IMPLEMENTATION OF THE EU SPACE STRATEGY FOR SECURITY AND DEFENCE – RECOMMENDATIONS FROM EUROSPACE

FROM A MAJOR & POSITIVE POLITICAL INITIATIVE TO IMPACTFUL PROGRAMMES FOR EUROPE

PREAMBLE

On March 10th 2023, the European Commission (EC) and the High Representative of the Union for Foreign Affairs and Security Policy published the Joint Communication "EU Space strategy for Security & Defence"[1].

The purpose of the European Union (EU) Strategy for Security & Defence is to find the right balance between continuing to preserve a safe and secure environment and the peaceful use of outer space, and enhancing the strategic posture and autonomy of the EU in this strategic domain.

Only two months after its publication, the European space industry, represented by Eurospace, published its official reaction to the Strategy in its Reaction Paper[2] published on May 15th 2023.

In a context where the Strategy will lead the way to new programmes and activities, the European space industry wishes to express recommendations for its implementation.

Indeed, the Strategy will have a **strong incidence on industry activities as well as on the activities of our European customers** - agencies and operators -, not only because of new needs for capabilities or space-based services, but also because of new requirements and constraints.

It is of key importance that the implementation of the Strategy shall be based on an adequate level of resources, both in terms of available funding and a technically competent workforce within institutions to be able to elaborate, manage and monitor the new requirements.

SUMMARY OF RECOMMENDATIONS

Cybersecurity

- **Prepare**:
  - **Complement the recognition of the entire space sector as a sector of high criticality** (i.e., including operators but also ground and space suppliers) either in the **NIS2 Directive**[3] itself (already covering operators) or in a complementary regulation, also addressing EU-owned assets;
  - Provide a clear **definition of** "**resilience**" in a space context and of "**maintenance in security conditions**[4]", to be included in the EU Space Law;
  - Ensure **seamless continuity of compliance with security requirements, regulations and certifications** while transitioning from the development to the end of life (including design and build, launch, operate & maintain, end of life).
- **Protect**:
  - Protect the ground and space systems from **electronic attacks** and **cyber-attacks** (i.e., cyber-electronic warfare) that are generated by ground and/or space entities. Such protection shall be achieved by cooperating and mutually complementing passive capability;
  - Protect the **ground-to-space command link, space-to-ground telemetry link and any cross-links** (uplink & downlink) by deploying protected waveforms and, whenever feasible and cost-effective, exploiting optical links;

[1] https://ec.europa.eu/transparency/documents-register/detail?ref=JOIN(2023)9&lang=en
[2] https://eurospace.org/eurospace-reaction-paper-eu-space-strategy-for-security-defence/
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555
[4] *Maintenance in Security Condition is composed of 4 main activities: Curative maintenance (Problem Management & Vulnerability Management), Defensive maintenance (Crisis management, Security Monitoring), Routine preventive maintenance (Patch policy / on-going arising vulnerabilities management, Obsolescence & cybersecurity management without design impact), Preventive Major maintenance (Obsolescence & cybersecurity management with design impact)*

    - Build a robust **strategy for cryptography key management** (if key management is inadequate or if the keys are compromised, encryption becomes less effective in providing protection), including Quantum Key Distribution (QKD) according to technical and regulatory timeframes;
    - On top of the ICT network, **protect the industrial supply and development chains** from compromise;
    - Ensure availability of all crucial competences for development & recovery.
- **Secure**:
    - Prepare for anomalies through planning and practice;
    - All stakeholders in the value chain, starting with the customer, need to ensure **secure software development procedures** (by collaborating throughout the software development lifecycle to proactively identify and mitigate security risks, but also following security standard and doing security validation and testing), following the principle of security by design;
    - Include **cybersecurity on-board all satellites** to ensure proper detection, recovery, and response to the related intentional (and not-intentional) threats. This is achieved by establishing and applying cybersecurity criteria that relate to the satellite characteristics (including customer(s)) and the consequences (risk likelihood and resulting impact) of a cybersecurity attack. For legacy satellites, due to the high costs and difficulty to update on-board, it is really important to be able to have a realistic view of the attack surface and the obsolescence to manage the risk on a case by case basis;
    - Ensure that a space or ground system is **not put in service without appropriate plans to ensure operation in security conditions** to prevent cyber risk to space or ground asset and ensure resilience of services;
    - Ensure **appropriate budgeting for cybersecurity (including R&D) and associated maintenance in security conditions** in line with the asset cybersecurity scope (i.e., benchmark indicates maintenance of critical operational system is around 10% Capex/year).

EU Space ISAC

- Support the creation of the **EU Space Information Sharing and Analysis Centre (ISAC)** to strengthen collaboration across the European space sector (public and private) and enhance our ability to prepare for and respond to the multiple threats faced;
- Offer **Information sharing**, **Analysis**, **Trust building** and **Capacity building** services as part of the EU Space ISAC;
- Embarking new actors/SMEs, alongside established space actors, in this endeavour is key as it would enhance the effectiveness of information sharing while **helping them to be equipped to deal with cyber threats**.

Pilot Project Space Domain Awareness (SDA)

- Continue to **set-up and support the establishment of funded programme lines** to further develop European SDA capabilities including the **emergence and profitability of a market of technologies and services** in combination with institutional assets;
- See the SDA Pilot Project as an opportunity to **bridge the gap between the activities of the EU SST Partnership** (more focused on safety of flight services for satellite operators) and **those under the purview of the European Defence Fund (EDF)** more geared towards capability development for Members States' military missions;
- Implement the Pilot Project in **two phases aiming at fast-time to operation**: a **feasibility assessment phase** & a **Design, Develop and Integrate, Test and Qualify phase building on the current EDF call**

related to initial operational capacity for space situational awareness Command & Control (C2) and sensors;

- **Implement a gap filler solution** where a set of Space Situational Awareness (SSA)-hosted payloads with surveillance and detection capabilities could be integrated and operated on board European satellites;
- Launch the Pilot Project **as early as possible** in order to provide a minimum set of initial capabilities to EU Member States;
- Organise **space exercises and wargames** for readiness and interoperability.

Pilot Project Copernicus new services

- Design the EU Earth Observation (EO) Governmental service with **legal binding, effective governance, ownership, and capabilities** that enable the European Union to address current and new geopolitical challenges;
- **Promote its use at the Member State level**, particularly by Ministries of Defence (MoDs) and security authorities;
- It should **not in any case jeopardise the developments of the planned Copernicus Sentinels, the Expansion Missions, nor the continuity of the Copernicus existing services**, particularly from a financial point of view, including in the next Multi-Annual Financial Framework (MFF);
- It should **rely on new capabilities and leverage Research & Development (R&D) programmes**;
- It should promote a **security-by-design approach**;
- It should follow **strict European eligibility and participation conditions.**

Mobility to & in space, and Logistics

- **Promote the concept of Space Access, Mobility & Logistics (SAML)** in order to develop a full spectrum approach to responsiveness, versatility and agility in space, leveraging technological developments in the field of **launch**, **on-orbit services**, **in-orbit refuelling**, **active debris removal** and **orbital transfer vehicles** applied to military space operations;
- Launch **initial studies involving Member States and industry focusing on the development of mobility to & in space and logistics operational concepts**, to be then tested in the frame of space exercises and wargames.

