7SHIELD

D8.4 Market analysis report v1

Work Package:	WP8 - Dissemination, Impact Creation and Exploitation Plan		
Lead partner:	CS GROUP (CS)		
Author(s):	Xavier Pothrat (CS)		
Due date:	M6		
Version number:	1.0	**Status:**	Final
Dissemination level:	Public		

Project Number:	883284	**Project Acronym:**	7SHIELD
Project Title:	Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats		
Start date:	September 1st, 2020		
Duration:	24 months		
Call identifier:	H2020-SU-INFRA-2019		
Topic:	SU-INFRA01-2018-2019-2020 Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe		
Instrument:	IA		

Horizon 2020
European Union Funding
for Research & Innovation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883284

Revision History

Revision	Date	Who	Description
0.1	02/10/2020	CS	First release of the draft version with preliminary Desk Study
0.2	15/01/2021	CS	Addition of a table identifying potential customers on each country of the consortium partners and integration of feedbacks from partners
0.3	16/02/2021	CS	Integration of feedbacks from partners Modification of the EO ground segment scheme
0.4	19/02/2021	CS, INOV, EETT	Integration of feedbacks from the two reviewers (INOV & EETT): ▪ Addition of more detailed descriptions to the revision history ▪ Completion of the table of acronyms ▪ Addition of Altice in the Portuguese domestic market ▪ Acronyms and terms consistency (U.S. VS US) ▪ Modification of Table 3.1 ▪ Few wording, typo and formatting changes ▪ Addition of "Amazon Web Services" and a endnote to the executive summary ▪ Modification of titles
0.5	25/02/2021	CS, ENG, CERTH	Refinements and minor changes
1.0	26/02/2021	ENG	Final version

Quality Control

Role	Date	Who	Approved/Comment
Internal review	18/02/2021	INOV	Accepted with minor changes
Internal review	19/02/2021	EETT	Accepted with minor changes
Internal review	25/02/2021	CERTH	Accepted with minor changes

Disclaimer

This document has been produced in the context of the 7SHIELD Project. The 7SHIELD project is part of the European Community's Horizon 2020 Program for research and development and is as such funded by the European Commission. All information in this document is provided 'as is' and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. For the avoidance of all doubts, the European Commission has no liability with respect to this document, which is merely representing the authors' view.

Executive Summary

The volumes of data generated by Earth Observation satellites or transferred by telecommunication satellites have experienced a sustained growth over the past decade with the deployment of open data Earth Observation programmes all over the globe and the advent of telecommunications and the internet in all aspects of our lives. For some years now, the arrival of new players in the Space ecosystem supported by private funding and willing to deploy global constellations of Earth Observation satellites or telecommunication constellations for IoT or Internet are forecasting an even stronger growth in data volumes in the coming years.

The development of the Ground Segment as a Service model promising to simplify and reduce the cost to access Space for new comers, attract major IT actors onto the Space ground segment ecosystem. For example, Amazon Web Services (AWS)[1] is deploying its own Ground segment throughout the globe for the benefit of all its customers.

While the Ground segment infrastructures have experienced a sustainable growth for the past decade, they are expected to continue growing in the years to come.

In parallel, the democratisation of information technologies and connected devices in all companies, institutions and processes has shifted the confrontation between advanced countries from battlefields to information systems. Cybernetic warfare is on the rise and aims to destabilise the economy and the functioning of a country rather than directly attacking its army. Organised crime is also investing in the cyber field with very high potential gains for a minimum of risk. The number of cyberattacks toward companies and the average cost induced by these attacks have boomed in a few years.

The complexity of attacks is increasing with the evolution of the protection systems. And new threats mixing cyber and physical attacks emerge.

In this context, Space ground segments increasingly appear as potential "new targets" of "new threats", especially the hybrid ones (e.g. cyber-physical). Indeed, a physical/cyber-attack toward Space ground segment installations or communication networks would cause debilitating impact on public safety and security of European citizens and could affect also other European critical infrastructures through cascading effects.

There is a strong need for a holistic framework covering both cyber and physical protection with cutting-edges technologies for prevention, detection, response & mitigation.

To date, no commercial offer proposes a holistic protection of Space ground segment by covering both physical and cyber threats.

Since Space ground segments are identified as critical infrastructures, their protection market is strongly driven by national and regional regulations. Space agencies are very

[1] https://docs.aws.amazon.com/whitepapers/latest/aws-overview/satellite.html

sensitive to the protection of their critical infrastructures and assets and are expected to be the main customers of the 7SHIELD framework.

Since they have to comply with national regulations and are very sensitive to their service continuity, the private grounds segment operators are also expected to represent a significant part of the future customer base.

Table of Contents

List of figures

List of Tables

Definitions and acronyms

AI	Artificial Intelligence
AWS	Amazon Web Services
CA	Consortium Agreement
CCTV	Closed-Circuit TeleVision
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
COTS	Commercial-off-the-shelf
C/P	Cyber/Physical
C2	Command & Control
DoA	Description of Action
DS	Decision Support
EC	European Commission
EO	Earth Observation
EU	European Union
FCC	Federal Communications Commission
GA	Grant Agreement
Gbps	GigaBytes per second
GEO	Geosynchronous Equatorial Orbit
GNSS	Global Navigation Satellite System
GPU	Graphics Processing Unit
GS	Ground Segment
GSaaS	Ground Segment as a Service
HTS	High-Throughput Satellite
IFE	In-Flight Entretainment
InfoSec	Information Security
IOT	Internet Of Things
IP	Internet Protocol
LEO	Low Earth Orbit
LIDAR	LIght Detection And Ranging
LWIR	Long Wavelength Infrared
MEO	Middle Earth Orbit
MMAS	Multi-Modal Automated Surveillance
M2M	Machin to Machin
NetOps	Network Operations
NMS	Network Management System
OSINT	Open Source INTelligence
OT	Operational Technology
PC	Project Coordinator
PDGS	Payload Data Ground Segment
PSIM	Physical Security Information Management
PTZ	Pan Tilt Zoom

QoS	Quality of Service
R&D	Research & Development
SAAS	Software As A Service
SATCOM	Satellite Communication
SC	Scientific Coordinator
SIEM	Security Information & Event Management
SIPS	Sensitive Industrial Plants and Sites
SOC	Security Operation Center
SSO	Single Sign-On
TCP	Transmission Control Protocol
TDSS	Tactical Decision Support System
TI	Threat Intelligence
TIP	Threat Intelligence Platform
TM	Technical Manager
TRL	Technology Readiness Level
TT&C	Telemetry, Tracking & Control
UAV	Unmanned Aerial Vehicle
UI	User Interface
UTD	Universal Tactical Display
VAS	Value Added Service
VNIR	Visible Near-Infrared
WP	Work Package

1. Introduction

The Copernicus programme has created a new ecosystem in Europe around the massive amounts of data produced by its satellites and received daily by its ground segments.

In the European security landscape, Space ground segments increasingly appear as potential "new targets" of "new threats", especially the hybrid ones (e.g. cyber-physical). Indeed, a physical/cyber-attack toward Space ground segment installations or communication networks would cause debilitating impact on public safety and security of European citizens and could affect also other European critical infrastructures through cascading effects.

On the one hand, a physical attack on a space ground segment could make the distribution of satellite data problematic and, on the other hand, a cyber-attack in its data storage, access and exchange could affect not only the confidentiality and integrity of space data, but also their FAIR standards: findability, accessibility, interoperability and reusability.

This market analysis aims to give a macroeconomic view of the Security Market for the Space Ground Segment and its competitive landscape, to evaluate its size (current and future) and identify its trends.

This analysis aims also to give insights on 7SHIELD key success factors and best strategy to access the market.

This market analysis will particularly focus on the European Earth Observation ground segment since it concentrates most of the challenges faced by the Space ground segment facilities and assets regarding Cyber and Physical threats.

The study is divided in two main axes:

- A documentary research, to give a macroeconomic view of the Security Market for Space Ground Segment
- Qualitative interviews with stakeholders and potential customers, to give insights on the challenges at stake and the best market access strategy for the 7SHIELD framework.

Please note that the description of 7SHIELD modules will be completed and harmonised in the final version of the Market analysis at M18. Indeed, some descriptions of 7SHIELD modules are partial due to the fact that we are still at an early stage of the project. Hence, the scope as well as the market proposition of some key results is not completely defined yet.

2. The Space Ground Segment

2.1. Presentation

The Space Ground Segment (GS) consists of an ensemble of facilities responsible for the acquisition, processing, distribution and archiving of the satellite data and of their derived products[2]. These facilities and their operators vary with the nature of the data collected by the satellites.

There are three main types of Space Ground Segments: **Earth Observation (EO) GS, Satellite Communication (SATCOM) GS and Navigation (GNSS) GS.**

2.1.1. Earth Observation value chain and ground segment

Earth Observation refers to the use of remote sensing technologies to monitor land, marine (rivers, lakes) and atmosphere. Satellite-based EO relies on the use of satellite mounted payloads to gather imaging data about the Earth's characteristics. The images are then processed and analysed in order to extract different types of information that can serve a very wide range of applications and industries.[3]

The Earth Observation industry is commonly divided into two segments: The **upstream segment** and the **downstream segment**.

The **upstream segment** refers to the space industry in charge of developing and manufacturing the infrastructures. This includes the space infrastructure (the satellites) and the ground segment for satellite operations (mission control and management of the payloads).The upstream also includes the launch operations.

The **downstream segment** is part of the EO value chain, and includes the companies and institutional actors whose activities revolve around the processing of EO data and the creation of Value Added Services (VAS) based on this data.

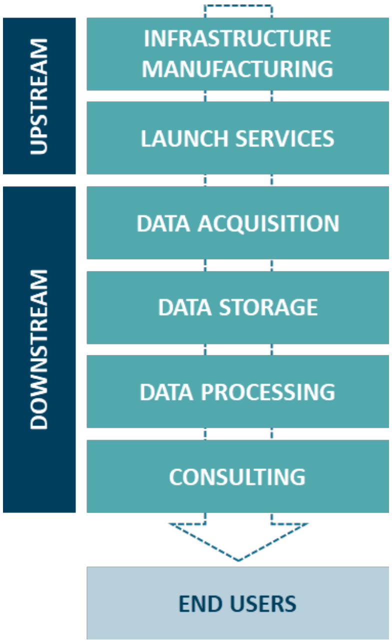


Figure 2-1 - EO value chain

The EO ground segment covers most of the EO downstream segment and is composed of various stakeholders that take part in the EO value-chain from raw data to value-added insights. The main stakeholders are :

- Space agencies
- Private satellite and ground station operators
- Payload Data Ground Segment (PDGS) operators

[2] https://earth.esa.int/web/guest/missions/esa-operational-eo-missions/ers/ground-segment
[3] https://www.copernicus.eu/sites/default/files/2019-02/PwC_Copernicus_Market_Report_2019_PDF_version.pdf

- EO platform operators

The main assets and facilities of the EO ground segments are:

- The data produced by EO satellites
- The ground stations including antennas, their control systems and the connection to their distribution network
- The mission control & operation centres that oversee satellite operations and give inputs for data rectification
- The PDGS, composed of archives and processing infrastructures
- The EO platforms composed of data storage and processing infrastructures

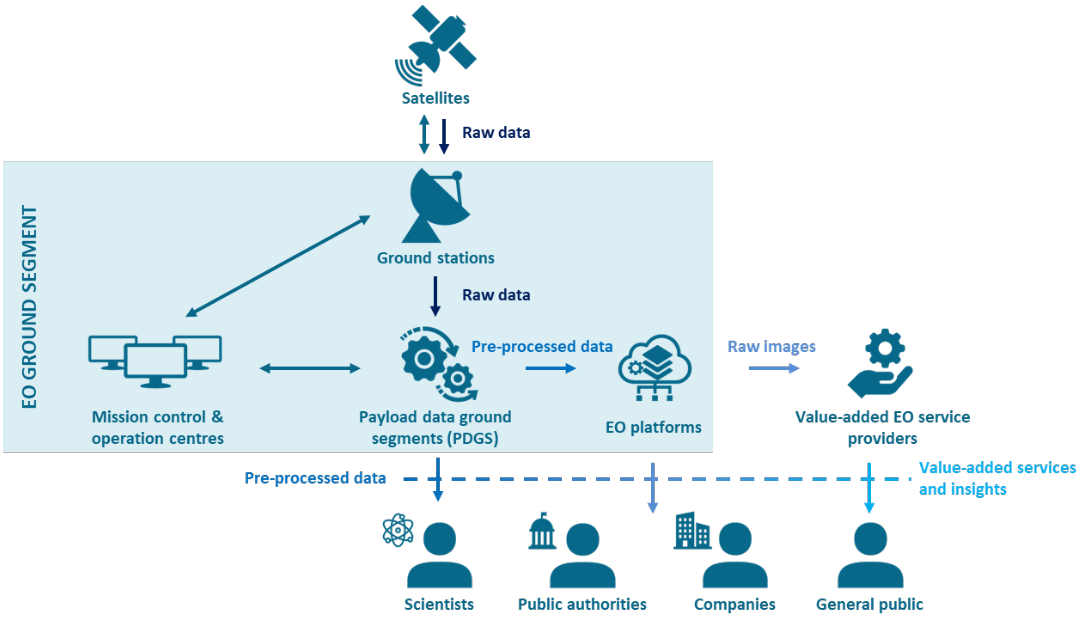


Figure 2-2 - EO Ground Segment

2.1.2. Satellite communication value chain and ground segment

Satellite communication refers to the use of satellites to relay and amplify radio telecommunications 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, radio, internet, and military applications.

Like the EO industry, the satellite communication industry is divided into two segments: The upstream segment and the downstream segment.

The upstream segment is quite similar to EO's one.

The downstream segment is part of the SATCOM value chain and includes all stakeholders responsible of communication

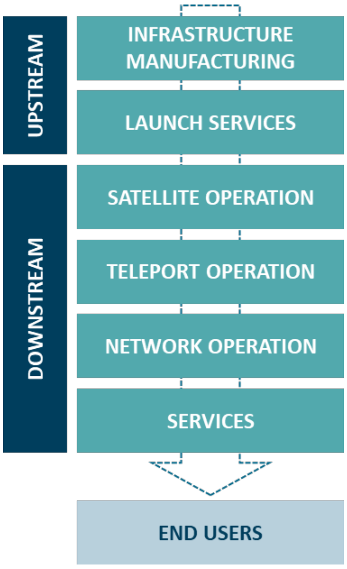


Figure 2-3 - SATCOM value chain

signal transmission, from content creators to end-users or from end-users to other end-users.

