EUROPEAN
COMMISSION

HIGH REPRESENTATIVE
OF THE UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 10.3.2023
JOIN(2023) 9 final

# JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

## European Union Space Strategy for Security and Defence

## INTRODUCTION – SPACE AS A STRATEGIC DOMAIN

Europe is a global space power. The European Union (EU) owns and operates space assets for positioning, navigation and timing (PNT - Galileo) and earth observation (EO - Copernicus) and will launch a third constellation, Union Security Connectivity Programme (IRIS²), for secure communications. Member States own and operate national space assets, including assets that serve security and defence purposes. The EU Satellite Centre (SatCen) provides a unique geospatial intelligence analysis capability, to support decision-making and actions of the EU and its Member States.

Space is critical for the strategic autonomy of the EU and its Member States. The functioning of economies, citizens and public policies increasingly relies on space-related services and data, including those in the field of security and defence. Space also contributes to achieving the EU's political agenda, enabling the digital and green transitions, and enhancing its resilience.

Yet, space is an increasingly contested area.

Some space powers have the capabilities to target critical space infrastructure. Some of them have developed and tested anti-satellite capabilities that can disrupt or destroy space systems and services. Most recently, in November 2021, Russia tested an anti-satellite (ASAT) weapon against one of its own satellites, generating a large amount of space debris.

China pursues its geopolitical agenda through its growing presence in space and is developing extensive space programmes and counterspace capabilities.

In a geopolitical context of increasing power competition and intensification of threats to the EU and its Member States, EU leaders have identified space as a strategic domain in the Strategic Compass[1] and have called for an EU Space Strategy for security and defence. The EU Security Union Strategy[2] recognises space infrastructure as essential services which must be adequately protected against current and anticipated threats and be resilient.

The EU and its Member States will continue to promote the preservation of a safe and secure space environment and the peaceful use of outer space on an equitable and mutually acceptable basis. The EU recognises outer space as a global commons. It is committed to the mutually reinforcing role of transparency and confidence-building measures, by reducing the risks of misperception, miscalculation, and unintended conflict escalation.

Additional measures are needed to defend the EU's strategic interests and to deter hostile activities in and from space. While privileging international cooperation and promoting responsible behaviours in space, the EU will also strengthen its strategic posture and autonomy in the space domain. It will make space systems and services more resilient, respond to any hostile activities or threats and further develop space-enabled services for security and defence.

---

[1] A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security

[2] COM(2020) 605 final

# 1. THE SPACE THREAT LANDSCAPE

## 1.1. Defining the space domain

The space domain includes any element relevant for the functioning of space systems and the delivery of space-based services in the EU and the Member States, e.g.: the outer space environment, the various relevant orbits and spacecraft and related information on the systems they belong to, the ground and launch infrastructure, radio frequency links, user terminals and cyber. It also includes the underlying industrial space sector.

## 1.2. Counterspace and threats in the space domain

Unlike safety risks arising from technical incidents, accidents and natural hazards, space threats are intentionally hostile activities through counterspace capabilities.

Counterspace is used to demonstrate capabilities, deter competitors, deny them the use of their space systems or gain an information advantage. They are directed to space assets in orbit, their supporting ground infrastructure, and the data links between them.

The effects of counterspace are to intentionally disrupt, degrade, destroy, deceive, or deny the use of space systems, and to inspect, manipulate, eavesdrop, or intercept corresponding data as well as deny access or freedom of movement in the space domain. The effects of counterspace may be reversible or irreversible

Counterspace capabilities can take many different forms, such as kinetic measures[3] against spacecraft or ground infrastructure, or directed energy[4]. The specific features of space infrastructure – both in orbit and on the ground – also make it particularly vulnerable to cyberattacks. Beyond space systems, counterspace can interfere with the space sector as a whole, including underlying supply chains and radiofrequency spectrum.