Positioning, Navigation & Timing (PNT)

- Galileo needs to continue **evolving towards upgraded services** in line with a fast-growing demand in terms of accuracy, availability and resilience;
- Galileo could be thought as a **multilayer system** where multiple components, such as **LEO PNT**, contribute to enhanced flexibility, high accuracy, resilience as well as new services like two-way communications for short messaging exchanges and additional capacity to disseminate critical information to the European citizens all over the world (like emergency messages);
- **Navwar** shall be at the heart of European preoccupations and Galileo Public Related Service (PRS) shall evolve quickly in order to continuously **increase its robustness**.

Governance:

- Given the limited amount of resources and competences in Europe, the EU and ESA would benefit from finding a mutually acceptable modus operandi when new developments are needed;
- **Involving MoDs** in the system developments will be the central political issue to determine development effectiveness in all future systems.

- The EU Space Strategy for Security and Defence can only achieve its goals if **European-wide interests are prioritised against national ones**;
- A solid governance at European level will be necessary to **devise and implement a genuine industrial policy** able to ensure that security and defence actors can be provided with the capabilities they require.

RECOMMENDATIONS FOR IMPLEMENTATION

CYBER-SECURITY & RESILIENCE IN THE EU SPACE LAW

A GROWING NEW FIELD LACKING DEFINITION

Technological innovations like flexible digital platforms and cloud-based ground segment are **bringing new vulnerabilities and threats**. Consequently, the increase of new services and applications will enable a larger panel of potential access points vulnerabilities.

Cyber-security and resilience of all ground and space assets is a must-have if one wants to bring certainty in missions' continuity, guarantee system resilience whatever the cyber vulnerabilities and compliance with security requirements, regulations and certifications are. In addition, **a resilient architecture** of ground and space systems which leads to persistent and robust space services, serves as a **deterrence factor**, especially if it leads to technical advantages that cannot be countered by potential opponents.

In this context of technical innovations and developments, more EU Member States have established space services or developed space-related products and are willing to offer them to the EU; this should not be seen as a competition but as a chance to **gain resilience through burden sharing** and potential redundancy.

The term "resilience" for the space sector is however today lacking a clear definition, as not all definitions given and currently used are specific or suitable for space systems. NATO, for example, has launched work to define the term "resilience" for the space sector without arriving at a single definition[5] (i.e., "*the ability of a space system architecture to provide persistent support for mission success despite hostile actions or adverse conditions*", "*the ability of a system to continue to operate or recover quickly after a disturbance of any kind and from any source to an acceptable level of service*", "*the ability to complete the mission in the face of man-made or natural interference*").

A definition of the term at European level is very much called for, given the impacts that this has in many areas.

In this regard, the European space industry wishes to propose **specific concepts related to resilience that may be used in a European conceptual framework**:

- **Service separation:**
  - It represents mainly the technical separation of services over certain platforms (and not using shared and hosted payloads on other space-based systems). This approach is also adaptable to ground infrastructure where non-bundled assets also give a certain level of hardening.
- **Distribution:**
  - It represents an increased number of nodes or assets to define a service. The degradation or the loss of one node would then just have a minor impact on the whole service provision.
- **Diversification:**
  - It represents using different platforms, orbits and/or systems to ensure access to a specific service. This also includes the use of national (military as well as governmental), international and commercial assets and services.
- **Proliferation:**
  - It means aiming at a high level of redundancy through diversification and/or distribution, e.g. by deploying more systems in space or use a wider network of ground-based infrastructure.

[5] https://www.japcc.org/wp-content/uploads/Resiliency-in-Space-as-a-Combined-Challenge-for-NATO.pdf

These systems can be different, as long as they are able to contribute or perform the same service.

- **Protection:**
  - It represents passive technical solutions in hardware and software protection, as well as, the use of redundant subsystems or maintaining in security conditions the systems. It also includes a certain level of organisational or active protection which includes Space Domain Awareness, as well as, the option of planning and conducting space operations.
- **Anticipation**:
  - Resilient space infrastructure requires a fully prepared organisation and terrestrial ecosystem, including recovery plans and dedicated training exercises. Each potential threat must be considered both in technical concepts and industrial set-up as well as operational staff and entities. Technical competences and production means must be available and in working condition to be able to react and adapt in case of need.
- **Recovery:**
  - The ability to restore service after a disturbance. It requires fast reaction times in operations and availability of the appropriate means and resources. Severe disturbances, such as loss of space hardware, requires the ability to launch and quickly replace any critical space asset.

NAVIGATING AMONG CYBER AND ELECTRONIC THREATS

Today the space sector faces four types of threats: Kinetic Physical, Non-Kinetic Physical, Electronic (uplink jamming, downlink jamming, spoofing), and Cyber (data intercept or monitoring, data corruption, seizure of control).

Within these threats, two are directly relevant to the to the implementation of the Space Strategy for Security and Defence:

- **Electronic attacks** target the channels through which space systems transmit and receive data by radio frequency (RF) signals. It is therefore necessary to develop countermeasures against unauthorised access, jamming and spoofing attacks;
- **Cyberattacks**, contrary to electronic attacks, target the data itself and the systems using the data. Therefore, the antennas on satellites and ground stations, the landlines that connect ground stations to terrestrial networks, and the user terminals that connect to satellites are all potential intrusion points for cyberattacks, e.g., directed towards data archives, C2 centres and the processing units that perform digital signal and/or AI computation.

And in the field of electronic attacks and cybersecurity, four main threats can be identified:

- **Global supply chain security**: intentionally faulty or counterfeit (“backdoored”) hard- or software can provide access to the design schematics, physical components, and software packages of a given satellite. There is also the issue of increasing the use of open-source software, without appropriate verification, security review and other quality measures, which exposes them further to cyber threats;
- **Attacks against the links between satellites and ground control stations** (uplink & downlink) with a possible capture or modification of the data. This may also lead to advanced attack methods, e.g. replay- or man-in-the-middle attacks;
- **Attacks on terrestrial C2 (Command & Control), data relay stations, and ground systems** that process data with also a possibility of capture or modification of the data as well as allowing advance attack methods;
- **Attacks against the user segment** of a space system (the terminals or devices).