The SATCOM ground segment is part of the SATCOM downstream segment and is composed of various stakeholders operating signal transmission infrastructures.

In the SATCOM industry, several terms may be used to designate the antennas and their stations that send and receive signals from satellites. For clarification matters in this document we decided to use the following terms:

A ground station is composed of antennas that send and receive Telemetry, Tracking & Control (TT&C) commands to operate and monitor the satellites. It can also receive satellite payload data.

A Teleport is not used to operate satellites but only to send and receive payload data.

The main stakeholders of the SATCOM GS are:

- Satellite and ground station operators
- Teleport operators

The main assets and facilities of the SATCOM ground segments are:

- Teleports & ground stations
- The mission control & operation centres that oversee satellite operations and give inputs for data rectification
- The network hubs that connect teleports & ground stations to ground-based communication networks

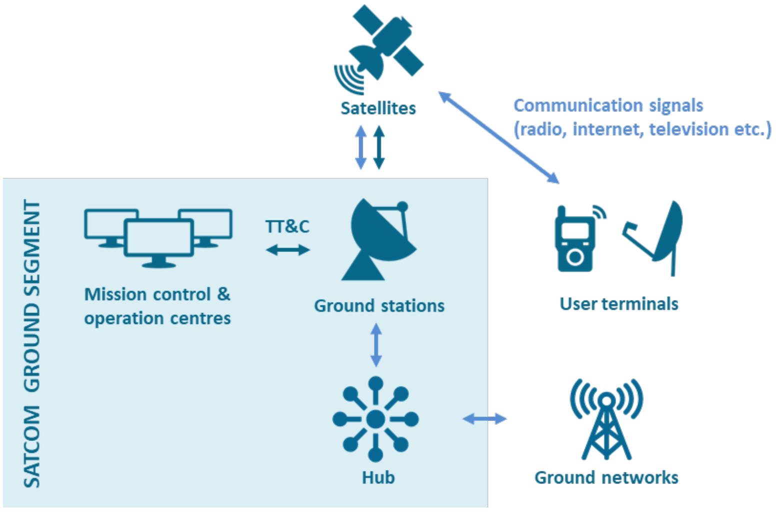


Figure 2-4 - SATCOM Ground Segment

2.1.3. Navigation satellites value chain and ground segment

Global Navigation Satellite System (GNSS) refers to a constellation of satellites providing signals from space that transmit positioning and timing data to GNSS receivers. The receivers then use this data to determine location.

The Global Navigation Satellite system value chain is composed of a downstream and upstream component. The upstream side is comprised of those entities that build the space infrastructure (satellites, ground segment) and provide a signal to users. The downstream component, on the other hand, supplies the products and services that use GNSS-based positioning and navigation as a significant enabler. These products and services encompass the entire value chain of GNSS-specific components, GNSS receivers, GNSS-enabled systems, GNSS-enabled software and added-value services.[4]

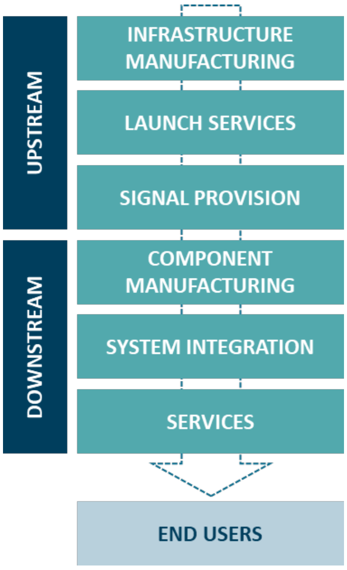


Figure 2-5 - GNSS value chain

Unlike other satellite applications, GNSS ground segment is consider as part of the GNSS upstream segment, since it contributes to build and deliver the signal used by GNSS receivers to compute their positioning and timing.

The main stakeholders of the GNSS ground segment are:

- GNSS agencies

The main assets and facilities of the GNSS ground segments are:

- The ground stations
- The mission control & operation centres
- The central computing centres, responsible for computing differential correction to GNSS signals errors and broadcasting these calculations to end-users' terminals using geostationary satellites that serve as an augmentation, or overlay, to the original GNSS message

[4] https://www.gsa.europa.eu/gnss-applications/gnss-industry-and-value-chain

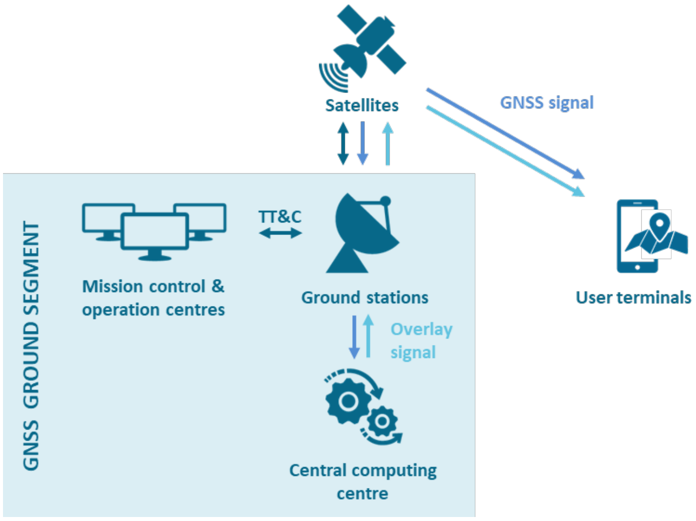


Figure 2-6 - GNSS Ground Segment

2.2. Ground segment trends and market drivers

2.2.1. A Sustained growth in Earth Observation data volumes

The volume of Earth Observation data produced by large-scale open data programmes (Copernicus, Landsat, Gaofen etc.) and stored on EO platforms is booming for a decade and is expected to continue growing for years to come. This growth will accelerate with the arrival of many private NewSpace players such as Planet, IceEye, Capella Space, Satellogic, SpaceWill or Zhuhai Orbita Aerospace, all targeting large-scale small EO satellites constellation.

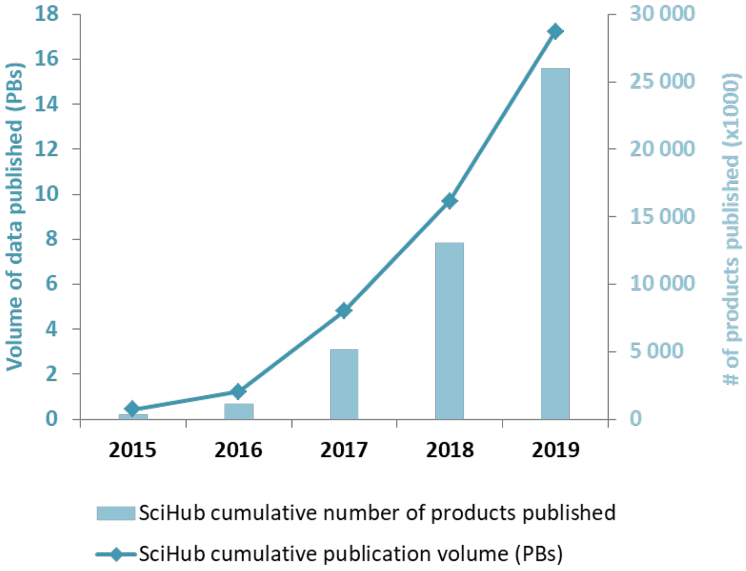


Figure 2-7 - Copernicus SciHub cumullative data publication from 2015 to 2019 – Copernicus Sentinel Data Access Annual reports[5]

[5] https://scihub.copernicus.eu/reportsandstats/

The sustained growth in the volume of Earth Observation data produced by public and private constellations generates a sustained demand for EO ground segment facilities such as ground stations, data storage, processing and distribution capacities.

2.2.2. An increasing demand for satellite-based communication services

The increasing demand for satellite-based communication services like inflight connectivity, maritime broadband services along with growth of telecommunication sector is anticipated to generate demand for new communication satellite launches.

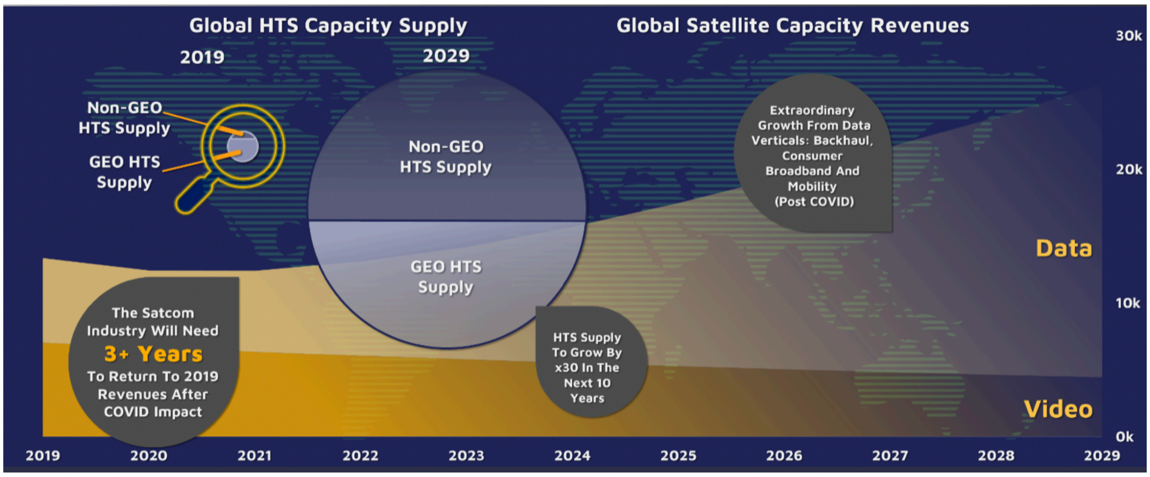


Figure 2-8 – Global satellite capacity supply & demand – NSR 2020 (17th edition)

Commercial satellite operators are investing heavily into construction and deployment of Geosynchronous Equatorial Orbit (GEO) high throughput satellites. To increase the consumer broadband benefits, the GEO satellite capacities are planned to be increased to 1000 Gbps in the years to come from 260 Gbps in 2019. This can be achieved by frequency re-use and spot beam technology. Further, several companies have plans to launch new high throughput satellites in LEO and MEO to provide additional high-speed broadband services at low latency levels.

The increasing demand for high throughput satellites to address new services (IFE, M2M / IoT etc.) and new geographical areas is sustaining the demand for SATCOM ground segment facilities such as ground stations.

2.2.3. An increasing number of ground segment infrastructures

2018 has entailed a point of inflexion in the ground segment industry with the preparation of the OneWeb ground network, the launch of additional High-Throughput Satellites and the need of further ground stations to provide connectivity with EO constellations.

After some years of market consolidation in the teleport industry for SATCOM applications, the number of ground sites is expected to grow from 2019 driven by new installations in emerging regions. In the EO ground segment, the number of ground stations is steadily growing to serve the increasing demand on EO data and value-added services.

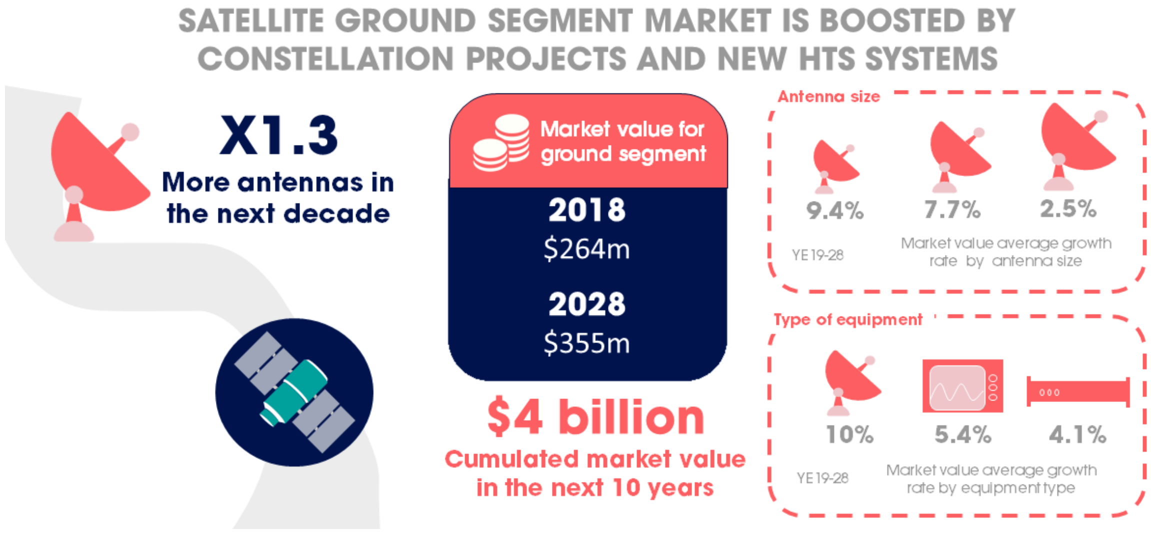


Figure 2-9 - Ground Segment market propsect - Euroconsult 2019

Each satellite mission, being in constellation or not, might have different communication needs (e.g. frequency bands, etc.) and so, the rationale for the use of ground segment can vary. The amount of data to download, the regional distribution of end-users, connectivity with ground networks, meteorological constraints, etc. might also impact in the definition and use of the ground segment.

The space sector is pushing for substantially more productive satellite infrastructure and ground segment at a lower cost. This trend is expected to intensify over the next decade, coupled with an increasing push for standardisation in satellite manufacturing and ground segment equipment. New technological developments (notably going to SaaS) seek a more productive infrastructure with the aim of making lower cost end-to-end services.[6]

The advent of new satellite systems usually calls for new terminals. Developing lower-cost ground terminals to serve mobility applications and connectivity with constellations is an important criterion for operators to overcome the "barrier of user terminals" and to increase the adaptability of data-centric applications.[7]

According to Euroconsult's 2019 report, the commercial satellite ground segment market, including SATCOM applications, EO applications and user terminals for user applications, is going through significant expansion in terms of both capabilities and demand. It is expected to grow from $264 million in 2018 to nearly $360 million in 2028. The aggregated market value in the next decade is expected to achieve $4 billion.