Several third countries have been developing and maintaining counterspace capabilities and related doctrines. However, since most space technologies are dual use, what constitutes a space threat cannot be identified by observing space objects, technologies or space capabilities in isolation, but by taking into account behaviour.

Assessing space threats requires a comprehensive analysis of capabilities and related behaviours in orbit, on the ground and in the cyber domain based on a thorough understanding of counterspace capabilities.

## 1.3. Towards a shared understanding of space threats

The Single Intelligence Analysis Capability (SIAC) under the High Representative, along with Member States military and civilian intelligence services, will increase their strategic understanding of space threats and counterspace. Such strategic understanding should also support the EU space programmes, as well as benefiting from information collected by the Commission through the monitoring of the EU space components.

***Way forward***

[3] This can include ASATs such as missiles launched directly from ground (direct ascent ASAT), or spacecraft activated when already in orbit (co-orbital ASAT), including robotic arms or projectile objects.

[4] For example, electronic warfare, lasers and other directed energy to dazzle satellites, damage their on-board electronic systems or jam or spoof their signals or intrude into their communications networks.

- The High Representative, with the support of the SIAC, will prepare a classified annual space threat landscape analysis that includes the evolution of counterspace capabilities. This would also benefit from the Commission's monitoring of its EU space components.

## 2. ENHANCING THE RESILIENCE AND PROTECTION OF SPACE SYSTEMS AND SERVICES IN THE EU

Space systems and services in the EU provide essential services for societal functions and economic activities. Thus, they need to be increasingly resilient and protected. The EU recognises space as a critical sector in its existing legislation on the resilience of critical entities (CER Directive[5]) and cybersecurity (NIS2 Directive[6]), covering ground based infrastructure of Member States, including in the EU outermost regions, and of private operators as well as satellites used for delivering telecommunication services[7]. Still, the level of resilience and protection of national space assets varies across Member States.

### 2.1. An EU-wide security framework for the protection of space systems, information sharing and cooperation on space security incidents

Some Member States have put national rules in place to regulate space operations, including security aspects. Without a common framework, these rules may differ. This divergence could affect the competitiveness of the EU space industry and the security of the EU.

To ensure a consistent EU-wide approach, and building on the joint communication on an EU Approach for Space Traffic Management[8], the Commission will consider proposing an EU Space Law. While protecting national security interests, such legislative proposal could provide the framework to collectively enhance the level of resilience of space systems and services in the EU and ensure coordination between Member States, including in remote strategic ground infrastructure locations such as the EU outermost regions.

It could provide a comprehensive and consistent framework for resilience of space systems and services in the EU, together with the NIS 2 and CER Directives. The Commission will take as a starting point, for stakeholder consultation and impact assessment of options, certain key features of those existing regimes, and the experience in their application, where relevant. For example, Member States could be required to identify essential[9] space systems and services. This could include major supply chain actors, to define and implement a common minimum level of resilience for critical space services and to develop coordinated national preparedness and resilience plans and emergency protocols. The initiative could also extend to developing security monitoring centres, to allow for the notification of security incidents in a systematic manner.

---

[5] Directive (EU) 2022/2557 on the resilience of critical entities

[6] Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.

[7] Cf recital 5 of Directive 2022/2557: "… The space sector falls within the scope of Directive (EU) 2022/2557 with respect to the provision of certain services that depend on ground-based infrastructure owned, managed and operated either by Member States or by private parties; consequently, infrastructure owned, managed or operated by or on behalf of the Union as part of its space programme does not fall within the scope of this Directive."

[8] JOIN(2022) 4 final

[9] Essential is to be understood as crucial for the functioning of economic activities, security and safety in Member States.

The Commission could also consider requirements to make sure that security, including cyber-security, is part of the design of all space systems delivering essential services. It could propose the more systematic integration of relevant security standards in the early design phase of these systems.

