ESPI

European Space Policy Institute

Full Report

Space in Support of Security Missions

An evolving landscape with untapped potential

Overview:

Title: "ESPI Report 80 - Space in Support of Security Missions - Full Report"
Published: February 2022
ISSN: 2218-0931 (print) • 2076-6688 (online)

Editor and publisher:
European Space Policy Institute (ESPI)
Schwarzenbergplatz 6 • 1030 Vienna • Austria
Phone: +43 1 718 11 18 -0
E-Mail: office@espi.or.at
Website: www.espi.or.at

Design: copylot.at

Cover page picture credit: Shutterstock

Table of Content

1 INTRODUCTION

Rationale and Background – an evolving "Space for Security" landscape

Today, Europe and its citizens are faced with a multifaceted set of security challenges, ranging from climate change and natural disasters to domains traditionally closer to law enforcement and defence. The solutions to all these challenges are increasingly being addressed through technological advances and space-based infrastructure and derived services are playing a major role in supporting and facilitating informed and timely decision making, both in terms of anticipation, response and recovery.

Indeed, space systems and their applications already support countless missions in the security domain handled by various actors, such as governmental authorities, international organisations, European institutions or non-governmental organisations.

In the future, the role of space in addressing security challenges on Earth will need to adapt to a changing security landscape which puts at risk the resilience of European citizens, industries and states. In recent years, several significant and unprecedented developments have demonstrated how the perception of security is impacted by broader societal developments, both in and out of Europe. A few examples illustrating this situation are:

- The global Covid-19 outbreak and its impact on public health, political stability and economic growth
- The strong migratory crisis hitting Europe
- The use of social media by terror groups to recruit their members and share their propaganda
- Cyberattacks against key infrastructures or to steal crucial information

All these trends and events may impact the national security of states and the security of their citizens. Therefore, political actors are eager to use all possible means to be prepared to face the upcoming changes in the international arena and their domestic environments and to counter potential threats.

"Space for Security" partnership between ESPI and ESA

Acknowledging these developments, in 2020 ESA and ESPI initiated a new partnership to examine the evolving "Space for Security" landscape and support the Agency on a possible future engagement in this domain in line with its Member States' views. More specifically, this ESA-ESPI partnership was implemented through a series of research studies and the organisation of two events with users and policy stakeholders.

This public ESPI Report provides the major findings and key takeaways (suitable for open-access publication), which have been identified by ESPI during the conduct of the two research studies in 2020 and 2021 and the numerous interactions with European policy stakeholders and users of space-based services from the security community.

In investigating how space-based capacities, data and services can be improved to better contribute to accomplishment of security missions, this ESPI Report addresses in more detail the following questions:

- What are the practices of organisations from the security domain when it comes to using space in support of their missions?
- What is the added value of space systems and services among the variety of other available technological tools?
- How are the space and security domains evolving and what consequences do these evolutions bear on the "Space for Security" landscape in the future?
- What are the major user needs and requirements of actors from the security community?

2 Space for Security – a Few High-level Considerations

2.1 Definition of "security" for this study

Despite a widely shared acknowledgement of "security challenges", the very concept of security, due to its broadness and ubiquity, can cover a vast number of meanings. Although often being linked in world politics with freedom from (or protection from) intentional threats by a given actor (state, coalition of states, armed groups, individuals…), and thus being sometimes jumbled with the concept of defence, it has to be noted that security is not restricted to that.

Indeed, over the years, the concept of security has broadened to encompass several dimensions reaching quite beyond intentional threats to also include freedom and protection from harm in general. Thus, in 1994, the United Nations Development Programme identified in its Human Development Report seven components constituting "human security"[1]:

- Economic security: guaranteeing a basic income to individuals
- Food security: physical and economical access to basic food, at any time
- Health security: guaranteeing minimum protection against diseases and unhealthy lifestyles
- Environmental security: protecting people from the short- and long-term ravages of nature, man-made threats in nature, and deterioration of the natural environment
- Personal security: being free from physical violence, whatever its sources
- Community security: protection of the groups (family, community, organisation, racial or ethnic group) which provide a cultural identity and a reassuring set of values to individuals
- Political security: respect of basic human rights

Security is thus a broad concept with a variety of definitions and meanings depending on the context and interpretations. While the UN identified security *dimensions*, this report will focus on security *missions* that help to implement them. Moreover, for the purpose of this study, the concept of "security" shall exclude military actors and activities, and focus on its "civilian" aspects.

Among the existing security missions, three primary pillars have been identified, which will be subject to further reflection in this report:

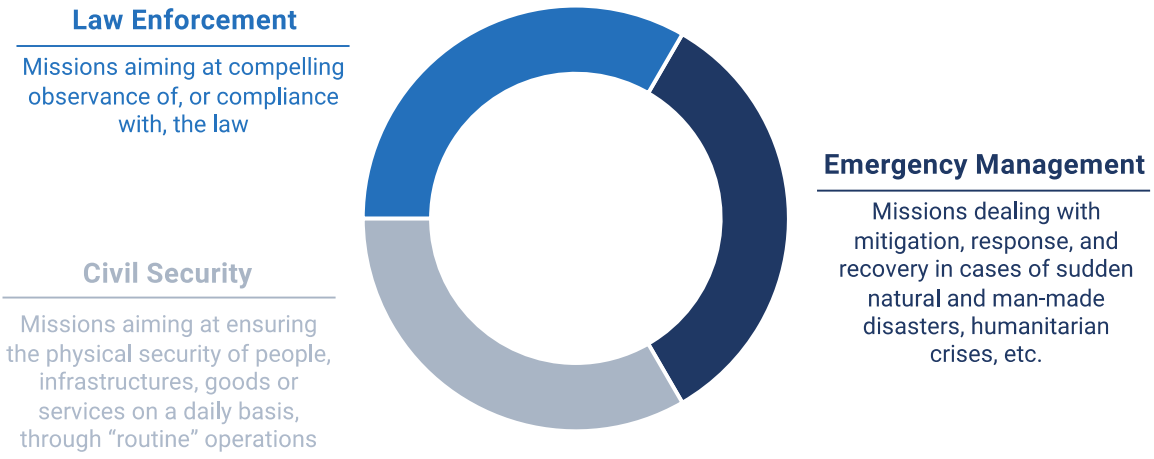


Figure 1: The three primary mission categories of security

1 United Nations Development Programme, Human Development Report 1994, Oxford University Press, 1994, p.24-33.

Each category involves a distinctive set of activities conducted by various institutions:

	Main actions and activities	Key actors
Law Enforcement	Border control, maritime surveillance, illegal immigration management, disarmament monitoring, fact-finding, illegal crop cultivation detection…	Police forces, customs, coast guards, justice organisations, fishery agencies, Frontex, EMSA…
Emergency Management	Construction of medical centres, shelters and camps, establishment of communication links, distribution of goods and services, evacuation of citizens, rapid situational assessment…	Emergency rescue teams on the field, headquarters, local authorities, diplomats, international organisations, NGOs…
Civil Security	Search and rescue, forest fires management, ambulance services, monitoring and protection of sensitive infrastructures and networks, guarantee of food and energy supplies' availability…	Local authorities, firefighters, coast guards, emergency medical assistance services, infrastructure operators…

Table 1: Core activities and actors for each security category

2.2 Interplay between space and security in Europe

European governments and organisations have already taken steps to better connect space and security matters and to enhance synergies between the two domains for mutual benefits.

2.2.1 Security themes are increasingly high in national and European policy agendas

Security has always been high on the political agenda, but the evolution of the international and domestic context in many countries is raising new security challenges. The emergence of new geopolitical issues and the intensification of natural disasters due to climate change are sources of concern for governments, including in Europe.

As observed in the report of ESA's High-level Advisory Group on accelerating the Use of Space in Europe, unprecedented safety and security challenges face Europe, characterised by unpredictability, rapid progress, and intensified impact, and require immediate response.

For these reasons, security is becoming once again a major focus for European governments and institutions. To handle these issues, enhancing the use of technologies to ensure safety and security of people and goods is being increasingly investigated.

In that context, space systems repeatedly demonstrated that they provide unique solutions, essential to respond to a variety of security challenges, from natural disasters, civil protection or maritime surveillance to unexpected global health crisis.

2.2.2 Space finds its way in national security strategies of European states but there is room for improvement

The national security strategies and related strategic documents of ESA member states display strong convergence in four specific areas.

Figure 1: Shared security priorities among ESA member states

First, by adopting **a whole-of-government approach**, states aim to streamline the coordination among both their domestic governmental agencies tasked with security missions and their different administrative levels (i.e. local, regional, and state-wide institutions).

Second, strategies advocate for an approach that emphasises **preventive mechanisms** to address their distinct security challenges more effectively. As a result, they express a strong interest in improving their information-gathering and surveillance capabilities.

Third, national strategies commonly emphasise the need for an **information- and data-driven approach** to security, while acknowledging that new threats manifested in digital and cyber spaces are increasingly significant. Most countries concur on the urgency of upgrading cybersecurity.

Finally, there is an extensive consensus on the importance of enhancing national security through **European and international cooperation** including in the framework of the European Union and of intergovernmental organisations such as the UN, NATO or OSCE.

These shared priorities can have an impact on the use of space and can also further benefit from greater uptake of space solutions. Space systems have repeatedly demonstrated that they provide unique solutions to support a variety of security missions, from monitoring to action. Although the singular added value of space solutions is now more broadly exploited by security users, **the emergence of new security challenges for Europe and the fast development of new space solutions are raising the stakes for both space and security stakeholders to ensure that space can support security missions to its full potential.**

ESA member states address space in different ways in their respective national security strategies. **Most national security strategies address space** along one or both of the following priorities:

- **Space as an infrastructure to protect:** guarantee freedom of access to space and ensure the security and safety of space systems for the uninterrupted provision of space capabilities.
- **Space as an enabler of security missions**: ensure that space systems can effectively support the conduct of security missions on Earth. Target security missions identified in national strategies encompass disaster management and humanitarian emergencies, development policies, and the protection of the environment and its natural resources.

Around a third of ESA member states does not mention yet the space domain in their national security strategy. Unsurprisingly, most of these states have limited national space capabilities.