2.2.4. An increasing need for secure spectrum usage

As a result of the increasing need for secure spectrum usage, National Authorities charged with spectrum monitoring heavily invest in more sophisticated and efficient Spectrum monitoring tools. The investment is driven by the need to secure spectrum for reliable

[6] https://www.euroconsult-ec.com/24_May_2019
[7] https://www.msua.org/post/2019/09/30/ground-segment-at-a-turning-point

communications in an environment where more and more spectrum is used by operators, the co-sharing of spectrum is increasing with more and more complex techniques, the protection of the provided service to the end user is of high priority as well as the fast response, the detection and the termination of an interference coming from earth stations (fixed or mobile) or satellites. High traffic and Internet of Things (IoT) are expected to grow and deploy everywhere and need for monitoring is increasing.

2.2.5. The development of a new business model: The Ground Segment as a Service

The emergence of NewSpace[8] has led to a surge in new satellite operators entering the market. In order to offer the best service to their customers, these operators need to communicate with their satellites, relying on an effective ground segment. The latter requires specific expertise and infrastructure, as well as significant resources – both human and financial. Yet, these new satellite operators do not always have the experience, the capital or the willingness to invest in their own ground segment – risking a financial overkill for their project. Satellite operators are thus looking for a ground segment sold "as a service", to flexibly and efficiently communicate with their satellite without having to invest upfront in a wholly dedicated ground segment or having to deal with licensing issues. However, until recently, there was no specific offer on the market adapted to answer these new needs. This mismatch between supply and demand created a gap in the ground segment market, which gave rise to a new type of offer: Ground Segment as a Service (GSaaS).9

The GSaaS supply landscape is composed of new start-ups (e.g. Leaf Space, Infostellar, RBC Signals, Atlas Space Operations, etc.), IT-born companies (e.g. AWS) and GS incumbents (e.g. SSC, KSAT). Building upon their experience in satellite operation and leveraging their global network of ground stations, GS providers incumbents designed solutions specifically adapted to small satellite operators and large constellations with SSC Infinity and KSATlite for example. To do so, incumbents standardised their ground station equipment and configurations, and developed web-based and API customer interfaces, notably to enable pass scheduling. The main GSaaS providers are mapped in the diagram provided below:

[8] https://www.airbus.com/public-affairs/brussels/our-topics/space/new-space.html

[9] https://www.pwc.fr/fr/assets/files/pdf/2020/11/en-france-pwc-space-practice-research-paper-gsaas.pdf

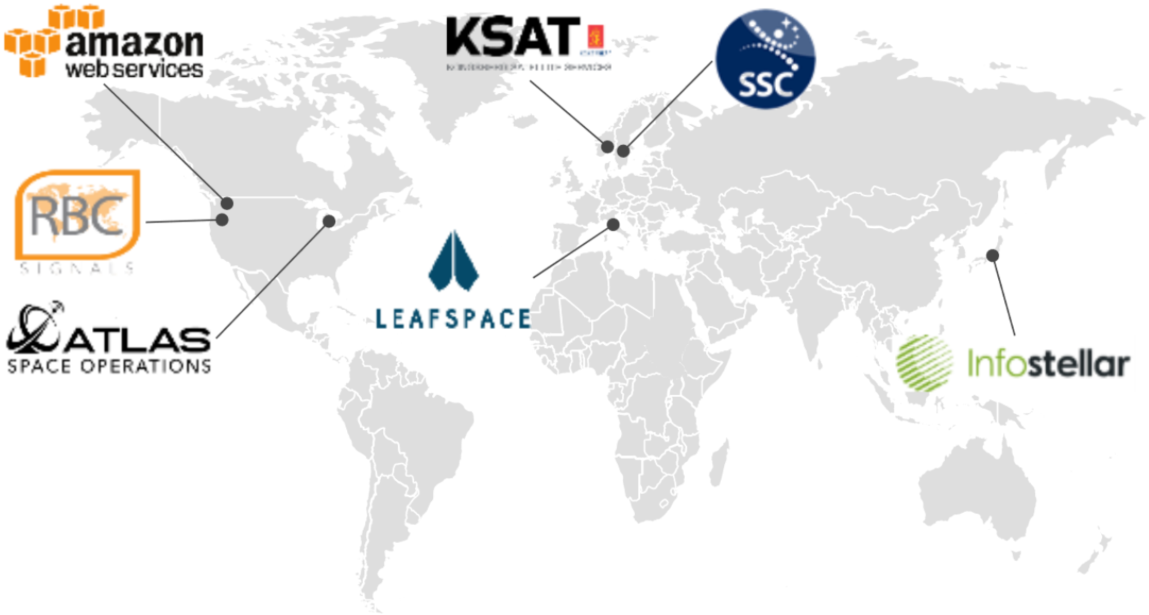


Figure 2-10 - GSaaS supply landscape

The development of a new GSaaS model attracts new players from the IT industry such as AWS. These new entrants to the Space Ground Segment ecosystem contribute to the development of ground infrastructure and its economic growth.

2.2.6. Other market drivers

The capacity for satellite operators to invest in dedicated ground stations will be heavily influenced by the evolution of national regulatory schemes. The latter today can make it hard for satellite operators to predict the date of completion and activation of their ground stations. Furthermore, these delays vary from one country to another, as the licensing frameworks (i.e. procedures, fees, etc.) are not harmonized on a global scale. Such harmonization could make it easier and faster for satellite operators to obtain licenses worldwide, and thus could facilitate the ground station building. Industry experts consider that the Federal Communications Commission (FCC) already attempts to streamline and provide various paths for licensing, which is expected to alleviate various pain points experienced by satellite operators.

However, if the regulatory framework does not evolve to adapt to the increasing satellite activity (i.e. forecasts show increasing satellites operated in the future), ground segment licensing could become an even bigger hurdle for satellite operators that wish to establish their own ground stations.

Finally, geopolitical conflicts could also prevent some countries to install ground stations in non-allied countries.

In such situations, the development of Ground Stations could be more limited than expected.

3. Security systems against cyber & physical threats for Space Ground Segment – The 7SHIELD market

3.1. Presentation

Currently, most Ground Segments of space systems incorporate the concept of cyber and physical threat security of their assets either within their Product Quality Assurance processes or within the Safety departments, or in some cases (such as in the case of the German Aerospace Agency) within both. The GS administration is usually responsible for the definition and controlling of product assurance activities and for acceptance of space equipment managed.

The responsibility of the implementation of security protocols does not lie within the GS administration though, but is outsourced to specialised 3rd party contractors.

Moreover, despite the fact that physical and logical security depend on each other, most critical infrastructures such as Ground Segment facilities treat them as separate systems, from both a device management and governance perspective.

Until recently, this was justified because the technology to integrate physical and logical security was not yet available. Regarding security, most organisations have at least three control & operation centres. The first two are primarily concerned with IP theft, malware, viruses, and so on: NetOps handles network security, while InfoSec manages data at rest and data in transit security. The third is physical security, which includes surveillance and access control. In most organisations, the guard at the gates is a separate operations centre.[10]

3.2. Figures, trends and market drivers

3.2.1. The Physical technologies are mature

Physical and logical security technologies have matured to the point that they can now be integrated. The convergence of the IP network and the migration of legacy sensors and appliances to TCP/IP are helping drive this transformation. Cameras are now IP-based; card readers use the IP network instead of a proprietary network; and access lists, policies, and procedures are stored and generated by computers.

3.2.2. The interfaces between Physical and Digital assets are increasing

Cybersecurity, meanwhile, depends greatly on physical security. Attackers who can gain physical access to a computer can almost always take advantage of that access to further their efforts. Merely getting access to a physical terminal where a memory device can be

[10] https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/pl-security.pdf

plugged in is usually sufficient. Any device present that is connected to the network must be physically protected to ensure that it cannot be turned into a tool to be used in an attack.

3.2.3. The Cyber-attacks are increasing in number and in sophistication

For a decade, cyber-attacks are increasing in number and in sophistication all around the world. The costs induced by these attacks have jumped by +12% in 2019 and by +72% in 5 years according to Accenture's ninth annual cost of cybercrime study[11].

At the same time, risks of physical attacks by terrorists or activists remain high and very hard to predict.

3.2.4. The security budget of companies are increasing

These phenomena are leading companies and institutions to increase their security budgets, particularly for critical infrastructure protection. The major factors driving the market include the need to secure Operational Technology (OT) networks due to the increasing sophistication of cyberattacks.[12]

Critical infrastructures are radically transforming on an unprecedented scale, boosted by a rapid adoption of 'smart' operational technologies. Cybersecurity is a growing part of that evolution.

According to Mordor Intelligence, the global critical infrastructure protection market was valued at USD 71.83 billion in 2019 and is projected to be worth USD 108.57 billion by 2025, registering a CAGR of 7.08% during the period from 2020 to 2025.[13]

Three primary drivers are pushing better security in critical infrastructures:

- Digital transformation and increased connectivity of operational technologies;
- Democratisation of cyber-attacks targeting critical infrastructure;
- A maturing market for industrial and IoT security.

According to Scott Borg, director of the US Cyber Consequences Unit, a non-profit research institute that advises the US government and critical infrastructure industries on the economic and strategic risks from cyberattacks "As long as organisations treat their physical and cyber domains as separate, there is little hope of securing either one."[14]

3.2.5. The security supervision systems market is fragmented

The market of security supervision systems is divided in three main segments:

- The **Physical Security Information Management (PSIM)** systems that centralise data streams from physical sensors and equipment (CCTV, face recognition, plate

[11] https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=40
[12] https://www.marketsandmarkets.com/Market-Reports/critical-infrastructure-protection-cip-market-988.html
[13] https://www.mordorintelligence.com/industry-reports/global-critical-infrastructure-protection-market-industry
[14] https://fedtechmagazine.com/article/2009/02/dont-put-walls-between-your-security-people

recognition, badges, guards, barriers etc.) and monitor equipment, people behaviour and building access.

According to Mordor Intelligence[15], the physical security information management market was valued at USD 588.5 million in 2020 and is expected to reach USD 1350.3 million by 2026 at a CAGR of 14.7% over the forecast period.

One of the major drivers of the market's growth includes increasing government initiatives for investment in safe city infrastructure in developing countries.

The physical security information management market is fragmented, owing to the presence of multiple players in the market. The solution provider is dependent on other value chain enablers, such as cloud service providers, which impacts their revenue aspects. Vendors with multiple functions and business units are better placed in the market, as they have an extended reach in the supply chain, which assists them in providing their services. Some key players in the market include Johnson Controls International PLC, CNL Software Ltd, Genetec Inc, Qognify Inc., Verint Systems Inc. and Vidsys Inc.

- The **Security Information and Event Management (SIEM)** systems that centralise data streams from digital sensors and equipment (firewall, anti-malware, logbook etc.) and monitor applications, user behaviour and data access.

According to MarketandMarket[16], Information and Event Management (SIEM) market size is expected to grow from USD 4.2 billion in 2020 to USD 5.5 billion by 2025, at a CAGR of 5.5% during the forecast period.

The major vendors covered in the Security Information and Event Management Market include SolarWinds (US), IBM (US), Micro Focus (UK), Rapid7 (US), RSA (US), McAfee (US), Splunk (US), ManageEngine (US), LogRhythm (US), Sumo Logic (US), Exabeam (US), Securonix (US), Alert Logic (US), Graylog (US), BlackStratus (US), AlienVault (US), Forinet (US), LogPoint (Denmark), Gurucul (US), and Cygilant (US).

- The **Network Management Systems (NMS)** that monitor, maintain and optimise network activities. They are generally used to monitor IT networks but some systems can monitor networks or physical equipment.

According to MarketsAndMarkets[17], the global Network Management System Market size is expected to grow from USD 7.0 billion in 2019 to USD 11.0 billion by 2024, at a Compound Annual Growth Rate (CAGR) of 9.5% during the forecast period.

The increasing need for in-depth visibility into network security and Quality of Service (QoS) and growing network infrastructure are major factors expected to drive the growth of the NMS market. Exponential growth in the global Internet Protocol (IP) traffic

[15] https://www.mordorintelligence.com/industry-reports/physical-security-information-management-market
[16] https://www.marketsandmarkets.com/Market-Reports/security-information-event-management-market-183343191.html
[17] https://www.marketsandmarkets.com/Market-Reports/network-management-market-1041.html

and cloud traffic, and prominence of the Internet of Things (IoT) are expected to offer vast market opportunities for NMS vendors in the next five years.

The major players in the Network Management System Market are SolarWinds (US), Cisco (US), IBM (US), Huawei (China), Juniper Networks (US), Nokia (Finland), SolarWinds(US), CA Technologies (Broadcom) (US), NETSCOUT (US), Riverbed Technology (US), Micro Focus (UK), Ipswitch (Progress) (US), BMC Software (US), ExtraHop Networks (US), Colasoft (China), Flowmon Networks (Czech Republic), ManageEngine (US), LiveAction (US), Paessler AG (Germany), SevOne (US), Cubro Network Visibility (Austria), Kentik (US), VIAVI Solutions (US), Accedian (Canada), Kaseya (US), HelpSystems (US), Extreme Networks (US), AppNeta (US), Ericsson (Sweden), eG Innovations (US), and Opmantek (Australia).

3.3. Conclusion

The sustained growth in the volume of data passing through satellite ground segments, the criticality of these data for a number of services and industries, the growing number of cyber-attacks around the world, the increasing costs they induce for the targeted companies and institutions, the increasing complexity of the attacks, the increasing interfaces between physical and digital assets, the maturity of the TCP/IP technologies etc. All that calls for the convergence of cybersecurity and physical security. This convergence is a topic discussed for years by security leaders but the solutions proposed are still at their infancy.

There is a thus a real need for the development of a holistic framework for Ground Segment protection against Cyber and Physical threats, that integrate high TRL technologies.

4. 7SHIELD: A holistic framework for Ground Segment protection against Cyber and Physical threats

7SHIELD is a holistic framework dedicated to the protection of Space Ground Segment infrastructures & assets against hybrid threats (cyber and physical threats). It integrates state-of-the-art methodologies, technologies and analytic capabilities to provide outstanding performances throughout the crisis management stages, namely preparedness, detection, response and mitigation.

7SHIELD framework is composed of two types of systems:

- **7SHIELD Core** systems, that together form the core functionalities of the framework;
- **7SHIELD Module** systems. Each 7SHIELD module can be seamlessly added to 7SHIELD Core to extend its functionalities and capabilities depending on the needs of the end-users.