Moreover, the Commission would incentivise the exchange of information on threats targeting space assets or their supply chain, focusing on actionable information to relevant security operation centres (SOCs). Building on its experience for Galileo, the EU Space Programme Agency (EUSPA) would ensure a consistent security monitoring of all EU space programmes. In close cooperation with the Commission, the Computer Security Incident Response Team of all the EU institutions (CERT-EU) and the European Union Agency for Cybersecurity (ENISA)[10], EUSPA will play a key role as space security monitoring and operations centre in the EU. On request, it may also assist operators of essential space systems and services in Member States.

Space services are provided by public and private operators, with an increasing and dynamic role for New Space[11]. A common understanding of what the essential space services are is necessary to share relevant security information, coordinate actions and facilitate EU cooperation.

In complement to such a possible legislative proposal, the Commission would raise awareness and facilitate the exchange of best practices among commercial entities on resilience measures, including cyber-related ones. Such supporting measures would be especially relevant for SMEs, including New Space. In this context, the Commission, with the support of EUSPA, would consider establishing an Information Sharing and Analysis Centre (ISAC), bringing together commercial entities, and relevant public entities, including possibly the European Space Agency (ESA).

In addition, the implementation of the NIS 2 Directive and the upcoming Cyber Resilience Act[12], as well as other existing cybersecurity frameworks[13], will incentivise the uptake of cybersecurity requirements for critical digital products that are used in space. Specific cybersecurity standards and procedures in the space domain could be considered as part of the EU Space Law where relevant.

Finally, greater steering of the EU in the development of standards and its better representation in international standardisation organisations are crucial, in particular to

---

[10] https://www.enisa.europa.eu/

[11] [11] New Space qualifies the emerging private space industry, driven by a series of technological trends and business model innovations and leading to a reduction in costs of space systems, shorter lifecycles in delivery and more risk taking.

[12] Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM (2022) 454 final

[13] This currently includes the delegated regulation of the Radio Equipment Directive, adopted in October 2021 and imposing obligations to the manufacturers of wireless devices to improve their level of cybersecurity, privacy and protection from fraud.

protect the security interests of the EU and its Member States. Coherence with North Atlantic Treaty Organization (NATO) standards will be encouraged.

### 2.2. Strengthening the technological sovereignty of the EU space sector

To increase the resilience of space infrastructure and ensure security of supply[14], the EU will strengthen its technological sovereignty by reducing strategic dependencies on third countries and boosting the resilience of critical industrial value chains.

Horizon Europe and the European Defence Fund (EDF)[15] will be fully leveraged to achieve this. The Commission, the European Defence Agency (EDA) and ESA will coordinate and synchronise activities in critical space technologies, building on a re-energised Joint Task Force (JTF)[16]. Building upon its expertise, the EUSPA could also contribute to this work. The activities of the JTF will also feed into the EU Observatory of Critical Technologies[17].

On the basis of the activities of the JTF and the EU Observatory of Critical Technologies, the Commission, together with Member States and industry, will assess the need to establish new industrial alliances related to technologies that are relevant for space and defence, in compliance with the EU competition rules. The Important Projects of Common European Interests (IPCEI) are also a tool that industry and Member States can use to develop space technologies in areas where it addresses a clearly identified and significant strategic dependency, while ensuring important positive spillovers beyond the participating countries and firms.

The Space Programme, the EDF and Horizon Europe, as well as Member States' collaborative projects and programmes support the technological maturation of resilience-related capabilities. Developing further synergies in programming and funding can ensure continuity in the development of technologies up to systems. To strengthen the protection and resilience of EU space systems, the Commission will promote joint programming through enhanced coordination between relevant EU programmes.

The Commission should be able to avail of the possibility to re-programme short-term actions in support of critical technologies in the face of major crises. It will ensure that space is more systematically taken into account in relevant EU policies and initiatives, such as on quantum technologies, or artificial intelligence, but also by ensuring access to raw,

[14] This includes access to raw, processed and advanced materials
[15] Including its precursors programmes the European Defence Industrial Development programme (EDIDP) and the Preparatory Action on Defence Research (PADR)
[16] The Commission-ESA-EDA Joint Task Force on critical space technologies for European non-dependence created in 2008.
[17] COM(2021)70 final

advanced, and processed materials and to semi-conductors through for instance the European Critical Raw Materials Act[18] and the Chips Act[19].