On the other hand, the majority of ESA member states' space strategies overlooks the role of space systems in support of security missions on Earth. Space strategies of most ESA countries focus predominantly on socio-economic benefits. The security dimension is often addressed in terms of protection of space systems from threats, e.g. space debris and space weather. Some countries (i.e., Denmark, Finland, Norway, Portugal, and Sweden) explicitly list security areas where they intend to scale up the use of satellites, which often include environmental security or emergency management.

2.2.3 EU and ESA: the link between space and security increasingly addressed through policies, programmes and other initiatives

In the EU-ESA Joint Statement signed in 2016, both organisations assert that, by 2030, Europe should be able to fully benefit from its space solutions to implement its policies and strengthen its security. One of the means to reach this goal is to "strengthen synergies between civilian and security activities of space". The new Financial Framework Partnership Agreement (FFPA), signed in June 2021 between the European Commission, ESA and EUSPA, provides the basis for a reinforced relationship for the next seven years.

European Union: Security an essential rationale for all the components of EU Space Programme

The EU has, over the past decades, increasingly focused on security challenges, and its member states have recently also equipped it with new instruments to intervene in the security domain. The strong relationship between space and security has been highlighted at various occasions. The 2016 EU Global Strategy, 2016 Space Strategy for Europe, as well as the new EU Space Programme Regulation (2021-2027), clearly stress the role of space systems for Union's security and call for further development.

It is worth noting that all components of the EU Space Programme have a security dimension:

- GALILEO, which provides PNT signals for a variety of applications including security ones, in particular through the Search and Rescue Service and the Public Regulated Service;
- EGNOS, which enhances the reliability and accuracy of GNSS signals for safety critical applications;
- COPERNICUS, which provides broad Earth Observation capabilities including the Security Service and the Emergency Management Service;
- GOVSATCOM, which aims at providing secure communications for security and safety critical missions and operations.
- SSA, which fosters greater knowledge of the space operational environment to support safety and security of European space infrastructure

European Space Agency: expanding involvement in Space for Security building upon long heritage

On ESA side, the relevance of space for security is a topic that has been increasingly acknowledged. The Agency emphasises the utility of space systems to tackle global challenges on Earth like natural disasters, food shortages, migration or competition over limited resources as these systems allow to better understand and react to these challenges through fast and up-to-date data, and to keep emergency services, decision-makers and other stakeholders informed, connected and secure.

ESA is a central actor of the development and implementation of these programmes, including for security-related requirements. The ESPI review of the contemporary ESA involvement in the realm of security showed that ESA is involved in 127 current and planned projects of different types and size that are related to security.[2] The security dimension of ESA activities has also profoundly evolved over recent

[2] Includes projects that have been concluded, ongoing, or planned between December 2019 (following the 2019 ESA Council at Ministerial level) and July 2021.

years. Figure 2 on the following page illustrates a few important milestones. Observations could be made concerning the evolution of the security dimension at ESA level:

- First, regarding the role of ESA in supporting security missions on Earth: The gradual involvement and contribution of ESA to the development of space solutions in support of safety- and security-related objectives culminated during the 2019 Council at Ministerial level (Space19+) with the adoption of a Safety and Security pillar for the Agency including substantial commitments to "Safety and Security Applications". Among other programmes, Member States committed €207 million to the Space Systems for Safety and Security (4S) Strategic Programme Line within the ARTES programme.
- Second, regarding the capacity of ESA to conduct security-related activities: ESA has taken several steps and measures to conduct security related projects and programmes and to reinforce the security of its own activities, including its ability to receive, store, and produce classified information, and to exchange classified information with third parties.

"Develop space for safety and security" is one of the top five priorities outlined in the ESA Agenda 2025 presented by ESA Director General, Josef Aschbacher in April 2021. The Agency seeks to give further impetus to the Agency's safety and security pillar, with the objective to contribute to the European effort to tackle new challenges.

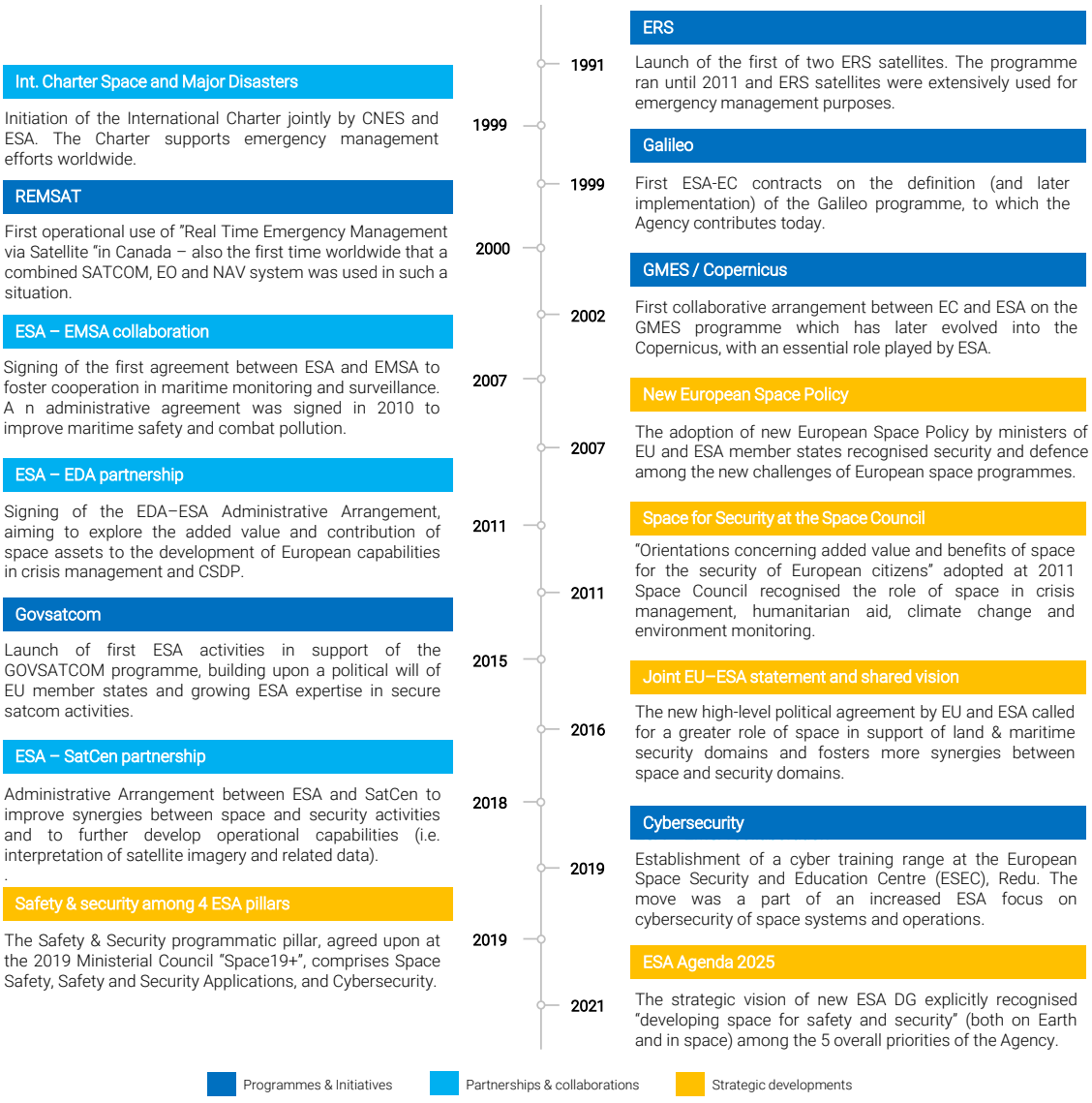


Figure 2: Timeline of the progressive ESA involvement with security issues

3 How can space support security missions?

European states, EU and ESA increasingly connect the domains of space and security. The unique added value that space systems provide to support security missions is one explanation behind this trend.

3.1 Operational space systems and services

Space systems and applications can provide great value to organisations in the security domain and support a variety of security missions especially through three main applications domains:

Earth Observation (EO)

Remote sensing satellites observe the Earth, be it individually or in a constellation. The majority of EO satellites is located in LEO (with the notable exception of meteorological satellites). Equipped with optical or other types of sensors (e.g. synthetic aperture radar), remote sensing satellites generate vast volumes of data, which are further processed and usually translated into analytical products. The main features determining capabilities of remote sensing satellites are: spatial resolution (measure of the smallest object that can be resolved by the sensor), spectral resolution (how many spectral bands the sensor can capture) and temporal resolution (revisit rate of a given location).

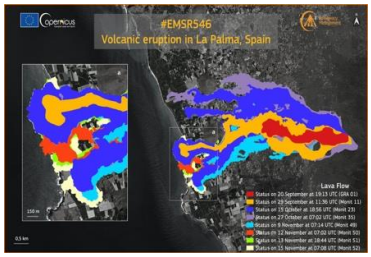
Satellite Communications (SATCOM)

Communication satellites relay and amplify radio or microwave signals, creating a link between a source transmitter and a receiver at different locations on Earth. The type of the communication link can vary (one-to-one, one-to-many, many-to-one, broadcast). Communication satellites can operate independently or as part of a constellation and could be positioned on various orbits (LEO, MEO, GEO, elliptical), with each providing unique features. From a user standpoint, bandwidth, coverage and latency are the main features. Characteristics of user terminals also vary according to the particular needs.

Positioning, Navigation and Timing (PNT)

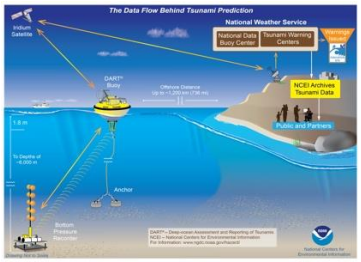
PNT systems use constellations of MEO and/or GEO satellites to provide geospatial positioning and time synchronisation. Utilising small receivers, navigation satellites determine their location (longitude, latitude, and altitude) to high precision (up to a few centimetres) using time signals transmitted along a radio line of sight from satellites. PNT systems always operate as part of a constellation. System design allows for global or regional PNT systems, common are also satellite-based augmentation systems. End-user receivers take various forms, including integration into portable electronic devices.