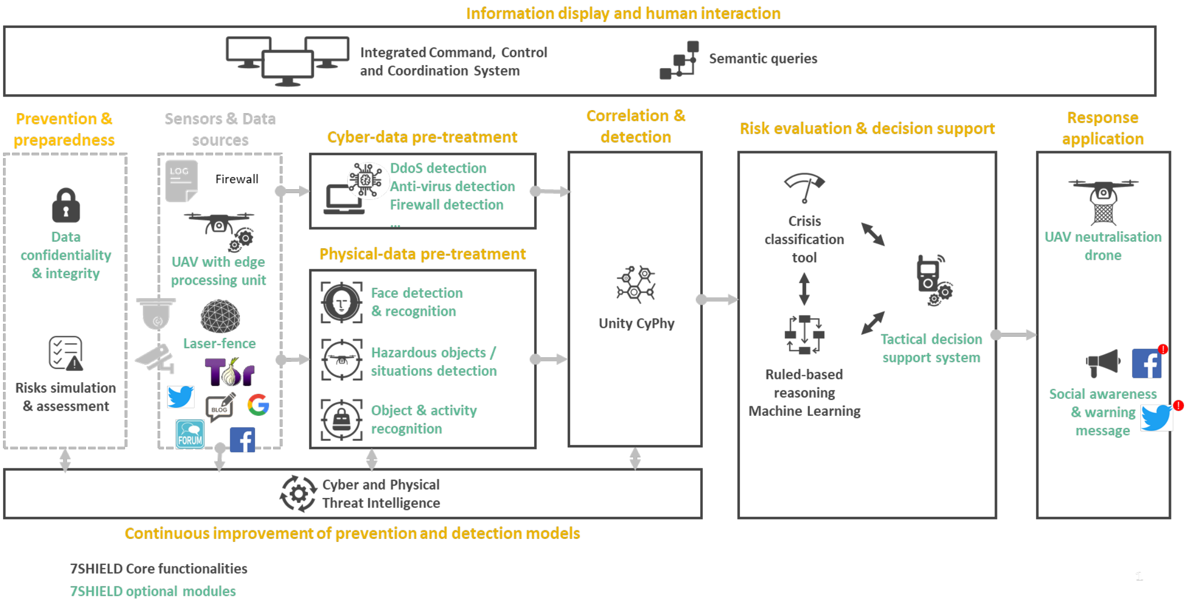

Information display and human interaction
Integrated Command, Control and Coordination System
Semantic queries
Prevention & preparedness
Data confidentiality & integrity
Risks simulation & assessment
Sensors & Data sources
LOG
Firewall
UAV with edge processing unit
Laser-fence
FORUM
BLOG
Cyber-data pre-treatment
DdoS detection
Anti-virus detection
Firewall detection
...
Physical-data pre-treatment
Face detection & recognition
Hazardous objects / situations detection
Object & activity recognition
Correlation & detection
Unity CyPhy
Risk evaluation & decision support
Crisis classification tool
Ruled-based reasoning
Machine Learning
Tactical decision support system
Response application
UAV neutralisation drone
Social awareness & warning message
Cyber and Physical Threat Intelligence
Continuous improvement of prevention and detection models
7SHIELD Core functionalities
7SHIELD optional modules

Figure 4-1 - 7SHIELD framework

4.1. 7SHIELD Core

7SHIELD Core merges both cyber security systems and physical security systems. Its holistic layer enables to interface Security Information and Event Management (SIEM), Network Management System (NMS) along with Physical Security Information Management (PSIM) by applying proven cyber protection methodologies and technologies to physical protection. It thus provides a centralised system of systems with enhanced analytic, prediction and decision-support capabilities, covering complex cyber and physical threats.

4.1.1. Value proposition

7SHIELD Core enables:

- **Strong preparedness of infrastructures and assets toward physical and cyber-attacks** thanks to its cascading effect simulation & resilience assessment tool;
- **Early detection of complex cyber and physical threats from various and heterogeneous data sources before any visible damage** thanks to its cross analytic capabilities based on a correlation framework, a knowledge base and deep-learning models;
- **Accurate evaluation of risks and informed decision support in complex situations** thanks to its crisis classification tool coupled with its rule-based reasoning machine learning model;
- **Holistic situational awareness** thanks to its integrated Command, Control and Coordination System;
- **Hybrid threat intelligence capacities**, with prediction capacities and continuously improved preparedness and detection models;
- **Semantic queries to retrieve specific data or information** thanks to its ontological representation model and its user-friendly interfaces.

7SHIELD Core is:

- **Cost effective** since it enables to have only one control room and one operator against two for separate cyber and physical protection systems.
- **Sustainable and always at the state-of-the-art** thanks to its cyber and physical threat intelligence that continuously improves 7SHIELD preparedness and detection models;
- **Highly adaptable and modular**, with a seamless integration of existing infrastructures and solutions in the framework and the possibility of adding or removing functional modules depending on users' needs;
- **Easy and quick to handle** thanks to its user-friendly interfaces and tailored Space Ground Segment ontological representation of the information.

4.1.2. Competitive landscape

7SHIELD is at the crossroad of the SIEM, PSIM and NMS segments. The desk research did not permit to identify any commercial system of systems that merge both cyber security systems and physical security systems. However, several research & development projects have been identified and are listed below:

	Cyber security		Physical security	Hybrid security					Space Ground Segment security
	Security Information and Event Management (SIEM)	Network Management System (NMS)	Physical Security Information Management (PSIM)	Cascading effect simulation & resilience assessment	Cyber & Physical data correlation and threat Intelligence	Cyber & Physical threat detection and early warning	Hybrid situational awareness & decision support	Semantic queries for Cyber and Physical Forensic	Designed for Space Ground Segment operation centres
7SHIELD	X	X	X	X	X	X	X	X	X
SABABA SECURITY[18] https://www.sababasecurity.com	X		X		X				
LABYRINTH https://www.labyrinth-yg.com/	X		X						
FINSEC https://www.finsec-project.eu/	X		X		X				
SAFECARE[19] https://www.safecare-project.eu	X		X	X			X		
InfraStress[20] https://www.infrastress.eu	X		X	X	X	X	X		

	Cyber security		Physical security	Hybrid security					Space Ground Segment security
	Security Information and Event Management (SIEM)	Network Management System (NMS)	Physical Security Information Management (PSIM)	Cascading effect simulation & resilience assessment	Cyber & Physical data correlation and threat Intelligence	Cyber & Physical threat detection and early warning	Hybrid situational awareness & decision support	Semantic queries for Cyber and Physical Forensic	Designed for Space Ground Segment operation centres
SecureGas[21] https://www.securegas-project.eu/	X		X	X	X	X	X		
SATIE http://satie-h2020.eu/	X		X		X	X	X		
RESISTO http://www.resistoproject.eu/	X		X	X	X				

4-1 - Supply landscape of hybrid protection frameworks

[18] https://www.sababasecurity.com/cyber-physical-siem/

[19] https://www.safecare-project.eu/?page_id=527

[20] https://www.infrastress.eu/objectives

[21] https://www.securegas-project.eu/wp-content/uploads/2020/09/SecureGas_project-presentation.pdf

4.1.3. Main target(s)

With its 7SHIELD Core, 7SHIELD consortium aims to address every entity that operates ground segment infrastructures and assets such as:

- EO Satellite Operators
- Telecommunication Satellite Operators
- Independent Telecommunication Ground Stations Operators
- National and regional Space Agencies
- National Meteorological Institutes
- EO platform operators
- Spatial Institute(s) / Research Centres
- Public Cloud Operators
- Specific Ground Segment infrastructure operator(s)
- Space technology companies

In the future, 7SHIELD framework could be adapted to address other types of critical infrastructures and enlarge its accessible market.

4.1.4. SWOT analysis

	FAVOURABLE FACTORS	ADVERSE FACTORS
INTERNAL FACTORS	**STRENGTHS** ▪ Most of the technology bricks developed are already at a high TRL; ▪ 7SHIELD framework is especially designed to meet the specificities of Space ground segment infrastructures;	**WEAKNESSES** ▪ 7SHIELD is a complex product. Its value proposition and competitive advantages could be difficult to be understood;
EXTERNAL FACTORS	**OPPORTUNITIES** ▪ Space ground segment infrastructures are developing all over the world; ▪ Security market for critical infrastructures is growing; ▪ Regulations are becoming increasingly strict and are pushing private players to invest in high-performance security systems; ▪ Hybrid threat protection is a global concern; ▪ No holistic commercial solution exist yet;	**THREATS** ▪ Multiple R&D programmes on Hybrid threat protection for critical infrastructures are ongoing and will lead to competitive solutions;

4.2. 7SHIELD modules

Please note that the description of 7SHIELD modules will be completed and harmonised in the final version of the Market analysis at M18. Indeed, some descriptions of 7SHIELD modules are partial due to the fact that we are still at an early stage of the project. Hence, the scope as well as the market proposition of some key results is not completely defined yet.

4.2.1. Cyber and Physical Threat Intelligence

This tool provides capabilities for acquiring knowledge from multiple sources about threats and for anticipating/identifying new and emerging cyber or physical threats, as well as complex/hybrid threats. Thus, relevant information will be searched in both public and deep web, and then collected, analysed, correlated and organized in order to support decision-making by providing information about attack techniques, indicators of compromises, and vulnerabilities.

The Cyber and Physical Threat Intelligence tool, starting from data stored in the Critical Infrastructure data model, builds a set of keywords that will be used to extract contents from OSINT, Social Medias and Dark web. The extracted contents will be processed to identify potential threats involving the CI.

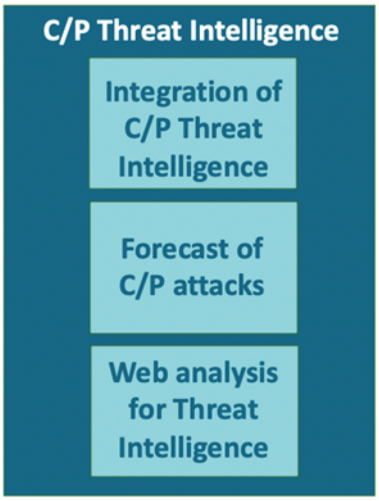

C/P Threat Intelligence
Integration of C/P Threat Intelligence
Forecast of C/P attacks
Web analysis for Threat Intelligence

Figure 4-2 - Cyber and Physical Threat Intelligence module architecture

4.2.1.1. Value proposition

Threat intelligence adds value on all stages of the attack life cycle. This is how the highest value of threat intelligence is achieved. The following main benefits have been identified from utilising Cyber and Physical Threat Intelligence tool:

- Implementing capabilities for threat discovery over Internet;
- Anticipate and forecast threats;
- Enabling threat analysis and raising warning;

- Threat categorisation and classification

4.2.1.2. Key comparison criteria

Technical criteria

- Sources Integrated: 5
- Threats identified: 3.5
- Interoperability: 4

Functional criteria

- Scalability: 5
- Management and Usability: 4
- Performance: 4

Commercial criteria

- Pricing level: TBD
- Customisation: 5
- Quality of support: 4.5

4.2.1.3.Competitive landscape

A small number of Threat Intelligence Platform (TIP) providers target this market. The majority are startups, and they drive this market in terms of features. Large, high-profile and small security providers recently shipped various threat intelligence (TI) capabilities or are signaling improvements in how native and third-party TI is handled for tactical and strategic benefit to customer security programs. The TIP is now considered a part of SOAR and competes for this function in security operations, investigation and automation.

Companies like, ThreatConnect, Anomali, LookingGlass Cyber Solutions, EclecticIQ, ThreatQuotient and Soltra offer different components and capabilities, with ThreatConnect and Anomali being the most common, offering offer different components and capabilities:

ANOMALI

Anomali (https://www.anomali.com/) was created in 2013 and has since grown to 200+ employees. It is privately held with several venture capital investors. It has offices in Redwood City, Belfast, Boston, London and Germany. Anomali is the leader in intelligence-driven cybersecurity. More than 1,500 public and private sector organizations rely on Anomali to see and detect threats more quickly, reduce the risk of security breaches, and improve security operations productivity. Anomali solutions serve customers around the world in nearly every major industry vertical, including many of the Global 2000. As an early threat intelligence innovator, Anomali was founded in 2013 and is backed by leading venture firms including GV, Paladin Capital Group, In-Q-Tel, Institutional Venture Partners, and General Catalyst. Anomali, Inc.'s main competitors are ThreatConnect, ThreatQuotient and Demisto[22,23].

Anomali ThreatStream aggregates millions of threat indicators to identify new attacks, discover existing breaches, and enable security teams to quickly understand and contain threats. In addition to the 140 open-source feeds included with the product, Anomali makes it easy to extend the information collected by the TIP through the Anomali App store. Here, users can evaluate and purchase additional intelligence feeds. This additional information contextualizes threats to greatly reduce the occurrence of false positives.

A key differentiator for Anomali is its highly accurate machine-learning algorithm that assigns scores to indicators of compromise (IOCs) so security teams can prioritize mitigation tasks. ThreatStream also allows for integration with many popular SIEMs and orchestration platforms in order to strengthen threat identification and remediation workflows.

Key features:

- De-duplication of data;
- Removal of false positives;
- Integration with third-party intelligence tools;
- Data extraction from suspected phishing emails;
- Offers some free threat intelligence tools[24].

Technical criteria

- Sources Integrated: 5
- Threats identified: 4.5
- Interoperability: 3

Functional criteria

- Scalability: 4
- Management and Usability: 4
- Performance: 5

Commercial criteria

- Pricing level: 5

[22] https://www.esecurityplanet.com/products/anomali-threatstream.html

[23]http://www.globenewswire.com/news-release/2020/09/24/2098776/0/en/Frost-Sullivan-Identifies-Anomali-as-the-Threat-Intelligence-Platform-Market-Leader.html

[24] https://www.esecurityplanet.com/products/top-threat-intelligence-companies.html?a#anomali

- Customisation: 4.5
- Quality of support: 4.5

ThreatConnect

ThreatConnect (https://threatconnect.com/) is a cyber-security firm based in Arlington, Virginia. They provide a Threat Intelligence Platform for companies to aggregate and act upon threat intelligence. The firm was founded in 2011 as Cyber Squared Inc. and renamed to ThreatConnect in 2014. ThreatConnect arms organizations with a powerful defense against cyber threats and the confidence to make strategic business decisions. ThreatConnect's headquarters is located in Arlington, Virginia. Built on the industry's only intelligence-driven, extensible security platform, ThreatConnect provides a suite of products designed to meet the threat intelligence aggregation, analysis and automation needs of security teams at any maturity level. More than 1,600 companies and agencies worldwide deploy the ThreatConnect platform to fully integrate their security technologies, teams, and processes with relevant threat intelligence resulting in reduced detection to response time and enhanced asset protection. ThreatConnect develops a threat intelligence platform that allows security professionals to aggregate, analyse and act on cyber-attacks. ThreatConnect's top competitor is Anomali, Inc[25,26,27].