The Commission will continue working with ESA on the development of EU space technologies, including security-related ones. To enhance this role, it is crucial that ESA puts in place relevant measures and mechanisms to ensure the protection of the security interests of the EU and its Member States. Close cooperation will ensure the complementarity and synchronisation of activities.

### 2.3. Addressing risks to security in the space sector in the EU

Ensuring the EU's security also relies on the protection of its supply chains. To that end, certain controls are already in place, i.e. dual-use export control and Foreign Direct Investments (FDI)[20] screening. The Commission will evaluate the FDI Screening Regulation by October 2023[21].

To be able to better assess the risks associated to FDI transactions in the space sector, the Commission will ensure it has access to information on direct and indirect providers of goods and services to EU space programmes, including when managed by ESA. Risks for the EU's security and public order relating notably to emerging and critical technologies for its space infrastructure should also be better detected and mitigated. Consideration should also be given to the economic and financial circumstances in which EU companies with strategic technologies may be vulnerable to foreign investments representing risks for security or public order; as well as to security of supply. As a mitigating measure, multiple sourcing of the most critical technologies and components will reduce the risks posed by certain foreign acquisition and ensure internal competitiveness.

Additionally, protecting EU security and its strategic interests requires procurement rules that fully guarantee security of supply. The Commission will ensure that EU competition rules and international trade instruments are fully applied to tackle new challenges faced by the EU space and defence sectors, such as the risk of distortive foreign subsidies. This should include investigating certain acquisitions of EU companies active in these sectors, which may be facilitated by illegal third country subsidies. If needed, prohibiting the acquisition or accepting binding commitments from the companies concerned could be considered to remedy the distortions caused by these foreign subsidies. [22]

### 2.4. Developing capabilities, including EU autonomous access to space, to increase resilience

There are many capabilities that can enhance the resilience of space systems and services such as self-protective infrastructure, versatile and responsive launchers, space situational awareness services, in-orbit servicing and secured sovereign cloud dedicated to space services. Such capabilities can make space assets stronger, protect them better, extend their lifetime, or replace them quickly.

---

[18] European Critical Raw Materials Act (europa.eu)
[19] European Chips Act (europa.eu)
[20] Regulation (EU) 2019/452 establishing a framework for the screening of foreign direct investments into the Union
[21] Article 15 of the Regulation
[22] Regulation of the European Parliament and of the Council on foreign subsidies distorting the internal market.

EU autonomous access to space is essential for the resilience of space infrastructure in the EU, including for the replenishment of constellations, the replacement of individual satellites or the deployment of future constellations.

Responsiveness and versatility in access to space are essential for ensuring that growing military and defence needs are met. Beyond consolidating current launch capabilities, the development of launch systems in the EU needs to be stimulated, including micro-launchers and reusable launchers, along with an agile manufacturing industry. The Commission will incentivise the development of standardised interfaces (covering security aspects) between satellites and responsive launch systems to ensure future satellites' interoperability and access to space solutions, and to support the development of innovative in-orbit transportation solutions. The EU's outermost regions of interest for automous access to space should be fully exploited.