Examples of security-enabled applications of EO, SATCOM and PNT satellite infrastructures



EO: Assessment of volcanic eruption through EU's Copernicus Programme (Credit: Copernicus EMS)

SATCOM: Deployment of emergency communications infrastructure in a disaster-struck region (Credit: Eutelsat)



PNT: Nautical buoys with PNT receivers to provide tsunami early warning capability (Credit: NOAA)

3.2 Integration: an increasingly relevant concept

Benefitting from a space-based service is evolving into a more complex phenomenon, increasingly revolving around the concept of integration. There are two distinctive dimensions of how space is becoming increasingly integrated:

1. Through development and implementation of Integrated Applications

Space-based services gain added value when they are integrated with other space or terrestrial services.

Users, both from the security domain and beyond, are increasingly interested in getting a "full package" of services, which is created through the combination of multiple space-based services (that are required to meet the mission). For instance, border surveillance can simultaneously make use of space-based Earth Observation data for enhanced situational awareness and of SATCOM links to keep control over patrol drones in locations where radio transmission would be complex.

Additionally, terrestrial means (telecommunication infrastructures, aerial or ground-based sources of data…) provide benefits that are similar or complementary to those enabled by space capabilities. To prevent unnecessary duplication, foster synergies and increase efficiency, space-based and terrestrial services data are more and more used together to conduct missions or produce information.

2. Through integration of space-based services into the user's environment

Users increasingly demand that space-based services be straightforward to exploit and to integrate with components of the technical and operational environment, in order to maximise their potential.

This can for instance be achieved through the establishment of standards or standardised products. This request for integration is particularly true for the security community, which often operates on a short notice. Yet, particularities of each actor regarding its mission, staff, processes or equipment make the conditions of integrating space services subject to unique settings.

Moreover, an additional way to further integration is to promote the interactivity of the services provided to users of space systems. In this sense, the end-user should have the possibility to easily select the layer of information that it needs for its purposes and to create its own tailor-made product. To reach this goal, access to the relevant information or to the necessary software is required, as well as correct training of the end-user in the manipulation of these tools.

Eventually, the path through which space systems contribute to security missions, either independently or through an integrated approach, can be described as follows:

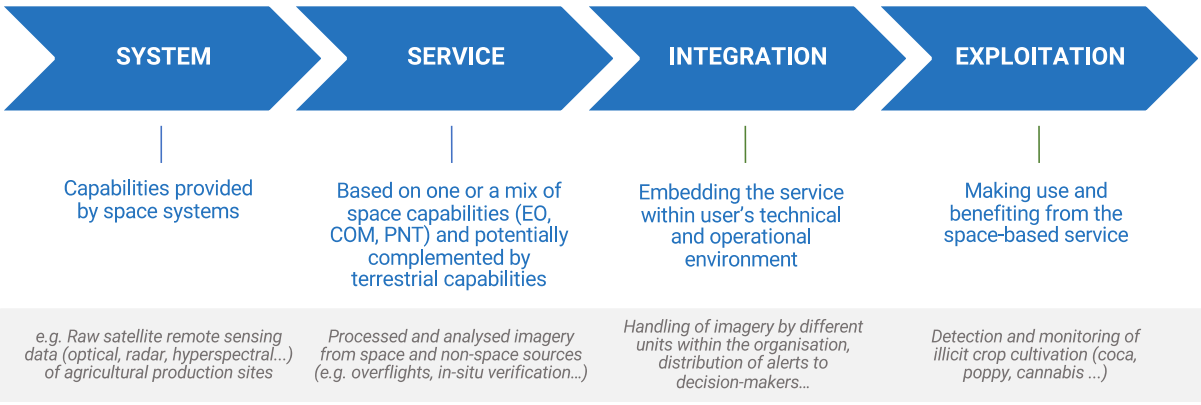


Figure 3: "Space for Security" simplified value chain

3.3 25 concrete use cases of "Space for Security": identifying the added value of space solutions in support of security missions

The wide scope of the concept of security translates into a rather diverse set of security missions, easily unique in nature and different from each other. As explained above, services enabled by the exploitation of space capabilities contribute to fulfilling these particular missions.

To illustrate the diversity and complexity of mission needs of security actors, and better understand the way space services meet needs of users from the security community, the research team identified and assessed 25 unique use cases. The examples are categorised according to the type of application used.

A description of each use case can be found in Annex A.

Earth Observation	1. Acquisition of credible insight for anticipation and reaction to upcoming security challenges 2. Unbiased assessment of illegal activities 3. Continuous monitoring of a fixed geographical site 4. Extension of situational awareness in areas where access is denied 5. Evidence for human rights violations in international court trials 6. Mitigating negative impacts of droughts on food security 7. Enhancement of environmental monitoring 8. Support to disaster management in adverse weather conditions 9. Early warning of dangerous land subsidence threatening the functioning of critical infrastructure
Satellite communications	10. Extension of coverage of border patrol drones 11. Rapid provision of connectivity in emergency management 12. Maintenance of trusted communication link for external action 13. Coordination of governmental authorities and national security systems 14. Permanent country-wide communications network for civil protection 15. Early warning of upcoming tsunamis 16. Emergency broadcast of warning messages to the public
Positioning, Navigation and Timing	17. Precise localisation of people in distress 18. Enhancement of emergency management activities 19. Improvement of law offenders' surveillance 20. Enhancement of firefighters' safety during operations 21. A source of evidence in court procedures 22. Surveillance system for the detection of natural disasters
Integrated Applications	23. Reduction of illegal poaching of protected wildlife species 24. Remediation of health crises outbreak 25. Prevention and control of wildfires

Table 2: 25 investigated use cases of "Space for Security"

Space systems and services are thus used for a variety of purposes in the security domain. The usefulness of space can also be demonstrated by several very recent safety and security-related events in Europe, which all involved deployment of space-based assets for functions ranging from detection of damage, continuous monitoring of situation up to support to first response. The events include, e.g.:

- Outbreak of the COVID-19 pandemic in early 2020 and its impacts on, public health, mobility, economic production, cybercrime, etc.
- Large-scale flash floods in Germany in July 2021
- Volcanic eruption on Spanish island La Palma during late months of 2021
- Massive migration waves on Polish-Belarussian border in late 2021

The particular utility of space may be explained by the advantages provided by space systems over other alternative technological solutions. More precisely, six of them have been identified in the examination of the use cases above: coverage, availability, cost-effectiveness, precision, threat mitigation and speed.

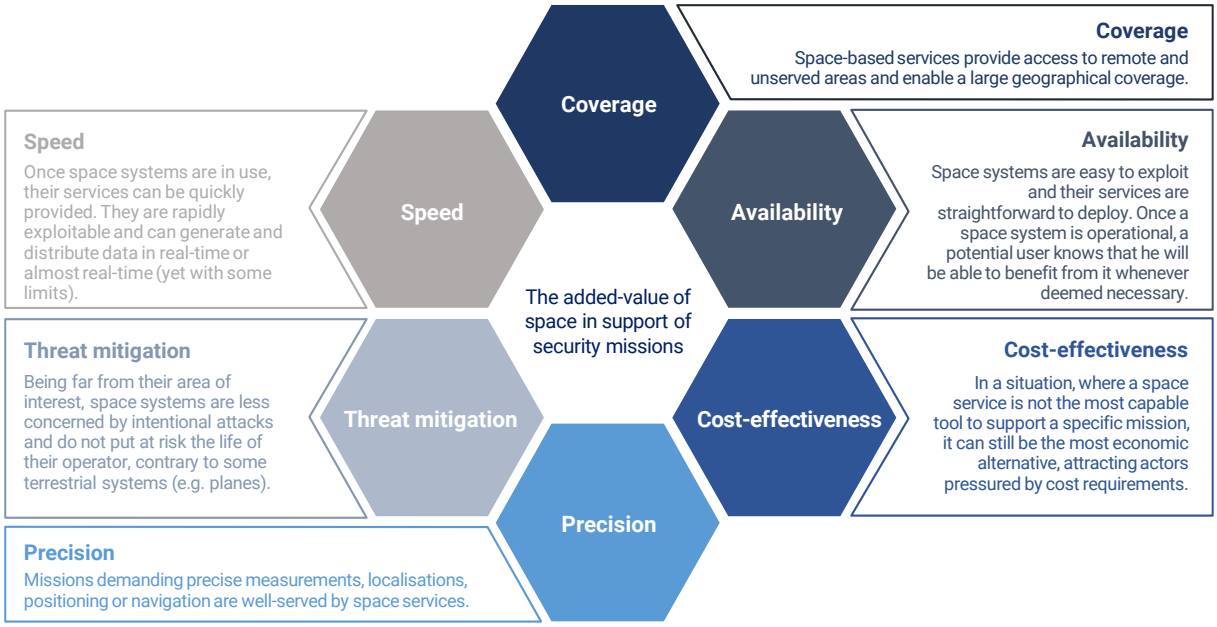


Figure 4: The added value of space in support of security missions

These advantages are not all exhibited during one given use case; instead, it is more common to observe that one or a combination of a few advantages is at play.

All in all, space often offers a unique value proposition and appears therefore as an enabling factor, allowing to perform security missions that could not be carried out otherwise. A few examples include:

- Provision of comprehensive situational awareness over vast geographical areas
- Monitoring of dangerous or otherwise inaccessible locations
- Transmission of data from remote sensors to provide early warning on natural and man-made risks
- Continuity of data exchange between an RPAS / plane and the ground, even beyond radio line-of-sight

Moreover, to exploit their potential at best, space data are increasingly integrated with data from other sources (e.g. other types of sensors, open source data, social networks…) to create broader sets of data providing a more complete picture of a situation or to provide a service in a more efficient way.