RECOMMENDATIONS

Based on the above elements, the European space industry recommends implementing the following measures:

- **Prepare**:
  - **Complement the recognition of the entire space sector as a sector of high criticality** (i.e., including operators but also ground and space suppliers) either in the **NIS2 Directive**[6] itself (already covering operators) or in a complementary regulation, also addressing EU-owned assets;
  - Provide a clear **definition of** "**resilience**" in a space context and of "**maintenance in security conditions**[7]", to be included in the EU Space Law;
  - Ensure **seamless continuity of compliance with security requirements, regulations and certifications** while transitioning from the development to the end of life (including design and build, launch, operate & maintain, end of life).
- **Protect**:
  - Protect the ground and space systems from **electronic attacks** and **cyber-attacks** (i.e., cyber-electronic warfare) that are generated by ground and/or space entities. Such protection shall be achieved by cooperating and mutually complementing passive capability;
  - Protect the **ground-to-space command link, space-to-ground telemetry link and any cross-links** (uplink & downlink) by deploying protected waveforms and, whenever feasible and cost-effective, exploiting optical links;
  - Build a robust **strategy for cryptography key management** (if key management is inadequate or if the keys are compromised, encryption becomes less effective in providing protection), including Quantum Key Distribution (QKD) according to technical and regulatory timeframes;
  - On top of the ICT network, **protect the industrial supply and development chains** from compromise;
  - Ensure availability of all crucial competences for development & recovery.
- **Secure**:
  - Prepare for anomalies through planning and practice;
  - All stakeholders in the value chain, starting with the customer, need to ensure **secure software development procedures** (by collaborating throughout the software development lifecycle to proactively identify and mitigate security risks, but also following security standard and doing security validation and testing), following the principle of security by design;
  - Include **cybersecurity on-board all satellites** to ensure proper detection, recovery, and response to the related intentional (and not-intentional) threats. This is achieved by establishing and applying cybersecurity criteria that relate to the satellite characteristics (including customer(s)) and the consequences (risk likelihood and resulting impact) of a cybersecurity attack. For legacy satellites, due to the high costs and difficulty to update on-board, it is really important to be able to have a realistic view of the attack surface and the obsolescence to manage the risk on a case by case basis;
  - Ensure that a space or ground system is **not put in service without appropriate plans to ensure operation in security conditions** to prevent cyber risk to space or ground asset and ensure resilience of services;

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

[7] *Maintenance in Security Condition is composed of 4 main activities: Curative maintenance (Problem Management & Vulnerability Management), Defensive maintenance (Crisis management, Security Monitoring), Routine preventive maintenance (Patch policy / on-going arising vulnerabilities management, Obsolescence & cybersecurity management without design impact), Preventive Major maintenance (Obsolescence & cybersecurity management with design impact)*

- Ensure **appropriate budgeting for cybersecurity (including R&D) and associated maintenance in security conditions** in line with the asset cybersecurity scope (i.e., benchmark indicates maintenance of critical operational system is around 10% Capex/year).

INFORMATION EXCHANGE ON SECURITY INCIDENTS

The consequences of cyberattacks on space systems is potentially catastrophic, impacting national security, economic stability, public safety, and essential services relying on satellite communications all around Europe and above.

In this regard, the European space industry supports the need identified within the "Space Strategy for Security and Defence" to **create an EU Space ISAC** (Information Sharing and Analysis Centre) to strengthen the collaboration across the European space sector (public and private) and enhance our ability to prepare for and respond to the multiple threats faced. It will also provide expertise, advice, support response, mitigation and resilience initiatives.

ISAC DEFINITION, OBJECTIVES AND NEEDS

An Information Sharing and Analysis Centre is a **central resource for gathering information on vulnerabilities, incidents, and threats (including but not only cyber threats**) and enables two-way sharing of information, experiences, knowledge and analysis between the private and public sectors.

The EU Space ISAC would offer different services:

- **Information Sharing**:
  - Share strategic and/or tactic information (threat analysis, vulnerabilities analysis, incidents, mitigations measures, challenges, best practice, trends, policy, etc.);
  - Collaboration styles and tools including regular meetings, working groups, platforms, conferences, webinars.
- **Analysis**:
  - Risk analysis/security tools/framework;
  - Vulnerabilities & Threats analysis, incidents response:
    - The ISAC needs to set a proper platform for members to share incidents and information (e.g., OpenCTI – a cyberthreat intelligence platform developed by the French National Cybersecurity Agency);
    - The creation of a Watch Centre working 24/24, 7/7 to centralise, filter and deliver processed information to members, dealing with all levels of threats.
  - Security trends, challenges.
- **Trust building**:
  - Regular interactions, opportunity for members to meet frequently, sharing of useful and clear information, technical tools, dedicated expert.
- **Capability building**:
  - Yearly space Cyberattacks large pilot/exercises;
  - Regular training;
  - Policy, certification.

EU SPACE ISAC SCOPE AND COORDINATION

The goal of the EU Space ISAC is to implement best practices (such as effective time-critical information sharing between institutional and private actors) and tailor them to the European context. Embarking new

actors/SMEs, alongside established space actors, in this endeavour is key as it would enhance the effectiveness of information sharing while helping them to be equipped to deal with cyber threats.

The EU Space ISAC should therefore try to **include all (public and private) entities[8], with specific expertise in cybersecurity for space**. In other words, the voice of a small company will have the same weight as a large one with equal expertise.

FUNDING MODEL

Regarding the fees for ISAC, different ways of financing can be considered, the main difference residing in the fact that EU stakeholders can't afford the same amount of membership fees than in the US (up to 40k€/year). It is indeed i**mportant to remain inclusive to ensure that all stakeholders (large, mid and small) can join the EU ISAC**.

The European space industry therefore recommends a **free membership to the EU ISAC**, in exchange for commitment to share threat & incident data, provision of experts, specific analysis, or sharing of infrastructure for exercises (e.g., through signature of a Charter). In this frame, the EU and EUSPA could act as facilitators.

GOVERNANCE MODEL

The governance can be similar to other ISACs (i.e., co-managed by the public and private side) **in order to spread good practices among their value chain and suppliers**.

INFORMATION COLLECTION AND DISTRIBUTION

The ENISA toolbox[9] is already set up and needs to be refined and adapted to the EU Space ISAC.

WORKING GROUPS AND COMMUNITIES

The creation of an EU Space ISAC is definitely mirroring what is in the NIS2 Directive concerning the information sharing on threats for the space domain. Yet, the European space industry considers that there is a **need to deepen the work on more elaborated and continuous cyber risks analysis of the space supply chain** first by creating Working Groups (WG), Communities of Interest (COI), and Task Forces (TFs) associated to clear mandates.

It is important to **include recognised experts** (e.g., from MS, EUSPA, ENISA, ESA, industry) who are already well advanced in their evaluation of cybersecurity risks.