***Way forward***

- To enhance the level of security and resilience of space operations and services in the EU, as well as their safety and sustainability, the Commission will consider proposing an EU Space Law. It will encourage the development of resilience measures in the EU, foster information-exchange on incidents as well as cross-border coordination and cooperation.
- By the end of 2023, the Commission, with the support of EUSPA, will establish an Information Sharing and Analysis Centre (EU Space ISAC) to strengthen the resilience of capabilities of the EU space industry (upstream and downstream), including New Space.
- By mid- 2024, the Commission, in close coordination with EDA under the authority of the High Representative and with ESA, will propose a roadmap to reduce strategic dependencies on technologies that are critical for ongoing and future space projects in the EU and EU space programmes.
- The Commission will develop joint programming between the EDF, the EU Space Programme and Horizon Europe to accelerate the development of capabilities that are relevant for the resilience of space systems.
- The Commission will take space and defence needs systematically into account in future initiatives, including assessing the need to establish industrial alliances.
- The Commission will ensure that broader EU initiatives, including the Chips Act and the Critical Raw Materials Act, are applied in a manner that strengthens security of supply and the resilience of space systems and services.
- The Commission will take actions to stimulate the responsiveness, versatility of EU access to space by boosting new EU launcher systems, by proposing preparatory actions to ensure long-term EU autonomous access to space and by addressing, in particular, security and defence needs, together with Member States.

## 3. RESPONDING TO SPACE THREATS

Given the increase in space threats and counterspace, there is a need to enhance the capability to detect, characterise and attribute a threat in the space domain and to react to it in a timely, proportionate, and coherent manner both nationally and at EU level.

### 3.1. Detecting and characterising space threats

Any EU response to a space threat requires both the EU and its Member States, as appropriate, to have access to timely, accurate and actionable information as a basis for their decision-making.

Besides the need to regularly update the space threat landscape, it is necessary to collect and analyse in near real time security incidents that affect the space systems and could signal a space threat. Complementary to security information collected through the monitoring of the EU space programme, an information exchange network could be established through the EU Space Law and would provide through EUSPA a first level of analysis and reporting of these weak signals.

The EU and its Member States also need to develop a shared understanding of the overall situation in orbit to address irresponsible or hostile behaviours in outer space.

Space Domain Awareness (SDA) consists of detecting, identifying and characterising space objects of interest in near real time, describing and understanding their behaviours[23], and connecting this information to underlying doctrines and related space systems. SDA feeds in real time the *recognised space pictures* of space commands, relying on intelligence on space manoeuvres and intents.

SDA is key for attributing space threats in orbit and triggering a potential EU response. Member States that own and develop the relevant capabilities should provide the necessary SDA services to the EU to ensure its strategic autonomy in the space domain.

### 3.2. Attributing and reacting to hostile behaviours in the space domain

Attributing a space threat to a third country and deciding on a possible response is a highly political decision.

The Council Decision on the security of systems and services deployed, operated and used under the Space Programme[24] lays down operational provisions enabling the EU[25] to attribute and respond to threats to or through systems set up and services of the EU Space Programme, if such threats would affect the security of the EU and/or of its Member States. The Decision foresees the possibility for the High Representative to take urgent provisional action. The European External Action Service (EEAS) operates the Space Threat Response Architecture supporting the implementation of the Decision.

In view of the growing threats, the High Representative would propose amending the Council Decision so that it becomes the cornerstone of the EU response in the space domain.

The scope of the Decision should be extended to cover threats in the space domain that may affect the security of the EU. The Space Threat Response Architecture could become the recipient at EU level of space security incidents through the Space Programme's

[23] Including manoeuvres and payload operations
[24] Council Decision (CFSP) 2021/698 of 30 April 2021 on the security of systems and services deployed, operated and used under the Union Space Programme which may affect the security of the Union, and repealing Decision 2014/496/CFSP
[25] Through a unanimous Decision of the Council on proposal from the High Representative.

Security Monitoring Centre and the SDA services. It would partner with the SIAC to support the attribution of space threats and the adequate response.

Complementary to the cyber diplomacy toolbox and the hybrid toolbox, the amended Council Decision would also facilitate the mobilisation of a dedicated toolbox. As part of the response, relevant EU tools could include:

- at technical level, the use of specific operational response modes developed as part of the security design of the space systems;
- at diplomatic level, discussions in multilateral forums, outreach through appropriate channels, and statements by the EU and by Member States to prevent and respond to irresponsible behaviours in the space domain;
- at economic level, tools including sanctions[26].