ThreatConnect's offering in this space is **TC Complete**, a solid threat intelligence platform solution that focuses on facilitating automated processes. TC Complete, the company's flagship product, is a security operations and analytics platform that aims to enable companies to efficiently run their security operation centre (SOC) by giving them the ability to orchestrate security processes, analyse data, respond to threats, and report progress from a single location. TC Complete incorporates the features and benefits of all the other ThreatConnect products such as the TC Analyse threat intelligence platform, which provides a central location for analysing data and integrating with existing security tools. The platform allows analysts to better understand which threats are relevant, gain visibility into attack patterns, and share threat intelligence with executives and other stakeholders. The product helps organizations to orchestrate security processes, analyse data, respond to threats, and report progress from a single location. It can also integrate with existing security tools and share intelligence with internal and external stakeholders.

Key features:

- Gain visibility of potential threats while maximizing efficiency;
- Adapt and create automation for their existing processes to speed up incident response;

[25] https://en.wikipedia.org/wiki/ThreatConnect

[26] https://www.crunchbase.com/organization/threatconnect-inc-

[27] https://www.owler.com/company/threatconnect

- Make informed strategic decisions about security strategy;
- Analyse data, respond to threats, and report progress[28,29,30].

Technical criteria

- Sources Integrated: 5
- Threats identified: 4
- Interoperability: 4

Functional criteria

- Scalability: 4
- Management and Usability: 4
- Performance: 4

Commercial criteria

- Pricing level: 2
- Customisation: 4
- Quality of support: 3

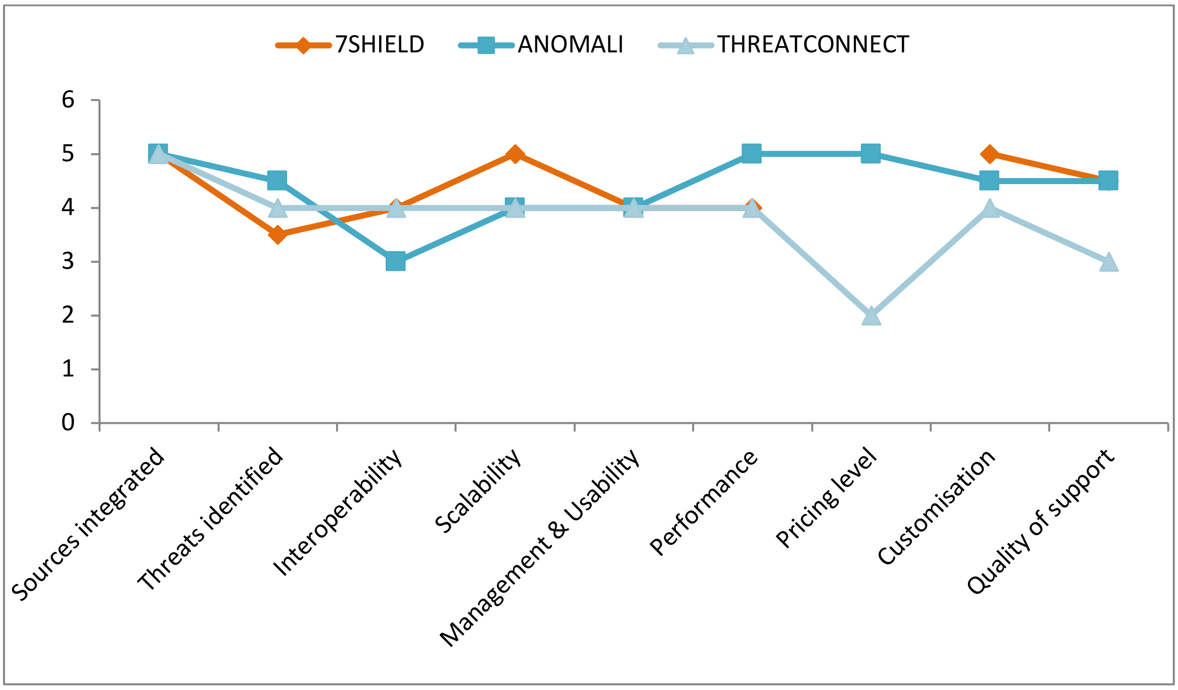


Figure 4-3 – Competitive landscape of Cyber & Physical Threat Intelligence

[28] https://www.scmagazine.com/review/threatconnect-tc-complete/

[29] https://www.securityweek.com/threatconnect-launches-new-threat-intelligence-products

[30] https://threatconnect.com/

4.2.1.4.Main target(s)

With its Cyber and Physical Threat Intelligence module, Engineering is targeting:

- ✓ Critical Infrastructure operators
- ✓ Public safety agencies

4.2.1.5.SWOT analysis

	FAVOURABLE FACTORS	ADVERSE FACTORS
INTERNAL FACTORS	**STRENGTHS** ▪ Better protection ▪ Integrated solution ▪ Rapid monitoring ▪ Capabilities for threat discovery	**WEAKNESSES** ▪ System not acceptable because of usability issues ▪ Management constraint due to diverging objectives ▪ No competitive advantage over competitors
EXTERNAL FACTORS	**OPPORTUNITIES** ▪ Secure platform supporting sources collection ▪ Increasing market penetration and position ▪ Real pilot experience	**THREATS** ▪ Implementation problems within the time and cost constraints ▪ Operation regulation in EU ▪ Cost limitation

4.2.2. Data confidentiality and integrity module

All-in-one data confidentiality and integrity module including multi-factor authentication, Single Sign On (SSO), innovative symmetric/asymmetric data encryption and blockchain-based data integrity service.

4.2.2.1. Value proposition

Open-source

- Used & maintained by a large and active community
- Drastically reduce risks of 0-day breaches
- Increase system sustainability

Single Sign On

- Drastically simplifies access and improves user experience

Multi factor authentication

- Increase authentication robustness

Cutting-edge hybrid data encryption protocol

- Benefits from both symmetric encryption rapidity and asymmetric encryption robustness

Cutting-edge blockchain-based data integrity service

- Ensure robustness of the data integrity checking service
- Enable to retrieve and control data processing and manipulation history

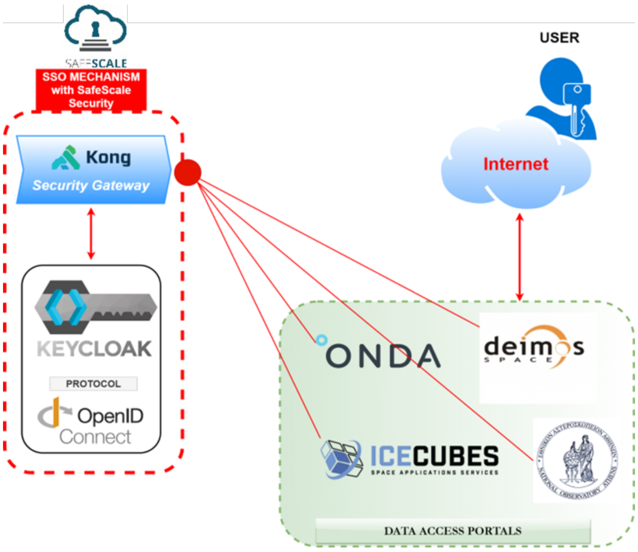


Figure 4-4: Single Sign On (SSO) Architecture

4.2.3. Video-based face detection and face recognition module

The Face detection and face recognition module will be able to process still frames or video streams, in order to export the detected and recognized faces that may belong to suspicious individuals. The framework will be linked with a criminal database, cloud or local, which will contain the list of suspects, as well as image data on which they should be clearly depicted. The main expected result is the production of alarms whenever a person is found to closely match one of the suspects.

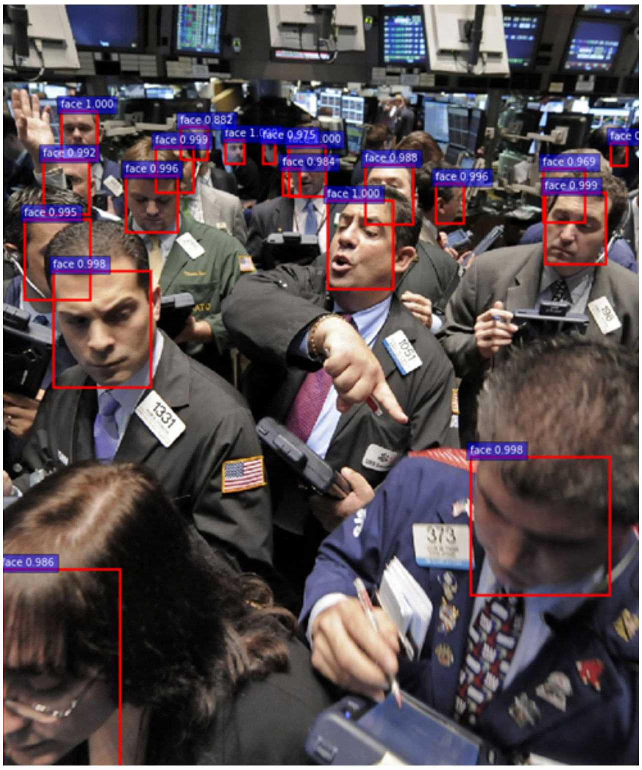


Figure 4-5: Illustration of a face detection & recognition solution

4.2.3.1. Value proposition

The module will ensure a restricted entrance in facilities where only authorised personnel are permitted. On the contrary, an unauthorised intrusion could be early identified, and the system could inform the security personnel via the proper alert.

Within this objective, critical infrastructure is protected from hazardous activities of unauthorised trespassers while the corresponding personnel and their daily activities are also secured. In addition, on many occasions, the accessibility of specific facilities may be limited only to a fraction of the personnel. Therefore, the operator could be engaged and aware of the current situation with an automatic and effective awareness framework.

4.2.3.2. Key comparison criteria

Technical criteria

- mAP: >95%
- Precision: >90%
- Recall: >90%
- FPS processing rate: >15fps

Functional criteria

- N/A

Commercial criteria

- Financial: No cost
- Technical: No involvement in the deployment of the service
- Skills related: No special skills are required-Only high level of understanding

4.2.3.3.Main target(s)

With its Video-based face detection and face recognition module, CERTH is targeting the market segments listed below:

- ✓ Critical Infrastructure Operators
- ✓ Security service companies
- ✓ Law enforcement

4.2.4. Video-based object and activity recognition

This module will process video streams or still images in order to locate and recognize objects of interest in the provided sources. Additionally, after detecting any human presence in the scene the corresponding results of object detection will be propagated to the activity recognition sub-module to identify suspicious and harmful activities. The main purpose of the module is the accurate and efficient visual interpretation of the surroundings of the surveillance area.

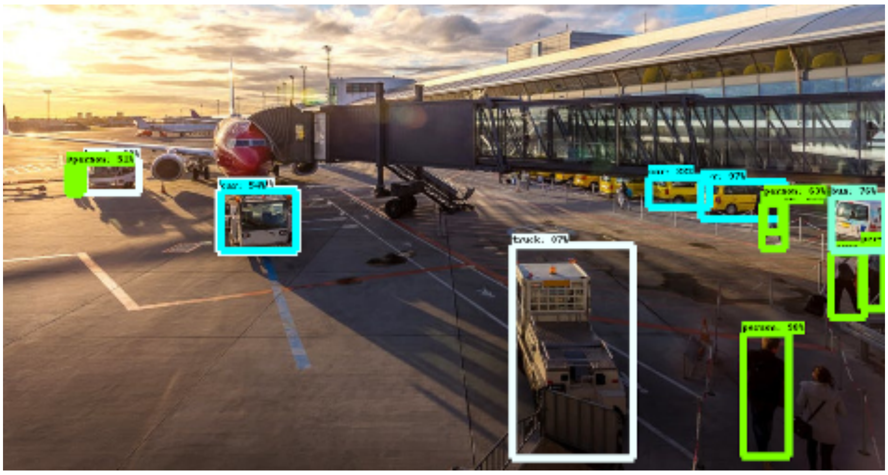


Figure 4-6: Illustration of a Video-based object and activity recognition solution

4.2.4.1. Value proposition

The key result involves the deployment of several software services with different objectives and goals. Video footages and/or live streams will be processed aiming to identify specific objects of interest as well as activities of such objects to early prevent harmful situations.

More specific, the object detection module will be fed with visual data either directly acquired from dynamic/static cameras or previously captioned footages, locally stored to the 7SHIELD physical server. The deployed deep learning module could identify specific objects of interest after a thorough analysis of the end-user requirements and the corresponding training process. Extracted confidence levels for each identified instance could produce the appropriate alerts towards an automatic information framework. The detection outcomes of specific objects could be further processed involving also time as a parameter in order to estimate potential activities strictly related to those objects. For example, the visual object detection service identifies two instances denoted with high confidence level as "person" and "bag". The outcome is further processed by the activity recognition module where a harmful activity could be identified such as "a person places the bag on the floor" which might be categorised as suspicious event based on the end-user needs.

4.2.4.2.Key comparison criteria

Technical criteria

- Object recognition: mAP >80%
- Object recognition: Precision and Recall >90%
- Object recognition: Processing rate >7fps
- Activity recognition: mAP >93%

Commercial criteria

- Financial cost: No cost
- Technical: No involvement in the deployment of the service
- Skills related: No special skills are required-Only high level of understanding

4.2.4.3.Main target(s)

With its video-based object and activity recognition module, CERTH is targeting the market segments listed below:

- ✓ Critical Infrastructure Operators
- ✓ Security service companies
- ✓ Law enforcement

4.2.5. Laser-fence

2D & 3D laser-based technologies for detection of ground-based intrusions by humans and vehicles, and aerial intrusions by drones.