ENABLERS AND FACILITATORS

A **list of barriers to entry** (e.g., maturity, competition, information secrecy and sensitivity) which could hinder the level of cooperation **needs to be identified and implemented** in order not for this structure to be used for lobbies, espionage activities, interference, etc... In the other hand, if there are too many different participants with too many levels of maturity, it will be difficult to manage the activities and streams supported by the ISAC.

[8] *Not restricting participation to criteria of sales, wealth, company size, etc. Only the expertise needs to be considered*
[9] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing

RECOMMENDATIONS

Based on the above elements, the European space industry recommends implementing the following measures:

- Support the creation of the **EU Space ISAC** to strengthen the collaboration across the European space sector (public, including EU entities such as ENISA or EUSPA, national security and defence entities, and private) and enhance our ability to prepare for and respond to the multiple threats faced;
- Offer as part of the EU Space ISAC **Information sharing**, **Analysis**, **Trust building** and **Capacity building** services;
- Embarking new actors/SMEs, alongside established space actors, in this endeavour is key as it would enhance the effectiveness of information sharing while **helping them to be equipped to deal with cyber threats**.

PILOT PROJECT SPACE DOMAIN AWARENESS

AN EU APPROACH TO STM & SDA

The EU Space Strategy for Security and Defence goes beyond the traditional notion of Space Traffic Management (STM) and stresses the importance of a holistic approach to Space Domain Awareness (SDA), highlighting the **importance of a coordination with EU SST capabilities and the involvement of Member States and EU Agencies** in order to identify gap and priorities, with the ultimate goal to foster/reinforce EU strategic autonomy.

THE NEED FOR AN INDEPENDENT AND UNIFIED SDA POLICY AND ROADMAP

The foundation of any Space Domain Awareness activities relies in the availability of sensor data provided by multiple heterogeneous and complementary sources and geographical locations. **Currently, Europe relies on national ground sensors which are associated in the EU SST network for Space Situational Awareness (SSA) data, coupled with openly available data from the US Space Surveillance Network (SSN)**. However, **government-owned sensors alone are not sufficient to guarantee independence from US assets**.

Recently, the EU SST has introduced the possibility to **acquire data also from commercial sources**. This is considered to be an **important step forward as it will help to close gaps in the coverage and allow access to different technologies**, each having distinctive advantages.

Nevertheless, three major issues shall be carefully addressed:

- First, the EU SST **budget allocated for commercial sensor data acquisition is far from the level of ambition** that the EU has stated in official papers and communications, thus risking slowing down the growth of EU capabilities;
- Second, a data-policy that would also aim at encouraging industry to invest in new technologies, in order **not to constrain a growing market for commercial entities**, is needed;
- Third, the complementary properties and respective advantages of commercial services and sovereign SSA assets should be carefully considered to define the optimal SDA Concept of Operations (CONOPS).

In a nutshell, the European space industry supports the role of the EU SST Partnership as a key operational capability and proposes a **stronger involvement of the European space industry, which is not only critical to develop new capabilities owned by Member States, but also to deliver commercial services and guarantee the expected customer's performance requirements in the evolving operational scenarios. Ultimately,**

guaranteeing high revisit and swath of observation is essential to ensure Europe's strategic autonomy vis-à-vis US capabilities.

Such step forward by the EU SST needs to be elaborated to effectively encompass and meet all views and needs (commercial, industrial, institutional - Governmental and Military - space users).

RESEARCH & DEVELOPMENT AS THE BACKBONE OF ANY EUROPEAN ACTION ON SDA

The role of the European space industry is key to progress on critical technologies for Space Domain Awareness. In particular, the European Defence Agency (EDA) has activated a Service Framework Contract for a "*Study for a Defence Approach to Space Traffic Management and Coordination (STM) and Enabling Space-Based Military Space Situational Awareness (SSA) Capabilities*" to define a military dimension to STM and identify tools, systems and sensor for an effective STM and surveillance capability.

The European Commission is also supporting Research Projects for Defence through EDIDP (European Defence Industrial Development Programme) and EDF (European Defence Fund). In the frame of EDIDP, two key projects for SSA have been activated, namely INTEGRAL on the development of a Space Command and Control system and SAURON on the development of new ground and space-based sensors. Those two projects will continue in EDF 2023, to progress in the direction of sensors technologies and interoperability across national systems, together with initial study and research on space sensors and solution for space assets protection.

Continue to set-up and support the establishment of funded programme lines to further develop European SDA capabilities (i.e., detection, tracking and prevention capabilities, characterisation and reconnaissance capabilities, protection capabilities and new designs to enhance safety), including the **emergence and profitability of a market of technologies and services in support to institutional assets**, is very much needed; **through coordinated R&D funding at European and national levels**, and through the strategic investment in the deployment of operational systems (e.g., data acquisition, data processing, service provision, etc.).

TOWARDS AN SDA PILOT PROJECT

Europe has to quickly go ahead with the announced plan to develop a pilot project on SDA, unifying the ongoing efforts related to SST and SSA and providing Europe with the **financial and regulatory instruments to manage and implement the overall SDA roadmap**.

Building on this SDA pilot project, it represents a key **opportunity to bridge the gap between the activities of the EU SST (more focused on safety of flight services for satellite operators) and those under the purview of the EDF (more geared towards capability development for Members States' military missions)**.

It will **encompass commercial, governmental and military infrastructures, capabilities and services with the relevant use cases and security provisions**. It shall constitute the **essential step to define a joint roadmap, maximising synergy between the various SSA activity streams at European level, while avoiding unnecessary duplication of assets**.

Industry can play a **key role in helping define the overarching requirements for a unified architecture blending government-owned systems (both already existing or to be developed in the frame of EDF activities) with commercial capabilities and services developed and implemented by the European space industry**.

This will necessarily include the **deployment and exercise of a constellation of optical and RF space sensors**, to complement the coverage of ground-based sensors (allowing observation of all orbital regimes, with no

limitations on geographic regions and atmospheric condition) and improving the performance of orbit determination and object correlation, which are key to detect and classify potential threats.

It is highly recommended that the **pilot project is defined and launched as early as possible, when the required budget is made available,** in order to provide a minimum set of initial capabilities to EU Member States.

To this goal, the SDA Pilot project should first perform an **SDA feasibility assessment**, with the following objectives:

- Evaluate and determine the SDA User Needs and Use Cases for commercial, governmental and military customers;
- Define the SDA policy, roadmap and evolution of capability mix that fit the operational needs and the objectives of the EU and its Member States;
- Define the SDA System and requirements, which will specify the performance, security, architectural and service requirements for the SDA Pre-Operational System, both encompassing the full set of SDA customers;
- Define the essential infrastructure and service constituents of the SDA project, possibly according to a phased development and deployment approach, with the goal to deploy and exploit a representative laboratory of integrated/federated ground and space assets, supporting the security and safety provisions to mitigate and counter-act multiple types of threats.

