at least one satellite from a new generation of satellites currently under procurement is estimated to cover the EU territories[2]. All of the capacity is currently in the Ka-band.

A major consideration is however the closed acquisition of Inmarsat by the Viasat company. Whether Inmarsat remains an operator standing in Category II may depend on the operation process after the acquisition. We have currently maintained Inmarsat capacity in Category II for the purpose of the report.

Avanti, with its Hylas-4 satellite, would be the second provider of capacity supply (also in Ka-band). Additionally, several Gbps of capacity supply in Ku-band is forecast to be provided over Europe by Telesat and Telenor (via the satellites Thor 7 and Thor 10-02). Telenor is also a supplier of HTS Ka-band capacity. This HTS capacity would however be primarily over maritime areas and/or focused on the Middle East and North African areas.

KEY UNDERLYING ASSUMPTIONS

- Impact of growing trends for mobility. Today, mobility currently consists of In-Flight and Maritime Connectivity markets as they are the most relevant. Over the period, interest in mobility may shift toward connected cars with the rise of IoT, connected devices and the overall digitalization of transportation.
- Renewal of spacecrafts to maintain Ka-band landing rights in the U.K.
- Potential impact of future Inmarsat depending on the closed transaction with Viasat.

Evolution over the 2025–2040 period

It is estimated that capacity could increase in the second part of the decade. However, this would be dependent on decisions by a limited number of operators. While we could anticipate new investments by Inmarsat in order to increase the capacity of its fleet for mobility services, the closed transaction with Viasat could result in a large revisit of investment priority, and a change of technology platforms (and potentially of qualification between Category II and other Categories).

[1] Viasat (U.S.) finalized the acquisition Inmarsat (U.K.) the 31st of May 2023
[2] Inmarsat orders GX7,8&9, Inmarsat, May 2019: Inmarsat partners with Airbus

Commercial NGSO supply from Cat II countries (2025–2040)

Situation up to 2025

The two companies having NGSO constellations under development in Cat II countries are OneWeb[6] and Telesat.

Following launch of all the Gen 1 satellites, OneWeb is forecast to offer full global coverage (including Polar regions) with more than 600 satellites and very low latency (< 50 ms) via LEO in Q3 2023[1]. OneWeb exclusively uses Ku-band.

Space Norway Heosat AS, due to the Ka-band commercial payloads embedded on the ASBM 1 & 2 satellites, will be able to offer a few Gbps of capacity supply from 2023 to 2025. Nonetheless, this capacity supply will not be offered to end-users directly by Space Norway Heosat AS. Indeed, those 2 Ka-band commercial payloads have been leased to Inmarsat and named Inmarsat GX-10A & GX-10B according to Inmarsat satellites fleet. Operating in HEO (Highly Elliptical Orbit), Inmarsat GX-10A and GX-10B payloads will ensure continuous coverage of Artic area (above 65°N) and are dedicated to mobile markets[2].

- In August 2023, Telesat announced that its Lightspeed project is fully funded and selected MDA a prime contractor for building the 198 satellites for the constellation. Satellites have been announced to include digital beamforming array antennas and integrated regenerative processor. Satellite launches are scheduled to commence in mid- 2026 and global services to begin in late 2027[3].

KEY UNDERLYING ASSUMPTIONS

- High level of uncertainty has been applied with the augmentation of OneWeb and Telesat capacity highly dependent on their commercial success in the coming years.
- Replacement of Inmarsat Arctic payloads in the second half of the 2030's with higherperformances satellites relies on growing strategic interests in the Polar region.

Evolution over the 2025–2040 period

For OneWeb, some evolutions plans have been identified. It is estimated that such an evolution would be more focused on flexibility than on additional capacity. Indeed, in October 2022, OneWeb and Eutelsat (in the frame of their planned combination of activity) announced they would work together on the conception of OneWeb's Gen 2 constellation, due to enter service by early 2028[4]. Such Gen 2 satellites are designed to introduce technological evolutions such as beam-hopping. Satellites with beam-hopping abilities will be able to remotely direct beams to boost coverage in certains locations, such as areas of high-usage where the network is struggling to cope with demand. In May 2023, OneWeb launched JoeySat a demonstration satellite previewing next-generation capabilities, planned for Gen 2[5].

Evolution of the programmes at this stage cannot be further evaluated for both OneWeb and Telesat, depending on commercial success, renewal strategy and technological evolution.

[1] Eutelsat, August 2023: Eutelsat Investor Presentation
[2] Inmarsat, 29th of January 2020: a new frontier for governmental users
[3] Telesat, 11th of August 2023: Telesat Contracts MDA as Prime Satellite Manufacturer for its Advanced Telesat Lightspeed LEO Constellation
[4] Eutelsat & OneWeb, 12th of October 2022: Eutelsat Strategy update on the proposed combination with OneWeb
[5] OneWeb, 20th of May 203: OneWeb confirms successful deployment of 16 satellites including next generation JoeySat
[6] To be noted that OneWeb has become part of the Eutelsat group during the report production, thus complementing the NGSO supply within Category I countries.

SECURE SATCOM TECHNOLOGY

Chapter Summary

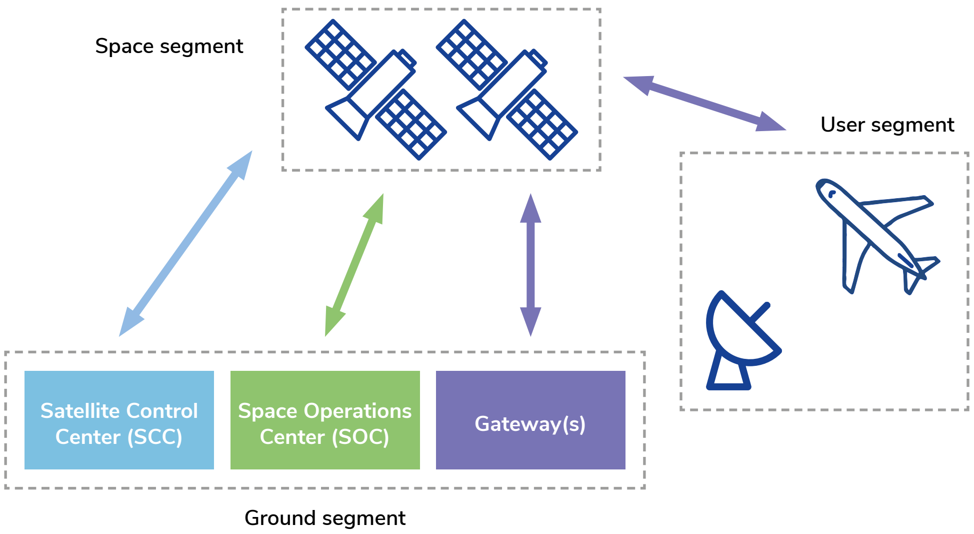
Following the exposition of the distinct constituents of the EU Space Programme, as well as the examination of secure SATCOM demand and supply, this chapter delves into the technical dimensions of secure SATCOM services. It explores how these technical aspects influence the performance, reliability, security, and adaptability of satellite-based connectivity. It helps in comprehending the symbiotic interaction of satellites, ground stations, and user terminals, which collaboratively facilitate secure SATCOM services. Furthermore, it provides insights into the technological trends and challenges inherent to secure SATCOM services across diverse regions and scenarios. The chapter covers the following topics:

- explains, within the space segment section, the advantages and disadvantages of different orbital regimes while also identifying some technological trends that are transforming the space segment.
- explains, within the ground segment section, the need for different communication links between the ground segment and the space segment and some technological drivers that are influencing the ground segment.
- describes, within the user segment, the building blocks and characteristics of different types of user terminals and some user terminal technological trends.
- presents the key technological factors that enable future EU secure SATCOM services. It analyses some upcoming radio protocols and some aspects of interoperability between satellite gateways and user terminals.
- provides a landscape overview of cybersecurity within secure SATCOM and evaluates some aspects of cybersecurity principles and factors that affect the security level of space systems as well as the motivations and examples of the key threat actors.

© Wirestock

Specificities of space-based systems for secure SATCOM

Block diagram of space-based system



Building upon the insights already shared, an illustrative overview of satellite telecommunication networks was presented on page 24. The intention was to familiarize readers with the components (subsequently referred to as actors) integral to the value chain. Additionally, a preliminary level of objectives for each segment was outlined. The forthcoming four sections within the secure SATCOM technology chapter delve into an in-depth exploration of the distinct segments constituting a space-based system for secure SATCOM. it is noteworthy that whether concerning SATCOM or secure SATCOM, the block diagram remains consistent. While the subsequent sections elaborate on these segments, particular emphasis is placed on this page, delving into the security facet of secure SATCOM.

Which specificities for secure SATCOM provision?

Secure SATCOM has to be provided in a **reliable, accessible and guaranteed manner.** Consequently, specific requirements have to be taken into account in the design & operation of the space-based system.

Space segment can be made of one satellite (in GEO, for instance) or several satellites, in the case of an NGSO constellation. Irrespective of the orbit (cf. pages 78 & 79 for the different possibles orbits), space segment remains vulnerable. It can be hacked, jammed or physically damaged. In addition to specific features against jamming and spoofing, a relevant way to increase the resilience of the space segment is to rely on NGSO constellation; indeed, even with a reduced number of satellites, an NGSO constellation can provide a service in a degraded mode. a step further to NGSO constellation is the multi-orbit space-based system. In addition to the complementarity between the different orbits (cf. pages 78 & 79 which present the advantages/drawbacks of each orbit), a multi-orbit system is resilient by nature. Multi-orbit space-based system includes the combination & interoperability between different systems (from different countries and/or from governmental/commercial entities). Pages 80 to 83 illustrate how the technological evolution of the space segment impact SATCOM in general and specially, the provision of secure SATCOM.

Ground segment is the unique interface to manage the space segment, which generally constitutes from the Satellite Control Center (SCC), the Space Operations Center (SOC) and the Gateways. From an operational point of view, it allows a continuous and deep monitoring of the satellites (platform and payload) performed 24/7. The TT&C and the M&C (Monitoring & Control) as well, need to be secured and protected against any type of threats in order to avoid, for instance, malicious commands to be sent to the satellites to damage or take the control of it. To increase the protection against vulnerabilities, SCC and MCC can be implemented in a redundant mode.

Beyond the security aspect of being resilient against threats and malicious data, the user segment encounters its principal characteristics and challenges, primarily addressing demands for **interoperability and flexible solutions**. As highlighted in the chapter about demand (from page 20), the missions and operational needs can be slightly different with a variety of secure SATCOM end-users.

In addition to the three previously mentioned segments, ensuring the protection of the **interconnections between these segments** is also essential. Consequently, to guarantee the confidentiality, integrity and availability of any transmitted information secure SATCOM has to incorporate encryption and any other security measures to protect data from unauthorized access and interception.

Main characteristics of SATCOM satellite(s)

© Thales Alenia Space

This page outlines the main characteristics of the space segment and their use for the provision of SATCOM services. Such characteristics are applicable to any type of SATCOM satellite. Relevant functions to secure SATCOM spacecraft have been highlighted in page 76.

A communication satellite is an artificial satellite that relays and amplifies radio telecommunication signals via a transponder; it creates a communication channel between a source transmitter and a receiver at different locations on Earth. Communications satellites are used for television, telephone, data, radio, and internet, in civil and military applications.

A communication satellite includes the satellite payload and the satellite platform, also known as the satellite bus.

The satellite platform provides all the necessary services to the payload:

- Structure to support all satellite units and mitigate mechanical stress.
- Thermal regulation system, often passive using Optical Solar Reflector (OSR), Multi-Layer Insulators (MLI), radiators and heat pipes. The thermal system is dedicated to temperature maintenance and dissipation capability.
- Electrical Power generation & Storage System (solar panels, batteries, power regulation and distribution) used to power all the satellite systems.
- Attitude & Orbit Determination & Control System (AOCS) used to keep the satellite in the right orbit, with its antennas pointing in the right direction and its power system pointed towards the sun. Sub-systems are used for the determination of the position (Inertial Measurement unit, on-board computer, star trackers, Earth sensors, GNSS receivers) and its control (Thrusters, Reaction wheels, magneto torquers).
- Propulsion system (predominately used to reach the operational orbit when injected by the launcher on a less energetic orbit).
- Telecommand and Telemetry system (using radio communications) to be operated from the ground. As low data rate is enough UHF-, VHF- or S-band are generally used.

The communication payload of the satellite is ensuring the SATCOM mission. It includes RF equipment (such as amplifiers, converters, multiplexers, and modems) and transmitting/receiving antennas. The communication payload **acts as a repeater** and basically consists of antennas and one or more transponders, operating in parallel, with separated amplification chains, on different channels in sub-bands of the total available bandwidth. The communication repeater can be **transparent**, often referred as a 'bent-pipe' repeater in the literature, or be an **onboard processing repeater**.

When the received signal is in reception mode, the **transparent repeater** undertakes channel separation and amplification. Subsequently, the aggregated channels are transmitted through the antenna in transmission mode. In the case of an **onboard processing repeater**, the baseband signals (modulated on the uplink carrier and received and amplified by the satellite), are demodulated on board and then modulated on the downlink carrier to be transmitted to ground.

Different orbits used for SATCOM satellites: GEO, MEO and LEO[1]

GEO (GEOSTATIONARY EARTH ORBIT)

Spacecraft situated in **GEO, located at an altitude of 35,786 Km**, have their orbits synchronised with the rotation of the Earth. Consequently, they stay in the same position in the sky with respect to a given point on the Earth's surface, meaning that **an antenna does not need to move to track the satellite**. a main feature of GEO's satellites is that they have a **large view of the Earth, approximately one-third (excluding the Polar Regions), meaning that three spacecraft can offer quasi-global connectivity**. When considering the Polar Regions, Geostationary orbits have a very low elevation angle, thus GEO satellite performance quickly decreases at the poles. **The highest Northern and Southern latitudes at which GEO satellites are still generally considered efficient are approximately 75 degrees, meanwhile, beyond 81 degrees they are below the horizon**. Given the altitude of the satellite, total delay experienced by the users would vary between 478 and 556 milliseconds (depending on where on the Earth's surface the user/Earth station is located). The received power on the ground is directly impacted by the orbit, the transmitted power by the satellite and the frequency-band used. This received power on ground dictates the required antenna gain, hence influencing some characteristics of the usable antenna types. Regarding other orbits such as MEO or LEO (closer to Earth than GEO), the received power on the ground would be less attenuated (as distance is lower).

MEO (MEDIUM EARTH ORBIT)

The MEO is a range of orbits that extends from 1,000 Km to 35,786 Km altitude. Most satellites currently operated in MEO orbits are at an altitude of about 8,000 km but many are also at higher altitudes. For satellites operated at 8,000 Km altitude, the total delay experienced by the users is approximately 200 milliseconds (this does not account for processing time that may occur in the satellite or on the terrestrial network). The satellites that operate in this orbit move across the sky with respect to a given point on the Earth's surface, meaning that **an antenna needs to track the satellit**e. Omni-directional antennas cannot be employed due to the required antenna gain, as such antennas need to be directed towards the satellite's transmission. When one satellite moves out of the visible arc of the antenna, the antenna will need to re-connect to the following satellite. This will mean an interruption to connectivity and of the service unless two antennas are engaged to allow for at least one to maintain connectivity whilst the other is repointing towards another satellite (Soft/Hard handover principles). a solution is the use of phased array antennas with beam steering on board the satellite to keep a fixed target on Earth: in this way, the complexity is transferred onto the space segment keeping the user equipment simple and less expensive. **The coverage areas of MEO satellites operated at 8,000 km altitude in an equatorial plane are limited in latitude to 50° North and South of the equator. Given the movement of the satellite compared to the Earth, several dozen satellites are needed to provide global coverage**. For example, O3b (owned by SES) achieves such global coverage through 20 satellites, and the currently deployed 03b mPOWER will do so initially with 11 satellites.

LEO (LOW EARTH ORBIT)

Satellites in LEO orbits operate in altitude ranges from 180 Km to 2,000 Km. Satellites move at a relatively high speed (8.2km/sec) through the sky with respect to a given position on the surface of the Earth. **The distance between the satellites and the user on/or close to the Earth's surface means that the total delays are very short** compared to GEO altitudes, namely in the order of dozens of milliseconds. In addition, the proximity means that there is not the same requirement for high gain, highly directional antennas as there are for orbits at higher altitudes. Due to the relatively low altitudes used by LEO satellites, in order to provide continuous coverage to any given point on the surface of the Earth, 1 satellite is not enough as in GEO but many satellites are needed. **LEO constellations require from a few hundred** (<200 for Telesat Lightspeed) **to several thousand** (Starlink, more than 4,661 satellites are on orbit as of August 2023) **of satellites to provide a user continuous availability of service from a global perspective**. Satellites of all sizes (nano, pico, etc.) can be employed in LEO orbits to offer SATCOM services (including secure SATCOM).