4.2.5.1. Value proposition

High probability of detection, low probability of false alarms, low probability of nuisance alarms

- Increase monitoring efficiency and reduces costs;

Detects objects up to distance of 300 meters radius ground based, and up to 250 m radius aerial threats

- Covers a large scope of threats;
- Enables very early detection of intruders ;

Supported by PTZ cameras (Pan Tilt Zoom) on existing monitoring network

- Drastically reduces investment costs

Operates in all weather, both day and night

- Reduce monitoring efforts and costs
- Increase monitoring efficiency

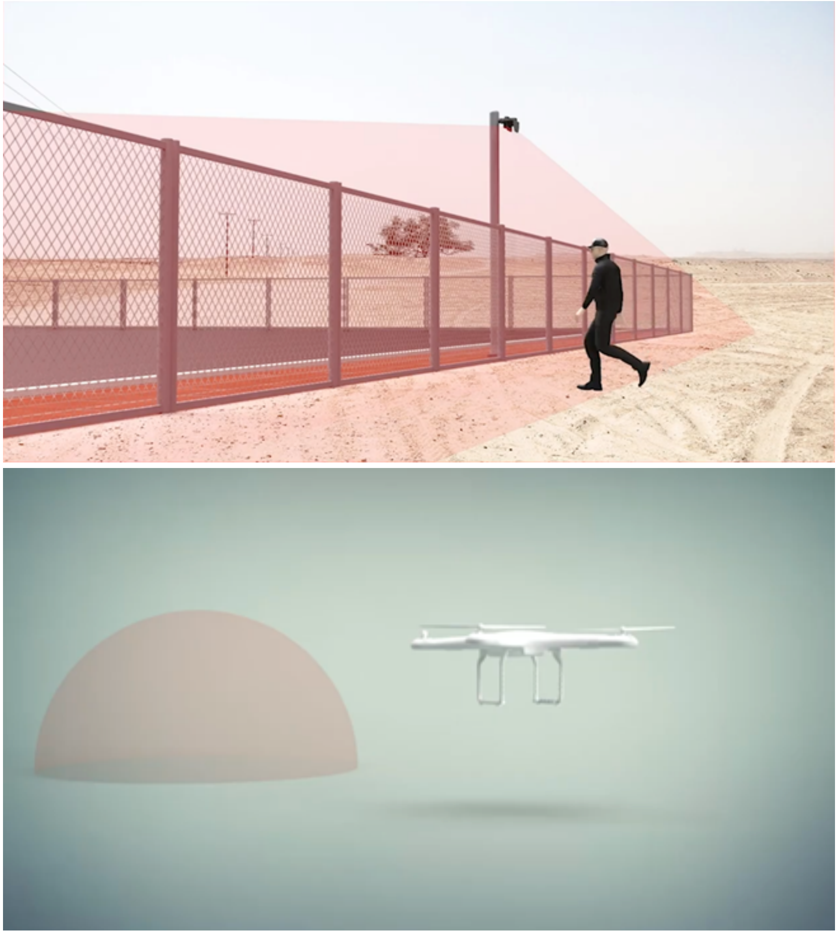


Figure 4-7: Illustrations of DFSL's 2D & 3D laser-based technologies

4.2.6. UAV neutralisation drone

Specially designed, developed and assembled drone, Flying Hunter (FH), that neutralise intruding mini-drones through green and robotic method – by catching it in its net and bringing it to the ground at pre-designated location.

4.2.6.1. Value proposition

Does not destroy unauthorized UAVs

- Enables forensic analysis for trespasser identification and location

Can operate with a 4kg payload

- Can catch and carry most of commercial UAVs

Specifically designed to absorb shocks

- Can operate safely, without risk for surrounding infrastructures and people

Highly secured communication channels

- Cannot be jammed or hacked

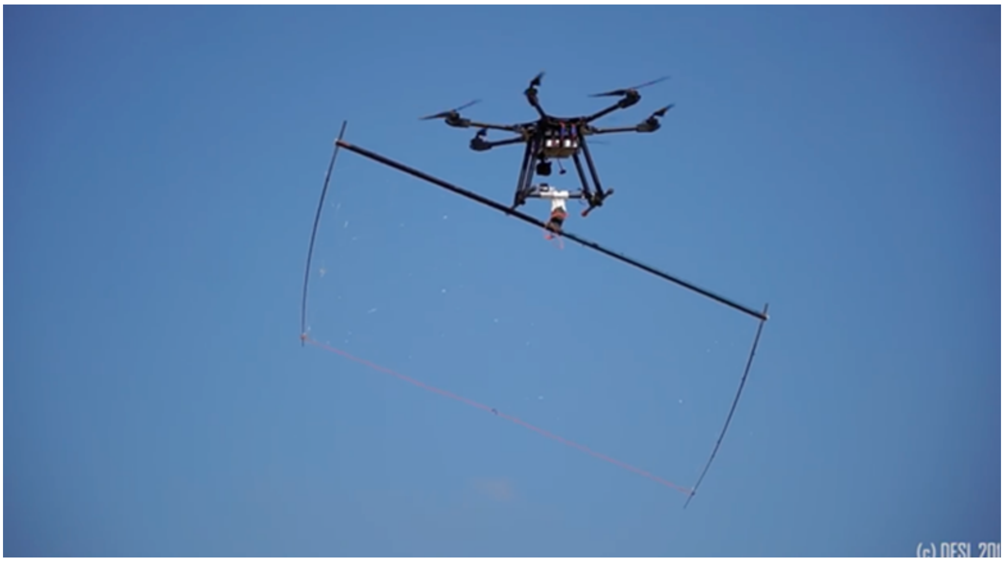


Figure 4-8: Illustration of DFSL's Flying Hunter drone

4.2.6.2.Main target(s)

With its UAV neutralisation drone specifically adapted to Space ground segment security, DFSL is targeting the market segments listed below:

- ✓ Critical infrastructure operators
- ✓ Security service companies
- ✓ Law enforcement

4.2.7. Thermal and near-infrared image processing for man-made threats detection

This module aims to use state-of-the-art technologies and methods for Thermal and Visible Near-InfraRed (V-NIR) image processing to detect man malicious activities near the infrastructure or the surrounding grounds like detection moving objects and people during the night. The MultiModal Automated Surveillance (MMAS) module, is composed by a network of Bi-spectral cameras (working in the Visible Near-InfraRed (VNIR) and in the Long Wavelength Infrared (LWIR), aka Thermal and a Processing Unit (server).

4.2.7.1. Value proposition

The work to be performed by the MMAS comprises three main features, which are detection, classification and tracking of targets of potentially physical attacks on a structure protected by 7Shield. It will give some awareness of surroundings via visualization of specific areas. The MMAS will also be capable, if necessary, to communicate with other 7Shield modules, permitting to acquire visual information and classification of targets detected by such modules (e.g., lidar).

An operator will have access to a User Interface (UI) to monitor the area under surveillance, the same interface will allow the operator to configure, manage alerts and warnings. The MMAS is expected to assist not to substitute the operator, so it will help in the detection of physical threats to critical infrastructures.

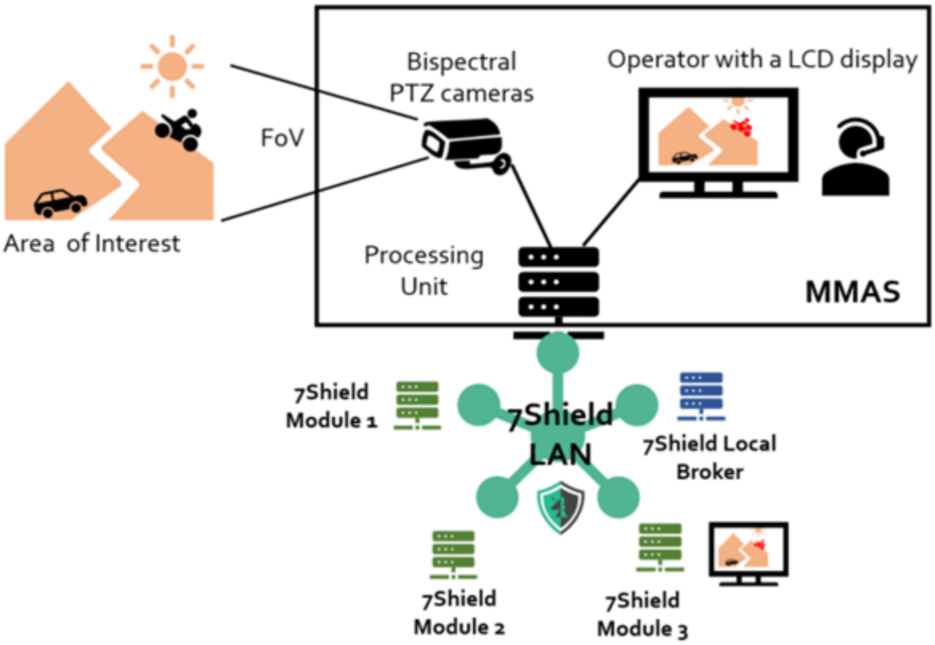


Figure 4-9 - MMAS within the 7SHIELD framework

4.2.7.2. Key comparison criteria

Technical criteria

- mAP: >90%
- Precision: 40 Elevation and 30 Azimuth
- FPS processing rate: >10fps

4.2.7.3.Main target(s)

With its Thermal and near-infrared image-based hazardous objects and situations detection module, INOV is targeting the market segments listed below:

- ✓ Critical infrastructure operators
- ✓ Security service companies
- ✓ Law enforcement

4.2.8. Tactical decision support system

A TDSS (tactical decision support system), is a complex system, which is based on a pro-security vest, embedded with wearables sensors, communication transceivers and UTD (Universal Tactical Display) for action team members. The TDSS is developed using commercial-off-the-shelf (COTS) components as much as possible, with a dedicated terminal to connect sensors with local IoT communications.

The use of a TDSS (Tactical Decision Support System) by first responder teams will enable teams to be self-aware and have more information to support effective decision making in the field without an infrastructure or C2 support.

4.2.8.1. Value proposition

Within the scope of the TDSS, a team leader will have a specific terminal to produce and receive DS (Decision Support) information, which in the field will help the team to take efficient decisions and to be more aware of the situation. Each team member will function as a sensor and at the same time will receive tactical information. Wherever possible the field collaborative sensors will be used, it depends on the scenarios' requirements.

Engagement rules and other hierarchical constraints and pre-operation relevant data is acquired and inserted in the TDSS to improve effectiveness and better support for the operation. Whenever possible the TDSS will connect to the main system of 7SHIELD to acquire data and provide feedback, and it will be capable with à priori information loaded (adding to any that is collected locally) to be able to operate and provide valid outputs.

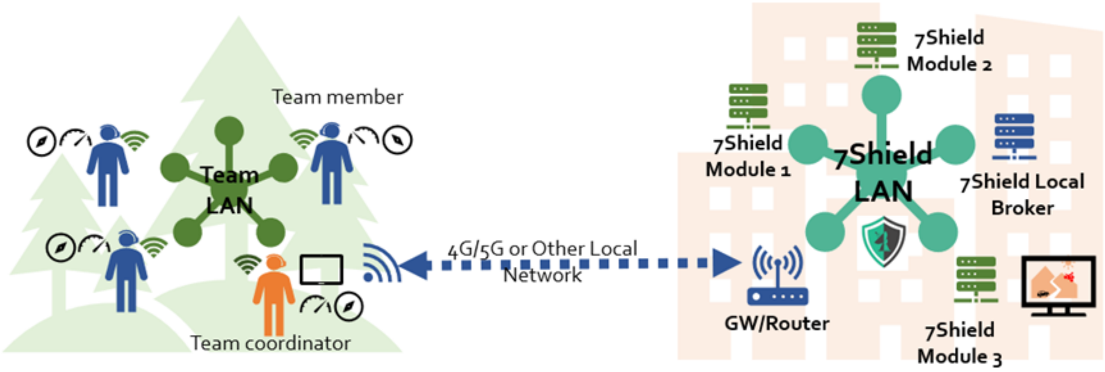


Figure 4-10 - TDSS (Tactical Decision Support System)

4.2.8.2. Key comparison criteria

Technical criteria

- Precision: < 4 meters
- Range from the team to protected infrastructure : <4km

4.2.8.3.Main target(s)

With its Tactical decision support module, INOV is targeting the market segments listed below:

- ✓ Critical infrastructure operators
- ✓ Security service companies
- ✓ Law enforcement

4.2.9. Social Awareness and Message Generation

A library of language agnostic-messages emergency messages for engaging and alerting local citizens during a security incident.

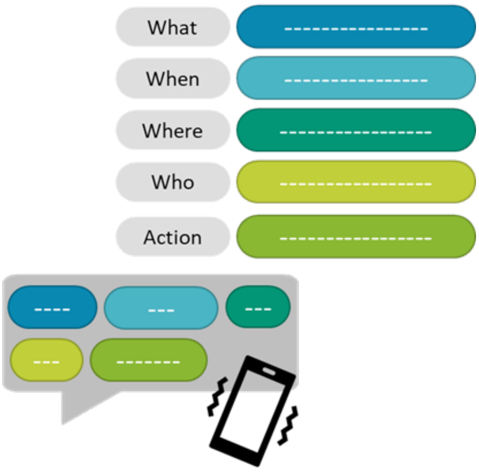


Figure 4-11: Illustration of Centric' Social Awareness and Message Generation module

4.2.9.1.Value proposition

The basis of a social media communication strategy that advises what and when information should be communicated to local citizens in a clear and concise format.

4.2.9.2.Competitive landscape

Based on current market research, message libraries are not currently offered directly to the market. At best they are a component or functionality available through a mass messaging or mass notification system (App or SMS-based). More likely these applications do not come with pre-loaded message libraries but with the option to create a bespoke library for a company's specific requirements. Advice on creating templates is shared through blog posts or similar. Thus there are few, if any, direct competitors for this specific result; there is, however, extensive research and recommendations in this area of what constitutes and optimal message.

Omnilert (https://www.omnilert.com/) is a US-based company that offers an extensive emergency communication system including business continuity planning, mass notification, and event detection

Omnilert Scenarios (https://www.omnilert.com/technology-scenarios) is Omnilert's solution that enables organisations to pre-plan their incident response including SMS and social media messaging for a range of different possible scenarios.

Functional characteristics

- Set of messaging templates to support citizen communication: Omnilert provides advice on possible templates that an organisation could set up (e.g., https://www.omnilert.com/resource-top-5-emergency-templates)

Klaxon (www.klaxon.io) offers Mass Notification and Messaging System for Incidents based in Leeds, UK.

Klaxon is a messaging and communication system for alerting and interacting with members of your organisation during a crisis incident in a controlled manner through a range of communication applications. Klaxon supports the use of pre-loaded templates within the system to quickly notify recipient to incidents. Klaxon contains an extensive template library that organisations can take advantage of.