Following the feasibility assessment, the project should:

- **Benefit and build from the results of the research and development Projects awarded in the frame of the EDF 2023 call related to initial operational capacity for space situational awareness C2 and sensors, including:**
    - **Design, Develop and Integrate, Test and Qualify the SDA System Architecture**, including the infrastructure components and the service components that are either available at appropriate TRL before representative prototypes are developed and ready for integration:
        - This could include a constellation of optical and RF space sensors, to complement the coverage of ground-based sensors (allowing observation of all orbital regimes, with no limitations on geographic regions and atmospheric condition) and improving the performance of orbit determination and object correlation, which are key to detect and classify potential threats;
    - **Design, Develop and Integrate, Test and Qualify the SDA Data Security architecture** relevant to the sensor data and the Ground C2 involved, ready for expansion and application in the future full-fledged European SDA system:
        - The initial Security Architecture will prepare the pre-operational Certification and Accreditation processes, managing the security of information exchange and storage (on-ground and on-board), authentication and authorisation of various profiles of end-users.
- **Benefit from the Space Intelligence services prototype**, already developed in the frame of the EDIDP project INTEGRAL (e.g., Spawning Detection, Anomaly Detection, Threat Assessment, Manoeuvre Detection, Pattern of life analysis);
- **Benefit from the Ground sensors, C2 and Space Surveillance Network prototypes,** already developed in the frame of the EDIDP projects SAURON and INTEGRAL;
- **Benefit from the results of the research and development Projects awarded in the frame of the EDF 2023 call related to initial operational capacity for space situational awareness C2 and sensors**;
- Organise **space exercises and wargames** for readiness and interoperability.

This pilot can later be combined with the STM flagship programme announced by the European Commission in the Action Plan on Synergies between civil, defence and space industries, once prototypes are finalised and additional sensors become operational to provide a solid set of data to start SDA and Space Intelligence analysis.

Since this is becoming a pressing issue due to a tense geopolitical situation and because time is of essence, a **gap filler solution is however needed**. As an option, a set of SSA-hosted payloads with surveillance and detection capabilities could be integrated and operated in an opportunistic fashion on board European satellites (whether publicly or privately-owned). This could be confirmed - from technical and operation standpoints - by the initial SDA feasibility assessment, to ensure that the hosted payload can be embarked and operated in compliance to the constraints imposed by the main mission on board the hosting satellite. As this would be a critical asset to gain strategic advantage in the space domain, it is **expected that the EU directly sustain the initiative by funding the project**. In addition, the European space industry supports a discussion between the European Commission and Member States in terms of perimeter (i.e., what would remain under the purview of MS vs. the EC), with the aim to increase EU strategic autonomy, promoting complementary of assets and avoiding duplication.

To sum up, SDA shall be hinged on development of new sensors and services. It will benefit from inclusion of commercial data in EU SST, opportunity payloads on future missions and the EU SDA space-based constellation. It will start from an initial capability generated by the EDF and later evolve into the pilot project to reach its maturity when integrated with new sensors.

RECOMMENDATIONS

Based on the above elements, the European space industry recommends implementing the following measures:

- Continue to **set-up and support the establishment of funded programme lines** to further develop European SDA capabilities including the **emergence of a profitable market of technologies and services** in combination with institutional assets (e.g., sensors and systems);
- See the SDA Pilot Project as an opportunity to **bridge the gap between the activities of the EU SST** (more focused on safety of flight services for satellite operators) and **those under the purview of EDF** more geared towards capability development for Members States' military missions;
- Implement the Pilot Project in **two phases aiming at fast time to operation**: a **feasibility assessment phase** & a **Design, Develop and Integrate, Test and Qualify phase building on the current EDF call related to initial operational capacity for space situational awareness C2 and sensors;**
- **Implement a gap filler solution** where a set of SSA-hosted payloads with surveillance and detection capabilities could be integrated and operated on board European satellites;
- Launch the Pilot Project **as early as possible** in order to provide a minimum set of initial capabilities to EU Member States;
- Organise **space exercises and wargames** for readiness and interoperability.

PILOT PROJECT COPERNICUS NEW SERVICES

The EU Copernicus programme offers an Emergency Management Service, as well as services for "Border surveillance", "Maritime surveillance" and "Support to EU External Action". An assessment of the status, benefits, strengths and weaknesses of these services would certainly bring relevant recommendations, and **industry is fully prepared to support the definition and implementation of an EU Earth Observation Governmental space and ground systems service upgrades**, in order to expand institutional users' potential needs.

The EU Earth Observation Governmental service would require early notification and frameworks but also guaranteed European autonomy through, inter alia, mandatory use of European cloud, applications as well as European satellites data preferences.

An extension of the new Governmental service towards security (in particular considering the "dual-use" scenario) **would mean a significant increase of its objectives which should not weaken the actual Copernicus capabilities** and in particular sustain the essential backbone of Sentinel, Sentinel Next Generation and Copernicus expansion missions, all key for environment monitoring.

Such objectives could include:

- **Identifying, gathering, maintaining, and evolving an EU database of EO-based governmental services**:
  - The pilot services should conduct an initial assessment of existing initiatives, identify gaps, and develop methodologies for gathering and maintaining requirements at both EU and national levels (responsible entities, such as EDA, EEAS, SATCEN, and EUSPA should be engaged in this assessment and address their involvement in the maintenance of the requirements).
- **Assess the data and product needs based on user requirements and scenarios**:
  - This assessment will determine the necessary data products and service chains;
  - A gap analysis should be conducted, and implementation mechanisms, funded at different levels, should be identified within the study.
- **Technical, governance, and organisational aspects are crucial elements to be assessed**:
  - Defining the overall architecture and working models for the space-based infrastructure, ground segment(s), data policy and security, data tasking and priorities, as well as services chains governance is key;
  - Various approaches, such as public/private partnerships, EU-owned infrastructure, and national contributions should be considered.
- Fully implement the EO governmental services and **ensure their operational uptake at both the EU and national levels**;
- **Assessment of products, certification, standards, validation, security, and integrity** to ensure the appropriate level of data and services uptake;
- **Contribution to other components of the EU Space Programme**;
- **Collaboration with third parties**, including with commercial EO sector increasingly involved in military operations.