[1] Trends about the deployment of NGSO systems are mentioned on page 80

Different orbits used for SATCOM satellites: HEO

HEO (HIGHLY ELLIPTICAL EARTH ORBIT)

Satellites in HEO orbits operate across altitude ranges, as the distance of the satellite will continuously vary along its rotation around the Earth. Indeed, this distance is satellite dependent and will vary between its perigee (minimum distance from Earth) to its apogee (maximum distance from Earth). Similarly, satellites in HEO move at a varying relative speed through the sky with respect to a given position on the surface of the Earth. Indeed, while the visibility of a typical GEO satellite decreases as latitude increases north or south towards the Earth's poles, **HEO satellite constellations can provide efficient communication services for latitudes higher than 67° South or 67° North, depending on the orbital parameters.**

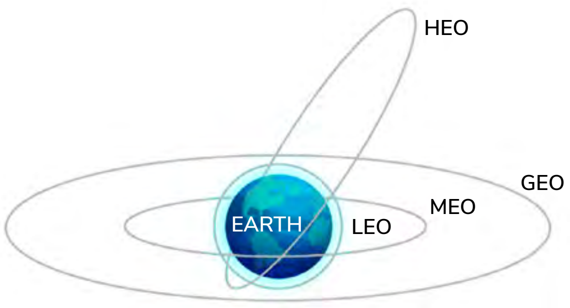
Therefore, they are generally well-suited to provide permanent coverage and high data rate services in polar regions poorly covered by GEO systems as the satellite will remain for a long period of time over the region of interest. When using a HEO satellite, good elevation angles may also be observed from regions other than the ones for which the satellite has been designed. Remaining in sight from multiple regions can also help to limit the amount of required antenna steering. Typically, for a user in Europe, a two to three-satellites HEO constellation can provide continuous coverage. Indeed, several types of configurations (different orbital parameters) can be considered for HEO constellations, and the number of satellites needed for coverage might depend on whether a constellation travels on one or more orbital planes. Nevertheless, several satellites are usually required to guarantee continuous coverage in polar regions. Molniya orbit is a HEO and was specially used for satellite communication satellites by U.S.S.R. (Union of Soviet Socialist Republics) from the 1960s[1].

MEO, LEO and HEO are the three different types of NGSO.

Features of different orbital regimes

Orbit	Distance	Operated as a constellation	Are multiple orbits possible?
GEO	Long distance from Earth (over 35,786 Km). ⇨ High latency	Can be (3 GEOs allow global coverage up to 75 degrees)	Only a single possible orbit due to spacecraft's dynamics
MEO	Medium distance from Earth (1,000 to 35,786 Km) ⇨ Medium latency	Small constellation (>8)	Multiple orbits are possible
LEO	Low distance from Earth (180 to 2,000 Km) ⇨ Low latency	Large constellation (>100), increasing system complexity	Multiple orbits are possible
HEO	Variable distance from Earth	Small constellation (>2)	Only a single possible orbit

Primary orbits used for communication networks



[1] Observatoire de l'Arctique: Surveillance de l'Arctique

Technological trends in SATCOM: HTS & NGSO

Multiple technological trends, accelerating in the past few years, are shaping the space segment of SATCOM systems. The most relevant trends include the adoption of high throughput payloads, the quick deployment of NGSO constellations, the emergence of software-defined satellites, the adoption of higher frequency bands, and the introduction of optical communications. These technological trends are being implemented in the EU, the US as well as in Australia, China and Japan. As an example, China is currently deploying its Guowang NGSO mega constellation (its ITU filing is for 30,000 satellites) directly to compete with Starlink. As such, these trends are impacting the entire SATCOM landscape, (including secure SATCOM), irrespective of geography.

HTS[1] adoption and growing data traffic

The ability to reuse frequencies in multiple spot beams is at the heart of the increase in the capacity per satellite that can currently be observed. The ability to increase the number of spot beams of a smaller size allows the market to move from satellites having a maximum of several Gbps of capacity to satellites offering up to dozens or hundreds of Gbps. While commercial satellite operators are now investing in their second or third generation of such systems, it remains a relatively emerging technology for government-owned satellites.

Such evolution copes with the growing need of capacity for secure SATCOM users (cf. chapter secure SATCOM market demand, page 20).

Not exhaustive list of GEO satellites with HTS payload from EU satellites operators

- Konnect (Ka-band), launched in 2019.
- Konnect VHTS (Ka-band), launched in 2022.
- Quantum (Ku-band), launched in 2021.
- Eutelsat 10B (Ku-band) launched in 2022.
- Amazonas Nexus (Ku-band), launched in 2023.
- Hellas Sat-4 (Ka-band), launched in 2019.

Deployment of NGSO constellation

In the coming ten years, commercial NGSO constellations will account for 70% of the satellite demand in number, feeding the growing demand for ground operations. SATCOM mega-constellations (Starlink, OneWeb) are expected to unlock new growth opportunities for latency-sensitive applications and ubiquitous coverage (including the poles). The growing importance of NGSO constellation in connectivity markets is impacting the FSS industry, with an increasing number of players implementing multi-orbit strategies (see list on the right). GEOs can provide more capacity to a specific region than NGSOs that must serve the globe, but NGSOs allow low-latency solutions that can integrate with terrestrial infrastructure more effectively than GEOs.

Secure SATCOM users can benefit from low-latency satellite communication services worldwide. In addition, a combination of GEO and NGSO can provide cost-effective solutions to end users.

Not exhaustive list of Multi-orbit strategies of EU satellites operators

- Eutelsat: a combination of activities with OneWeb is closed since 28th September of 2023..
- Intelsat: Global distribution partnership for IFC market in 2022. An RFP for 18 satellites MEO constellation is planned to be released in the summer 2023.
- SES: Acquisition of MEO operators O3b Networks in 2016/order of 11 O3b mPOWER satellites since 2017. O3b mPOWER services planned to start in Q3 2023. A combination of activities with OneWeb is closed since the 28th of September 2023.

[1] HTS's (High Throughout Satellites) payload can offer from a few dozen Gbps to several hundreds of Gbps (500 Gbps for Konnect VHTS). a more comprehensive definition of HTS is available in the Annex 2.

Reference status on high-throughput NGSO constellations

The following table, updated as of August 2023, is a non-exhaustive list which focuses only on NGSO high-throughput for FSS systems. Other NGSO constellations exist for MSS such as Iridium and Globalstar[1].

	SES	Telesat	SpaceX	OneWeb	Amazon
Constellation	O3b mPOWER	Lightspeed	Starlink	OneWeb	Kuiper
Size	11 satellites	198 satellites	1st Gen: 4,408 satellites	1st Gen: 648 satellites	Up to 3,236 satellites
Development	4 operational satellites, 4 slated for launch in 2023, and 3 in 2024	Telesat's contract with MDA to build the satellites was announced in August 2023, aiming to start launches in 2026.	The 1st generation is operational. Over 4,6612) satellites are currently in orbit out of 12,000 planned for 1st and 2nd Gen combined.	The 1st generation is fully deployed, and full coverage is planned to start in January 2024. 2nd generation satellites planned to be launched in 2028.	Deployment has not started; the current timeline is to fully deploy by July 2026.
Total capacity	~2.7 Tbps (200 – 315 Gbps /satellite)	~10 Tbps (50 Gbps /satellite)	~88 Tbps (~20 Gbps /satellite for 1st Gen)	~5 Tbps (~7.5 Gbps /satellite for 1st Gen)	~164 Tbps (~50 Gbps /satellite estimated)
Frequency band (user link)	Ka-band	Ka-band	Ku-band	Ku-band	Ka-band
Orbit	MEO (8,062 Km)	LEO (1,000 - 1,350 Km)	LEO (550 Km)	LEO (1,200 Km)	LEO (600 Km)
Satellites mass	~1,700 Kg	~700 Kg	~260 Kg	~150 Kg	~650 Kg
Satellites life	>10 years	~10 years	~5 years	~7 years	5 to 7 years
Latency[3]	~150 ms	<50 ms	<50 ms	<50 ms	<50 ms

[1] Iridium is an operational constellation in its second generation (Iridium NEXT). The system provides L-band voice and data through 82 operational satellites. Globalstar is also a fully deployed system in its second generation (with the third generation expected to be launched by 2025). The 25 satellites LEO constellation provides lower frequency bands to satellite phones.

[2] Number of Starlink satellites in orbit as of 27/08/2023; source: Jonathan's Space Pages Note: some satellites in orbit are not operational, but the precise number is not publicly disclosed.

[3] Low latency (below 250 ms) is defined on page 33.

Technological trends in SATCOM: flexibility and higher frequency

Introduction of software-defined satellites

Fully software-defined satellites have emerged as a major trend in the sector. This is particularly true for GEO-HTS satellites which account for the bulk of recent GEO software-defined satellite orders. Over the 2021–2022 period, 70% of GEO-HTS satellite orders were fully software-defined platforms manufactured by Airbus (OneSat), Thales (Space Inspire), and Astranis (Micro-GEO). This adoption is being driven by the **key operational advantages of software-defined satellites** including the flexibility to change parameters such as coverage, power, and frequency bands through on-board processing and active antennas with beam forming capability. Such advantages will benefit to secure SATCOM users which are characterised by a diversity of users (who can be deployed worldwide) and who can need an important volume of capacity in an urgent manner (for instance, Forces Deployment, Civil Protection, Humanitarian Aid or Institutional Communications use cases).

Software-defined satellites carry other advantages such as manufacturability, wherein standardized design-to-manufacture approaches leveraging modular techniques result in reduced time to market and lower costs compared to the traditional approach to GEO system design/manufacturing.

Not exhaustive overview of recent software-defined GEO satellite orders

OneSat (Airbus Defence & Space)

- Superbird-9 (JSAT), 2021.

Space Inspire (Thales Alenia Space)

- Astra-1Q (SES), 2021.
- Arabsat-7A (Arabsat), 2022.
- IS-41 (Intelsat), 2022.
- IS-42 (Intelsat), 2022.
- SES-26 (SES), 2022.

Micro-GEO (Astranis)

- Anuvu-1 (Astranis), 2021.
- Anuvu-2 (Astranis), 2021.
- Andesat (Astranis), 2021.

Use of higher frequency bands

In recent years, the use of the Ka frequency band by satellite systems has largely contributed to the increase in the secure SATCOM capacity being offered (as frequency-band are more and more used). Several upcoming commercial systems will use the Q/V-band to communicate with their gateways, while the use of the Ka-band will be reserved for end-users in order to further increase the capacity. Ability to offer higher volume of capacity clearly fits with the growing need of capacity for secure SATCOM users (cf. chapter secure SATCOM market demand, page 20).

On 30th of June 2021, the first-ever satellite with a W-band radio transmitter on board was launched by ESA. The objective is to improve the understanding of the atmospheric effects in the propagation of radio signals at such a high frequency band[1].

Examples GEO satellites using Q/V-band

- Konnect VHTS spacecraft (launched in 2022) uses Q- and V-band for gateway feeder links to optimise the amount of Ka-band available to customers.
- Jupiter-3 (launched in 2023) also uses Q/V bands for gateways like Konnect VHTS.

[1] ESA: First W-band transmission from space

Technological trends in SATCOM: Optical communications

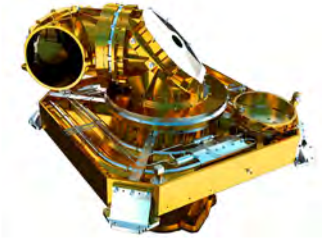
Optical communications

In a world with more and more connectivity needs, the capability to transfer a very large amount of data in real time is becoming crucial for any type of organisation, either private or governmental. As the space environment is complex and requires the development of specific and demanding products, the cost of terminals for wireless optical communications between satellites remained too high to allow widespread adoption and a diversity of applications. However, the rise of NGSO constellations creates the need for inter-satellite links (ISL) to enable increased capabilities of the systems. Intra-constellation links can be defined as communications between two or more satellites of the same constellation through optical links. ISLs are especially useful for NGSO constellations targeting services all over the world. It also avoids the deployment of a significant number of gateways on the ground, saving costs and avoiding facing refusal of landing rights in some geographical areas. Having OISLs (Optical ISLs) is very relevant for NGSO constellations as RF link capacity and bandwidth are not always high enough to support many users at the same time.

Optical features can be used for **communications with third-party satellites, typically for data relay services**. Traditional RF communications means could be used but optical communications can be very relevant for some use cases as it allows a larger amount of data to be transferred with lower latency and thus more real-time data transmission on top of improved security, which is a key criterion for most data relay clients. As an example, the public-private European Data Relay System (EDRS), has proven effective in implementing ISL technology, significantly increasing the speed of downlink of Copernicus images. The system enables the transmission of data very quickly, avoiding waiting for a satellite to be in view of a ground station to transmit the data to the ground.

Direct-To-Earth (DTE) laser communications are defined as communications from a spacecraft located in orbit to the ground. As moving from RF frequency to optical use improves the data rate, Optical Ground Stations (OGS) enable obtaining even higher data rates while having smaller receiving apertures. However, optical links are also sensitive to the background noise that any ambient light sources cause. Deployment of OGS requires the assessment of clear sky availability due to this technology's sensitivity to weather. Certain regions in the Middle East and Africa, Australia, or the United States are therefore privileged. a diversity of stations is necessary for regions such as Europe to maximize the probability of communication in these regions.

Secure SATCOM can benefit from Optical communications at two level: First, in the frame of an NGSO constellation (via OISL) and secondly with a huge amount and data that can be transferred, including from satellites to the ground. Such disruptive evolution leads to higher perspective than the move to higher RF frequency band, as mentioned in the previous page.



© ESA

Note : The picture on the left shows a European Data Relay System laser communication terminal capable of transmitting 1.8 Gbit/s of data between LEO and GEO. Developed by the DLR German Space Center and TESAT-Spacecom (DE), it is the most advanced of its kind.

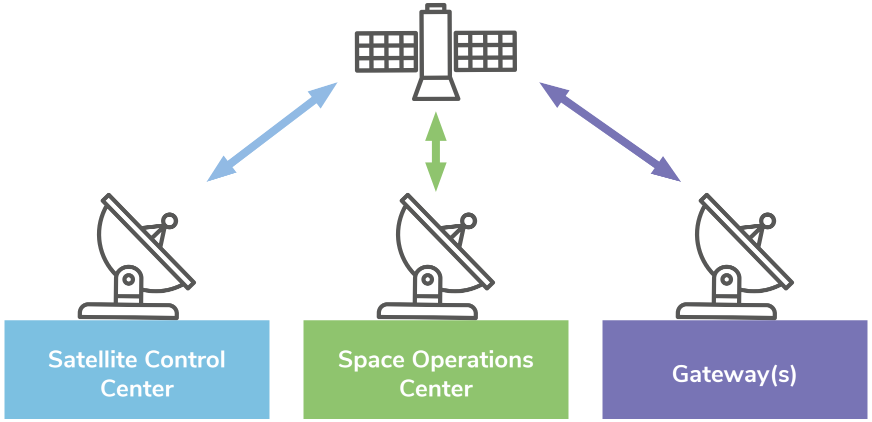
The ground segment: a growing key element for space-based infrastructure

The unique interface with the satellite

The ground segment is the part of a satellite communication system that consists of all the ground-based elements. The ground segment enables the exchange of data and commands between the satellites, the staff in charge of the control/operations of the satellites and the end users. The ground segment is a critical component of a satellite communication system, as it contributes to the reliability, security, and performance of the space segment and the user segment. The ground segment may vary depending on the type and size of the satellite mission, the number and location of the ground stations, and the requirements and preferences of the operators and users. However, the ground segment includes three sub-segments, as described below:

- The **Gateway** is a ground station that transmits data to/from the satellite to the local area network. It houses the antennas and equipment that convert the Radio Frequency (RF) signal to an Internet Protocol (IP) signal for terrestrial connectivity. Along with key advancements in satellite technology over the past decade, ground equipment has similarly evolved, benefiting from higher levels of integration and increasing processing power, expanding both capacity and performance boundaries. The system of Gateways provides all network services for satellite and the corresponding terrestrial connectivity. Each gateways provides a multiservice access network for subscriber terminal connections to the Internet.
- Satellites need a ground-based control system, in order to place them in orbit and then to track them during their lifetime. The **Satellite Control Centre (SCC)** is responsible for collecting and sending the telemetry data generated by the satellites and for the distribution and the uplink of the control commands that are necessary to maintain the satellites and constellation operative. a Satellite Control Centre (SCC) is responsible for a large range of functions but mainly to support satellite(s) management and more specifically the monitoring and control (M&C) activities for nominal as well as emergency spacecraft operations. Such activities are applicable for the M&C of the satellite platform and payload, the mission planning and AOCS (cf. page 77) functions that allow safe operations.
- In addition to that, the Telemetry Tracking and Control (TT&C) and payload data communication links are managing the platform and traffic configuration aspects respectively. The overall number of Telemetry Tracking and Control (TT&C) stations, with its associated RF equipment, modems and baseband equipment, may vary depending on the constellation dimension and the orbital location. TT&C stations are used to communicate with each satellite on a scheme combining regular, scheduled contacts, long-term test campaigns and contingency contacts. All these components are interconnected via a dedicated network.
- Satellite Control Centre is dedicated to control and manage the satellite platform, the payload embarked on the platform needs also its driver, whose functionality is demanded to the SOC (**Space Operations Center**). Due to the introduction of complex payloads in the core missions, featuring new architectures with multiple spot beam coverage, flexible frequency and power resource allocation demand, complex and variable channel to beam allocation requirements, digital signal processing[1], adaptative wave-form etc., the activities managed within the Mission Control Centre related to the planning and resource optimization are becoming more and more complex. Resource optimization is performed via the SRM (Satellite Resource Management) which is a major element in the frame of the operations of space and ground segment.