EU Military Staff would also prepare a military contribution to the EU's response in the space domain.

The creation of a horizontal group under the Common Foreign and Security Policy (CFSP) would enable the prompt mobilisation of relevant expertise when confronted with a space threat. It would support the Council in its response to space threats, including for their attribution.

Any Member State can invoke the mutual assistance clause enshrined in the EU Treaties (Article 42.7 of the Treaty of the European Union), should a space threat or incident amount to an armed attack on its territory.

### 3.3. Space exercises for readiness and interoperability

The High Representative, together with the Commission and the Member States, will set up regular exercises in the space domain or exercises with a space domain component to:

- test, develop and validate the EU's response to space threats,
- test and explore concrete solidarity mechanisms in case of attacks from space or threats to space systems, and
- develop synergies with partners and allies in space security and defence.

***Way forward***

- The High Representative and the Commission will explore with Member States owning SDA capabilities the modalities to use SDA in support of an EU response.
- The High Representative will propose amending Council Decision (CFSP) 2021/698 to respond to all threats in the space domain that may affect the security of the EU and its Member States, with a view to ensure that all available EU tools can rapidly be mobilised, thereby improving its Space Threat Response Architecture.
- The High Representative, the Commission and Member States will participate in, develop, and conduct relevant space exercises including the use of solidarity mechanisms.

[26] The Commission may propose complementary economic measures falling within its competence, such as export control requirements.

## 4. ENHANCING THE USE OF SPACE FOR SECURITY AND DEFENCE

Space systems and services play an increasing role in support of defence and security. Dual-use services provided by EU space programmes and by commercial entities, including New Space, will be further developed to increase the strategic autonomy of the EU and its Member States.

### 4.1. EU space systems and services supporting security and defence

More systematic cross-fertilisation between EU space, defence and security initiatives would facilitate the development of dual-use EU space components taking into account defence and security needs under an overarching capability-driven approach[27].

EU space flagship initiatives can support security and defence capabilities. It is therefore necessary to explore to what extent they can provide secure and reliable services.

While respecting the civilian nature of EU space programmes, specific and tailor-made rules for the delivery of security-sensitive services, applications and data will be established to provide the appropriate level of trust for security and defence users (such as priority rights and access control - including in the context of military operations, the anonymisation of requests, the restriction of the dissemination policy).

The Commission will embed military and security user requirements in the design of relevant new EU space systems and the upgrade of relevant existing systems. It will rely on the support from relevant EU agencies, namely EDA and EUSPA. EDA will continue to play a key role in identifying military requirements[28], defining capability priorities and fostering cooperation among Member States, including through the 'Defence in Space Forum'. EUSPA will support the identification of security-related needs, the accreditation and exploitation of dual-use systems and services. In addition, the EU Military Staff will take forward the conceptual developments required at military level for the use of space in EU operational engagements.

When preparing the future development of the EU space programmes, the Commission will consider the long-term defence and security user requirements (time horizon 2035), in close cooperation with Member States. It will consider system interoperability and piggy backing payload options for defence as well as security on existing or future space systems.

To this end, synergies will be encouraged through EDF, so that defence research and development can accelerate the deployment of payloads enabling services for defence. In addition, the different governmental services enabled by EU space programmes will be consistently operated and exploited.

#### *4.1.1. Positioning Navigation and Timing (PNT)*

Resilient PNT services such as the Galileo Public Regulated Service (PRS), are critical enablers for military operations. The continuous evolution of PRS and complementary payloads in orbit will make it more robust. Building on PESCO projects such as the EU Radio Navigation Solution (EURAS) or future defence Navigation Warfare (NAVWAR),

[27] In accordance with the Action Plan on synergies between civil, defence and space industries.