Industry identifies many direct and indirect opportunities (such as Very High Resolution imagery, revisit, near-real-time availability, dual pole characteristics, increased use of Artificial Intelligence) stemming from the development of a governmental service but insists that such a service shall **not jeopardise - particularly from a financial point of view, including in the future MFF - the developments of the planned Sentinels, Copernicus Expansion Missions, nor the continuity of the Copernicus existing services as well as the development of a competitive imagery services sector.**

FROM AUGMENTED OJECTIVES TO NEW CAPABILITIES

If the EU and its Member States takes the decision to launch and finance such a governmental service, **industry anticipates the need for several new capabilities, to be financially supported by R&D,** including:

- Earth Observation (EO) VHR imagery;
- Near Real Time availability;
- Revisit capability up to persistency of observation that could be achieved through geo-stationary space assets based on Synthetic Aperture Radar (SAR) and Optical sensors allowing permanent observation on selectable specific areas;
- Night & Day Vision Mission;
- Infrastructure with optical payload allowing video capabilities and interferometric multi-static SAR missions;
- Increased use of AI to concentrate the information to the users' needs, including AI & reactive tasking/ programming up to the development of cognitive satellite solutions;
- Guaranteed and Secured access to data through data encryption techniques;
- Processes to ensure confidentiality regarding the taskings;
- Capability to inter-operate with national security dual-use missions;
- Flexible, reactive and reconfigurable operational profile for real-time crisis management;
- Tip & cue (i.e., process of monitoring a point or object of interest using two or more satellites to execute a request) capability in data tasking, increased persistency in observing from space areas were critical infrastructures are installed both on land, sea and underwater;
- Use of non EO data such as RF signal, Automatic Identification System (AIS) data, data derived by mobile phone (phone traffic, app cookie data), Open Source data (e.g. OSINT), etc.

LEVERAGING ON RESEARCH & DEVELOPMENT PROGRAMMES

European projects already funded and upcoming ones within the EDA, EDIDP, EDF programmes, as well as with space agencies' studies and development programmes, are fostering the combination of large enterprises and versatile groups of SMEs into capability-driven globally competitive upstream and downstream solutions within the defence sector at institutional level. **These solutions give ground for further innovation and interdependent development of the defence sector in Europe and the new EU Earth Observation Governmental services for Security shall leverage on and complement the results coming from projects** such as EDA SBEO, PEONEER (EDIDP-ISR-PEO-2019), NEMOS (EDIDP-MSC-MFC-2020), AI4DEF (EDIDP-AI-2020), and EDF-2022-SPACE-DA-ISR.

Successful bilateral initiatives for secure EO governmental services and imagery sharing between EU Member States (such as French SAR-Lupe Ground Segment and French SARah Partner Ground Segment) should also be considered for the development of this new EU service. As formal security requirements must be fulfilled, it is also important to assess the application of national (military) security standards as well as national regulations for the handling of classified information to the interface between the partners.[10]

As far as the Ground Segment is concerned, the secure component of the EU Earth Observation Governmental services system shall build upon the concepts studied and developed in other European projects and past and existing interactions and Intelligence, Surveillance, and Reconnaissance (ISR) cooperation programmes established between Member States' MoDs. For instance, the EDA SBEO project is proposing an architecture for a Multi-Mission Ground Segment allowing interoperability among multiple users and Member States while

[10] *Requirements such as the German Federal Office for Information Security could be used as an example in order to increase the possibility of smooth interaction with military ground segments and ensure proper hardening against manipulation.*

guaranteeing the required level of security and national sovereignty, in case of contributing missions. Another important reference ground architecture come from the EDF NEMOS project where an innovative Ground Segment architecture has been developed, with the possibility to include advance technologies for responsive data downlink and dissemination (e.g., Inter satellite links, use of higher frequency bands or High-Altitude Platform Stations). Finally, EDF-2022-SPACE-DA-ISR Call will build on SBEO and NEMOS experience to design and develop an ISR system combining dedicated assets with innovative technologies as well as contributing mission. From the Ground Segment stand point, the project – if awarded – will propose a solution for an interoperability layer across multiple missions and Member States as well as innovative ground segment technologies. The former will feature a unique entry point for user orders, tasking, satellite data cataloguing and delivery and a single interface to different satellites user segment. The latter will implement responsive and intelligent tasking in order to anticipate user needs and increase data timeliness performance.

Furthermore, these **new requirements can be synergetic with the European Secure Connectivity Programme[11] IRIS²**, in order to ensure the secure and rapid availability of the data. The use of optical inter-satellite links (ISL) could allow a secure data-relay through the connectivity constellation and, more generally, ensure an efficient management of the enormous quantity of data generated by these future EO missions. Furthermore, there may be an interest investigating whether specific Earth Observation payloads (e.g., Thermal Infrared, RF & Multi and Hyper spectral detectors expanding detection beyond the visual band into the far-infrared or ultraviolet) might be included as opportunity payloads in the IRIS² constellation satellites to leverage its peculiar configuration and deliver new EO data streams in Real Time to deliver actionable EO-based products in support to aid intervention and citizens protection, complementing the current and planned European capabilities in the Earth Observation domain.

Such an evolution of the programme would allow industry to **leverage funded and co-funded (e.g. EDIDP, EDF, FP6, FP7, H2020, Horizon Europe) past investments** and developed capabilities done in the frame of national and European (including ESA) security programmes and offer an **opportunity to open new markets**. Besides, it will **allow the European space industry to complement its products with subsystems coming from the whole European supply chain, while national programmes often focus on national supply chains**.

IMPLICATIONS REGARDING THE RESILIENCE AND SECURITY OF THE EU EARTH OBSERVATION GOVERNMENTAL PROGRAM ITSELF

Resilience and continuity are key aspects for users and the downstream industry. The first priority is of course to **secure the know-how and competencies of the European space industry**, built over 20 years of experience also thanks to the Copernicus programme, including throughout the whole supply chain.

Obviously, the more the EU Earth Observation Governmental service would be used for security-related missions, the more stringent the security-requirements applicable to the new Governmental programme will need to be. The Programme would need a **secure design at several levels**: launch segment, space segment, ground segment, data and application production, downstream services provision, data exploitation and sharing. Securing data thanks to Cloud architectures and top-notch cybersecurity measures and policies would also become a must to guarantee data availability and integrity, and it reinforces the necessity of a certification scheme (see above).

More generally, **strict European eligibility and participation conditions** need to be defined to improve the security, integrity and resilience of the EU Governmental Programme infrastructures and services.

From a governance point of view, the establishment of a European Operational Security Authority component including various stakeholders and the EU industry for the EU Governmental services would also be required. It

[11] https://defence-industry-space.ec.europa.eu/eu-space-policy/eu-space-programme/iriss_en

is essential to reuse existing European investment, assets, and public entities existing know-how in order to be as efficient as possible for cost and time effectiveness.

To guarantee resilience and security, the launch of the Copernicus satellites needs to be performed **by European launchers from European territory**. Launcher and satellite stakeholders in Europe need to work hand in hand to guarantee their compatibility.