The different links for satellite communication



[1] Digital Signal Processor is designed to provide flexible channelization and transparent routing capability for advanced space telecommunication applications

Ground segment has a key role to play for satellite and 5G network integration

The development of the 5th Generation of communication networks provides a unique opportunity for a seamless integration of satellite with terrestrial networks as an integral component of the 5G system. Satellites can offer complementary connectivity options and seamless user experience and provide important benefits when integrated in the overall 5G system, owing to its intrinsic advantages including universal coverage, multicasting and broadcasting capability. Satellite ground segment is the key element to reach such objective.

SATCOM & 5G: a bidirectional relationship aiming for an integrated connectivity model

There is typically a 5–7 year lag between the start of commercial network deployment and the deployment of satellite connected BTS (Base Transceiver Station). a new mobile network generation such as 5G will require significant technology improvements to reach the required price point to be economically viable. Tests for satellite 5G started in 2020, and a 4-year lag for the start of satellite deployment can be anticipated.

Prior to the growth of satellite-based services, each standard usually requires the involvement of operators and solutions providers to promote and optimise the usability of the satellite solution. Such initiatives are currently undertaken for 5G, largely driven by global satellite operators. Nonetheless, it is noteworthy to mention that in 2017, a Joint Statement between ESA and the European Space Industry on their concerted efforts on “satellite for 5G” was signed. GEO and NGSO players are investing extensively in advanced technology to support terrestrial/hybrid 5G solutions as well as promoting and regulating space/Non-Terrestrial Network policy to meet all stakeholders’ requirements for upstream/downstream markets.

5G enables the seamless interworking of different technologies and networks, mobile, fixed, wireless, satellite, as well as their orchestration. To reach such objective, satellites will have to be transparent, requiring the ground segment to work in line with the orchestration of the core network; that’s why 5G requires standardisation of protocols. a satellite operator and a terrestrial service provider sharing 5G protocols are able to propose multiple and compatible type of services, relying on standardised procedures.

Satellite technological evolutions are in line with 5G requirements

The key advantage of 5G networks lies in the ability of the technology to provision more capacity from a site, with lower latency and higher quality-of-service than 4G technology within the same swath/band of spectrum.

While growth opportunities are certainly presented by the growth of 5G fixed wireless services and 5G mobile network rollouts into rural areas, most 5G deployments require levels of population density and throughput per tower that are challenging to address with the capabilities/economics of today’s HTS systems. In addition, several relevant and important trends are already underway:

- In the space segment (lower cost per bit, flexible payload technologies, low-latency with the deployment of NGSO constellation).
- In the ground segment (Q-/V-band gateways, software-defined networking, virtualisation, low-cost LEO terminals, etc.).

These trends will significantly improve the ability of satellite solutions to meet the requirements of 5G networks (higher capacity/QoS (Quality of Service), lower cost, etc).

Which satellites for 6G?[1]

While 5G optimises terrestrial network design to allow the integration of satellite for coverage an availability, 6G is expected to optimise network design, implementation and operation considering the characteristics of terrestrial and satellite communications to create unified networks. Launch of 6G is anticipated around 2030.

[1] Satellite communications and their role in enabling 6G © GSOA

Technological driver: use of higher frequency bands

In relationship with the move to higher frequency-band for the space segment (as depicted on pages 82–83), the user segment and the ground segment are logically impacted. The user segment has to integrate the technological features for higher frequency-band, but the ground segment is impacted in a slightly different manner.

Crowded spectrum leads to move to Q/V-band

Demand for spectrum has continued to grow at a rapid pace with satellite and other allocated services. SATCOM operators have been required to seek higher frequency-band and move to develop commercial operational capabilities in the Q/V-band[1].

The satellite industry is used to sharing spectrum among operators and some fixed terrestrial services, but the increasing demand for connectivity has led to greater and more frequent tensions. In the Ka-band, there are now growing concerns from satellite operators that regulators could repurpose spectrum in the 28 GHz band for 5G. Crowding in the lower frequencies has led to a move to higher bands, like Q/V. Use of E-band is also studied by Space X, for instance[2].

The ability to provide commercial satellite communications in the Q/V bands meets two fundamental needs for today's GEO and NGSO satellite operators: available bands of spectrum and significantly higher rates of data throughput. Depending on the configuration, use of Q/V-band can lead to more than twice the available bandwidth available in Ka-band.

Operators using Q/V-band may also look forward to deploying less gateways than if they used Ka-band. With more available bandwidth and ability for reuse, operators need fewer gateways and fewer diversity sites, which translates into less associated hub equipment. It also allows to reduce the number of hardware equipment to be deployed in different locations.

Nonetheless, due to the technological evolutions brought by higher frequency bands, the different equipment (such as antennas, amplifiers, transmitters ….) are more expensive to build.

Operating challenges for ground segment

Moving to Q/V-band requires an unobstructed line of sight between transmitter and receiver and sufficient power to propagate through the atmosphere. At the Q/V operating frequency, attenuation and atmospheric effects are particularly severe, and the effects of rain, clouds and atmospheric gas can impair the availability and quality of service.

Some of these issues can be compensated at the gateway by uplink power control (UPC) functionality and/or switching to a backup diversity site when disruptions reach a certain threshold—which is done today by operators in the Ka and Ku bands. But relevant mechanisms and algorithms have to be specially developed and implemented to retain the benefits of moving to Q/V-band.

Examples of companies moving to Q/V

As mentioned previously (cf. page 81) some GEO VHTS satellite with capacity of around 500 Gbps (Konnect VHTS[3], Jupiter-3) will use Q/V-band for their gateways feeder links. However, it is noteworthy to mention that moving to Q/V for GEO VHTS with several hundreds of Gbps capacity has to be specifically investigated, with several trade-offs in relationship with the operational use cases (cf paragraph about « Operating challenges »). For instance, the three Viasat-3 satellites (1st one was launched in May 2023) will stick to the use of Ka-band.

Regarding NGSO constellations, SpaceX holds an authorization for an additional constellation of 7,518 very-low-Earth orbit (VLEO) Starlink satellites using V-band frequencies. However, SpaceX no longer plans to launch separate V-band satellites and will instead seek a modification to add V-band frequencies to a subset of its 2nd Gen Starlink satellites. OneWeb has plans to use Q/V-band and is estimated to begin operating Q/V payload before November 2023, according to the ITU (International Telecommunication Union). Finally, in August 2021, and in the frame of its LEO project (Lightspeed), Telesat ordered LEO 3, a prototype satellite that would be able to transmit and receive in Q- and V-band spectrum in addition to Ka-band.

[1] Kratos, August 2022: Crowded Spectrum Pushing Satcom Operators into Q/V Band
[2] Data Center Dynamics, January 2023: Starlink building or expanding more than 20 US ground station sites to operate in E-band
[3] Konnect VHTS, capacity of 500 Gbps, Thales Alenia Space, September 2022: Lancement réussi du satellite de télécommunnications EUTELSAT KONNECT VHTS

Introduction to the different types of terminals

Satellite communication terminals are devices that enable communication services. These terminals cater to various operational needs and associated services, leading to the identification of different types of user terminals. User terminals can be classified based on their operational use, installation, and technical features. These technical features encompass:

- Radio electrical performance, including factors such as sensitivity and signal reception quality.
- Power consumption and autonomy, indicating the energy requirements and battery life of the terminal.
- Availability, referring to the terminal's ability to establish and maintain a connection under different conditions, beyond just received power level.
- Dimension and weight, specifying the physical size and mass of the terminal.
- Operational bands, indicating the frequency ranges at which the terminal can operate.
- Resilience against interference, highlighting the terminal's capability to withstand and mitigate the effects of external interference sources.
- Cost, representing the economic considerations associated with the terminal's design and production.

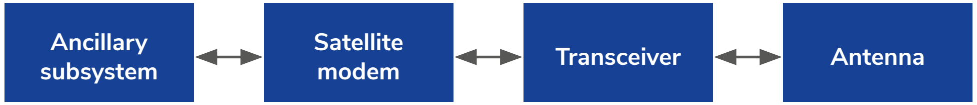
Understanding the different types of two-way user terminals is crucial as they are designed to meet the diverse requirements of various applications and services. By considering factors such as performance, mobility, and the environments in which they operate, a comprehensive classification of user terminals can be achieved. This classification aids in the selection and deployment of appropriate terminals for different use cases and services.

A non-exhaustive list of terminal manufacturers is given on page 25.

Building blocks of SATCOM terminals

A user terminal typically consists of several components (see. schema below), including:

- **Antenna**: This component facilitates the transmission and reception of signals between the terminal and satellites. It also includes the Up/Down converters, the amplifiers (LNA – Low Noise Amplifier).
- **Transceiver**: The transceiver adjusts the signal levels of radio frequency (RF) and performs frequency conversion between the RF band and a lower frequency band.
- **Satellite modem**: The satellite modem is responsible for handling the modulation and demodulation of information between the terminal's baseband and the network.
- **Ancillary subsystem**: This subsystem varies in function and composition depending on the specific operational needs of the terminal. For instance, it can include encryption/decryption subsystem, multiplexer/demultiplexer (to mix different frequency bands) and interfaces module.



On the following pages, different types of two-way terminals for SATCOM use (also applicable for secure SATCOM) are presented. It is noteworthy to mention that Flat Panel Antenna (FPA)/Electronically Steered Antenna (ESA) can be used for Land, Aero and Maritime environments.

SATCOM user terminals – Land

Optical communications

Land–Fixed terminals are generally dedicated to remote connectivity, information distribution and network redundancy. They require a stable placement, and the diameters of the dish-shaped reflector can range from small size (up to 80 cm) to large size (up to 5 m). The dish-shaped reflector is mounted on a pedestal without mechanisms for motion.

They are made of: Antenna, Transceiver, satellite modem, Ancillary equipment (as antenna non-penetrating and ballast, set of coaxial cables and power supply cable).

Deployables

Deployable terminals are of two types: Handheld and Fly-away.

Handheld terminals are characterised by low weight and dimension so it can be transported by a single person inside a backpack. This terminal has been developed for tactical communications in which the operations require the minimum weight and setup time. Handheld terminals mainly consist of: Manual pointing antenna, transceiver, and satellite modem.

Fly-away terminals are characterised by antenna size ranging from 0.5 m up to 2.4 m. The terminal is equipped with an auto-pointing system, so a low skill is required for operation. The fly-away terminal is made of the same equipment as a manpack.

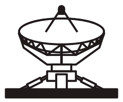
COTM

Communication-On-The-Move (COTM) terminals allow to communicate with an GEO/NGSO constellation when installed on a moving platform as they are capable to track the satellites in continuous movement. The related equipment can include a mobile parabolic antenna consisting of a dish-shaped reflector on a pedestal with a servomotor to orient the dish. The equipment can include flat panel antennas (FPAs).

Another category of mobile terminals exists, the Communication-On-The-Pause (COTP). Those terminals have been developed for applications in which the operations require the vehicle to stop in order to allow the pointing of the antenna. They are generally used to quickly reach disadvantaged sites and to allow quick and easy installation; in particular, no systems are required for the operations (such as power supply), with the exception of the space to park the vehicle and satellite visibility. COTP terminals mainly consist of: auto-pointing antenna with integrated transceiver, satellite model with hybrid capabilities, Wi-Fi access point, and auxiliary equipment.

SATCOM user terminals – aero, maritime, and flat panel antenna/ electronically steered antennas

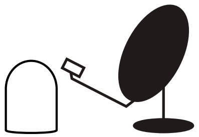
Aero



Due to the constraints related to an embedded equipment (size, weight, power-consumption), the aero terminals are generally small. Aero terminals are installed onboard aircraft, helicopter and UAVs. The aero terminal have an auto-tracking antenna able to point and track the satellite during the movements of the platform.

Flat panel antennas (FPA)/Electronically steered antenna (ESA) are very relevant for the aero needs, as their flat shape ensures a small footprint and a low drag.

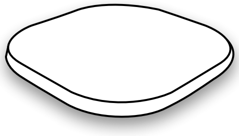
Maritime



Maritime terminals include a dish antenna ranging from around 36 cm to 3.5 m (also depending of the size of the vessels) and are able to provide satellite communications services between ships and land and intra-ship communication. The possible data rates, in most cases, range from 300 Kbps to 100 Mbps.

Similar to an aero terminal, the maritime terminal shall integrate an auto-tracking antenna to compensate the movements of the platform and stay pointed to the satellites.

Flat panel/electronically steered anten



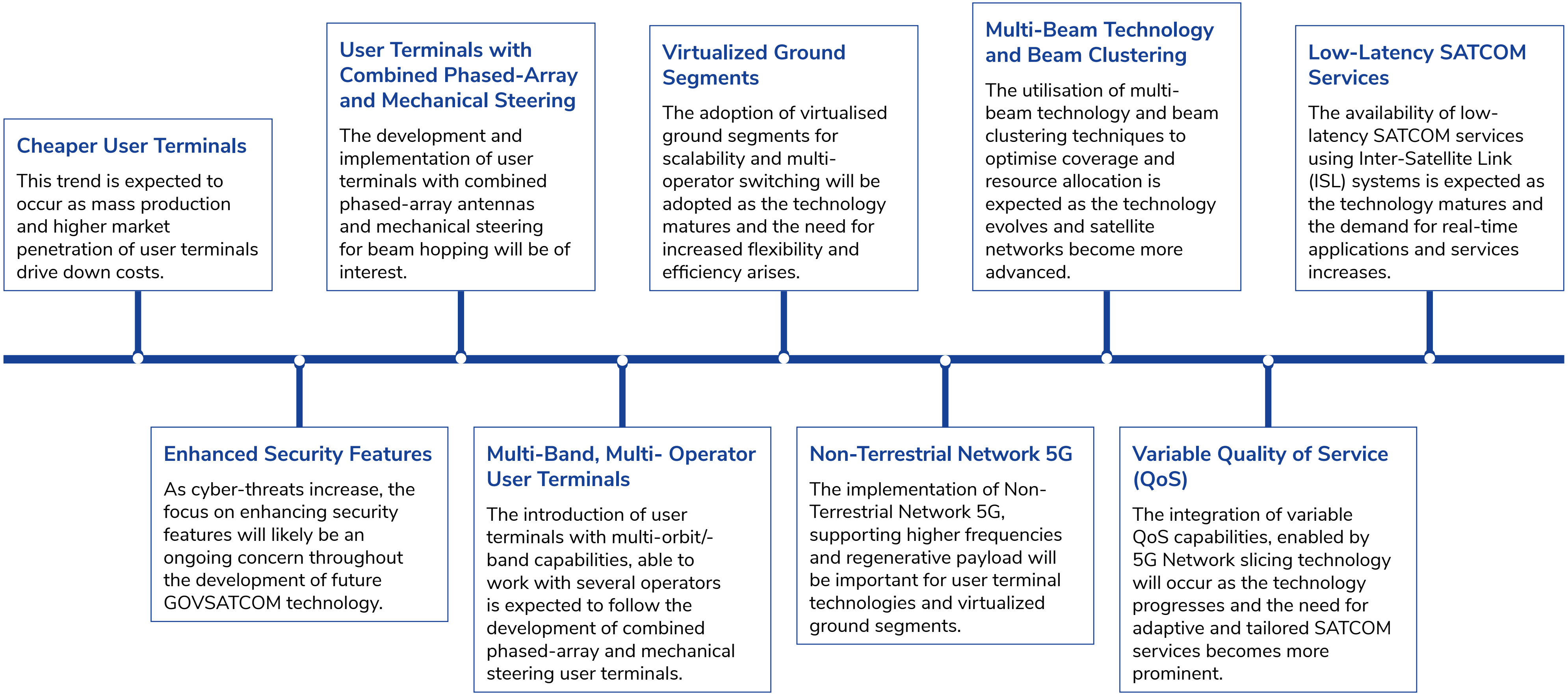
Flat Panel Antennas (FPAs) consist of metallic and dielectric materials and do not need a reflector. a common configuration is to assemble multiple patch antennas on an array to increase the antenna's gain and to obtain a flat shape better suited for mobile applications. Contrary to parabolic antennas, the beam pointing orientation can vary electronically. Indeed, the single radiators can be fed with different phase shifts and, as a result, the common antenna pattern can be steered electronically. The electronic steering is much more flexible and requires less maintenance than the mechanical steering of the antenna.