[28] EDA contributed to the definition of military user requirements for the GOVSATCOM and Space Situational Awareness (SSA) components of the EU Space Programme.

surveillance capabilities will enable the creation of a consolidated situational picture, and to cope with situations where access to PRS is contested. In this context, the EDF supports activities related to an unlimited and uninterrupted access to PRS worldwide to strengthen the security and defence component of the EU's PNT capabilities.

#### *4.1.2. Earth Observation*

Space-based Earth Observation supports autonomous assessment and decision–making. It is a key enabler for security and defence. It has proven to be a game-changer for the Ukrainian Armed Forces to resist the Russian attacks.

SatCen provides a unique geospatial intelligence analysis capability to support high-level decision-making and action of the EU and its Member States, and also supports EU policies.

Although Copernicus delivers security services, it was not designed to comply specifically with defence requirements.

Therefore, as part of the evolution of Copernicus services, and as already presented to Member States, an EU Earth Observation governmental service would be beneficial to provide a fully reliable, highly resilient, and continuously available situational awareness service. To provide added-value, it would complement national, commercial and European satellite imagery infrastructure, for instance through new sensors, frequent revisit and advanced processing techniques[29]. The Commission will gradually implement this evolution of Copernicus services, starting with a pilot in the current Space Programme.

The development of such service will leverage the complementarity of the SatCen and EUSPA. Building on its expertise, EUSPA, under the supervision of the Commission, will play a key role in the security accreditation, security monitoring and contract implementation of the future system's space segment. The SatCen will play a key role in contributing to the identification of user needs in geospatial intelligence and in disseminating sensitive products and services.

#### *4.1.3. Secure Communication*

Uninterrupted, worldwide access to secure and highly resilient communications can support defence and security missions and operations. In addition to regional govsatcom Member States' assets, IRIS² will provide added value services such as anonymity of use, low latency and flexibility. Member States will have effective control through mechanisms equivalent to those used in Galileo PRS.

[29] It will leverage Research and Development (R&D) activities of the EDF, including advanced payload technologies and data processing techniques, and be complemented in the future by highly reactive small satellites for space-based Intelligence, surveillance, and reconnaissance. Synergies with PESCO Projects, such as the Common Hub for Governmental Imagery (CoHGI), will be considered.

IRIS² services will include space data relays able to interconnect Member States' space capabilities (including defence) permanently and securely. These services can be used by space-based national or multinational defence capabilities such as Earth Observation systems to improve their operational effectiveness. The Commission will fully exploit upcoming low earth orbit (LEO) constellations for new capabilities, including augmented services that may be of use to the military by offering piggybacking payloads. The Commission will further explore the extent to which IRIS² can support the establishment of an EU critical communications system[30].

The EDF supports the development of technological building blocks for resilient space-based communications[31] implementable through IRIS² and their uptake by defence end-users, through actions targeting the user segment (e.g. standardising of the interfaces to facilitate their integration into land, sea and air vehicles[32]).

#### *4.1.4. Space Domain Awareness and Space Surveillance and Tracking*

The synergies between Space Domain Awareness (SDA) and the already existing EU Space Surveillance and Tracking (SST) system are high to detect space objects with dedicated sensors.

Increased performances for SST are required to reinforce the precision of advanced collision avoidance manoeuvres and of fragmentation and re-entry analysis. Those Member States developing SDA, who are also SST partners, will therefore benefit from more performant SST assets, including defence assets, to detect and track smaller and more agile spacecraft through the SST component of the EU Space Programme. Additional sensors and analysis capabilities for defence and intelligence will be needed to support SDA.

EU budget could support Member States in the development of SDA sensors and capabilities provided that:

- complementarity with the existing mechanism supporting SST is ensured, and
- the necessary flow of SDA information and services is made available to support the EU Space Threat Response, including to protect EU satellites.

SST partners benefitting from SDA support would in turn help improving SST by improving the identification of spacecraft, thereby contributing to an autonomous EU catalogue of space objects, an objective of the EU Space Programme.