Finally, as Copernicus (and the other EU space infrastructures) is becoming increasingly critical for Europe, its citizens and its businesses, the need for an EU Governmental **efficient and autonomous space situational awareness and space traffic management systems** are becoming more and more indispensable.

RECOMMENDATIONS

Based on the above elements, the European space industry recommends implementing the following measures:

- Design the EU EO Governmental service with **legal binding, effective governance, ownership, and capabilities** that enable the European Union to address current and new geopolitical challenges;
- **Promote its use at the Member State level**, particularly by Ministries of Defence (MoDs) and security authorities;
- It should **not in any case jeopardise the developments of the planned Copernicus Sentinels, the Expansion Missions, nor the continuity of the Copernicus existing services**, particularly from a financial point of view, including in the next MFF;
- It should **rely on new capabilities and leverage on R&D programmes**;
- It should promote a **security-by-design approach**;
- It should follow a **strict European eligibility and participation conditions.**

MOBILITY TO & IN SPACE, AND LOGISTICS

As commercial and scientific space is now expanding beyond the traditional LEO to GEO orbits, the operational area of responsibility for military space is also growing to incorporate all "frontier" areas. **The reality of space as a military domain of operations will now soon encompasses three distinct areas**:

- **Higher airspace** (between 20 km and 80 km altitude), because of its growing military importance, as the flight domain of high-altitude balloons and pseudo-satellites (HAPS), as well as hypersonic glide vehicles (HGVs);
- **LEO, MEO and GEO orbits**, where military systems provide space support to operations;
- **Cislunar space and Earth-to-Moon** logistical lines of commerce in the context of rising tensions between US and Chinese lunar ambitions.

This enlarged vision of military space also deepens the challenges associated with the need for modern militaries to support, sustain and increase the resilience of military assets and operations in space.

In this context, **independent and robust access to space is the sole enabler for all space activities. Beyond sole space transportation, it increasingly needs to be paired with in-space mobility & logistics as an integrated function of any modern space power. As such, the Strategy would benefit from an expanded view of space mobility as a dual function** with specific challenges and opportunities for the development of strategic and economic opportunities in line with European priorities in the field of energy, environmental sustainability as well as space security & defence. **In-space mobility and logistics capabilities** are also powerful means to enable increasing the resilience of space infrastructure. These encompass the ability to inspect, relocate, upgrade (or augment through technology upgrades) and repair, extend the life and refuel satellites in orbit, so that they can be maintained and kept in service for longer. Moreover, these kinds of technologies can be used to improve safety of operations in space, through the cleaning of orbits with removal of debris. The ability to remove debris or other objects from orbit is a crucial defensive capability to protect Europe's assets and ambitions in space.

Europe could thus promote the concept of Space Access, Mobility & Logistics (SAML) in order to develop a full spectrum approach to responsiveness, versatility and agility in space, leveraging technological developments in the field of launch, on-orbit services, in-orbit refuelling, active debris removal and orbital transfer vehicles applied to military space operations[12]. In this way, Europe would drive a space ecosystem based on maximisation of the economic values, and by minimising deterioration effects of valuable orbits.

As an initial step, the European Commission should launch initial studies, also involving Member States and industry, focusing on the development of mobility to & in space and logistics operational concepts. Those CONOPS could then be tested within dedicated "*space exercises for readiness and interoperability*" alluded to within the Strategy in order to yield useful recommendations in terms of doctrine and capability development at European level. The recommendations thus generated could be used as useful high-level strategic inputs for future capability development roadmaps at EU or EU MS level (including EDF, PESCO and EDA's Capability Development Plan CDP), with the ultimate aim of developing mobility **to** space but also **in**[13] and **from** space using dual-purpose space systems.

The European space industry is ready to support the European Commission as it seeks to develop a full spectrum view of Security & Defence objectives in space.

[12] *All these concepts are dual by nature and needed for a sustainable future of space operations*
[13] *e.g., preparing future EU flagship programmes for servicing, bringing consistency with current development funded by the EU on OOS*

RECOMMENDATIONS

Based on the above elements, the European space industry recommends implementing the following measures:

- **Promote the concept of Space Access, Mobility & Logistics (SAML)** in order to develop a full spectrum approach to responsiveness, versatility and agility in space, leveraging technological developments in the field of **launch**, **on-orbit services**, **in-orbit refuelling**, **active debris removal** and **Orbital Transfer Vehicles (OTVs)** applied to military space operations;
- Launch **initial studies involving Member States and industry focusing on the development of mobility to & in space and logistics operational concepts (CONOPS)**, to be then tested in the frame of space exercises and wargames.

POSITIONING, NAVIGATION AND TIMING (PNT)

In a context of Navwar (Navigation Electronic Warfare) and a growing number of critical applications and economy relying on high quality and robust Positioning, Navigation and Timing (PNT), it is **necessary for Europe to continue to increase resilience of its sovereign Navigation & Timing system**.

The value chain and economy surrounding this critical information can only **rely on European warrantied infrastructures**, in which Galileo is the basis. Meanwhile, Positioning-Navigation-Timing (PNT) solutions from LEO satellites are emerging as a trend of evolution for space-based PNT, relying on multi-layer architectures.

As a matter of fact, Galileo **needs to continue evolving towards upgraded services in line with a fast-growing demand in terms of accuracy, availability and resilience**.

In order to address the upcoming challenges, **Galileo could be thought as a multilayer system where multiple components, such as LEO PNT, contribute to enhanced flexibility, high accuracy, resilience as well as new services like two-way communications for short messaging exchanges and additional capacity to disseminate critical information to the European citizens all over the world (like emergency messages**).

Regarding the Public Regulated Service, the Russian invasion of Ukraine has demonstrated how far Europe shall be prepared to face symmetric conflicts. **Navwar shall be at the heart of European preoccupations and Galileo Public Related Service (PRS) shall evolve quickly to be turned continuously more robust**. A multi-layer approach should be considered for a very high-end and highly resilient PRS.

To this goal, effort is also recommended to leverage on the most recent EDIDP and EDF initiatives (e.g., EDIDP GEODE and EDF NAVGUARD) and to ensure adequate European investments through specifically-funded actions in the EU Multi Financial Framework.

In order to prepare for the worst (i.e., a GNSS denied environment in case of conflict), an additional recommendation is to study all solutions of Alternate PNT, define a range of options fitting with EU and its Member States operational needs, and finally technology roadmaps enabling those options.

RECOMMENDATIONS

Based on the above elements, the European space industry recommends implementing the following measures:

- Galileo needs to continue **evolving towards upgraded services** in line with a fast-growing demand in terms of accuracy, availability and resilience;
- Galileo could be thought as a **multilayer system** where multiple components, such as **LEO PNT**, contribute to enhanced flexibility, high accuracy, resilience as well as new services like two-way communications for short messaging exchanges and additional capacity to disseminate critical information to the European citizens all over the world (like emergency messages);
- **Navwar** shall be at the heart of European preoccupations and Galileo Public Related Service (PRS) shall evolve quickly to be turned continuously **more robust**.