Flat panel antennas (FPAs) are often portrayed as a game changer when it comes to expanding the role of satellite connectivity in specific markets. These antennas are seen as a critical milestone for the adoption of NGSO connectivity. Their flat design is especially suitable to answer aero needs, where clients search for a solution with minimum drag (specifically to reduce fuel consumption). Other type of users (such as land users) see FPAs as a **market enabler** if the price point corresponds to their needs. The deployment of FPAs used to track satellites from NGSO constellations is estimated to be one of the main drivers in coming years and bringing down the cost or user terminals to meet price points that encourage widespread adoption is one of the greatest challenge that NGSO constellation face. They can also open the addressable market to smaller platforms (e.g., low SWaP (Size, weight and power) of FPAs can be attractive for smaller aircrafts or UAVs).

SATCOM user terminal technological trends

Technology Overview

As has been the trend over the past decades within the space industry, SATCOM ground segment equipment will likely continue to integrate commercial telecom technologies (MIMO (Multiple-Input Multiple-Output) system, phased arrays, etc.) to increase the efficiency, the market penetration, to reduce the development time and the production cost, etc. There are several features and technologies enablers which could contribute to these above-mentioned benefits. The scheme below presents the main user terminal technology trends.



Cheaper User Terminals

This trend is expected to occur as mass production and higher market penetration of user terminals drive down costs.

Enhanced Security Features

As cyber-threats increase, the focus on enhancing security features will likely be an ongoing concern throughout the development of future GOVSATCOM technology.

User Terminals with Combined Phased-Array and Mechanical Steering

The development and implementation of user terminals with combined phased-array antennas and mechanical steering for beam hopping will be of interest.

Multi-Band, Multi- Operator User Terminals

The introduction of user terminals with multi-orbit/-band capabilities, able to work with several operators is expected to follow the development of combined phased-array and mechanical steering user terminals.

Virtualized Ground Segments

The adoption of virtualised ground segments for scalability and multi-operator switching will be adopted as the technology matures and the need for increased flexibility and efficiency arises.

Non-Terrestrial Network 5G

The implementation of Non-Terrestrial Network 5G, supporting higher frequencies and regenerative payload will be important for user terminal technologies and virtualized ground segments.

Multi-Beam Technology and Beam Clustering

The utilisation of multi-beam technology and beam clustering techniques to optimise coverage and resource allocation is expected as the technology evolves and satellite networks become more advanced.

Variable Quality of Service (QoS)

The integration of variable QoS capabilities, enabled by 5G Network slicing technology will occur as the technology progresses and the need for adaptive and tailored SATCOM services becomes more prominent.

Low-Latency SATCOM Services

The availability of low-latency SATCOM services using Inter-Satellite Link (ISL) systems is expected as the technology matures and the demand for real-time applications and services increases.

SATCOM user terminals for multi-orbit & multi-band

The next generation of satellite communication encompasses the expansion from GEO satellites to NGSO constellations (MEO and LEO), the increase in orders of magnitude of bandwidth (Very High Throughput Satellites — VHTS) and the introduction of low latency orbits. These advancements were developed to enable ubiquitous connectivity for fixed and mobile assets across land, sea, and air. The driving force behind the concept of 'multi-orbit' is that operators can provide their customers with the ideal characteristics of all orbits in a transparent way. From an end-user point of view, multi-orbit is defined as the ability to work concurrently with different orbits and/or move **seamlessly from one orbit to another one**.

NGSO constellations offer low latency needed to integrate with terrestrial systems more effectively, while GEO satellites provide more capacity in a specific geographical area, than a constellation does; a constellation is primarily designed to serve the entire globe. Several geostationary (GEO) satellite operators mentioned that they have a strategy for constellations, where operators combine GEO satellites with non-geostationary orbit (NGSO) systems to provide SATCOM services aiming at combining the strengths of both. On the other hand, multi-service ground segment platforms are built with new, advanced architecture, that enable terminal providers to extend their core capabilities into the next challenges of satellite communications. Moreover, SATCOM ground terminal/manufacturers for multi-orbit operations will enable deployment on GEO as well as NGSO constellations including seamless handovers between orbits, implementing an **uninterrupted and transparent user experience, which operates a single and unified multi-orbit network**.

As the industry shifts towards a multi-orbit model to boost performance and resiliency, some terminal manufacturers are leading the way with a **flexible open architecture platform to support connectivity from every orbit and every mission** (cf. page 92). The demonstrated architecture leveraging the phased-array antenna and open-standards modem has the versatility to interoperate with satellites in GEO and non-geostationary (NGSO) orbits, ensuring global connectivity that meets different vertical markets such as government/military, maritime, and in-flight connectivity. For instance, the demonstrated high-performance solution leverages phased-array antenna and ultra-fast-roaming capabilities between satellites to support also critical manned and unmanned C2/ISR government missions.

In addition to multi-orbit capabilities, the integration of multi-band elements is essential for satellite communication terminals. By incorporating support for multiple frequency bands, these terminals can provide enhanced capacity, improved resilience against interference, and the ability to optimise performance based on specific use cases and requirements. This multi-band capability enables terminals to cater to a wider range of applications and vertical markets, offering comprehensive and adaptable connectivity solutions.

Leading satellites operators with multi-orbit strategy

On page 80, a non-exhaustive list of operators with multi-orbit strategy is presented. In line with their multi-orbit strategies, the following satellite operators support the development of multi-orbit terminals (list non-exhaustive) :

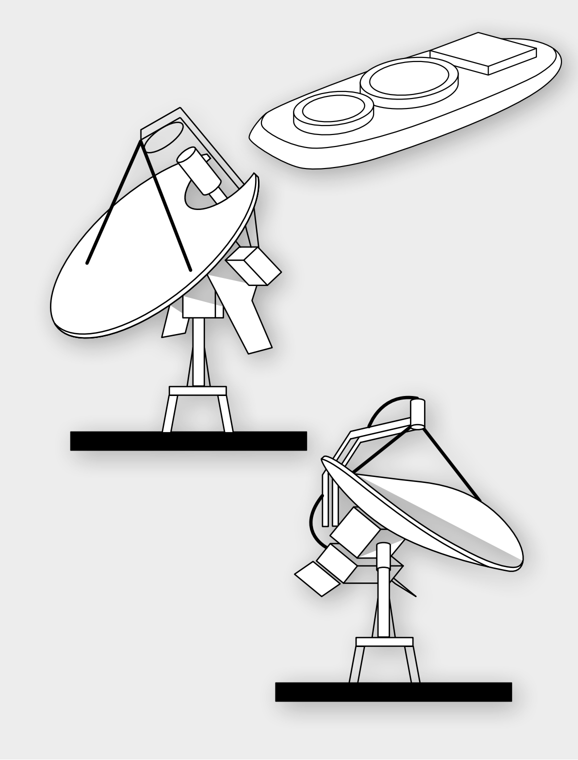
- Intelsat.
- SES.
- EutelSat/Oneweb.

User terminals for multi-orbit

Examples of manufacturers of multi-orbit terminals

The table below highlights several manufacturers developing new terminals to serve customer's needs for multi-orbit (including a market positioning in terms of product availability). It is important to mention that the list is not exhaustive even if it presents a wide overview of the manufacturers developing new multi-orbit terminals. Nevertheless, some products may be in development and/or not publicly announced.

Terminal providers	Samples of products	Comments
Intellian	V240MT, Tri-band (C/Ku/Ka). XEO Series dual-band (Ku/Ka): X100D and X150D.	Terminals installed for mobility use. The XEO Series has seen great traction with the X130D and X130D PM across commercial and military markets since they were first unveiled in 2022. X150D will be available in Q3 2023.
ThinKom	ThinAir (Ku/Ka) for air and sea. ThinSat (Ku/Ka) for land.	Most of the demos were conducted for aviation/IFC but, land terminals are also capable for multi-orbit, according to ThinKom.
Kymeta	Kymeta u8 terminal – (LEO/MEO/GEO).	Kymeta was involved in multi-orbit demonstrations (LEO/GEO). Kymeta supports Mobility, defence and security markets.
Hughes	HL1100 terminal (LEO terminal), prototypes available.	Hughes has a major contribution on multi-orbit demos for commercial and military, especially as a satellite Modem provider (Model: HM400).
Cobham SATCOM	Sea Tel 2400 (2.4m), Tri-band – SeaTel 1500 (1.5m), dual-band.	A demonstration was conducted with SES on MEO/GEO. The terminal supports maritime, enterprise, and government/defence.
ALL.SPACE	S2000 series terminal (60cm-1m) support (LEO/MEO/GEO).	ALL.SPACE, based in U.K., is an emerging technology using optical beamforming antennas. Their plan is to launch the commercial product in 2023/2024.
SatixFy	Onyx Aero terminal – support (LEO/MEO/GEO).	SatixFy, based in U.K./Israel, is also an emerging technology, mainly focused on mobility services. Also, plans to support COTM for defence, and moving ground vehicles. SatixFy plans to launch the commercial product in 2023.



User terminals for multi-orbit (continued)

Benefits of the development of multi-orbit capability

The utilisation of multi-orbit terminals has emerged and has led to transformative opportunities. Notably, this technology facilitates the exploration of new, bandwidth-intensive applications, while also delivering **significant cost improvements per gigabit**. Furthermore, multi-orbit terminals offer the potential to support hybrid connectivity by **seamlessly integrating with terrestrial networks**. This advancement brings about improvement for terminals technology, marked by continuous reductions in production costs and enhanced user-friendliness.

Selected key criteria for multi-orbit considerations	GEO	MEO	LEO	LEO/GEO	MEO/GEO
Geographical coverage[1]	◕	◐	●	◕	●
High throughput on a limited geographical area	●	◕	◐	●	●
Resilience/Availability[2]	◕	◕	◕	●	●
Latency	◔	◕	●	●	◐

○ Low performance

◐ Medium performance

● High performance

LEO/GEO opens the way to seamless global coverage (while MEO/GEO is still missing the polar coverage or high latitude areas to cover)
Multi-orbit systems enhance the space-based systems performances in terms of latency, higher flexibility, usability and cost-efficiency

[1] In LEO, the satellites are closer to Earth and can provide a more precise coverage but need a high number of satellites. In MEO or GEO, the satellites are far away from the Earth and can provide global coverage with a limited number of satellites.

[2] Orbit diversity increases both availability and resilience against any type of threats.

Key technological factors enabling future EU secure SATCOM

The key technological factors, enabling future EU secure SATCOM, are briefly presented on this and following pages, and in more detail on the following pages. They are impacting, at different levels, the segments of the secure SATCOM system.

Radio protocol to be used in SATCOM: 5G, DVB-S2X	The landscape of radio protocols in satellite communication encompasses several key standards and technologies. In commercial SATCOM, two primary protocols are widely used: 5G and DVB-S2X. The DVB-S2X standard currently serves as a prevalent choice for commercial satellite communication. However, military organisations either use their own standard for instance MIL-standard in the U.S. or its NATO (North Atlantic Treaty Organisation) equivalent, or custom confidential waveforms for other nations. DVB-S2X is mainly used as a current standard in commercial SATCOM, however over the long term, it could be anticipated that the upcoming non-terrestrial 5G (which will be updated soon) is estimated to pave the way and become another important standard. Indeed, it will benefit from the 5G terrestrial eco-system.
Interoperability between satellite gateways and user terminals enabling roaming and full mobility and dynamic tracking	Generally, the terminals discussed in the above sections do not currently support newest industry trends appearing in terrestrial 5G such as roaming and network slicing. Non-terrestrial 5G terminals is a relatively new concept which is estimated to still evolve in the coming years. This evolution is likely to prompt SATCOM terminal manufacturers to transition from DVB-S2X to 5G, driven by the advantages offered by non-terrestrial 5G's integration with the terrestrial 5G ecosystem. Although there are differences in the air interfaces, the efficiency disparity from a radio efficiency standpoint is relatively small. The key benefit of non-terrestrial 5G lies in its ability to facilitate seamless integration between non-terrestrial 5G SATCOM terminals and the terrestrial 5G infrastructure. Terrestrial 5G modem chipsets will have to be modified to accommodate SATCOM links. Nevertheless, it is expected that the integration of non-terrestrial 5G will enable some cost saving, ease of roaming capabilities for mobile terminals among different geographical regions, and easier handover from terrestrial network to SATCOM network (some mobile terminals already offer this feature, but the engineering is rather complex as the air interface is not the same, e.g.: 4G to DVB-S2X etc.).
High-level assessment of virtualisation techniques	With the emergence of the technologies such as virtualisation/cloud but also artificial intelligence, the concept of process flow (i.e. computer traffic in general or more specifically SATCOM traffic in this report) and its lifecycle are changing. Historically, the process flow was defined as a sequence of tasks, statically encoded in a flowchart during the design phase, and then deployed in a run phase. Now, with virtualisation and artificial intelligence technologies, the process flow can be dynamically updated according to its context and environment. This technique can also be used in telecom system orchestration and traffic monitoring, etc. In fact, ground segment providers are working actively to integrate those techniques to ground segment system in order to reduce infrastructure costs and improve performance and scalability, etc. The increased SATCOM capacity in GEO and NGSO systems in the coming decades will imply that the ground segment will have to be scaled accordingly. NGSO constellations (and perhaps to certain extent GEO constellations offering global coverage) will require more interconnected infrastructure with several dozens of gateways connected to Point-of-presences, and backbone infrastructure. Moreover, customer services will become more and more sophisticated with various QoS (Quality of Service) prioritisation rules, and various coverages needs, beam handover to extend coverage in GEO and NGSO systems.

Key technological factors enabling future EU secure SATCOM (continued)

Prioritisation rules	Prioritisation rules has been defined by different telecom standards. For instance, 3GPP (3rd Generation Partnership Project) 5G group defined prioritisation rules. The core network makes it possible to define network slices as dedicated or shared. The ability to change the QoS (latency, throughput) of different communication traffic in limited bandwidth communication channels is called network slicing. The concept can be very useful for prioritise more critical traffic (emergency calls, etc.). Network slicing could be a very useful technology for future secure SATCOM services. Indeed, for example, it is estimated to provide the ability to prioritise an “emergency crisis telecom link” versus a “non–urgent traffic” use case. Network slicing is one core feature of 5G.
Cyber-threat capability trends versus security techniques in end-to-end secure SATCOM links	The cyber-threat is expanding and is targeting more and more of the space industry with cybercriminal activities becoming increasingly professional. Running a risk analysis allows to define an exhaustive list of informational assets, to understand the threat landscape, the potential vulnerabilities and risks, their likelihood of occurrence, the potential impact, and how to find risk mitigation techniques. In particular, the process of risk analysis should allow to identify various types of supply chain attacks which may be a concern for the secure SATCOM infrastructure. The rapid evolution of technology may disrupt space systems which are being currently developed. In particular, quantum technologies may trigger not only significant opportunities but also threats to the current type of communications and their associated encryption techniques.
Laser communications, data relay, inter-satellite links:	It is not believed that ISL (Inter-Satellite Link) will have a direct impact on user terminals but more on gateways and communication latency. ISL technology is maturing, and European players are very active in this sector with at least 3 European suppliers (Mynaric, Tesat ADS, Thales). The production cost is going down mainly due to mass production for upcoming NGSO constellations. Each supplier, generally offers several products depending on the link distance and characteristics (either LEO -to-LEO or LEO-to-ground or LEO-to-GEO, etc.). The optical ISL generally implies the use of and On-Board Processing system (OBP), i.e. to decode packets on-board and direct packets to the right ISL head, etc. Note that Laser communication is already used in EDRS (European Data Relay System) as part of Copernicus programme.. Moreover, Quantum Key Distribution (QKD) will be presented and is more and more important to secure link. It is a cutting-edge technology that uses the principles of quantum mechanics to securely distribute cryptographic keys between two parties, ensuring secure communication.