4 SPOTLIGHT ON USERS' PERSPECTIVES

During the research, an extensive consultation campaign involved dedicated interviews with 50 unique operational actors from the security field to assess the operational practices of security actors regarding the use of space solutions to support their missions. In particular, this exercise aimed to:

- Identify outstanding user needs and requirements of organisations tasked with security missions
- Investigate difficulties, challenges and limitations that users from the security community face

The organisations interviewed are involved in a broad range of security missions spanning across the three categories in the scope of this report (i.e. law enforcement, emergency management, civil security). The sample of 50 interviews involved the following types of organisations:

- National authorities from ESA member states tasked with security missions
- EU institutions and agencies
- International organisations and initiatives, including but not limited to UN entities
- International NGOs

4.1 Security users: a broad and heterogeneous community

Organisations tasked with security missions do not form a homogeneous community. The realm of security includes a variety of actors such as police forces, firefighters, customs, coast guards, justice organisations, maritime agencies, emergency rescue teams, medical assistance services, etc. These actors are involved at different levels of security missions, including teams conducting field operations as well as headquarters and coordination centres.

Even within the limited scope of security in this study, the spectrum of security missions is extensive, ranging from border control, maritime surveillance and disarmament process monitoring to search and rescue, forest fires management and infrastructure protection. The heterogeneity of national security communities makes it difficult to identify and single out specific common needs across all organisations.

The experience of security actors with space varies greatly both in terms of use of space technologies and awareness of the potential benefits of space solutions for security missions: some have gained an extensive experience in exploiting space for their routine activities over multiple years, while others are only starting to explore a possible acquisition of space services.

The role of organisations in the security domain also impacts their perception and knowledge of space systems and services. Two categories can be identified:

- End users: organisations using space services themselves for their own purposes.
- Brokers: organisations serving as intermediaries that process / enhance / distribute space solutions to their security user community.

Due to their activities, representatives of the latter type are often more experienced and aware of the added value of space systems. Their expertise is also valuable to end users, who are often indifferent to the technologies used to achieve their missions. In addition, brokers can potentially expand the use of space to a broader range of operational actors.

Finally, operational actors are generally open to exploring new technical solutions in support of their missions. This creates a window of opportunity for space actors to increase engagement and better demonstrate the utility of space technologies, data and services to users, which have not yet embraced space in their operational practices.

4.2 Security users seek new tailored capabilities rather than enhanced security features

The identification and assessment of user requirements was performed with each organisation individually. The user needs and requirements were classified into three overarching categories, themselves broken down into several subcategories:

- Functional needs and requirements, covering performance and associated functionality features of space-based systems. This category includes user needs and requirements related to:
  - Increased performance
  - New capabilities
- Security needs and requirements, encompassing the necessary security characteristics of the services provided. This category includes user needs and requirements related to:
  - Confidentiality
  - Integrity
  - Availability
  - Reliability
  - Resilience
- Usage needs and requirements, describing the integration of space-based services into the user's technical and operational environments. This category includes user needs and requirements related to:
  - Simplicity of use
  - Flexibility
  - Ease of access
  - Interaction
  - Cost-effectiveness
  - Education and Training

The detailed definitions of these categories are provided in Annex B. The Figures 7 and 8 below provides the overall findings and detailed overview concerning the assessment of user needs.

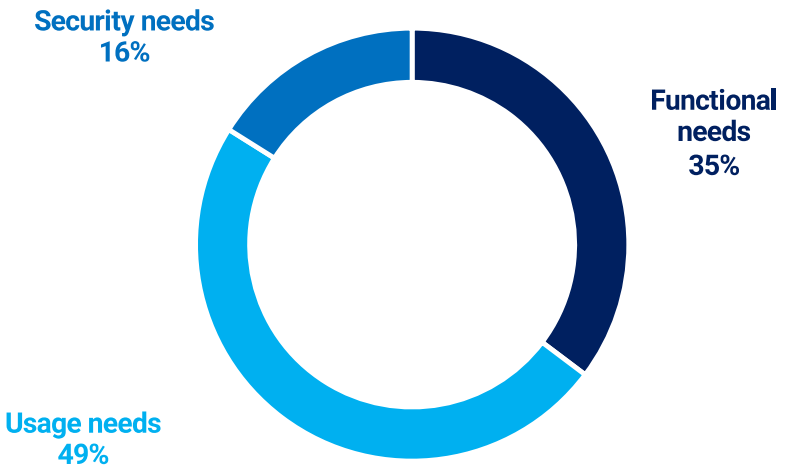


Figure 5: High-level breakdown of user needs and requirements of space users from the security community

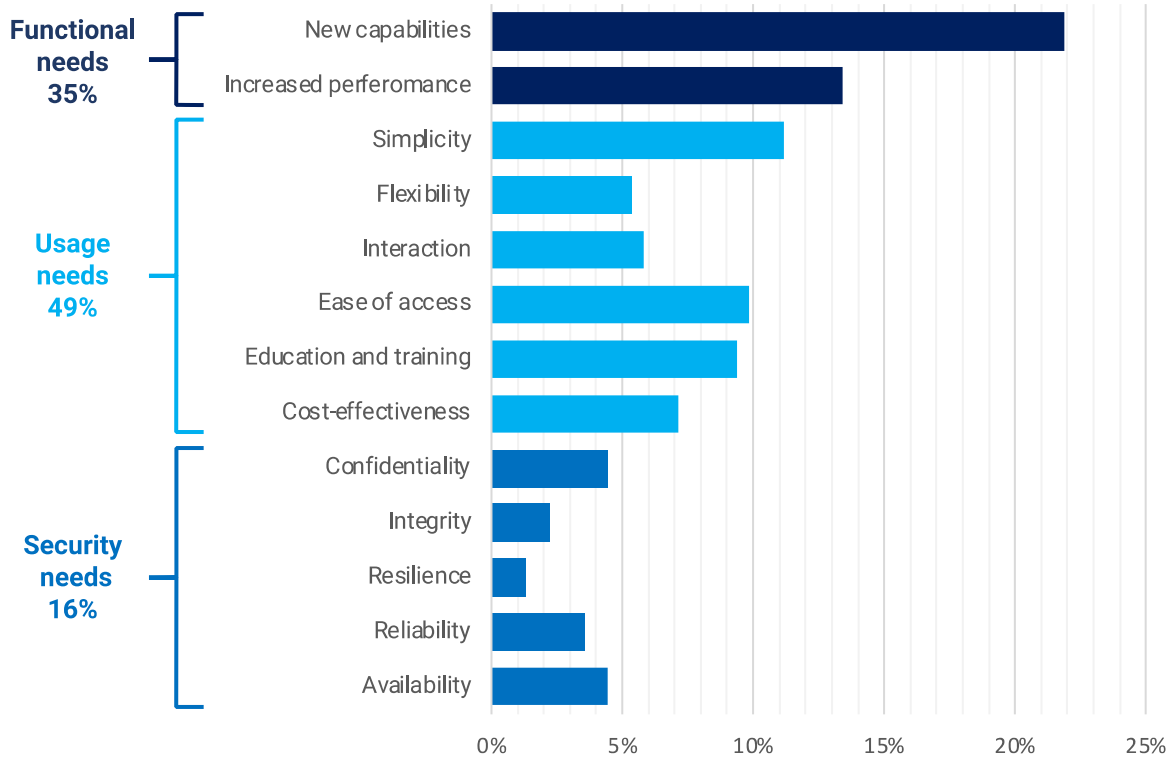


Figure 6: Detailed breakdown of user needs and requirements of space users from the security community

At operational level, security users are often technology-neutral – not expressing any particular preference for technological solutions used, as long as the information or service they need is provided. However, interviewees often particularly recognised that space will be increasingly important for their missions.

Important to note, capabilities and services enabled by space systems are also often provided by other "non-space" technologies. While offering synergies, some users would also consider these **non-space solutions as strong alternative solutions** to satellites.

In this situation, the user-driven approach pursued by space actors will be an important criterion conditioning greater uptake of space data, technologies and services by users from the security community. This need for a user-focused engagement has two underlying considerations:

- Space systems and services need to be **better adapted to meet user needs** and requirements of security actors,
- The uptake of space solutions in the security domain is hindered by **various barriers to adoption** related to security users' awareness or technical competences among others.

For what concerns user needs, the consultation with operational actors highlighted three major findings:

- Users from the security community mainly **seek new adapted and improved capabilities** to support their missions
- These capabilities should also be **easy to access, intuitive to use and readily integrable** in their operational environments
- Needs and requirements for security features (confidentiality, resilience, availability, etc.) are **not the main concern**

4.2.1 Detailed assessment of security stakeholders' needs and requirements

Increased performance

Because of the predominant use of satellite imagery over other space-based services in the consultation group, operational actors tend to focus on improving the spatial resolution of EO data. In particular, crime agencies and disaster management organisations require access to Very High Resolution (VHR) imagery for space to be really useful for their missions. This request for higher resolution is clear for optical imagery and is sometimes expressed with regards to radar technology.

Search and rescue organisations also note that obtaining satellite imagery in near-real time would improve their ability to rescue people in distress. Near-real time capabilities (particularly in the framework of the Copernicus Services) could be achieved through higher temporal resolution (i.e. higher revisit times) and/or faster delivery rates of EO data.[3]

> **Note: Ground truthing**
>
> In Law Enforcement, Earth observation is rarely used alone; ground truthing is almost always carried out to confirm the reliability of the image and the correctness of its interpretation. Law enforcement organisations are also keen on using satellite imagery for "tipping and cueing": a satellite with coarser resolution is used to detect "hot spots" on large areas; then a higher resolution system is used to get valuable information over the areas of interest.

New capabilities

While the improvement of current capabilities is important, some organisations also want to adopt space-based systems or services that they are not currently using. Here, there is a clear pattern among search and rescue organisations, which want to use new services related to satellite communications. Bidirectional communication links to better contextualise the situation of people in distress and the use of satellite communication systems to enable the storage of information in cloud services are amongst the requirements declared by such organisations.

There is also an interest in gaining access to different technologies related to Earth Observation, including satellites with hyperspectral resolution, Remotely Piloted Aircraft Systems (RPAS) and High-Altitude Pseudo-Satellites (HAPS). Finally, some operational actors want to improve the exploitation of available data by employing Artificial Intelligence and machine learning algorithms, or by creating a digital platform that enables the combination of different datasets.