GOVERNANCE

Europe's effort towards gaining credible and assured autonomy in space for the implementation of its strategic autonomy is now a reality, and a shared effort across the continent. If the EU and its Member States do support the successful implementation of the Space Strategy for Security and Defence, it makes no doubt that **all efforts, whether civil or military, national or European, public or commercial must now converge towards efficiency and reliability for security users, as well as towards budgetary efficiency**.

The successful implementation of the Strategy will gnaw on traditionally nationally protected sectors, including in terms of procurement and benefits to industrial actors. **The major change that the Strategy is bringing to space policy in Europe is that it shall not be an EU-policy that will superimpose itself to national and multilateral ones, as it is in a way the case with the EU space programme**.

The realisation of the Strategy will require a coordination and prioritisation system – not only to encourage synergies and budgetary efficiency, but also to avoid that a fragility in one part of the system (a loophole in a national legislation, a weakness in the cybersecurity of a private ground-segment, an unidentified dependence in a particular technology…) eventually weakens Europe as a whole.

The European space industry is of course not the most legitimate actor to provide recommendations about the responsibilities and roles of institutions. Nevertheless, based on the experiences of the last 20 years in Europe, there are a few observations and points of attention, hereunder, that need to be highlighted as they have consequences on Industry.

The development of the space sector in Europe has been hindered considerably by two decades of endless power struggles that have mobilised a considerable amount of time of the political decision-makers. The geopolitical situation requires a sense of urgency and pragmatism: considering that current security-related EU space infrastructure are being undertaken by ESA on its behalf, **the EU ought to work hand-in-hand with ESA when new developments are needed, while ESA most probably needs to adapt in order to provide the necessary security guarantees to the EU and Member States via institutional solutions (accreditation, security of information, decision-making, data access and processing, security by design, staffing etc.).**

One lesson from GPS vs. Galileo and the extreme delays in admitting that the PRS would have military users and defining its security framework illustrates a core governance shortfall in Europe. While GPS is military, and thus designed and owned by MoDs, Galileo was designed by civil administrations which has led to a development obstacle, based on mistrust by MoDs, from the onset. **How to involve MoDs in the system developments will be the central political issue to determine development effectiveness in all future systems.**

In the past, MS have sometimes succumbed to the temptation of using EU-wide dependence assessment studies to promote national priorities instead of focusing on truly strategic dependence items from an EU standpoint. The implementation of the Space Strategy for Security and Defence should **prioritise capabilities fostering EU strategic autonomy using a robust and coordinated industrial policy** to deliver best-in-class European-made capabilities.

RECOMMENDATIONS

Based on the above elements, the European space industry recommends implementing the following measures:

- Given the limited amount of resources and competences in Europe, EU and ESA would benefit from finding a mutually acceptable modus operandi when new developments are needed;

- **Involving MoDs** in the system developments will be the central political issue to determine development effectiveness in all future systems;
- The Space Strategy for Security and Defence can only achieve its goals if **European-wide interests are prioritised against national ones**;
- A solid governance at European level will be necessary to **devise and implement a genuine industrial policy** able to ensure that security and defence actors can be provided with the capabilities they require.

ANNEX 1 – EUROSPACE MEMBERS STATUS

Company	Country
Aerospacelab	Belgium
Air Liquide Advanced Technologies	France
Air Liquide France Industry	France
Airbus Defence & Space Gmbh	Germany
Airbus Defence & Space Ltd	United Kingdom
Airbus Defence & Space Netherlands B.V.	Netherlands
Airbus Defence & Space Sas	France
Airbus Defence & Space Sau	Spain
ALTEC	Italy
ALTER Technology-TÜV Nord France	France
ALTER Technology-TÜV Nord S.A.U.	Spain
ALTER Technology-TÜV Nord UK	United Kingdom
AntwerpSpace N.V.	Belgium
APCO technologies	Switzerland
Arianegroup Gmbh	Germany
Arianegroup Sas	France
Arianespace	France
Avio Spa	Italy
Azur Space	Germany
Beyond Gravity AB	Sweden
Beyond Gravity Austria	Austria
Beyond Gravity Swiss	Switzerland
CGI France SAS	France
CGI Deutschland B.V & Co. KG	Germany
ClearSpace	Switzerland
CS Gmbh	Germany
CS GROUP - France	France
CS Romania	Romania
Dassault Aviation	France
Deimos Engenharia	Portugal
Deimos Space	Spain
Deimos Space Romania	Romania
Deimos Space UK	United Kingdom
eGEOS	Italy
Elecnor Infrastrutture e Aerospaziale	Italy
Enpulsion	Austria
GMV Aerospace & Defense S.A.U.	Spain
GMV GmbH	Germany
GMV Innovating Solutions B.V	Netherlands
GMV Innovating Solutions S.R.L. (B)	Belgium
GMV Innovating Solutions S.R.L. (RO)	Romania

GMV Innovating Solutions SARL	France
GMV Innovating Solutions Sp.z o.o.	Poland
GMV NSL Limited	United Kingdom
GMV Soluciones Globales Internet S.A.U.	Spain
GMVIS Skysoft S.A.	Portugal
Indra Sistemas SA	Spain
Kongsberg Defence & Aerospace	Norway
Loft Orbital	France
MOLTEK	Netherlands
MT Aerospace AG	Germany
Neuraspace	Portugal
OHB ITALIA	Italy
OHB Systems AG	Germany
Pangea Aerospace	Spain
REOSC	France
RHEA Group	Belgium
SABCA	Belgium
Safran Aero Boosters	Belgium
Safran Aircraft Engines	France
Safran Data Systems	France
Safran Electrical & Power	France
Safran Electronics & Defense	France
Safran Engineering Services	France
Safran Filtration Systems	France
SENER Ingeniería y Sistemas, S.A.	Spain
SITAEL S.p.A.	Italy
SpaceAble	France
ST Engineering iDirect Europe CY NV	Belgium
Telespazio Belgium SRL	Belgium
Telespazio Germany Gmbh	Germany
Telespazio Italy Spa	Italy
Terma A/S	Denmark
TESAT Spacecom GmbH&Co. KG	Germany
Thales Alenia Space Belgium	Belgium
Thales Alenia Space France	France
Thales Alenia Space Germany	Germany
Thales Alenia Space Italy	Italy
Thales Alenia Space Luxembourg	Luxembourg
Thales Alenia Space Poland	Poland
Thales Alenia Space Spain	Spain
Thales Alenia Space Switzerland	Switzerland
TNO	Netherlands
TTTech Computertechnik GmbH	Austria