Functional characteristics

- Set of messaging templates to support citizen communication: Functionality for including preloaded messaging templates for use in the event of an emergency. https://www.klaxon.io/emergency-notification-system

Several public organisations have also made available their own template libraries for specific incidents.

4.2.9.3.Main target(s)

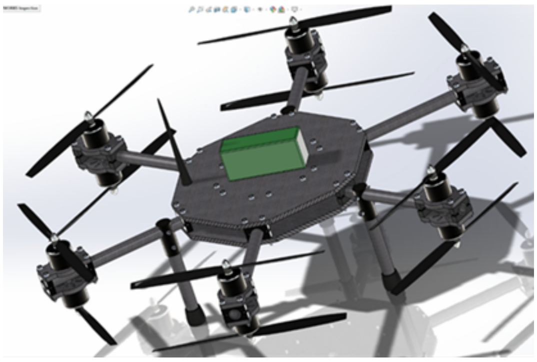
With its Social Awareness and Message Generation module, CENTRIC is targeting the market segments listed below:

- ✓ Critical Infrastructure Operators
- ✓ Public Safety Agencies

4.2.9.4.SWOT analysis

	FAVOURABLE FACTORS	ADVERSE FACTORS
INTERNAL FACTORS	STRENGTHS ▪ Specific to the ground space and critical infrastructure domains ▪	WEAKNESSES ▪ Does not form part of a larger system ▪ Is not a technical product but a template library and additional guidance and therefore is not marketable alone ▪ Limited target market for CI and ground space specific messages
EXTERNAL FACTORS	OPPORTUNITIES ▪ CENTRIC already offers a mass notification product (SCAAN) and this could add to its feature set.	THREATS ▪ Extensive market for mass notification systems already exists ▪ Limited market for actual message templates usually included for free as part of larger product

4.2.10.Autonomous UAVs equipped with embedding artificial intelligence



Acceligence's customised UAVs compared to the other drones on the market has a high autonomy (~1h fly time), a dedicated computer with GPU that runs Machine learning algorithms (for example, collision avoidance and advanced path planning). It can also be integrated with multiple sensors such as 3D sensors (Intel RealSense), sonars, etc. Its size is 1.4m * 1.4m * 0.8m and it contains a 360o 8k Camera integration for the best user experience, hand gestures drone control, Collision Avoidance path planning, 3D Tracking for the best tracking results, high precision landing with image processing, multispectral cameras integration and index map generation and an Autonomous Landing Area. A landing area that is powered by 8 solar panels; where the drone can take-off, execute a mission, land, store the drone inside and finally charge from the power of the solar panels. This base can be completely autonomous.

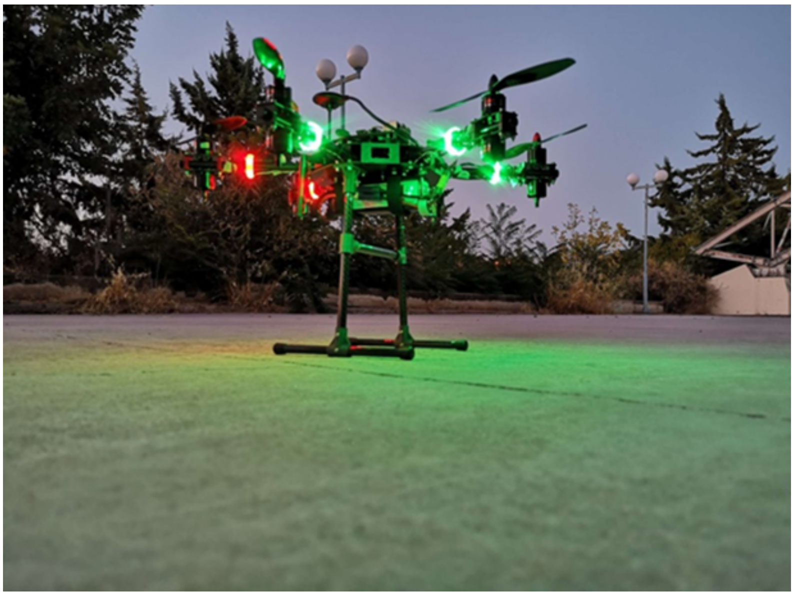


Figure 4-12: Illustration of Acceligence's sutonomous UAVs equipped with embedding artificial intelligence

4.2.10.1.Value proposition

The benefits of the system from owners/operators point of view are summarised as follows:

1. The landing area is at the same time storage area;
2. Inside landing area the UAV can be charged with the 8 solar panels for the next mission;
3. The system is completely autonomous meaning no human effort;
4. UAV's embedded GPU can recognise and discriminate by itself any detection avoiding false alarms for example in a large-scale area can easily understand if detection is an animal or other threat. The system is also trained to all kind of threats using artificial intelligence (AI) and Deep Learning algorithms;
5. UAVs not only will be able to give the exact location of any threat but also stream and record to the control room real-time action by following the intruder;
6. The system can be also expanded up to 10 or more UAVs, that are controlled and managed by one, with the same planning algorithm (Drone Swarms), one control action is broadcasted to all models and interpreted according to its environment;

In light of the above UAVs, can go and survey any area, with their equipment (cameras 8k, infrared, thermal) can locate anything that standing or move, with their embedded GPU can recognise and understand any possible threat avoiding false alarms and with their GPS can give the exact location of the threat. Last but not least, UAVs are able to stream live image of the situation, follow the threat or the master UAV can give order to another UAV from the "SWARM" to continue and follow the threat to the next area.

4.2.10.2.Key comparison criteria

Technical criteria

- Open Source: Software with source code that anyone can inspect, modify, and enhance;
- GPU support: Embedded AI-driven operation for enhanced decision support capabilities;
- Location accuracy: GPS ZED-F9P RTK2 with 1 centimetre precision;
- UAV neutralization capacity: Automation of the overall procedure with no "time to react" delays;
- Transmit live video to the control room: accessible via FPV Goggles;
- Perform image/video processing Threat detection and forecasting: using advanced anomaly-based detection models to indicate deviations to normal system activity w.r.t. the application and signify potential threats before they cause critical damage.

Functional criteria

- Max Flight Time: About 60 minutes
- Max Extra Weight: 12-15 Kg
- Level of autonomy in flight: Fully Autonomous

Commercial criteria

- User friendly: Easy to be used by anyone with minimum training;
- Ecosystem friendly: Option to be recharged with solar energy via solar panels;
- Customer relationship: Acceligence is available 24/7 for technical support and any update to the purchased system

4.2.10.3.Main target(s)

With its Autonomous UAVs equipped with embedding artificial intelligence, Acceligence is targeting the market segments listed below:

- ✓ Critical Infrastructure Operators

4.2.10.4.SWOT analysis

	FAVOURABLE FACTORS	ADVERSE FACTORS
INTERNAL FACTORS	**STRENGTHS** ▪ Integrated solution for ground segments of space systems; ▪ Multiple modules (KRs) of already high TRL; ▪ Protection of extremely large datahubs of satellite data; ▪ State-of-the-art Computer Vision techniques for event detection and knowledge extraction; ▪ Anti-drone mechanism and UAV neutralisation.	**WEAKNESSES** ▪ Potential lack of extensibility to other types of critical infrastructure.
EXTERNAL FACTORS	**OPPORTUNITIES** ▪ Support service continuity in space ground segments that serve the Copernicus market in EU; ▪ Support the space sector and governmental bodies by continuously providing data that meet all FAIR principles; ▪ Solutions from other types of critical infrastructures not directly extendable to ground segments of space systems.	**THREATS** ▪ Legislation and regulations among EU member states.

4.3. Overall competitive landscape

The critical infrastructure protection market is highly competitive, owing to the presence of many small and large players in the market operating their business in domestic and international markets. With the advent of infrastructure attacks, many vendors respond to the rising threat by offering critical information security solutions. These offerings have to lead to new services, technologies, and partnerships with leading essential providers of infrastructure.

The top 5 major players are composed of[31]:

- BAE Systems PLC
- Honeywell International Inc.
- Raytheon Co.

[31] https://www.mordorintelligence.com/industry-reports/global-critical-infrastructure-protection-market-industry

- Airbus SE
- Hexagon AB

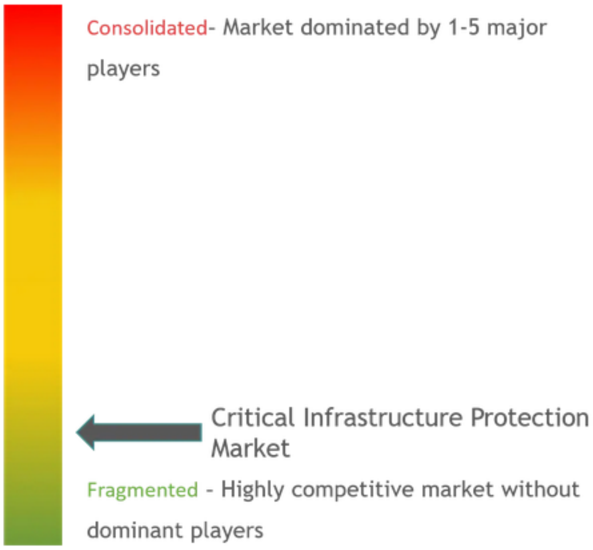


Figure 4-13 - Critical Infrastructure Protection Market Concentration – Mordor Intelligence 2019

4.4. Market segmentation

To protect Space Ground Segment facilities against Cyber and Physical threats, 7SHIELD framework integrates methodologies, tools and technologies covering Prevention, Detection, Response and Mitigation stages of crisis management for both cyber and physical security functions.

This system of systems can be addressed to different stakeholders depending on the crisis management stage covered. It could be Critical Infrastructure Operators (Ground station operators, control centre operators, data storage and processing facility operators etc.), public safety agencies, Physical and Cyber security service companies, law enforcement, regulatory authorities or emergency response services.

Space agencies	More than assuring a continuity of service, national and regional Space agencies are very careful to conserve and protect sovereign interests. They thus are very sensitive to threats against their critical infrastructures. They are also a prime target in case of cyber warfare. Their innovation and investment capacity can drastically vary from one country to another. **Expected willingness to pay: High**
Space ground segment infrastructure operators	Regulations concerning Space ground segment infrastructures are becoming increasingly stringent as risks to populations and the potential impact on countries' economies increase.

	Moreover, customers are less and less inclined to accept defects in service. These trends are leading Space ground segment infrastructure operators to invest in innovative and efficient solutions against cyber and physical threats. **Expected willingness to pay: Average**
Physical security service companies	Physical security is often the poor relative of the security industry. It often implies easily replaced low-skilled labour. In the other hand, technologies against physical threats are very rarely scalable and are often very expensive, limiting the customers' capacity to invest. **Expected willingness to pay: Low**
Cyber security service companies	Cyber security service companies integrate third-party technologies and solution into their customers' infrastructures. They can see 7SHIELD framework as a key differentiator to seize new market shares. Due to the significant increase in spending on cyber security, their financial capacities are rather high. **Expected willingness to pay: Average**
Public security agencies and National Authorities in charge with Spectrum Management and Monitoring	Public security agencies ensure the protection of people, organisation and institutions in their territory. They include cyber-security agencies, law enforcement, fire and emergency medical services. In general, they do not own critical infrastructures but help protecting others. **Expected willingness to pay: Low**

4.5. Regulation

GS administration usually requires adopting a modern quality control system. This is done on the basis of the European Space Standards issued by the European Cooperation for Space Standardization (ECSS1) and taking into account other well-established standards (e.g. ISO), and space asset specific individual requirements. The ECSS is an initiative established to develop a coherent, single set of user-friendly standards for use in all European space activities. Among others, ECSS has defined a set of Active Product Assurance standards that include Product Assurance Management, Quality and Safety Assurance for Space Test Centres, and a Hazard Analysis standard. The latter defines the principles, process, implementation, and requirements of hazard analysis of ground segments of space systems as well. It is applicable to all European space projects where during any project phase there exists the potential for hazards to personnel or the general public, space flight systems, ground support equipment, facilities, public or private property or the environment. However, although this is an active standard used by most

European GS operators, the Hazard Analysis standard was created in 2008 and is considered outdated.

4.6. Other barriers to entry

Despite the fact that physical and cybersecurity are intrinsically connected, many organisations still treat cyber and physical security functions as separate systems. Until recently this was justified because the technology to integrate physical and cybersecurity was not yet available. But now, the problem comes down to governance.

Indeed, the merge of cyber and physical security functions implies changes at the organisational level. These changes can be seen as a threat for some key people in a company and could thus induce resistance to the adoption of a solution such as 7SHIELD.

4.7. 7SHIELD total accessible market in Europe

4.7.1. European market

At the European level, several agencies are operating GS infrastructures:

The European Space Agency (ESA) directly manages the Sentinel Core Ground Segment and the Data Access Coordinated System of the Copernicus programme.

The Sentinel Core Ground Segment allows all Sentinel data to be acquired systematically, processed and distributed.

The main elements are:

- **The Flight Operations Segment (FOS)**, responsible for all aspects of Sentinel flight operations, including monitoring and control, the execution of all platform activities and command of payload schedules.
    - Germany (Darmstadt) at ESA's European Space Operations Centre (ESOC)
- **The Core Ground Stations**, where the Sentinel data are downlinked and products are generated in near-real time. A network of X-band ground stations allows Sentinel data to be downlinked. The network is complemented by the European Data Relay Satellite (EDRS) for the additional downlink of Sentinel data to EDRS ground stations:
    - Italy (Matera) operated by e-GEOS
    - Spain (Maspalomas) operated by INTA
    - USA (Alaska) operated by KSAT
    - Norway (Svalbard) operated by KSAT
    - Canada (Inuvik) operated by KSAT
    - Sweden (Kiruna) operated by ESA

- **The Processing and Archiving Centres (PACs)**, where systematic non-time-critical data processing is performed. All data products are archived for online access by users. A network of PACs supports all the processing and archiving of Sentinels data.
    - Germany (Darmstadt) operated by Eumetsat
    - Germany (Oberpfaffenhofen) operated by DLR
    - Spain (Madrid) operated by Indra
    - France (Nice) operated by ACRI
    - France (Toulouse) operated by CLS
- **The Mission Performance Centres (MPCs)**, responsible for calibration, validation, quality control and end-to-end system performance assessment. The MPCs include expert teams for specific calibration and validation, offline quality control and algorithm correction, and evolution activities.
- **The Sentinel Precise Orbit Determination (POD)** facility makes use of the GNSS receiver data on the Sentinels to deliver the orbital information needed to generate the data products.
    - Spain (Tres Cantos) operated by GMV (Sentinel 2)
- **The Copernicus Space Component Wide Area Network (CSC WAN)**, allows all products and auxiliary data to be carried across the various ground segment facilities and provides disseminated data products to the end users.