Simplicity

Several organisations do not have in-house expertise to analyse raw satellite imagery, and therefore require EO products that include both data and their analysis. Similarly, it is requested that these products be easily integrated into the users' operational procedures, including by providing an appropriate format for the processed EO data. Crime agencies and disaster management organisations frequently cite this requirement as important.

Moreover, to enhance the simplicity of use, some organisations are interested in the integration of various space services. Although this need is not widely expressed through the consultation group, the combination of various space services appears as a high-potential solution to ensure the simplicity of use.

[3] The issue of speed can affect two dimensions: the time needed from the acquisition of imagery to the delivery of the service; and, before that, the delay required between the request time and the acquisition of imagery.

Flexibility

Satellite-based services should be tailored to the needs and requirements of operational actors. This characteristic is largely mentioned by crime and law enforcement agencies. Thus, it is argued that providers should take into account the heterogeneity of law enforcement tasks when offering their services. For instance, a border police agency noted that while the EUROSUR's Fusion Services are specialised in maritime surveillance, they are not as effective for land border surveillance.

Ease of access

The timespan between the activation of the request for EO data and the reception of the subsequent product is often too long, especially when using the Copernicus Services, thus leading to numerous calls for a quicker delivery time. Because of that, several organisations argue that Copernicus is not well prepared to address emergency scenarios. Indeed, organisations covering search and rescue missions or tasked with disaster management functions emphasise that if the delivery time of satellite imagery were faster, they could expand the use of space-based systems for time-sensitive missions.

Education & training

Limited awareness at the operational level on the potential benefits of, and on access to, satellite-related services represents an obstacle for security users to increase their uptake of these services. As a result, several operational actors call upon the space community to engage with security actors so that the latter can progressively integrate space-based services into their operational domain. This engagement can be translated into workshops and *fora* whereby space actors demonstrate how satellites can contribute to fulfilling the needs of security stakeholders. Specifically, the points of interest for the users are:

- Who are the relevant points of contact to get information on what the space sector can offer?
- What are the benefits of space systems for their work?
- How can they get access to space-based data and services?
- How can this data be used?

This requirement is particularly widespread across crime agencies and organisations working on disaster management.

Cost-effectiveness

Limited budgets may prevent a greater use of space-based systems among the national security communities. As such, many operational actors request services that can provide added value for their missions while maintaining financial expenses under control.

Organisations dealing with search and rescue operations and those that aim to enhance security and safety in the maritime domain are particularly sensitive to using cost-effective services. In the former case, the emphasis is on acquiring satellite communications services that are affordable, due to the price of the commercial solutions currently used. While other security organisations do not include financial considerations into their needs, it is noteworthy that the vast majority largely uses Copernicus services, which are free of charge.

Note: Importance of free and commercial sources

A non-negligible amount of users use commercially available and free sources to access space-based systems and services. For instance, the importance of Sentinel satellites was often raised, including by non-European users; yet, these satellites are mostly used as additional means, and not as the primary tool of investigation (at least in Law Enforcement, due to the need to "tip and cue"). This reliance on commercial and free services was particularly observed with those actors that are not national authorities, which is likely caused by the fact that they are not granted direct access to restricted (military or governmental) satellites.

Resilience

Ensuring that space-based systems are able to withstand and overcome (un)intentional interferences is important for a handful of organisations. In particular, enhancing the resilience of positioning, navigation, and timing (PNT) signals is important to guarantee maritime safety.

Confidentiality

The protection of satellite data against unauthorised access or theft by third parties is relevant both when referring to satellite imagery (not disseminating the data to everyone) and satellite communications. Thus, within the consultation group, there is an emphasis on secure communication links among units deployed on the field, or between these units and coordination centres.

Reliability

Some operational actors require a robust chain of custody to ensure that both the satellite service provider and the EO-based information can be trusted. This requirement is particularly acute among crime agencies, which often use satellite imagery as evidence during criminal investigations. As this evidence may be brought forward during judicial proceedings, satellite imagery must be reliable to be accepted.

4.3 The uptake of space solutions is hindered by various barriers to adoption

Organisations from the security domain often share common difficulties in the use of space in support of security missions. Overall, the consultation highlighted a few key limitations that could hinder a greater adoption of space-based services for operational purposes by actors from the security community.

Limited awareness

One of the major challenges for the further uptake of space-based solutions is the lack of knowledge of space capabilities and potential benefits for security missions.

Security end-users are frequently unaware of the significant contributions that satellites can provide to their missions. Even when they have sufficient awareness, as is the case for broker organisations for instance, security actors may have difficulties in identifying points of contact that could offer space-based services and provide details on the services' features.

In occasional cases, decision-makers or high-level policy stakeholders of the security field can also prove hesitant to invest in space-based capabilities because they are also not aware of their potential benefits or because administrative and political processes hinder the adoption of new technological solutions.

Unserved needs of actors from the security community

As demonstrated above, space solutions do not meet all functional and usage needs of security actors, which may curb their further adoption. In parallel, requirements on the security of space systems remain quite limited and are not considered as a priority.

There is a lack of readily available technical capabilities required to adopt, use and integrate new space solutions in routine security activities. For some users, the current technologies are not adapted and should be improved to really support them in their missions; other consider that new capabilities should be developed or put at their disposal.

Operational actors also express specific needs concerning the way they work with these tools. In particular, there is a strong call for improving the simplicity of use and access to space solutions, and for combining them with data and services from non-space technologies. These demands are particularly voiced by users with limited in-house expertise or awareness on the use and benefits of space solutions.

Lack of structured channels for the expression of space-related needs

In addition, security actors also have limited capacities, means and channels to express their needs towards the space sector and set up formal links with space organisations.

Expression of user needs and requirements is often realised through existing internal channels, with limited options for space actors to formally step in. These channels involve other units and departments that do not face or share the issues of operational actors, which may create some additional challenges for greater adoption of space solutions.

Availability of alternatives to space solutions

Occasionally, security actors argue that their countries have ground-based, aerial or other technical alternatives that decrease the relative value of using space-based systems and put the spotlight on the trade-off between the added-value of space solutions and the burden of adopting new technologies. For instance, these non-space alternatives could be:

- Aerial surveillance and reconnaissance, relying on crewed or uncrewed flights to provide remote sensing data
- In-situ data collection, relying on close-up observations and examination of the addressed issue
- Ground-based communication infrastructures, relying on cable-based (e.g. fibre) and mobile networks for two-way communication

In addition, terrestrial infrastructure for communication or remote sensing is of good quality in European states. As a consequence, operational actors from national organisations are less likely to use space systems to conduct their missions compared to actors operating in other parts of the world, where distances are greater and terrestrial network is less developed.

Limited financial resources

The size of the budget is a recurrent factor that influences the decision to invest on further space-based capabilities. In particular, the commercial acquisition of VHR imagery and of satellite communication services (including satellite phones) depends on the availability of financial resources.

This limitation and the previous ones are not mutually exclusive. For instance, limited awareness at the policy level can amplify the reluctance to allocate funds for space-related investments. Likewise, the perception that non-space-based systems provide sufficient value to conduct security missions may create additional obstacles to secure funding for satellite-related services.

5 SPACE AND SECURITY – EVOLVING LANDSCAPES

With major political and technological changes underway in both security and space domains, the use of space systems to support security missions is undeniably going to evolve in the next years.

5.1 Evolution of "Security" and security missions

The concept of "Security" is gradually evolving over time, reflecting on changes to the well-being of human population and on political, technological, economical and societal macro-trends. While difficult to predict, some probable developments could be pointed out.

First, one can wonder if the non-traditional dimensions of security will not become increasingly important compared to the classic dimension of "physical security". For instance, climate change will probably make food and environmental security take a bigger share of the missions conducted to ensure the security of people; similarly, the outbreak of pandemics put at the forefront public health and economic security. From another angle, with the ever-growing reliance of people on cyberspace, concerns related to cybersecurity and data protection will likely grow in magnitude.

Second, technology will influence the perception of the security concept as well as the development of new tools addressing security challenges. On the one hand, the evolution of technology will be the source of new types of threats. On the other hand, a greater uptake of technology to conduct security missions could be anticipated as it could facilitate the reactivity and effectiveness of security actors. For instance, more and more cities are adopting facial recognition systems to better ensure security in public spaces.

Moreover, the development of technology will lead to the increase of dual-use systems or applications, where military systems contribute to civil missions, including in the field of security, and where civil systems are used by military actors to conduct their operations.

In any case, the hereby addressed security missions, entailed within the boundaries of law enforcement, civil security and emergency management will likely endure as foundational missions underpinning the concept of security. The expected evolution of each of these missions is assessed below:

Law enforcement
• There will be an increase in cooperation between police and judicial forces, and with other communities (social workers, NGOs…). Law enforcement will gradually transform beyond the mere punishment of offences and be integrated within a broader effort of solving social problems. Its "coercive" dimension will be more and more accompanied by an "integrative" dimension. • More data is going to be collected and analysed, which will lead to outsourcing. Because of a lack of means and training, law enforcement authorities cannot collect and handle all the data and information that will be used. As a consequence, it is likely that this kind of activities will be outsourced to third parties, a situation which raises new questions. • An increased use of technology, especially in policing could be expected (e.g. social media, facial recognition, predictive policing, GPS applications towards the society, drones…), while maintaining the balance with the human dimension of the job will still be required. • More transparency and public visibility in the mission conduct will become necessary, engagement with civil society to justify the mission and the ways it is conducted will be more and more required. • As the law naturally evolves over time, it is possible to expect it will create new law enforcement missions and make others outdated.