Radio protocols to be used in SATCOM

Protocols, key technological factors for SATCOM

There are two main radio protocols used in commercial SATCOM (5G and DVB-S2x). Moreover, anti-jamming and interference avoidance in SATCOM have not been addressed as it is believed to fall inside the military perimeter and is considered as out of scope with respect to this technology report.

Hence, DVB-S2x is the mainly used current standard in commercial SATCOM, however over the long term, it could be anticipated that the upcoming non-terrestrial 5G to be released soon is estimated to pave the way and become another **important standard** because it will benefit from the 5G terrestrial eco-system.

5G NTN protocol description and design options

The 3rd Generation Partnership Project (3GPP) has been working on the support of non-terrestrial networks with 3GPP defined radio interfaces since 2017 as part of the Release 15, i.e. adding the capability to support NTN in existing 3GPP technical specifications. a key differentiator is whether the satellite provides direct or indirect access to the 5G terminals.

In the indirect case, the handheld is using the 5G terrestrial protocol to communicate with a base station. The base station uses equipment like a VSAT terminal and SATCOM link to reach the data network.

In the direct case, the handheld is communicating to the satellite using the 5G radio interface. The handheld has in general a low-gain antenna which combined with propagation loss from the satellite to the handheld **significantly reduces the channel throughput**.

For high throughput applications using 5G NTN, future handheld devices may have to use high frequency and high directive antennas (on both ends: satellites and terminals) to use **direct connections from the handheld to the satellite**.

DVB-S2x highlights

DVB-S2X is the standard on forward link. On return link, some manufacturers are implementing RCS2, others are implementing proprietary waveforms that are very similar to RCS2 (MF-TDMA). These will need proprietary modems both in Gateway and user terminal, but also and on-board a satellite with regenerative payloads.

The DVB standard provides efficient support for all applications even if there is some weakness on the uplink for some applications like trunking. DVB-S2X offers a good spectral efficiency but lower than 5G NR (New Radio) on uplink

Roaming: interoperability between satellite gateways and user terminals

Interoperability can be considered at various levels. Indeed, it can be considered at the level of a SATCOM terminal with various satellite links and various gateways, but in the context of secure SATCOM, one should also consider the interoperability of a complete connection between two end-points on the globe.

Interoperability with ground infrastructure[1] 1

Interoperability should be considered between different infrastructure, i.e. the need for connecting institutional ground infrastructure to existing SATCOM capacity. This connectivity can be part of the service providers' packages if the service packages already offer direct connectivity to the institution's HQ, but it could be the case that connectivity with this HQ is non-existent.

Thus, an ad-hoc (or automated which is currently the case in the telecom terrestrial industry) connectivity is required to enable the connection between the different communication channels. As an example, a connection might be required between the HQ and the end-user or resource (RPAS, etc.) on the field via different means: Firstly, the HQ connects to a gateway via a terrestrial line to a satellite; secondly, a connection establish to another gateway via an undersea cable and then, hop to another satellite and then reaches the end-user/resource. Depending on the number of requests per day or the urgency of the request, the setup and installation of this new communication path may need to be setup rather quickly and efficiently. One technology exists in the terrestrial telecom industry and is called the MEF standard. Various telecom operators ubiquitously use it to establish communication paths and bridges across the world.

Interoperability between deployed terminals[1] 2

Interoperability between the different systems inside a communication network is an important topic. One of the key use-cases behind this is communication across different mission needs.

For instance, some users may want to communicate using SATCOM mobile phones while other users may want to communicate using VSAT terminals and still want to talk or exchange information with each other.

At a very high level, there are different means to achieve inter-operability:

- Either through **protocol standardisation** e.g., DVB-S2X and 5G (this is what happened in the mobile terrestrial industry through the 3GPP group for example). This topic is being discussed in a section above called radio protocols.
- Or through more **flexible hardware** (e.g.: user terminal modem, modem gateway, etc.) capable of switching from one protocol to another one on the fly.

One current problem preventing interoperability in the SATCOM industry is that terminals are vendor-specific and tied to gateway technologies. Roaming across different networks is generally not possible with the same terminal contrary to terrestrial cellular networks. "Software-defined" terminals allow components of the protocol stack (either control or data plane functions) to be replaced on-demand, even during runtime. Migration from hard-wired to reconfigurable logic; already exists in some models e.g. ViaSat CBM-400. If standardisation of space radio systems do not converge toward unified radio standards (like it is done in terrestrial system with 3GPP 5G) then one other way to implement interoperability is by accommodating arbitrary software from third parties (i.e. different HW and protocol stack vendors). Key driving technologies enabling this interoperability are **Software-defined Radio (SDR), Software-defined Networking (SDN), Network Functions virtualisation (NFV) as well as fully software-defined terminals (entire L1-L7 stack in software)**.

[1] Numbers are associated to the ones in the scheme presented on page 98.

Roaming: interoperability between satellite gateways and user terminals (continued)

Challenges of interoperability between terminals and gateways[1]

3

Interoperability between terminals and gateways would enable the entire stack to be downloaded and dynamically reconfigured, allowing automatic configuration and operational readiness within minutes of service setup. a positive development in this direction is the introduction of highly reconfigurable terminals like the ViaSat CBM-400 modem, which can switch among a predefined set of waveforms. However, there is still work to be done to achieve true vendor-neutrality and complete interoperability. As an alternative, the adoption of software-defined gateways could be considered, enabling their reconfiguration to serve groups of traditional terminals. This option, although more technically complex, would be particularly valuable for GOVSATCOM customers with a significant number of installed terminals that are impractical and expensive to replace or upgrade. In such cases, software-defined gateways could be employed by Satellite Network Operators (SNOs) to load a protocol stack compatible with the terminals, and associate specific carrier(s) over which the service will operate. In any case, key technological enablers towards the **increasing use of software** for either terminals or gateways are:

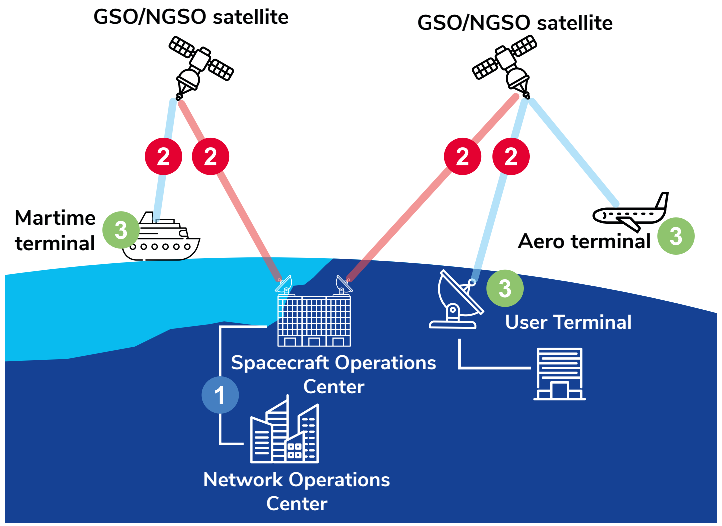
- **IT virtualisation techniques**, allowing complete functional modules to be deployed as Virtual Machines (VMs) or Containers (depending on the depth of virtualisation).
- Software-use trends in the networking industry, built around the fundamental pillars of **Software-Defined Networking (SDN)** and **Network Functions Virtualisation (NFV)**.

Moreover, Software-Defined Radio (SDR), is a well-established concept which has become commodity over the past two decades. Several other technologies have been also standardised, such as the Common Public Radio Interface (CPRI).

Interoperability is a true key technological factor for SATCOM

Interoperability between satellite gateways and user terminals enables roaming and full mobility and dynamic tracking. Moreover, most of the existing terminals do not currently support the newest industry trends appearing in terrestrial 5G such as roaming, network slicing, etc. The non-terrestrial 5G terminal concept is relatively new and is estimated to still evolve in the coming years and so will eventually lead some SATCOM terminal manufacturers to switch from DVB-S2X to 5G.

From a radio efficiency point of view, despite the air interface differences, the efficiency difference is rather small. The advantage of the non-terrestrial 5G is that it will facilitate the integration of non-terrestrial 5G SATCOM terminal with the terrestrial 5G eco-system. Terrestrial 5G modem chipsets will require upgrades to accommodate SATCOM links, but overall, it is expected that the integration of non-terrestrial 5G will enable some cost savings, ease of roaming capabilities for mobile terminals among different geographical regions, and easier handover from terrestrial network to SATCOM network (some mobile terminals already offer this feature, but the engineering is rather complex as the air interface are not the same, e.g.: 4G to DVB-S2X, etc.).



Roaming: interoperability between satellite gateways and user terminals (continued)

Software-defined terminals/gateways for interoperability

Interoperability could be achieved using software-defined terminals/gateways. These concepts need to match the specificities of a SATCOM network, as well as address SATCOM-specific challenges, such as synchronization constraints. It is believed that the technological development steps to bring interoperability using software-defined terminals/gateways to maturity could be the following:

1. **Development of software-based protocol stacks**. This implies the transfer of the protocol stack functions currently implemented in bespoke hardware and/or embedded software into a format appropriate to be hosted in a generic platform (see 2. below), using specific APIs (Application Programming Interfaces), library calls and descriptors for deployment and management. Licensing, as well as integrity check mechanisms should also be in place to protect the software stack from unauthorized duplication, modification or reverse engineering.
2. **Design, development and prototyping of a reconfigurable generic terminal/gateway platform** to be able to host virtually any software-based protocol stack, such a terminal/gateway should normally include i) generic computation and storage of resources to accommodate and execute the software and ii) a Software-Defined Radio (SDR) front-end (typically supported by FPGAs (Field Programmable Gate Arrays) for acceleration) to process the input/output waveforms. It should also include mechanisms for remote automated provisioning and reconfiguration of the protocol stack.
3. **Development of a centralised orchestrator/traffic management platform**, on the SNO (Satellite Network Operator) side, which should manage the deployment and configuration of software stacks, as well as properly steer the traffic across beams/hubs/satellites in mobility/roaming scenarios.
4. **Extensive tests and validation, to assess the interoperability, performance and stability** of the software-driven stack (common issues in software-driven networks in general).
5. **Standardisation and harmonisation**. The effort towards reconfigurable terminals and/or gateways will be successful only if there is major industry adoption. In other words, the engagement of a wide community of vendors must be sought. They will have to agree on common specifications on HW<>SW APIs, capabilities, drivers, libraries, descriptors etc.

It is envisaged that this effort will be driven by a critical mass of vendors who will form an industry alliance specific for this purpose and produce de-facto standards, which, upon global adoption, may be further taken to an international SDO (Standard Developing Organisation) for formal standardisation.

Ground station antenna for gateway

© AdobeStock

IT virtualisation techniques for ground segment

Virtualisation techniques in the computing world have been around since the 1960s. However, with the emergence of cloud computing, this technique has become widespread. Cloud computing allows for the seamless scaling of computing systems in real-time, dynamically adjusting cloud capacity to meet instantaneous demand.

In essence, virtualisation involves separating the software layer of a computer, server, or network element from its hardware layer. This is achieved by introducing a new layer called Virtual Network Slice, which acts as an intermediary. This process can be thought of as creating multiple virtual resources from a single physical resource (computer or server), or vice versa, creating one virtual resource from multiple physical resources. Virtualisation extends its reach into various domains, including networking, storage and hardware.

There are two key functionalities that enable virtualisation: Network Function Virtualisation (NFV) and Software Defined Network (SDN). NFV allows different network functions to be performed independently on a single hardware, with the added benefit of easy migration between equipment. On the other hand, SDN enables on-the-fly configuration of network elements based on the specific needs of different services and applications.

One practical application of virtualisation can be seen in VSAT (Very Small Aperture Terminal). It leverages external network element resources, such as computing resources, to increase the flexibility of the VSAT equipment.

Notably, the traditional approach of embedding all Network Functions within gateways has evolved. Virtual Network Functions (VNFs) are now utilised and integrated into centralised software controllers, powered by SDN. Additionally, the physical partitioning of infrastructure through network slicing further **enhances flexibility and interoperability with terrestrial networks**.

More generally, IT virtualisation can enhance SATCOM systems in different manners: Resource optimization (virtualisation allows to run multiple virtual instances of software and hardware on a single physical server or satellite ground station), flexibility and scalability (the SATCOM system can adapt to changing demands, such as increased traffic during peak times or the need to allocate more resources to specific satellite services), cost savings (by consolidating multiple virtual machines (VMs) on a single physical server, hardware and operational costs can be reduced), redundancy and high-availability (virtualisation can help achieve redundancy and high availability in SATCOM systems). Isolation and Security (VMs can be isolated from each other, providing a layer of security).

IT virtualisation, a key technological factor for SATCOM’s ground segment

Interoperability between terminals and gateways would enable the entire stack to be downloaded and dynamically reconfigured, allowing automatic configuration and operational The concept of process flow and its lifecycle are changing with the emergence of the technologies (virtualisation/cloud, artificial intelligence, etc.). Historically, the process flow was defined as a sequence of tasks, statically encoded in a flowchart during the design phase and then deployed in a run phase. Now, with artificial intelligence technologies, the process flow can be dynamically updated according to its context and environment. This technique can also be used in telecom system orchestration and traffic monitoring, among others. In fact, ground segment providers (e.g.: Gilat, Hughes, Newtec, Kratos, etc.) are working actively to integrate those techniques to ground segment systems. It will help to reduce infrastructure costs and improve performances, scalability, among others.

The increased SATCOM capacity in GEO and NGSO systems in the coming decades will imply that the **ground segment will have to be scaled accordingly**. NGSO constellations (possibly also GEO constellations offering global coverage) will require more interconnected infrastructure with several dozen gateways connected to Point-of-presence, and backbone infrastructure. Moreover, customer services will become more and more sophisticated with various QoS, and various coverages needs, beam handover to extend coverage in GEO and NGSO systems.

Traffic prioritisation rules for ground segment

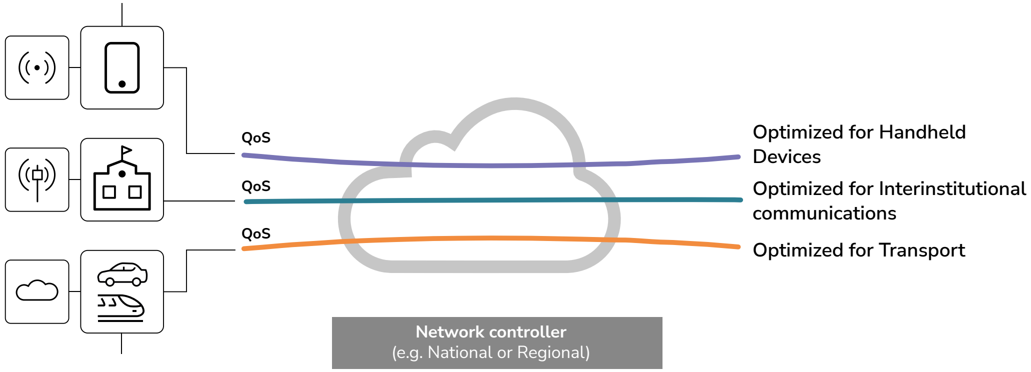
Network slicing and prioritisation rules

Network slicing is the ability to adapt the QoS (Quality of Service) of different users sharing the same communication channel. Network slicing could be very useful for future secure SATCOM services because it would provide for example the ability to **prioritise an “emergency crisis telecom link” versus a “non–urgent traffic”**. Network slicing is one core feature of 5G whereas DVB-S2x is relying on IPv4, IPv6 for the Network layer, and thus prioritisation could be possible but in a much less flexible manner.

In the design phase, the core network allows for the creation of network slices with dedicated or shared user-plane, control-plane, or data-plane network functions (NFs). When a device or application requests to connect, subscription and policy controls determine the network slice instantiation of NFs to use. a dedicated User-Plane Function (UPF) is needed to provide optimal redundancy level, eliminate the risk of interruption from other services and ensure low latency, allowing the user data traffic to stay on-premises.

When the control-plane and data-plane functions are dedicated, the slice constitutes a fully independent logical network. The cloud native 5G Core enables some NFs, such as the UPF, to be deployed closer to the user for latency-sensitive applications. In the picture on the right, the different slices (corresponding to different applications and QoS) are represented by the different colours all along the different network entities.

Network slicing examples


QoS
QoS
QoS
Optimized for Handheld Devices
Optimized for Interinstitutional communications
Optimized for Transport
Network controller
(e.g. National or Regional)

Prioritisation rules is another key technological factor for SATCOM

Prioritisation rules have been defined by different telecom standards (e.g.: 3GPP 5G group). The core network makes it possible to define network slices within the communication channel. Network slicing is the ability to change the QoS (latency, throughput) or different communication traffics in limited bandwidth communication channels.