The European Space Operations Centre (ESOC) in Darmstadt, Germany operates a number of ground-based space-tracking stations for the European Space Agency (ESA) known as the European Space Tracking (ESTRACK).

ESTRACK ground segment is composed of a control centre based in ESOC's facility and 7 ground stations in Portugal (Santa Maria Island), French Guiana (Kourou), Belgium (Redu), Sweden (Kiruna), Spain (Cerebros), Australia (New Norcia) and Argentina (Malargue).

The European Organisation for the Exploitation of Meteorological Satellites (EUMETSAT) in Darmstadt, Germany operates a multi-mission ground network made up of:

- A central Mission Control Centre (MCC), located at EUMETSAT headquarter;
- Primary Ground Stations (PGS) composed of 2 remote Telemetry, Tracking and Control Facilities (TTCF) in Italy (Fucino) and Romania (Cheia);
- A Back-up and Ranging Ground Station (BRGS) located in Spain (Maspalomas);
- 2 remote Mission Data Acquisition Facilities (MDAF) in Switzerland (Leuk) and in Italy (Lario);
- The EUMETSAT Polar System (EPS) composed of a ground station located in Norway (Spitsbergen);
- Data processing facilities at EUMETSAT headquarters.

EUMETSAT also supervises and coordinates the distributed network of **Satellite Application Facilities (SAFs)** that are 8 dedicated centres of excellence for processing satellite data. They form an integral part of the distributed EUMETSAT Application Ground Segment. The SAFs are located within the National Meteorological Services (NMS) of EUMETSAT Member States, or other agreed entities linked to a user community.[32]

Eventually, EUMETSAT will integrate the EPS-SG Overall Ground Segment (OGS) that will support the ground functions required to meet the EPS-SG Missions objectives.

The OGS will consist of three main blocks:

- Mission Control and Operations (MCO). The MCO block will ensure the end-to-end monitoring and control of the Metop-SG spacecraft including Tracking, Telemetry and Control (TT&C) station.
- Payload Data Acquisition and Processing (PDAP). The PDAP block will ensure the end-to-end chain from data acquisition to the generation of level 1 and level 2 products.
- EUMETSAT Multi Mission Elements (MMEs). The Multi Mission Elements (MMEs) are EUMETSAT operational facilities and common infrastructure used by existing programmes. They are split in four groups: infrastructure, data centre, monitoring and dissemination. They will be used by EPS-SG after extension and upgrade.

4.7.2. Domestic markets of 7SHIELD consortium members

7SHIELD consortium is composed of 22 partners from 12 different countries. The domestic market of each partner for the commercialisation of 7SHIELD is composed of:

- EO Satellite Operators
- Telecommunication Satellite Operators
- Independent Telecommunication Ground Stations Operators
- National Space Agency
- National Meteorological Institutes
- EO platform operators
- Spatial Institute(s) / Research Centres
- Public Cloud Operators
- Specific Ground Segment infrastructure operator(s)
- Space technology companies

[32] https://www.eumetsat.int/satellite-application-facilities-safs

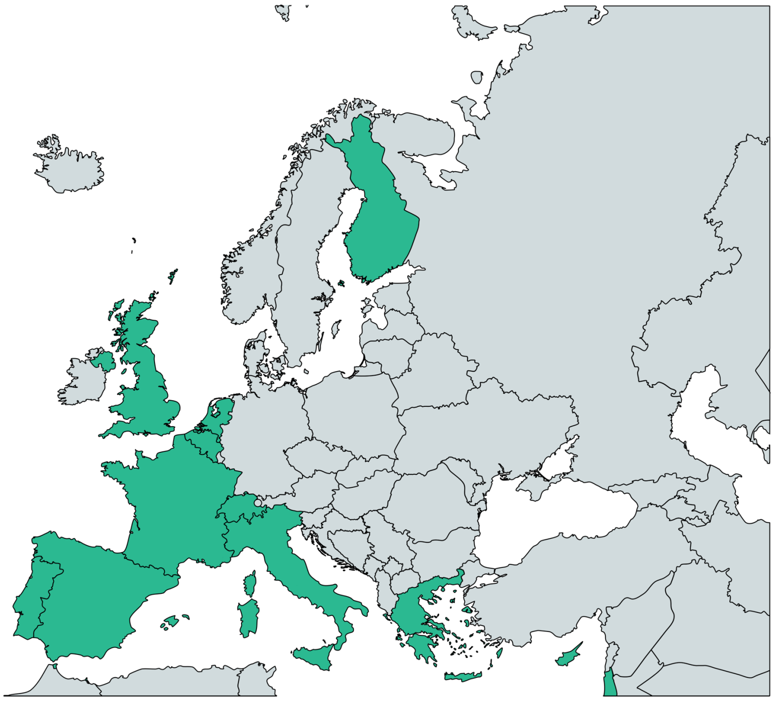


Figure 4-14 – Geographical coverage of 7SHIELD consortium

4.7.2.1. Belgian domestic market

1	**Telecommunication Satellite Operator(s)**	GlobalTT	Ground Station – Belgium (Brussels)
1	**Specific Ground Segment infrastructure operator(s)**	Space Applications Services	Ice Cubes control centre - Belgium (Sint-Stevens-Woluwe)
1	**National Meteorological Institute(s)**	Institut Royal Météorologique (IRM)	
2	**Spatial Institute(s) / Research Centre(s)**	Institut royal d'Aéronomie Spatiale de Belgique	
		Belgian Federal Science Policy Office	

4.7.2.2. Cypriot domestic market

1	**Telecommunication Satellite Operator(s)**	Cytaglobal	Teleport - Cyprus (Makarios)
			Teleport - Cyprus (Pera)
			Teleport - Cyprus (Ermis)

4.7.2.3. Finnish domestic market

1	**National Meteorological Institute(s)**	National Meteorological Institute	Arctic Space Centre – Finland (Sodankylä)

4.7.2.4.French domestic market

2	EO Satellite Operator(s)	Collecte Localisation Satellites (CLS)	Teleport - USA (Wallops Island)
			Teleport - USA (Fairbanks)
			Teleport - Norway (Svalbard)
			OC - France (Toulouse)
			OC - USA (Washington)
		Airbus DS Geo	
1	Telecommunication Satellite Operator(s)	Eutelsat	OC - France (Paris)
			OC – Italy (Cagliari)
			OC – Italy (Turin)
			OC - Mexico
			Teleport - France (Rambouillet)
			Teleport - Italy (Cagliari)
			Teleport - Italy (Turin)
			Teleport - Mexico (Iztapalapa)
			Teleport - Mexico (Hermosillo Sonora)
			Teleport - Portugal (Madère)
1	Independent Telecommunication Ground Stations Operators	Globecast	
1	National Space Agency	CNES	Launch base: French Guyana (Kourou)
1	National Meteorological Institute(s)	Météo-France	
2	EO platform operator(s)	Airbus DS Intelligence	SOBLOO
		Atos	Mundi Web Services
1	Spatial Institute(s) / Research Centre(s)	ONERA	
2	Public Cloud Operator(s)	OVH	OVH Cloud
		Orange	Orange Cloud
1	Technology company(ies)	ACRI	Processing & archiving centre (PAC) - France (Nice)

4.7.2.5.Greek domestic market

2	Telecommunication Satellite Operator(s)	Hellas Sat OTE	
1	National Meteorological Institute(s)	Hellenic National Meteorological Service	
1	Spatial Institute(s) / Research Centre(s)	National Observatory of Athens	

4.7.2.6.Israeli domestic market

1	National Space Agency	Israel Space Agency	

4.7.2.7.Italian domestic market

1	EO Satellite Operator(s)	Telespazio	Teleport - Italy (Fucino)
			Teleport - Italy (Lario)
			Teleport - Italy (Scanzano)
1	Independent Telecommunication Ground Stations Operators	Ministero della Difesa	Ground station - Italy (Roma)
1	National Space Agency	Agenzia spaziale italiana	Ground station - Kenya (Broglio Space Centre)
1	National Meteorological Institute(s)	Ufficio Generale Spazio Aereo e Meteorologia	
2	EO platform operator(s)	E-Geos	Ground station – Italy (Matera)
		SERCO	ONDA DIAS platform – Italy (Frascati)
			Copernicus Sentinels rolling archive – Italy (Frascati)

4.7.2.8.Dutch domestic market

1	National Space Agency	Netherland Space Office (NSO)	
1	National Meteorological Institute(s)	The Royal Netherlands Meteorological Institute (KNMI)	
1	Spatial Institute(s) / Research Centre(s)	Netherlands Institute for Space Research	

4.7.2.9.Portuguese domestic market

1	**National Meteorological Institute(s)**	Instituto Portugues do Mar e da Atmosfera (IPMA)	
1	**Telecommunication Satellite Operator(s)**	Altice	Satellite Centre – Portugal (Alfouvar)

4.7.2.10.Spanish domestic market

1	**EO Satellite Operator(s)**	Deimos	
1	**Telecommunication Satellite Operator(s)**	Hispasat	Teleport - Spain (Maspalomas)
			Teleport - Brasil (Guaratiba)
			Teleport - Argentina(Balcarce)
			Teleport - Mexico(Mexico city)
			Teleport - Colombia(Bogota)
			Teleport – Chilly (Arica)
			Teleport - USA (Laredo)
			Teleport - USA (Hauppauge)
			Control Centre - Spain (Arganda del rey)
			Control Centre - Spain (tres cantos)
			Control Centre - Spain (Las palmas)
			Control Centre - Spain (Flamengo)
4	**Independent Telecommunication Ground Stations Operators**	AXESS Networks	Teleport - Germany (Cologne)
			Teleport - Mexico
			Teleport - Colombia
			Teleport - UAE (Dubai)
			Teleport - Peru
		Telefonica Servicios Audiovisuales (TSA)	Teleport - Mexico (Guadalajara)
			Operation Centre - Spain (Tres Cantos)
		Santander teleport	Teleport - Spain (Cantabria)
		Overon	Teleport - Spain (Madrid)
			Teleport - USA (Miami)
			Teleport - Bulgaria (Sofia)

1	National Space Agency	Centre for the Development of Industrial Technology (CDTI)	
1	National Meteorological Institute(s)	Agencia Estatal de Meteorología (AEMET)	
1	Spatial Institute(s) / Research Centre(s)	Instituto Nacional de Técnica Aeroespacial	Teleport - Spain (Maspalomas-Canary islands)
			Teleport - Spain (Torrejon de Ardoz)
2	Technology company(ies)	GMV	Sentinel Precise Orbit Determination (POD) - Spain (Tres Cantos)
		INDRA	Processing and Archiving Centre (PAC): Spain (Madrid)

4.7.2.11.Swiss domestic market

1	National Meteorological Institute(s)	MétéoSuisse	

4.7.2.12.British domestic market

2	Telecommunication Satellite Operator(s)	Avantiplc	Teleport - England
			Teleport - Germany
			Teleport - Germany
			Teleport - Turkey
			Teleport - Cyprus
			Teleport - Nigeria
			Teleport - South Africa
			POP - Netherland
			POP - Germany
			POP - Nigeria
			POP - South Africa
		Inmarsat	Teleport - New Zealand (Auckland)
			Teleport - New Zealand (Warkworth)
			Teleport - The Netherlands (Burum)
			Teleport - Italy (Fucino)
			Teleport - Canada (Laurentides)

			Teleport - Canada (Winnipeg)
			Teleport - USA (Lino Lakes)
			Teleport - Greece (Nemea)
			Teleport - Hawaii (Paumalu)
			Teleport - Australia (Perth)
			Teleport - Australia (Merredin)
			Network Operations Centre (NOC) - UK (London)
3	**Independent Telecommunication Ground Stations Operators**	Arqiva	Teleport - UK (Chalfon Grove)
			Teleport - UK (Bedford)
			Teleport - UK (Martlesham)
			Teleport - UK (Crawley court)
			Teleport - UK (Morn Hill)
		Talia	Teleport - Germany (Munich)
			Teleport - Iraq
		Satellite Mediaport Services Ltd. (SMS)	Teleport - UK (Rugby)
1	**National Space Agency**	UK Space Agency	
1	**National Meteorological Institute(s)**	Met Office	

5. Conclusions and future outlook

5.1. Key success details

The desk research has shown a sustained growth in all the security market segments covered by the 7SHIELD framework. And the implementation of a holistic security framework, covering both cyber and physical threats protection, seems to be a highly trendy topic for Chief Information Security Officers for some time now.

Despite the strong demand for such holistic system of systems, several critical factors seem to emerge:

The modularity: Potential customers want to limit both investment costs and technological risks. It is thus mandatory for 7SHIELD framework to be modular and easily interfaced with existing devices, software and infrastructures. So that any customer can choose just what he needs to complete its holistic security framework while being sure that it will work smoothly.

The ergonomics: Implementing a new system is always a risk as it implies a period of adaptation for the operating team, and necessitates a wide adoption by all the stakeholders to generate its full benefits. These aspects are even more crucial when dealing with security matters and critical infrastructures, since no security weakness is allowed. The ergonomics of 7SHIELD framework is thus a key success criterion to shorten the period of adaptation, increase and fasten its adoption at large scale and thus lower induced risks for critical infrastructure operators.

The cost efficiency and ROI: As any investment, the people in charge of infrastructure security must justify the Return On Investment to get the budget. 7SHIELD framework should clearly demonstrate the cost efficiency to merge cyber and physical security management.

The efficiency: Critical infrastructures cannot offer any weakness. It is thus mandatory for Chief Security Officers to be reassured of the efficiency of any solution before implementing on their infrastructure.

5.2. 7SHIELD perceived value and possible measures for improvement

Pilot partners and Advisory Board members will be solicited to give us their feedbacks regarding the 7SHIELD framework and its value proposition.

5.3. Most promising segments

Security systems market is strongly dominated by the United States and Israel. However, the security systems market for critical infrastructures is a very regional market, driven by national or regional preferences for security and sovereignty matters. That is why the most accessible geographical segment for 7SHIELD seems to be the European market.

While several stakeholders can be addressed by 7SHIELD, the ones that will benefit the most from 7SHIELD breakthrough technologies and value propositions seems to be the public and private satellite operators that operate their own ground stations.

Horizon 2020
European Union Funding
for Research & Innovation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883284