Emergency Management
• There will be a change of the field in which interventions are conducted. With the growing urbanisation of the world, more and more operations will take place in cities, which have specific advantages and disadvantages for rescue teams. • The prevention phase will likely be reinforced, with a need for a better assessment of the interrelated consequences of events. An important feature of this is a sophisticated environmental scanning and research to understand the potential consequences of new and unfamiliar risks. • Increase of the use of social media in disaster management activities could be expected, to obtain more accurate information on the local conditions and better prepare the response to the emergency, be it in terms of resources or management of the operations. • Interoperability will grow in relevance, as well as asset-sharing among emergency teams. The number of countries and regions developing their own emergency management mechanisms has increased, thus multiplying the avenues for cooperation but also creating new challenges. • The rapprochement between civil and military actors in this domain will likely be questioned (not only for natural disasters, but also and especially to handle humanitarian crises in countries undergoing social or political crises)
Civil Security
• Adverse effects of climate change will adjust the environmental conditions of civil security missions. With deteriorating environments and weather conditions regularly reaching previously unimaginable extremes, missions and tools will require adaptation to these new realities. • Mission objectives will likely evolve also due to demographic changes, including large-scale societal movements. Demographic characteristics are dramatically changing (e.g. ageing, urbanisation, population growth outside Europe). These developments will lead to a new nature and new geographical distribution, and an increased demand for civil security missions. • Infrastructures to be monitored and secured will evolve. As the cyber domain takes greater prominence, there will not only be monitoring of the hardware (servers, cables…) but the insides of the cyberworld will increasingly have to be scrutinised.

Table 3: Anticipated Evolution of Security Missions

5.2 Evolution of "Space" and space services

One of the most striking trends characterising the evolution of the space sector is the steep increase in the number of actors – both public and private – capable of conducting space activities. The number of spacefaring countries has grown to a much wider group of countries, with diverse capabilities. The technology factors underpinning this profound change span across the space systems value chain. Space systems have benefitted from the miniaturisation of technologies, they are being built through mass production processes, commercial-off-the-shelf technologies are now used like in other industrial domains. Moreover, the integration of space systems with terrestrial systems is deepening.

The increased level of investment and intensification of worldwide space efforts by public and private stakeholders are directly linked to, and driven by, a more wide-ranging approach to space. Usually referred to as *New Space*, this term generally indicates a commercially driven approach to space, marked by ambitious undertakings aiming to capture space markets with innovative schemes and business models.

In this new ecosystem, private actors are playing a more prominent role, pursuing the eventual goal of conducting space business independently from governments.

For what concerns the practice of security actors, robust legacy systems (governmental or private), traditionally used to satisfy a variety of mission needs, continue to be operated and developed throughout the globe. Even though interest for them grows, new private commercial systems and services still encounter difficulties in meeting strict governmental or military requirements. However, at the same time, their proliferation noticeably expands the supply side. What is more, it is also the nature of the supply which is rapidly changing (e.g. offer of readily available commercial products, end-to-end solutions…).

The utilisation of space also brings about security concerns related to dependence on space infrastructures and to their vulnerabilities. Space has become ubiquitous to the daily life of citizens and essential to vital governmental missions.

The range of threats to space systems is proliferating, from unintentional to intentional threats. First, the multiplication of active spacecraft and debris greatly increases the risk of collisions especially in the Low Earth Orbit. Second, major space powers are developing anti-satellite assets capable of depriving their adversaries of the benefits of space. These intentional activities include physical and non-physical threats, especially cyberattacks, which can be as damaging as the destruction of a satellite. Integrity and availability of space systems are thus at risk.

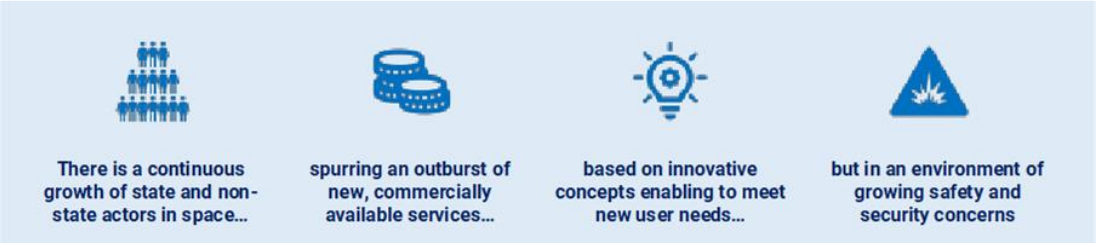


Figure 7: Ongoing evolution of the space sector

The three individual application domains – EO, SATCOM and PNT will continue to serve security missions. Currently, each domain is undergoing a transformation on its own.

Major developments in Earth Observation	The global EO market has been steadily growing both in terms of numbers of satellites launched every year and in terms of data generated and services offered. New technologies allow to obtain the same degree of precision with smaller spacecraft and sensors. SAR market is seemingly entering a major growth period. Providers also increasingly rely on distributed constellations of smaller satellites, which leads to unprecedented revisit rates and massive amounts of data, which calls for new data management approaches.
Major developments in satellite communications	The SATCOM sector is undergoing a major transformation, as market and technology forces converge, and newer technologies emerge. The geostationary (GEO) market is now at a crossroads with two main directions: larger satellites integrating maximum capacity (such as VHTS) and flexible reprogrammable satellites that are lighter and enable customers to adapt to evolving demands. The telecommunications non-GEO mega-constellation sector is swiftly developing with first projects already entering service provision stages. The increase in capacity translates into growing bandwidth and spectrum needs by different users.

Major developments in Positioning, Navigation and Timing	The PNT sector is facing a high level of dynamism, with a rapidly evolving global market for PNT technologies and services. Upstream developments continue to be led by public stakeholders, while downstream activities see a mounting engagement by several space and non-space industries. The gradual replacement of legacy systems with next-generation satellites and approaching full operational capability of Galileo improve the capabilities of available GNSS-enabled solutions. As GNSS become more widely used, the risk of hacking, jamming, spoofing has been steadily increasing and requires strong cybersecurity measures.

Table 4: Major global developments in EO, SATCOM and PNT

In sum, this complex evolution creates implications on the use of space systems, including in support of missions of actors in the security community:

Figure 8: Implications of the evolution of space on security missions

On top of that, there are also new developments outside the space sector, which provide alternative solutions to space for the provision of data, signals or communication links (e.g. High-Altitude Platform Stations supplying imagery and connectivity, or terrestrial fibre or wireless telecommunications providers reaching areas previously covered solely through space with novel connectivity concepts, such as 5G).

6 Conclusions and Way Forward

6.1 Security: an unavoidable dimension of modern space activities

The rapid evolution of the geopolitical, environmental and technological contexts is raising new security challenges, including in Europe. The recent wave of major crises and their dreadful consequences (economic, sanitary, terrorist, natural disasters, etc.) is raising concerns over Europe's actual resilience and preparedness to face these new security challenges.

Security has always been high on the political agenda of European governments and of the European Union but recent developments and expectations of a deterioration of the situation due to climate change and to a tense international and domestic context is putting security into sharper focus.

Security has evolved to become a broad and transversal domain requiring faster adaptation and closer cooperation at all levels. In this context, European countries pursue a whole-of-government approach to security building on international and European cooperation. To address new threats, governments seek to strengthen preventive mechanisms and to better integrate data and information in support of modern security measures and operations.

Even though Europe is progressing fast on these strategic goals, much remains to be done. At national level, responsibilities over security policy are spread and unevenly coordinated across multiple ministries and inter-ministerial bodies, which may hinder decision-making processes and intergovernmental cooperation. European cooperation has progressed considerably in recent years, including at political level through the European Union, but a whole-of-Europe approach to security is still far out of sight.

In its opening speech of the EDA Annual Conference in December 2020, Josep Borrell, High Representative of the Union for Foreign Affairs and Security Policy, recalled that "the time has come for Europeans to converge more broadly on the definition of what kind of security actor and security provider we want to be, and which are the sources of insecurity."

The national sovereign dimension of security continues to prevail and the European approach to security is still largely influenced by the history, culture, geography, policy, economy and international relations of each European state. Notwithstanding differences in national security strategies of European governments, many areas of shared interests and priorities exist, including for example:

- Terrorism & organised crime
- Illegal transnational migration
- Non-proliferation and disarmament
- International crisis management
- Maritime safety & security
- Critical infrastructure protection
- Securing strategic supplies
- Natural and man-made disaster management

Stakes are high in these European security priority areas. Actors must adapt to an operational landscape that is changing fast, marked by the emergence of new risks and threats that require the development and implementation of new methods and solutions. It is in this context that space-based applications, which repeatedly demonstrated that they provide unique solutions to respond to a variety of security challenges, are progressively adopted by a growing number of security actors in support of their missions.

It is also in this context that security needs and requirements are increasingly influencing the development of public space programmes and creating new market opportunities for commercial solutions.

The space infrastructure, including governmental and commercial systems, now directly or indirectly supports a broad range of security missions with different contributions across space application domains. In turn, the protection of the space infrastructure from accidental risks or deliberate attacks and the assurance of uninterrupted space services provision have become top priorities of space policy.

The relation between space and security has deepened and security has become an unavoidable dimension of modern space activities. The emergence of new security challenges and the (fast) development of new space solutions are however raising the stakes both for space and security stakeholders to ensure that space can support security missions to its full potential. Despite a growing interest from policy and operational actors to foster synergies between space and security, many challenges remain.

At policy level, space and security are still addressed independently in most European countries and governments have not yet developed a clear strategy and consistent action plan on this matter.

At operational level, even though the singular added value of space solutions is now more broadly understood and exploited in support of various security missions, the potential of space applications is still largely untapped due to various barriers to security users' adoption of space applications. Additional steps could also be taken in the space sector to better assess and address the quickly evolving needs of security users for the development of space programmes.

Better serving the needs of security users and driving adoption is essential to ensure that space can fully support European efforts to address security challenges but also to ensure that the development of security applications can become a driver of growth for the space sector.