Laser communication, data relay, inter-satellite links

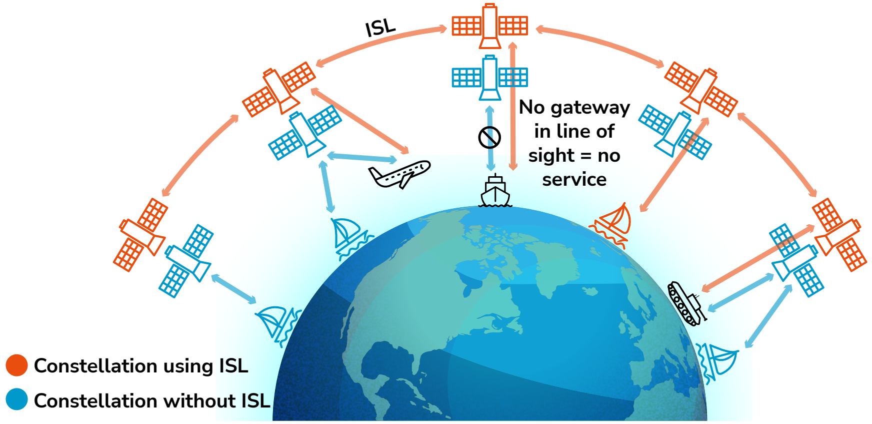
Inter-satellite links (ISLs) establish high-speed communication channels between satellites, typically through optical or RF technology, enabling data routing between adjacent satellites and creating a large mesh network that communicates with ground stations. It is not believed that ISL will have a direct impact on user terminals per se but more on gateways and overall communication latency. ISL are used to create high-speed communication channels (traditionally optical but it can also be RF) between satellites. In addition to communicating with the users' terminal in its footprint, each satellite also maintains contact with two to four adjacent satellites using the ISL and routes data between them to create a large mesh network communicating with ground stations.

In general, optical ISL goes in pair with OBPs (on-board processing) to route traffic on the right spacecraft optical head (North, South, East, West). **ISL improves/accelerates data uplink/downlink and reduces the footprint of the ground segment** (IRIDIUM constellation only operates four gateways but has a global coverage). To date, some examples of ISL systems are Iridium's constellation or NASA's GEO TDRS (Tracking and Data Relay Satellite). The TDRS will keep a continuous communication link with the ISS (International Space Station).

Because of ISL, station-to-station data exchange from one user terminal to another can be routed directly through space without going through a ground station improving the exchange's security. Intersatellite links have existed for a couple of decades and several systems have been put in place around the world (the TDRS and EDRS (European Data Relay Satellite System) optical for instance but not only). Inmarsat also offers a low-cost RF intersatellite link service with a more modest throughput. EDRS is a ISL service which can be used to connect with other ISL enabled satellites in LEO for instance. It is used by the Copernicus satellites and Airbus offers it also as a commercial service.

ISL technology will likely become ubiquitous, especially amongst NGSO systems, as the technology matures and cost decreases. It will enable a decrease in the amount of gateway infrastructure to be deployed and thus help reducing the CAPEX cost of those NGSO systems and in turn help reducing capacity cost €/Mbps/month (the CAPEX ISL cost saving must be offset by the CAPEX gateway saving).

Constellation with/without ISLs representation


ISL
No gateway in line of sight = no service
● Constellation using ISL
● Constellation without ISL

Examples of Optical ISL manufacturers and products

	Product	Examples of application
TESAT	LCTI35	GEO SATCOM data relay
	Smart LCT70	Earth observation LEO satellites connected to GEOs in data relay scheme
	SCOT80	LEO Broadband constellation data relay
	Cube LCT	CubeSat LEO data relay
Mynaric	Condor Mk2	LEO constellation (ex: compatible with SDA tranche 0) data relay
	Condor Mk3	Evolution of CONDOR Mk1
Thales Alenia Space/ RUAG	OPTEL-C, OPTEL-μ	Data relay

Roaming and Inter-satellite links

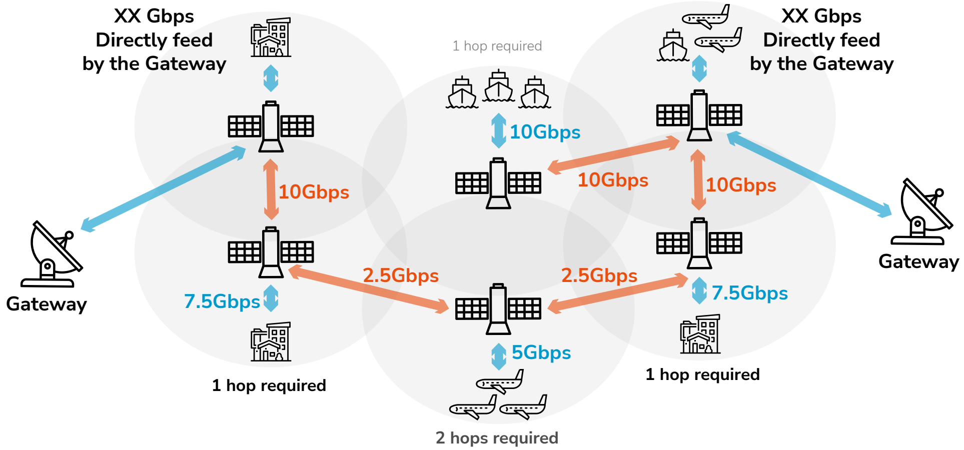
Intersatellite link and roaming, key technological factors for SATCOM

ISL technology is maturing, and European players are very active in this sector with at least 3 European suppliers (Mynaric, Tesat, Thales) while production costs continue to decrease thanks to mass production for the upcoming NGSO constellations. Each supplier generally offers several products depending on the link distance and characteristics (either LEO-to-LEO or LEO-to-ground or LEO-to-GEO, etc.), see previous page. The optical ISL generally implies the use of an onboard processing system (OBP), i.e. to decode packets on-board and direct packets to the right ISL head, etc.

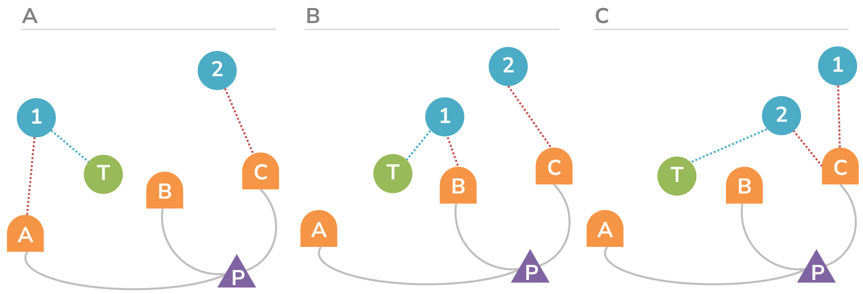
Two main challenges for Inter-satellite links

1. **Intersatellite links bottleneck**: Even if Intersatellite Links can be seen from a network point of view as simple ethernet cable, their implementation in space is far more expensive for optical units. All traffic from all linked satellites not in range of a gateway must pass through the satellite that does have gateway coverage. **This creates a bottleneck, requiring very tight resource planning and allocation**. When a satellite supplies traffic to a high-density area without being in visibility of a gateway, the traffic can only be supplied itself by the ISLs. The congestion effect is illustrated on the figure on the right and is amplified by two factors: number of ISL hops required to reach a Ground Station and capacity served by adjacent satellites/Number of high-density areas served by adjacent satellites. Hence, ISL is required for spatial mesh but will add DC/mass/cost/network constraints that have to be accounted at the earliest phase of the system design.
2. **Roaming aspects**: Roaming, including all handovers aspects, is a critical topic in satellite constellations as it must be seamless for the user. The figure on the right illustrates a typical roaming scenario. In step A, the UT is served by satellite 1, which is currently connected to gateway A, and in turn to Point of Presence (POP) P via ground fiber. In step B, a few seconds later, the satellite has moved closer to gateway B, and roams onto it. The UT's context must be switched from gateway a to gateway B but maintaining the satellite and POP assignments in the network path topology. In step C, a few seconds later, the UT roams from satellite 1 to satellite 2, as it is in a better position.

ISL congestion effect illustration



Roaming scenario illustration



The various handovers (inter/intra satellite) can be done in "break before make" (link interruption, need to create the next link in few tens of ms) or "make before break" mode (Next link prepared in advance).

Cybersecurity principles and factors influencing secure SATCOM

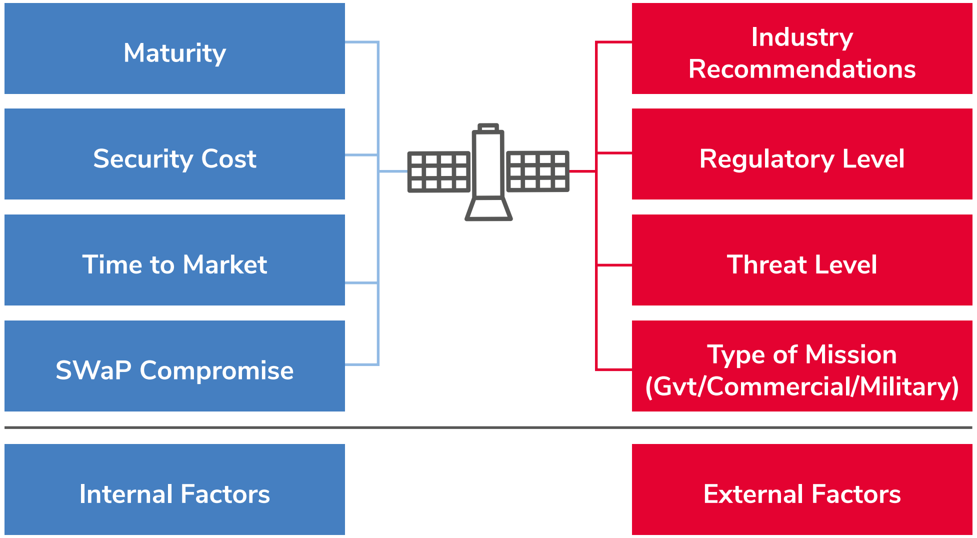
Cybersecurity concerns the capability to prevent, protect from, detect and mitigate unauthorised access and/or criminal use as well as investigation of cyber incidents related to computers, electronic communications systems, electronic communications services, wire communications, and electronic communications , including information contained therein. The ultimate objective of Cybersecurity is to ensure Confidentiality, Integrity, and Availability (CIA). The security requirements for different systems may vary, but they usually include the basic triad of CIA. In addition, some systems may also require authentication, non-repudiation and access control to ensure the security of the data and the users.

In addition, different mission types may require different level of assurance of operation for each security service. For example, high-security missions will require many security services and the highest assurance that those services are operating as intended (e.g., use of high grade, government-approved cryptographic algorithms). Moderate security missions may require the same security services as high security missions, but with lower levels of assurance. Minimal security missions will require the fewest security services, and the lowest levels of assurance.

When implementing cybersecurity on a space mission, satellite manufacturers are constrained by a number of factors, whether internal or external, making the implementation of cybersecurity more or less robust. First, the type of mission, whether commercial, governmental or defence-related may influence its cybersecurity level. Defence and governmental missions usually comply with the highest security requirements. On the other end, commercial missions due to financial or time-to-market reasons, and sometimes due to lower awareness or maturity regarding cybersecurity, may not set significant efforts on cybersecurity implementation. In any case, **implementation of cybersecurity represents a technical tradeoff** as it may have significant impacts on the overall size, weight, and necessary power (SWaP) of the satellite. External factors such as the evolution of the threat level, or the current level of recommendations issued by the industry may also be strong incentives to improve the global cybersecurity level of space-related systems.

It is noteworthy to mention that ground and user segment (not only space segment) design are also impacted by cybersecurity requirements.

Factors impacting the cybersecurity level of a space system from a satellite manufacturing perspective


Maturity

Security Cost

Time to Market

SWaP Compromise

Industry Recommendations

Regulatory Level

Threat Level

Type of Mission (Gvt/Commercial/Military)

Internal Factors

External Factors

Cybersecurity is key in increasingly contested scenarios

Cybersecurity landscape overview

In recent years, the importance of cybersecurity in the space industry has significantly increased due to various factors. This shift in focus has been prompted not only by the industry stakeholders, researchers, and military entities but also by the malevolent activities of ransomware and criminal groups. Understanding how to protect and exploit space infrastructure has become crucial for all these parties involved. Traditionally, satellites have relied on "security through obscurity," leveraging system complexity and high equipment costs to deter adversaries. However, the landscape has evolved due to the widespread use of space assets in our daily lives, the adoption of off-the-shelf hardware and software components, the growing number of space assets, and other trends within the New Space domain. These **developments have significantly expanded the potential attack surface, increasing the need for robust cybersecurity measures**.

Alongside this expanding playground for cyber attackers, the complexity and connectivity of space systems have also risen, amplifying the risk level and the challenges associated with protecting space-related infrastructure. The taxonomy of threat actors can be divided into different broad categories ranging from state-sponsored military groups which are approaching cyberspace as a new battlefield with its geopolitical implications, to individual hackers or insiders looking for their own interest or local disruption. In the last 3 years, national security agencies have particularly highlighted the significant development of ransomware activities which had an operational and financial impact on all the major industries. Ransomware groups revenues are estimated to be over $1.5Tn per year which offers these criminal actors the opportunity to professionalise their service (through affiliate or partnership programmes) and to improve their products (with better encryption rate or exfiltration speed). Many attacks on the aerospace industry didn't have any direct financial interest and were mainly done to steal intellectual property or spy on sensitive activities and information. These attacks are usually perpetrated by **actors with substantial financial means and are often state-sponsored**. Even if a specific focus is made here on ransomware, the attacks on the aerospace industry may also involve and imply other types of malwares and are also driven by different motivations beyond direct financial gain. It is important to recognise that the increasing attention towards cybersecurity in the space industry is not merely a result of industry interest but a **response to a changing landscape guided by governmental directives and policies**. An example of such initiatives is the EU Space Strategy for Security and Defence, which plays a significant role in shaping the approach to space cybersecurity. By acknowledging and addressing these challenges, the space industry and relevant stakeholders can work together to enhance the security and resilience of space infrastructure in the face of evolving cyber threats.

Main objectives of EU Space Strategy for Security and Defence

In the current geopolitical landscape, marked by escalating power competition and an intensification of threats faced by the European Union (EU) and its Member States, space has emerged as a strategic domain of paramount importance. Recognizing this, EU leaders have outlined the significance of space in the Strategic Compass and have called for the formulation of an EU Space Strategy for Security and Defence. The EU is taking proactive measures to safeguard its interests, deter hostile activities in space, and bolster its strategic position and autonomy. The European Union Space Strategy for Security and Defence is designed to achieve several key objectives[1]:

- Enhancing Resilience and Protection of Space Systems and Services.
- Responding to Space Threats and Strengthening the EU Space Threat Response Architecture.
- Enhancing the use of EU Space capabilities for Security and Defence.
- Partnering for responsible behaviors in outer space.

By doing so, the EU aims to ensure its resilience, strengthen its capacity to address emerging threats, and assert its autonomy in space affairs.

[1] European Commission, 2022: EU Space Strategy for Security and Defence

Actual cyberattacks and potential scenarios

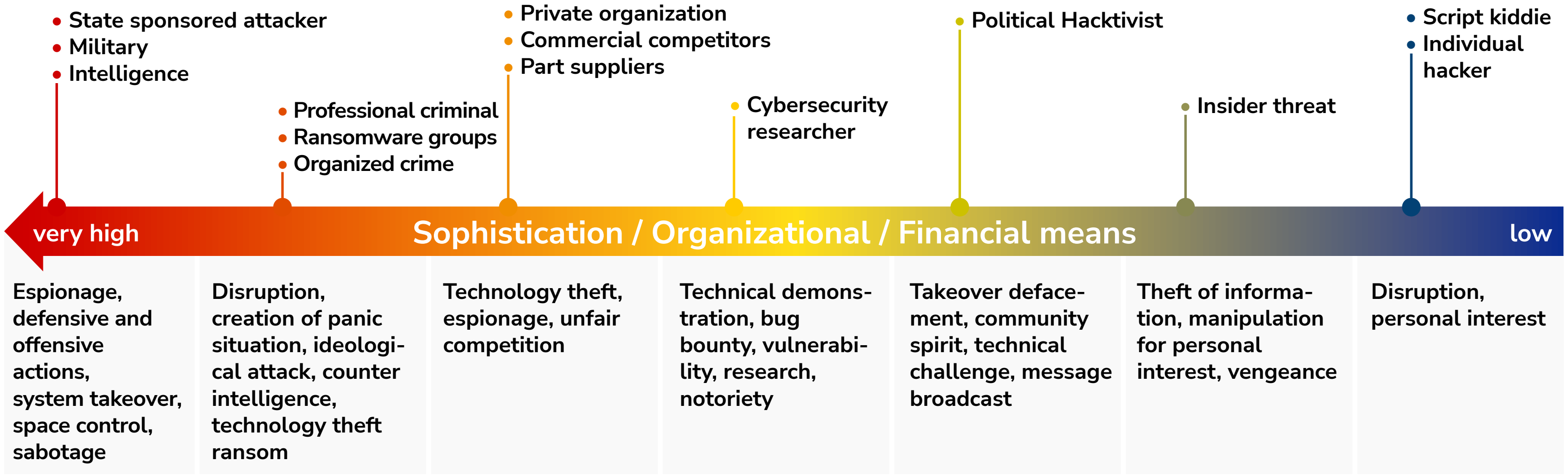
Actual cyberattacks and potential scenarios

Research in the domain of space cybersecurity usually defines **three broad categories of attack surfaces**: those relating to **satellite signals**, those relating to **space platforms**, and those targeting satellite ground systems. Providing a detailed description of cyberattacks is out of scope for the present report. However, public information exists which either refers to cyberattacks belonging to the public domain or to cyberattacks that have been declassified after an extended period of time.

Scenarios of cyberattacks are either built from actual empirical cases of cyberattacks for which detailed information is available or by a scenario-oriented approach based on common risk assessment methodologies, such as the NIST SP 800-30 or the ISO 27005:2011. This table of cyberattacks demonstrates various levels of sophistication for a flaw to be exploited. Threats targeting the satellite payload generally require very sophisticated attack scenarios and are not within reach of any type of threat actor. There are only very few cases of actual examples of a cyberattack on the satellite payload as it usually requires a complex and early supply chain compromise with significant technical resources and knowledge.

On the other side, many cyberattacks are documented which target the satellite signal such as jamming, signal injection, or eavesdropping type of attacks. Such attacks are particularly hostile as they don't necessarily require important financial means and the required level of sophistication is moderate to low. Attacks to the ground infrastructure have significant commonalities with the attacks targeting more common IT network infrastructure.

Overview of threat actors and their motivations



• State sponsored attacker • Military • Intelligence	Espionage, defensive and offensive actions, system takeover, space control, sabotage
• Professional criminal • Ransomware groups • Organized crime	Disruption, creation of panic situation, ideological attack, counter intelligence, technology theft ransom
• Private organization • Commercial competitors • Part suppliers	Technology theft, espionage, unfair competition
• Cybersecurity researcher	Technical demonstration, bug bounty, vulnerability, research, notoriety
• Political Hacktivist	Takeover defacement, community spirit, technical challenge, message broadcast
• Insider threat	Theft of information, manipulation for personal interest, vengeance
• Script kiddie • Individual hacker	Disruption, personal interest

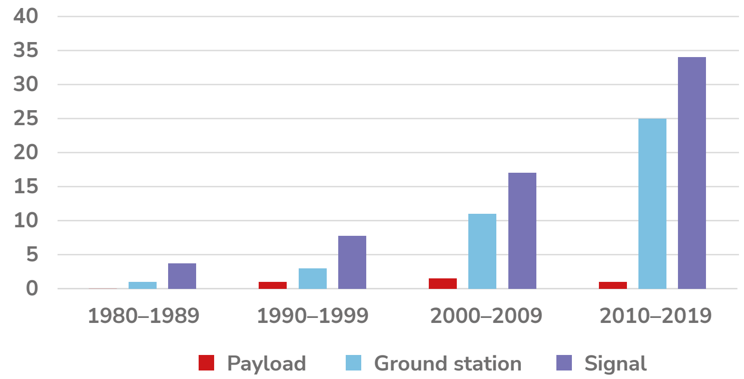
Actual cyberattacks and potential scenarios (continued)

Evolution of Cyberattacks on Space-Based Systems (then applicable to SATCOM)

Cyberattacks against satellite systems have been occurring for decades perpetrated by attackers from across the globe. In the early days, from 1980 to 1989, the principal information security concerns revolved around the ability of adversaries to compromise satellite flight control signals. However, military satellites were presumed secure due to the complexity of the requisite equipment. The main concern was on commercial missions, especially during the Cold War, where jamming and replay attacks have been a concern between American and Soviet adversaries. The first major satellite hacking incidents are generally thought to have occurred in the 1980s with cases of hijacking of television shows in the U.S., cases of eavesdropping against satellite imagery services, and attacks against ground station networks. The acceleration of satellite usage in the 1990s saw a rise in cases of jamming attack perpetuated by states to control flows of information. This period also saw the emergence of cryptographic systems against satellite television piracy. The 1990s also saw high profile incidents where hackers claimed to have accessed systems which could allow the issuance of flight control commands to orbiting satellites (intrusion in NASA's Goddard Space Flight Center and ROSAT satellite alteration).

From the 2000s, one major trend was the emergence of organized non-state attackers. Significant attacks against ground stations during this period include a complete flight control takeover of two NASA satellites in 2007 and 2008. The 2000s also saw the first public case of malware infection in orbit. Since 2010, a wave of jamming incidents in the Middle East and North Africa was kicked off by the Arab Spring protest movements. Attacks against ground stations and satellite control systems grew more sophisticated as well, with many being linked to state actors. Commercial ground systems were also demonstrated to have severe vulnerabilities, including many hard-coded passwords and backdoors. New attention has recently been paid to the satellite cybersecurity field with the U.S.A.F. (U.S. Air Force) launching the Hack-a-Sat challenge inviting teams of hackers to uncover vulnerabilities on real space systems.

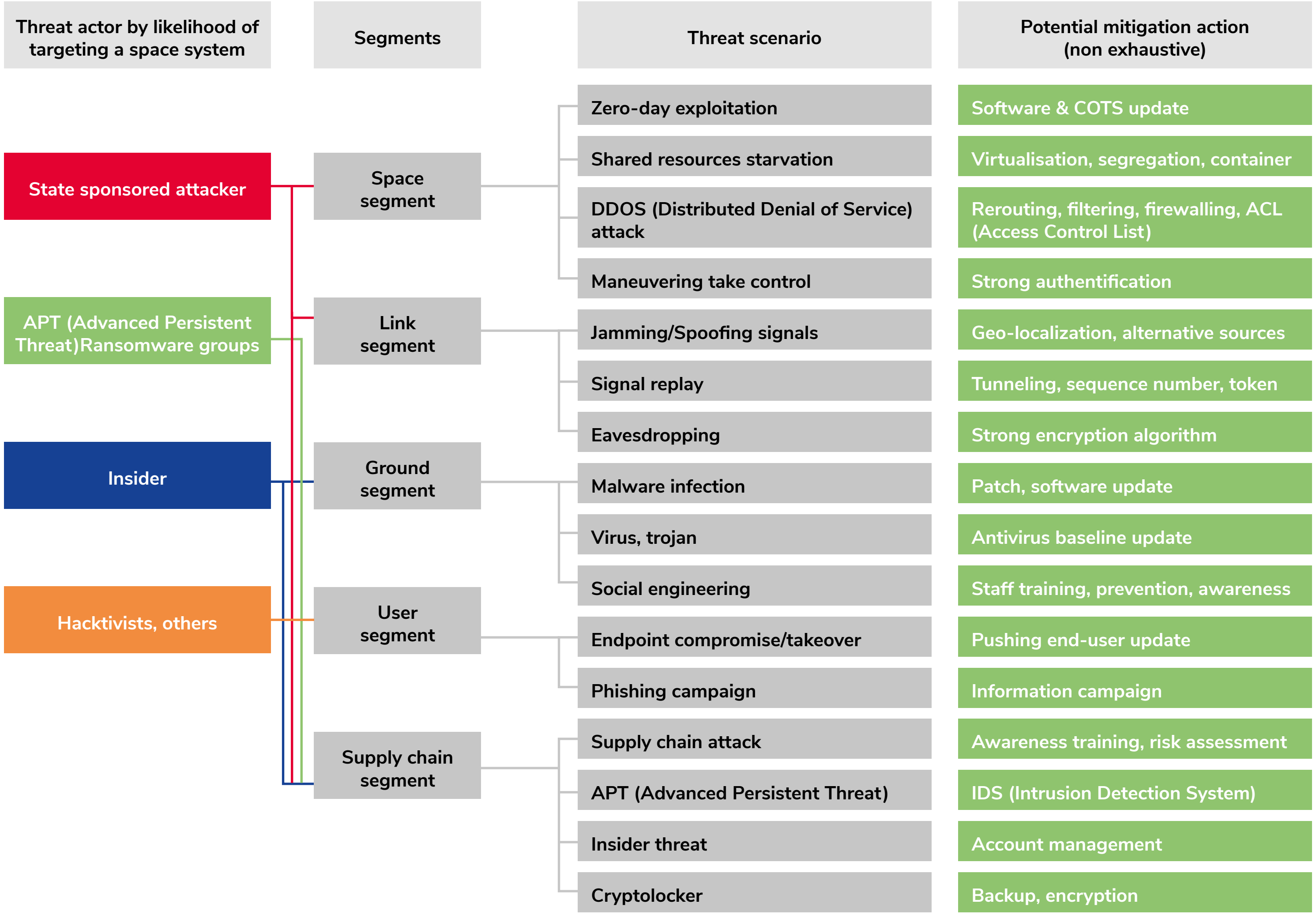
Evolution of cyberattacks on Space Systems (number of attacks /year over the last fourty years)



Source: James Pavur, Securing new space: on satellite cyber-security - ORA - Oxford University Research Archive

Examples of cyberattacks include eavesdropping (interception, delete or modification of transmitted data), signal interference (addition of same type of signals as the ones used by the satellite, leading to a partial or total loss of the signal), spoofing (intentional interference, usually nefarious form of interference done using fake satellite signals), jamming (use of white noise leading to a partial or total loss of the signal) and network intrusion (unauthorized penetration of enterprise network or an individual machine).

Actual cyberattacks and potential mitigation actions examples



Threat actor by likelihood of targeting a space system

- State sponsored attacker
- APT (Advanced Persistent Threat)Ransomware groups
- Insider
- Hacktivists, others

Segments	Threat scenario	Potential mitigation action (non exhaustive)
Space segment	Zero-day exploitation	Software & COTS update
	Shared resources starvation	Virtualisation, segregation, container
	DDOS (Distributed Denial of Service) attack	Rerouting, filtering, firewalling, ACL (Access Control List)
	Maneuvering take control	Strong authentification
Link segment	Jamming/Spoofing signals	Geo-localization, alternative sources
	Signal replay	Tunneling, sequence number, token
	Eavesdropping	Strong encryption algorithm
Ground segment	Malware infection	Patch, software update
	Virus, trojan	Antivirus baseline update
	Social engineering	Staff training, prevention, awareness
User segment	Endpoint compromise/takeover	Pushing end-user update
	Phishing campaign	Information campaign
Supply chain segment	Supply chain attack	Awareness training, risk assessment
	APT (Advanced Persistent Threat)	IDS (Intrusion Detection System)
	Insider threat	Account management
	Cryptolocker	Backup, encryption

The graph on the left illustrates a non-exhaustive list of possible countermeasures that can mitigate vulnerabilities associated to threat scenarios at various levels (Space, Link, Ground, User and Supply Chain). It also highlights that all the segments are vulnerable to cyberattacks but in a different manner. Consequently, each one has to be protected specifically. It matters to protect all the segments, as any vulnerability in the transmission chain can be exploited.

Annex 1: List of acronyms

3GPP	3RD GENERATION PARTNERSHIP PROJECT
ACL	ACCESS CONTROL LIST
ADS-B	AUTOMATIC DEPENDENT SURVEILLANCE-BROADCAST
AEHF	ADVANCED EXTREME HIGH FREQUENCY SATELLITE
AI	ARTIFICIAL INTELLIGENCE
AIS	AUTOMATIC IDENTIFICATION SYSTEM
AOCS	ATTITUDE & ORBIT DETERMINATION & CONTROL SYSTEM
API	APPLICATION PROGRAMMING INTERFACE
APT	ADVANCED PERSISTENT THREAT
ARPU	AVERAGE REVENUE PER USER
ASBM	ARCTIC SATELLITE BROADBAND MISSION
ATM	AIR TRAFFIC MANAGEMENT
B2B	BUSINESS TO BUSINESS
BGAN	BROADBAND GLOBAL AREA NETWORK
BSS	BROADCAST SATELLITE SERVICE
BTS	BASE TRANSCEIVER STATION
C2	COMMAND & CONTROL
C3S	COPERNICUS CLIMATE CHANGE SERVICE
CAGR	COMPOUND ANNUAL GROWTH RATE
CAMS	COPERNICUS ATMOSPHERE MANAGEMENT SERVICE
CAPEX	CAPITAL EXPENDITURE
CEMS	COPERNICUS EMERGENCY MANAGEMENT SERVICE
CEPOL	EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING
CHIME	COPERNICUS HYPERSPECTRAL IMAGING MISSION
CIA	CONFIDENTIALITY, INTEGRITY AND AVAILABILITY
CIMR	COPERNICUS IMAGING MICROWAVE RADIOMETER
CIR	COMMITTED INFORMATION RATE
CLMS	COPERNICUS LAND MONITORING SYSTEM
CMEMS	COPERNICUS MARINE ENVIRONMENT MONITORING SERVICE
CO2M	COPERNICUS ANTHROPOGENIC CARBON DIOXIDE MONITORING
COMSATCOM	COMMERCIAL SATELLITE COMMUNICATIONS
COTM	COMMUNICATIONS ON THE MOVE
COTS	COMMERCIAL OFF THE SHELF
COTP	COMMUNICATIONS ON THE PAUSE
CPF	CENTRAL PROCESSING FACILITY
CRISTAL	COPERNICUS POLAR ICE AND SNOW TOPOGRAPHY ALTIMETER
CSDP	COMMON SECURITY AND DEFENSE POLICY
DDOS	DISTRIBUTED DENIAL OF SERVICE
D2D	DIRECT TO DEVICE
DGA	DÉLÉGATION GÉNÉRALE DE L'ARMEMENT
DG DEFIS	DIRECTORATE GENERAL FOR DEFENCE INDUSTRY AND SPACE
DLR	DEUTSCHES ZENTRUM FÜR LUFT- UND RAUMFAHRT
DOD	DEPARTMENT OF DEFENCE
DSC	DIGITAL SELECTIVE CALLING
DTE	DIRECT-TO-EARTH
EC	EUROPEAN COMMISION
ECHO	EUROPEAN CIVIL PROTECTION AND HUMANITARIAN AID OPERATIONS
ECMWF	EUROPEAN CENTRE FOR MEDIUM-RANGE WEATHER FORECAST
EDA	EUROPEAN DEFENCE AGENCY
EDRS	EUROPEAN DATA RELAY SYSTEM
EEA	EUROPEAN ENVIRONMENT AGENCY
EEAS	EU EXTERNAL ACTION SERVICE
EFCA	EUROPEAN FISHERIES CONTROL AGENCY
EGNOS	EUROPEAN GLOBAL NAVIGATION OVERLAY SYSTEM
EHF	EXTREMELY HIGH FREQUENCY
EMEA	EUROPE, MIDDLE EAST AND AFRICA
EMPACT	EUROPEAN MULTIDISCIPLINARY PLATFORM AGAINST CRIMINAL THREAT
EMSA	EUROPEAN MARITIME SAFETY AGENCY
EO	EARTH OBSERVATION
EOL	END-OF-LIFE
EPIRB	EMERGENCY POSITION INCLUDING RADIO EACON
ERA	EUROPEAN UNION AGENCY FOR RAILWAYS
ERCC	EMERGENCY RESPONSE COORDINATION CENTRE
ESA	ELECTRONICALLY STEERED ANTENNA
ESA	EUROPEAN SPACE AGENCY

Annex 1: List of acronyms (continued)