6.2 Serving the needs of security users and driving adoption

The consultation campaign highlighted that policy and operational security stakeholders commonly foresee a growing role of space solutions and anticipate additional investments in space from security actors. However, they also report practical difficulties that create barriers to the uptake of space applications in the security domain including, among others:

- Unserved security users' needs, in particular regarding some functional and usage requirements
- Uneven awareness across security actors of space solutions and of their potential added value for security missions
- Lack of readily available technical capabilities required to adopt, use and integrate new space solutions in routine security activities
- Lack of structured channels toward the space sector to express needs, find appropriate solutions, get information/support, etc.
- Budget constraints making it difficult for organisations to bear, alone, the full costs of development or purchase of tailored space solutions

Lowering these barriers will be essential to accelerate the uptake of space applications and successfully enhance the role and contribution of space to address European security challenges. For the space sector, this will require to address three complementary and interrelated dimensions:

- Developing space technologies, systems and services that serve the quickly evolving needs of security users

- Driving the adoption of space solutions by a broader community of users and supporting the incorporation of space-based data and services in operational users' activities
- Fostering cooperation vertically and horizontally between all actors involved in the development and use of space solutions to promote synergies including to gather competencies and share costs

Although the transversality of security challenges calls for the elaboration of an overarching strategy and coordinated approach to issues at stake, the diversity of security actors and missions will hamper the development of one-size-fits-all solutions. An effective and efficient approach would therefore require focusing on verticals (e.g. border management, search and rescue, wildfire management, maritime safety) carefully selected on the basis of the following criteria:

- National interests: capacity to gather a community of countries sharing similar priorities and converging interests in the development of space solutions for the vertical.
- Relevance of space solutions: contribution of space solutions to address security challenges taking into account expected impacts and fitness with users' needs.
- Cooperation added value: benefits of cooperation in terms of technical needs, costs sharing, enlargement of user base, etc.
- Commercial potential: market opportunities for space solutions on the vertical.
- Complementarity: synergies between national and European activities and avoidance of duplication.

Working across these verticals will require an innovative approach with a sharp focus on creating and strengthening links: between national actors, between security users and space stakeholders, between early concepts and operational services and between technologies for integrated applications. As far as the space sector is concerned, this will entail to set up:

- A suitable framework of European space and security policy officials for decision-making
- An active two-way dialogue between security users and space stakeholders
- A coordination of activities between space application domains
- A framework for technology maturation from early concept to operational system/service

Ultimately, enhancing the role of space to address European security challenges is a matter of driving technological change, in this case the overall process of targeted innovation and diffusion of space technologies in the security domain. This requires addressing both drivers of technological change:

- Demand-pull mechanisms that stimulate the demand for space technologies (e.g. solution fitness, user experience, channels, price, etc.)
- Technology-push mechanisms that increase the supply of technological options by directing advances in R&D (e.g. exploration of new concepts, integrated applications, etc.)

Strengthening the link between these two drivers as part of a comprehensive user-oriented and technology-driven approach will be a key success factor in the endeavour of fostering the use of space solutions in support of security missions. The capacity to assess user needs and translate them into technical requirements and the capacity to anticipate potential security applications of space technologies are at the heart of this process.

ANNEXES

Annex A – List of 25 investigated use cases of "Space for Security"

Earth Observation

1. Acquisition of credible insight for anticipation and reaction to upcoming security challenges

In October 2015, Copernicus images provided the information that four rubber boats were leaving the coast of Libya. The Frontex International Coordination Centre, which was coordinating the operation TRITON, received their exact position and transmitted it to vessels taking part in the operation EUNAVFOR MED Sofia. The vessels arrived on site and saved the lives of 350 people.

2. Unbiased assessment of illegal activities

The United Nations Office on Drugs and Crime has been monitoring coca cultivation in Bolivia for several years. To this end, the Office used images from the Pléiades satellite with a resolution of 50 cm. The satellite images, combined with air and land field missions, and additional satellite imagery to complement the dataset (e.g. Sentinel imagery) allowed the UNODC, in cooperation with the Bolivian government, to get a precise idea of the situation over a sample area in order to extrapolate the quantity of coca cultivated in the country.

3. Continuous monitoring of a fixed geographical site

A refugee camp dedicated to the Rohingyas was built by the Bangladesh authorities on the Char Piya island, despite the dangerousness of this location. To monitor the construction of this camp, the EU Satellite Centre used imagery from the Copernicus' satellites Sentinel-1 and -2 acquired between 2017 and 2018. Automatic change detection algorithms were applied on Sentinel-1 images to better see the evolution of the situation. This information was then used to feed the EU CFSP

4. Extension of situational awareness in areas where access is denied

During the second seizure of Palmyra by the Islamic State (ISIS), and aware of the destructions that took place during the first one (already spotted by satellite), UNESCO requested UNOSAT to analyse the status of the cultural heritage site next to the city. The acquisition of satellite imagery from DigitalGlobe, dated from December 2016 and January 2017 and with a resolution of 50 cm, allowed the organisation to assess the damages perpetrated to the Roman Tetrapylon and to the Amphitheatre of the ancient city.

5. Evidence for human rights violations in international court trials

Satellite imagery was first used in international criminal proceedings during the Srebrenica trials at the International Criminal Tribunal for the former Yugoslavia (ICTY), providing evidence of mass executions of Bosnian Muslims in 1995, and eventually supporting the court procedure to prove guilt beyond reasonable doubt. The analysis of U.S. satellite imagery showed areas of freshly dug soil on the dates when executions were occurring. This led the prosecutors to identify locations suspected to contain mass graves, which were eventually confirmed by on-site investigations.

6. Mitigating negative impacts of droughts on food security

Since 2001, the Famine Early Warning Systems Network (FEWS NET), an international network funded by the U.S. Agency for International Development (USAID), has been monitoring crop performance and relative production using satellite-derived data and simulation models in Africa,

Central America, and central Asia, particularly where ground-based monitoring is limited because of a scarcity of weather stations. Within the network, 19 field offices work with U.S. government science agencies, national government ministries, international agencies, and NGOs to enhance monitoring of 28 of the world's most food-insecure countries. One of the main FEWS NET products, a vegetation index map of a given location (e.g. Africa), relies heavily on hyperspectral satellite imagery.

7. Enhancement of environmental monitoring

The detection and monitoring of oil spills with Synthetic Aperture Radar images have been an established method for several years. Oil slicks look very dark on SAR imagery as opposed to the ocean in the background. In Europe, the Joint Research Centre (JRC) of the European Commission has long been engaged in marine oil spill research with respect to European seas. Following R&D experiences, the European Maritime Safety Agency (EMSA) has launched the CleanSeaNet service, an operational service for the detection of oil spills, providing useful information, among others, for national coast guards to tackle maritime accidents or illegal discharges.

8. Support to disaster management in adverse weather conditions

In 2017, floods struck the areas of Montreal and Gatineau, in Canada. Thanks to the information provided by RADARSAT, the Canadian Armed Forces were able to monitor the rise of water despite unfavourable weather conditions. They could then better prepare they response, for instance by pre-positioning sand bags and pumps in critical and strategic locations where the water was migrating.

9. Early warning of dangerous land subsidence threatening the functioning of critical infrastructures

Since 2002, the Arizona Department of Water Resources (ADWR) has relied on an interferometric synthetic-aperture radar (InSAR) technique enabled by radar satellites (e.g. Sentinel-1, RadarSat-1 and -2, ALOS-1…) to determine the spatial extent, deformation rates, and time-series history of land subsidence features identified around the state. Late identification of land subsidence could lead to damages to water retention and retarding structures (dams, floodways, etc.), resulting in public safety hazards and economic losses. Around the world, other safety-related applications of InSAR, such as monitoring of transport infrastructure (railways, highways…) are increasingly explored.

Satellite Communications

10. Extension of coverage of border patrol drones

EMSA's service of Remotely Piloted Aircraft Systems (RPAS) is being used by the Spanish maritime safety agency SASEMAR in the southern province of Huelva for the purpose of identifying and monitoring oil spills as well as for additional assistance during search and rescue missions. The use of satellite communication links enables the RPAS – drones, to fly further from the coastline (line-of-sight connection sufficiently covered through VHF radio), giving them a greater geographical reach than radio line of sight operations.

11. Rapid provision of connectivity in emergency management

In the aftermath of the Hurricane Matthew in Haiti in 2016, satellite communications were used to provide rapid communications alternative for first humanitarian responders. The SES-developed "emergency.lu" service was deployed in close collaboration with the World Food Programme (WFP). To overcome potential overload or unavailability of communication networks, a dedicated SATCOM solution served to re-establish vital communication links in order to improve the effectiveness of rapid response efforts.

12. Maintenance of trusted communication link for external action

The EUs, in addition to foreign policy activities by its member states, is conducting an array of external action missions. These include more than 100 EU delegations around the globe, field offices of the Department for Humanitarian Aid and a number of civilian CSDP (Common Security and Defence Policy) missions often in risk-exposed locations. In this context, SATCOMs are vital for EU institutional communication as they allow quick decision-making through the exchange of information from any location, especially in high-risk areas. Each EU delegation or field office has at least one satellite link as a security back-up; SATCOM are also used in countries where terrestrial network are not reliable.

13. Coordination of governmental authorities and national security systems

During the outbreak of COVID-19 in Italy, coordination between political authorities and security actors occurred through the setting up of videoconferencing between personnel in the field in the affected "red zones" and the headquarters of the Presidency of the Council of Ministers in Rome. To respond to the increasing broadband need and to establish reliable communication, the Civil Protection Department and the Italian army used the services of Ovzon, a SATCOM provider. This service was used by people on the field, who had to move a lot, and was implemented in temporary buildings installed in areas where fixed infrastructure was unavailable or insufficient.

14. Permanent country-wide communications network for civil protection

In Spain, a satellite communications network (RECOSAT) has been operational since 2002 for the needs of civil protection. The ground segment consists of one central station in the Directorate General of Civil Protection and Emergencies and more than 50 stations around the country as well as remote stations mounted on vehicles. The objective of RECOSAT is to ensure the existence, in emergency situations, of a communications channel with the Coordination Centres of the affected areas with the goal to collect information, monitor the situation, coordinate response operations.

15. Early warning of upcoming tsunamis

In the USA, the NOAA-led Deep-ocean Assessment and Reporting of Tsunamis (DART) project, as part of the U.S. National Tsunami Hazard Mitigation Program (NTHMP), utilises a set of nautical buoys that are connected to an anchored seafloor bottom pressure recorder and equipped with a satellite link for relaying data to Tsunami Warning Centers (TWCs). The more advanced second generation, operational since 2008, has utilised Iridium LEO constellation (in contrast to GEO-based first generation), allowing for a more valuable two-way communication link between the buoys and TWCs.