ESS	EVOLVED STRATEGIC SATELLITE
ESSP	EUROPEAN SATELLITE SERVICES PROVIDER
EU	EUROPEAN UNION
EU NAVFOR	EU NAVAL FORCES
EU RDC	EU RAPID DEPLOYMENT CAPACITY
EU SST	EU SPACE SURVEILLANCE AND TRACKING
EU-LISA	EUROPEAN UNION AGENCY FOR THE OPERATIONAL MANAGEMENT OF LARGE-SCALE IT SYSTEMS IN THE AREA OF FREEDOM, SECURITY AND JUSTICE
EUCPM	EUROPEAN UNION CIVIL PROTECTION MECHANISM
EUROCONTROL	EUROPEAN ORGANISATION FOR THE SAFETY OF AIR NAVIGATION
EUROJUST	EUROPEAN UNION AGENCY FOR CRIMINAL JUSTICE COOPERATION
EUROPOL	EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION
EUSPA	EUROPEAN UNION AGENCY FOR THE SPACE PROGRAMME
FCC	FEDERAL COMMUNICATIONS COMMISSION
FPA	FLAT PANEL ANTENNA
FPGA	FIELD PROGRAMMABLE GATE ARRAYS
FRONTEX	EUROPEAN BORDER AND COAST GUARD AGENCY
FSS	FIXED SATELLITE SERVICE
GB	GIBABYTE
GBPS	GIGABITS PER SECOND
GDP	GROSS DOMESTIC PRODUCT
GEO	GEOSTATIONARY EARTH ORBIT
GHSL	GLOBAL HUMAN SETTLEMENT LAYER
GMDSS	GLOBAL MARITIME DISTRESS AND SAFETY SYSTEM
GMS	GALILEO MISSION SEGMENT
GNSS	GLOBAL NAVIGATION SATELLITE SYSTEM
GOVSATCOM	GOVERNMENT SATELLITE COMMUNICATIONS
GPS	GLOBAL POSITIONING SYSTEM
GSMC	GALILEO SECURITY MONITORING CENTRE
GSO	GEOSTATIONARY
GSS	GALILEO SENSOR STATION
HALE	HIGH ALTITUDE LONG ENDURANCE
HQ	HEADQUARTERS
HTS	HIGH THROUGHPUT SATELLITE
HW	HARDWARE
HEO	HIGHLY ELLIPTICAL ORBIT
IDS	INTRUSION DETECTION SYSTEM
IMSO	INTERNATIONAL MOBILE SATELLITE ORGANISATION
IOT	INTERNET OF THINGS
IRIS^2	INFRASTRUCTURE FOR RESILIENCE, INTERCONNECTION AND SECURITY BY SATELLITES
ISL	INTER SATELLITES LINK
ISO	INTERNATIONAL ORGANISATION FOR STANDARDISATION
ISS	INTERNATIONAL SPACE STATION
ISR	INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE
IT	INFORMATION TECHNOLOGY
ITU	INTERNATIONAL TELECOMMUNICATION UNION
KPH	KILOMETRES PER HOUR
KPP	KEY PERFORMANCE PARAMETERS
LEO	LOW EARTH ORBIT
LNA	LOW NOISE AMPLIFIER
LPV	LOCALISER PERFORMANCE WITH VERTICAL GUIDANCE
LRIT	LONG RANGE IDENTIFICATION AND TRACKING
LSTM	COPERNICUS LAND SURFACE TEMPERATURE MONITORING
MALE	MEDIUM ALTITUDE LONG ENDURANCE
M&C	MONITORING & CONTROL
MBPS	MEGABITS PER SECOND
MCC	MISSION CONTROL CENTRES
MEA	MIDDLE EAST AND AFRICA
MEO	MEDIUM EARTH ORBIT
MFF	MULTIANNUAL FINANCIAL FRAMEWORK
MILSATCOM	MILITARY SATELLITE COMMUNICATIONS
MLI	MULTI-LAYER INSULATORS
MOD	MINISTRY OF DEFENCE
MRCC	MARITIME RESCUE COORDINATION CENTRE
MSCHOA	MARITIME SECURITY CENTRE – HORN OF AFRICA

Annex 1: List of acronyms (continued)

MSS	MOBILE SATELLITE SERVICE
NATO	NORTH ATLANTIC TREATY ORGANISATION
NF	NETWORK FUNCTION
NFV	NETWORK FUNCTION VIRTUALISATION
NGO	NON-GOVERNMENTAL ORGANISATION
NGSO	NON-GEOSTATIONARY SATELLITE ORBIT
NLES	NAVIGATION LAND EARTH STATION
NOC	NETWORK OPERATIONS CENTER
NTN	NON-TERRESTRIAL NETWORK
OBP	ON-BOARD PROCESSING
OGS	OPTICAL GROUND STATIONS
OISL	OPTICAL INTER SATELLITES LINK
OLAF	EUROPEAN ANTI-FRAUD OFFICE
OSR	OPTICAL SOLAR REFLECTOR
PFI	PRIVATE FINANCE INITIATIVE
POP	POINT OF PRESENCE
PRS	PUBLIC REGULATED SERVICE
QKD	QUANTUM KEY DISTRIBUTION
QOS	QUALITY OF SERVICE
RDC	RAPID DEPLOYMENT CAPABILITY
RF	RADIO FREQUENCY
RIMS	RANGING & INTEGRITY MONITORING STATIONS
R&I	RESEARCH AND INNOVATION
RPAS	REMOTELY PILOTED AIRCRAFT SYSTEMS
ROSE-L	COPERNICUS L-BAND SYNTHETIC APERTURE RADAR
SAR	SYNTHETIC APERTURE RADAR
SATCEN	EUROPEAN CENTRE FOR MEDIUM-RANGE WEATHER FORECAST
SBAS	SATELLITE-BASED AUGMENTATION SYSTEM
SDN	SOFTWARE DEFINED NETWORK
SDR	SOFTWARE DEFINED RADIO
SDO	STANDARD DEVELOPING ORGANISATION
SD-WAN	SOFTWARE-DEFINED WIDE AREA NETWORK
SLA	SERVICE LEVEL AGREEMENT
SME	SMALL AND MEDIUM-SIZED ENTERPRISE
SNO	SATELLITE NETWORK OPERATORS
SOC	SPACE OPERATIONS CENTER
SOL	SAFETY OF LIFE
SRM	SATELLITE RESOURCE MANAGEMENT
SSA	SPACE SITUATIONAL AWARENESS
SSAS	SHIP SECURITY ALERT SYSTEM
SSRS	SHIP SECURITY REPORTING SYSTEM
SST	SPACE SURVEILLANCE AND TRACKING
STM	SPACE TRAFFIC MANAGEMENT
SW	SOFTWARE
SWAP	SIZE WEIGHT AND POWER
TCR	TELEMETRY, COMMAND AND RANGING
TDRS	TRACKING AND DATA RELAY SATELLITE
TETRA EQUIVALENT	TRANS-EUROPEAN TRUNK RADIO TPE TRANSPONDER
TT&C	TELEMETRY TRACKING AND COMMAND
UAV	UNMANNED AERIAL VEHICLE
UHF	ULTRA-HIGH FREQUENCY
UKMTO	U.K. MARITIME TRADE OPERATIONS
UPF	USER-PLANE FUNCTION
UN	UNITED NATIONS
UNHCR	UNITED NATIONS HIGH COMMISSIONER FOR REFUGEES
US	UNITED STATES
UT	USER TERMINAL
USAF	U.S. AIR FORCE
USSR	UNION OF SOVIET SOCIALIST REPUBLICS
VHF	VERY HIGH FREQUENCY
VHTS	VERY HIGH THROUGHPUT SATELLITES/SYSTEMS
VLEO	VERY LOW EARTH ORBIT
VM	VIRTUAL MACHINE
VMS	VESSEL MONITORING SYSTEM
VNF	VIRTUAL NETWORK FUNCTION
VSAT	VERY SMALL APERTURE TERMINAL
WASH	WATER, SANITATION AND HYGIENE
WGS	WIDEBAND GLOBAL SATCOM

Annex 2: Key terms

ACL (Access Control List)

An access control list (ACL) is a list of rules that specifies which users or systems are granted or denied access to a particular object or system resource. Access control lists are also installed in routers or switches, where they act as filters, managing which traffic can access the network. Access control lists are used for controlling permissions to a computer system or computer network. They are used to filter traffic in and out of a specific device.

APT (Advanced Persistent Threat)

An advanced persistent threat (APT) is a sophisticated, sustained cyberattack in which an intruder establishes an undetected presence in a network in order to steal sensitive data over a prolonged period of time.

Capacity demand

This refers to the satellite capacity that a customer contracts to a satellite operator/service provider for SATCOM needs. In certain cases, customers may acquire a large capacity that will not be directly used. This typically occurs when certain customers lease entire satellite payloads.

Capacity demand can be of two type: FSS (Fixed Satellite Services) and MSS (Mobile Satellite Services).

Capacity supply

This refers to the satellite capacity that satellite operators provide via their satellite assets. Such satellite capacity can be provided to end-users directly by satellite operators or via service providers.

COMSATCOM

COMSATCOM refers to SATCOM capacity and service provided on the global open market, generally with a degree of ‘on-demand’ access. These services encompass a wide range of sectors, including telecommunications, broadcasting, internet access, maritime communication, aviation, and more. COMSATCOM systems contribute to global connectivity and information dissemination.

DDOS (Distributed Denial Of Service)

DDoS stands for Distributed Denial of Service, and it's a method where cybercriminals flood a network with so much malicious traffic that it cannot operate or communicate as it normally would. This causes the site's normal traffic, also known as legitimate packets, to come to a halt.

GOVSATCOM

GOVSATCOM encompasses the communication services specifically tailored to meet the needs of governmental entities, as defined in the Working document of the European External Action Service of 15/03/2017[1]. This involves the deployment of satellite communication systems to ensure reliable, secure, and resilient communication for government operations, including defence, emergency response, public safety, and diplomatic communication.

GOVSATCOM are highly assured SATCOM offering a certain robust security level with some resilience. GOVSATCOM systems are generally considered less protected than MILSATCOM systems but offer a higher degree of protection with respect to COMSATCOM systems.

HTS (High Throughput Satellite) capacity

This term refers to capacity transmitted through the latest generation of satellite payloads. Coverage from HTS payloads includes a multiplicity of small beams, which allow some of the frequencies to be reused in different spot beams, resulting in a larger volume of capacity that is sellable to customers. Volumes can significantly vary based on the network architecture.

IDS (Intrusion Detection System)

An Intrusion Detection System (IDS) is a monitoring system that detects suspicious activities and generates alerts when they are detected. Based upon these alerts, dedicated staff can investigate the issue and take the appropriate actions to remediate the threat.

[1] Council of the European Union. 2017. Cover Note: High Level Civil Military User Needs for Governmental Satellite Communications, March 22nd.

Annex 2: Key terms (continued)

MILSATCOM

MILSATCOM is a highly protected and guaranteed SATCOM, generally provided by military systems, offering highly assured and protected satellite communication capacity both in terms of nuclear hardening, anti-jamming/dazzle capacity and highly secure Telemetry, Tracking, and Command (TT&C), supplemented by an equally robust and resilient ground segment. The security and technology are highly specific and largely sovereign in nature. Those MILSATCOM systems are primarily designed for military purposes and are under national control.

Narrowband

Narrowband refers to telecommunications applications and services that utilise a narrower set (around 100 Khz) or band of frequencies in the communication channel. These utilise the channel frequency that is considered flat or which will use a lesser number of frequency sets. Traditionally, narrowband telecommunications applications and services uses UHF, S-band and L-band, but can also use other frequency bands.

Phishing

Phishing is a common type of cyber attack that targets individuals through email, text messages, phone calls, and other forms of communication. a phishing attack aims to trick the recipient into falling for the attacker's desired action, such as revealing financial information, system login credentials, or other sensitive information.

Regular capacity

This term refers to capacity supply through satellite payloads with a largely classical design—that is, with coverage usually including at least a full country and up to a full region (wide beam). The bulk of the regular capacity is in the C- and Ku-band frequencies, with an increasing presence of Ka-band capacity. Typical regular payloads have a capacity of up to 1,260 MHz (approximately 35 TPEs (TransPonder Equivalents)).

Secure SATCOM

Secure SATCOM is defined as satellite-based, one or two-way communication capacity/service that is able to provide reliable, accessible and guaranteed satellite capacity/service for communications.

Secure SATCOM can be provided with any type of frequency band by GOVSATCOM, COMSATCOM, MILSATCOM.

Transponder

The term 'transponder' in this document refers to a normalised capacity of 36 MHz, unless otherwise specified.

Use case

In the frame of the EUSPA Secure Satcom Market and Technology report, a use case describes how the actors of the value chain would use secure SATCOM to achieve specific goals and/or tasks. The description of use cases also include the trends which could affect the use of secure SATCOM (for those actors) in the future.

User demand

User demand is similar to capacity demand (cf. page 112).

Specially, the user demand can be of two type: FSS (Fixed Satellite Services) and MSS (Mobile Satellite Services).

About the authors

European Commission

European Commission (EC) and more specifically the Directorate General for Defence Industry and Space (DG DEFIS) has overall responsibility for the implementation of the Union Space Programme and its components (Galileo, EGNOS, Copernicus, GOVSATCOM and SSA).

This includes:

- Overseeing the implementation of all activities related to the programme;
- Defining its priorities and long-term evolution;
- Managing the funds allocated to the programme;
- Ensuring a clear division of responsibilities and tasks, in particular between the EU Agency for the Space Programme and the European Space Agency;
- Ensuring proper reporting on the programme to the Member States of the EU, the European Parliament and the Council of the European Union.

DG DEFIS further contributes to shaping the EU space policy and fostering a strong, innovative and resilient EU space ecosystem. It supports the emergence of New Space in the EU, including SMEs and new entrants, fosters entrepreneurship and access to finance, and contributes to the growth of the EU space industry.

DG DEFIS promotes EU space research fostering a cost-effective, competitive and innovative space industry and research community. It ensures that space technology, services and applications meet EU policy needs, and the R&I needs of the EU Space Programme. It also ensures that the EU can access and use space with a high level of autonomy.

The EU space policy addresses some of the most pressing challenges facing the EU today, such as fighting climate change, supporting EU's priorities, whilst strongly contributing to the green and digital transitions and to the resilience of the Union.

European Union Agency for the Space Programme

EUSPA is the operational European Union Agency for the Space Programme. It adopts a user-oriented approach to promote sustainable growth and improve the security and safety of the European Union. EUSPA's mission revolves around three core principles: service provision, market growth, and security.

The EU Agency for the Space Programme:

- Provides state-of-the-art, safe and secure positioning, navigation and timing services based on Galileo and EGNOS, cost-effective satellite communications services for GOVSATCOM and soon IRIS^2, and Front Desk services of the EU Space Surveillance Tracking whilst ensuring the systems' service continuity and robustness;
- Promotes and maximises the use of data and services offered by Galileo, EGNOS, Copernicus, GOVSATCOM and soon IRIS^2 across a broad range of domains.
- Fosters the development of a vibrant European space ecosystem by providing market intelligence, and technical know-how to innovators, academia, start-ups, and SMEs. The agency leverages Horizon Europe, other EU funding, and innovative procurement mechanisms.
- Implements and monitors the security of the EU Space Programme components in space and on the ground with the aim to enhance the security of the Union and its Member States; EUSPA operates the Galileo Service Monitoring Centre.
- The Security Accreditation Board established within the Agency is the security accreditation authority for all of the Programme's components, where Member States take accreditation decisions in a strictly independent manner from the Programme.

The authors would like to convey special thanks to the contributors to this report:

- Euroconsult
- VVA
- FDC

EUSPA Mission Statement

The mission of the European Union Agency for the Space Programme (EUSPA) is defined by the EU Space Programme Regulation. EUSPA's mission is to be the user-oriented operational Agency of the EU Space Programme, contributing to sustainable growth, security and safety of the European Union.

The EU Agency for the Space Programme:

- Provides state-of-the-art, safe and secure positioning, navigation and timing services based on Galileo and EGNOS, cost-effective satellite communications services for GOVSATCOM and soon IRIS^2, and Front Desk services of the EU Space Surveillance Tracking whilst ensuring the systems' service continuity and robustness;
- Promotes and maximises the use of data and services offered by Galileo, EGNOS, Copernicus, GOVSATCOM and soon IRIS^2 across a broad range of domains.
- Fosters the development of a vibrant European space ecosystem by providing market intelligence, and technical know-how to innovators, academia, start-ups, and SMEs. The agency leverages Horizon Europe, other EU funding, and innovative procurement mechanisms.
- Implements and monitors the security of the EU Space Programme components in space and on the ground with the aim to enhance the security of the Union and its Member States; EUSPA operates the Galileo Service Monitoring Centre.
- The Security Accreditation Board established within the Agency is the security accreditation authority for all of the Programme's components, where Member States take accreditation decisions in a strictly independent manner from the Programme.

EUSPA is "Linking Space to user needs".

market@euspa.europa.eu
www.euspa.europa.eu

X @EU4Space
f EU4Space
in EUSPA
@space4eu
EUSPA
@EUSPA@social.network.europa.eu

#EUSpace

EUSPA
European Union Agency for the Space Programme

ISBN: 978-92-9206-076-3
TS-03-23-438-EN-N