16. Emergency broadcast of warning messages to the public

J-Alert is Japan's emergency broadcast system used to instantly and automatically disseminate emergency information from governmental authorities to the public via satellite (Superbird-B2 GEO satellite) and an array of equipment (nationwide loudspeakers, television, radio, email and cell broadcasts), in cases of natural disasters such as earthquakes, tsunami or floods, or attacks on Japan such as missile launches. The main stakeholders in J-Alert are the Fire and Disaster Management Agency and the Cabinet Office of Disaster Management.

Positioning, Navigation & Timing

17. Precise localisation of people in distress

In August 2017, during an overnight voyage from Madeira to mainland Portugal, a Belgian yacht collided with an unknown object. The damage caused a leak, putting the yacht at risk of sinking. The sailors

launched a life raft and sent a radio distress signal through the emergency radio alert present on the boat, which was detected by the EU constellation Galileo. Satellites enabled rescue teams in Portugal, Belgium and Morocco to get the boat's exact location to prepare their mission and to send a container ship nearby to save the passengers. The two sailors were brought to safety in less than five hours.

18. Enhancement of emergency management activities

Chinese authorities utilised the BeiDou satellite navigation system in handling the COVID-19 coronavirus crisis in early 2020. Equipment based on the BeiDou Navigation Satellite System (BDS) provided high-precision positioning service and accelerated the construction of emergency hospitals in the Wuhan region. Additionally, drones based on the BDS have been utilised to spray disinfectant and to transport supplies to medics in severely infected areas; support from satellites allowed them to accomplish their task with a centimetre-level precision. In addition, the Beidou constellation facilitated the creation of an app re-planning the travel route of its users so that they can avoid contagious areas.

19. Improvement of law offenders' surveillance

In 2019, the UK Ministry of Justice announced roll-out of dedicated GPS tags by justice and prison authorities to monitor people that serve their sentence outside of a prison. The tags will transmit an offender's location 24/7 to a specialist monitoring unit in Manchester. Among other uses, this form of location monitoring can be used to enforce an exclusion zone, to keep a given distance from a point or address or to monitor an offender's attendance at a certain activity – for example work or a rehabilitation programme.

20. Enhancement of firefighters' safety during operations

Acknowledging recent cases of firefighters' deaths in combating wildfires, in 2014, the Florida Forest Service (FFS) began utilising GPS in support of safety of firefighting operations. The FFS equipped frontline firefighters with GPS units that provide location points on supervisors' laptops. By using GPS tracking software, supervisors obtained the ability to know the location of each firefighter at any time, which greatly improved situational awareness and emergency decision-making. The GPS tracking programme does not require cell phone or Internet service, but instead relies on "packets" of data sent to supervisors' laptops provided they are within a two-mile range of the GPS units.

21. A source of evidence in court procedures

A 2015 study identified that the number of criminal or civil court cases involving GPS evidence has dramatically increased since the turn of millennium. While the admissibility of GPS evidence in court proceedings continues to face hurdles (constitutional constraints or potential human or technological errors), GPS evidence is nevertheless being introduced in a variety of criminal and civil cases. In a 2010 case at the Taiwanese Supreme Court, the defendant claimed that GPS evidence presented resulted from human error on the fishing vessels. The Court overruled this opinion and held that the map of the vessel's routes was based on the data received from the GPS system, which was processed and printed automatically without any human interaction.

22. Surveillance system for detection of natural disasters

In Italy, the Istituto Nazionale di Geofisica e Vulcanologia (INGV), aresearch institution, runs the Italian National Seismic Network and other networks at national scale for monitoring earthquakes and tsunami as a part of the National Civil Protection System coordinated RSN is composed of about 400 stations, mainly broadband, installed in the Country and in the surrounding regions; about 110 stations feature also co-located strong motion instruments, and about 180 have GPS receivers and belong to the National GPS network.

Integrated Applications

23. Reduction of illegal poaching of protected wildlife species

Different African countries have embarked on utilisation of various space-enabled services in combatting wildlife poaching. The practice has been long used, e.g. by Tanzanian authorities in country's national parks and natural reserves. GNSS-enabled animal collars have been used by the authorities in support of preservation of elephant population. The collar consists of a GPS receiver, a radio-modem for data communication, a non-volatile memory, and an independent VHF transmitter. Beyond this mission, GNSS-enabled telemetry from animal collars also allow for other application uses, such as scientific ones, e.g. to study migration routes of elephants and their behaviour. Another service, a SATCOM-enabled solution, has been used to directly identify suspicious movements in sensitive locations. A network of AI-enhanced cameras has been deployed throughout parks and reserves, with a satcom link (BGAN terminals using Inmarsat L-band network) to the operations centre, allowing for rapid detection of people and potentially illegal activity and thus enabling rapid initiation of law enforcement countermeasures. The Earth observation data has also turned out as valuable tool for Tanzanian authorities, which now make use of satellite imaging enhanced by AI tools as a viable method for tracking elephants.

24. Remediation of health crises outbreak

During the Ebola outbreak of 2014-2015, the World Health Organization deployed in Guinea the "Biological Light Fieldable laboratory for Emergencies" (B-LiFE), developed in the frame of ESA's Integrated Applications programme. B-LiFE integrates satellite communications, Earth observation and PNT capabilities with laboratories on the field. SATCOM enable the laboratory to be in direct contact with its home base and other stakeholders, and to transmit analytical results in real time; Earth observation technologies are useful to choose the site where the laboratory should be built and to monitor it during the operations as well as to create epidemiological maps; finally, PNT capabilities geolocate samples to analyse as well as teams on the field. In brief, all relevant information (i.e. medical, epidemiological, biological, etc.) is delivered in a timely manner to the right stakeholder, with accurate geo-location information and in a secured way through an autonomous and robust satellite communication system. During the COVID-19 outbreak, B-LiFE was also deployed in Italy to support the testing of frontline healthcare staff, civil protection volunteers and police forces. The satellite used at that time was GovSat-1, from Luxembourg.

25. Prevention and control of wildfires

Spanish national and regional governmental authorities tasked with preventing, mitigating and remediating the destructive force of wildfires have integrated EO, SATCOM and PNT in combatting large-scale forest fires in Andalusia, one of the southern regions of Spain prone to heatwaves and droughts increasing the wildfire hazard. In recent years, the EO-enabled Copernicus Emergency Management Service's European Forest Fire System has been regularly used for rapid provision of situational awareness and prognosis of worst-hit areas. More recently, INFOCA, the local Andalusian authority for forest fire prevention has begun deploying Globalstar satellite-enabled rugged, pocket-sized safety devices (messaging + GPS localisation) to provide 24/7 operational safety to firefighters in a potentially volatile environment.

Annex B – Definitions of 13 subcategories of user needs and requirements

Functional needs and requirements	
Increased performance	• Improvement of the capabilities to which the organisation already has access. The following dimensions can be highlighted, among others: ○ For EO: temporal, spatial and spectral resolution ○ For SATCOM: reduction of latency, increase of bandwidth… ○ For Navigation: increase in precision, in coverage…
New capabilities	• Getting access to systems and services that the organisation does not use currently or that may not exist at the moment
Security needs and requirements	
Confidentiality	• Protection of data and services against unintentional, unlawful, or unauthorised access, disclosure, or theft.
Integrity	• Maintenance, and assurance, of the accuracy and consistency of data over its entire life-cycle.
Resilience	• The system is able to withstand and overcome intentional or unintentional damaging effects, disruption or denial
Reliability	• The origin and quality of the service and data can be trusted
Availability	• Access to the service is critical and is guaranteed, for instance, but not only: ○ Through a permanent, persistent and all-weather capacity and the ability to monitor all kinds of environments (e.g. forests, deserts…) ○ Without impediment from other organisations' choices and priorities
Usage needs and requirements	
Simplicity	• The final product and/or service is easy to exploit (e.g. it is easily integrable into the user's operational environment or easy to understand by non-expert staff)
Flexibility	• The final product and/or service can adapt to users' requests and demands (e.g. need for a tailored service)
Interaction	• Refers to the contacts that the organisations have with its partners, such as: ○ Quality of the customer-provider relationship ○ Other cooperative arrangements
Ease of access	• Relates in particular to: ○ Speed of delivery ○ Accessibility of systems and services
Training and education	• Relates in particular to: ○ The training of people working with data coming from space systems (e.g. imagery analysts) ○ Awareness-raising of third parties (e.g. "customers" of imagery analysts) on the possibilities offered by space systems and on their limits
Cost-effectiveness	• Accessing enhanced capabilities at fixed cost or achieving improved value in comparison to the resources spent on the service

AUTHORS

Mathieu Bataille

Research Fellow, European Space Policy Institute, mathieu.bataille@espi.or.at

Tomas Hrozensky

Research Fellow, European Space Policy Institute, tomas.hrozensky@espi.or.at

Sebastien Moranta

Research Manager, European Space Policy Institute, sebastien.moranta@espi.or.at

Aleix Nadal Campos

Research Intern, European Space Policy Institute

About ESPI

Policy & Strategy

Economy & Business

Security & Defence

International & Legal

ESPI is the European think-tank for space. The Institute is a not-for-profit organization based in Vienna, World capital of space diplomacy, providing decision-makers with an informed view on mid to long-term issues relevant to Europe's space activities since 2003.

ESPI is supervised by a General Assembly of member organizations and supported by an Advisory Council of independent high-level experts.

ESPI fulfils its objectives through various multi-disciplinary research activities leading to the publication of books, reports, papers, articles, executive briefs, proceedings and position papers, and to the organisation of conferences and events including the annual ESPI Autumn Conference.

Who we are	What we do
Independent think-tank specialised in space policy	Research and analysis on major space policy issues
Multinational team with interdisciplinary expertise	Monitoring of global space trends and policy developments
Part of a network of European and international partners	Organization of thematic conferences and workshops

Download our reports, check our events and subscribe to our newsletter online

www.espi.or.at

Schwarzenbergplatz 6 | A-1030 Vienna, Austria | (Entrance: Zaunergasse 1)
Phone +43 1 718 11 18 - 0 | E-Mail: office@espi.or.at

www.espi.or.at