---

[30] A ground-based broadband system intended to link Member States next generation communications systems for civil security and safety organisations, allowing them to operate throughout the EU and Schengen countries.Based on the Horizon 2020 BroadMap and BroadWay projects, as well as the Internal Security Fund BroadNet Preparation project

[31] EDF-2021-SPACE-D-EPW

[32] EDIDP –DA- ESSOR

### 4.2. Fostering innovation and competitiveness

Beside large industrial players, New Space plays an increasing role in service-delivery, including for security and defence. It can propose new ideas, solutions, disruptive technologies and efficient industrial processes, which can also support security and defence. Member States increasingly rely on commercial services to complement national assets, test new capabilities, or develop public assets.

A competitive industry is essential for strengthening the EU's resilience and capabilities. The Commission will stimulate New Space to scale up in the EU with the support of the CASSINI programme[33]. This will include a more systematic development of anchor-customer contracts, further mobilisation of grants-loans-equity with the support of the European Innovation Council, the European Investment Bank, the European Investment Fund, synergies with the EU Defence Innovation Scheme, and the organisation of space/defence hackathons and challenges on a yearly basis.

The Commission will incentivise more collaborative work between space, security and defence start-ups in the areas of research and development. Technologies developed with the support of Horizon Europe, for example for the development of Quantum Space Gravimetry, On-Orbit-services or access to space, could be further developed for defence purposes. The Commission will expand its In-Orbit-Validation / In-Orbit-Demonstration programme to space technologies of relevance to security and defence users. The EDA's Capability Technology group on space will also foster cooperation between Member States and their industries in space research.

### 4.3. Developing skills, education and training

Both the EU and its Member States, face a shortage of expertise in space security and defence. The Commission and the High Representative will mobilise existing tools to support skilling, upskilling and reskilling.

To meet Member States' demand, EDA, will map all EU and national educational and training activities relating to space security and defence, to develop skills relevant both for policy design and at technical level. In close coordination with the European Security and Defence College (ESDC), it will promote the exchange of best practices and define curricula.

To meet industry demand, the Commission will contribute to up- and reskilling in the space industry, focusing in particular on space for security and defence, also aiming at increasing women's participation[34]. It will support concrete initiatives organised at EU, national and regional level. It will build on the existing large-scale partnership for aerospace and defence skills of the Pact for Skills[35]. It is also working with stakeholders to develop a new large-scale partnership to further enhance upskilling and reskilling activities of students and professionals required by the downstream industry, including to cover extra needs for

[33] CASSINI is the European Commission's initiative to support entrepreneurs, start-ups and SMEs in the space industry. https://defence-industry-space.ec.europa.eu/eu-space-policy/space-entrepreneurship-initiative-cassini_en
[34] Communication "A Union of Equality: Gender Equality Strategy 2020-2025". COM/2020/152 final
[35] https://ec.europa.eu/social/BlobServlet?docId=23220&langId=en

qualified workers. With the support of the EUSPA, the Commission will develop the EU Space Academy to create space development programmes related to security.

***Way forward***

To enhance the use of space systems and services for defence purposes:

- By the end of 2024, the Commission, in close cooperation with the High Representative, will propose a pilot for the delivery of initial SDA services in support of EU response and to explore synergies with the SST subcomponent of the Space Programme, with a view to future developments.
- When developing future EU space programmes, the Commission will take into account long-term military requirements (time horizon 2035) for space-based defence services with the support of EDA.
- The Commission will consider military needs and requirements when defining of the service portfolio of IRIS².
- In order to support the autonomous decision-making and action of the EU and its Member States, the Commission will work towards the gradual set-up of a new Copernicus governmental service, starting with a pilot. It will build on the complementary role of SatCen and EUSPA.
- The Commission will incentivise collaborative work between space, security and defence start-ups to develop disruptive services for security and defence.
- By the end of 2024, the High Representative and the Commission, with the support of EDA, EUSPA and ESDC, should improve the skills of public administration and industry to further develop space services for security and defence, including through: the mapping of space security and defence training activities, and the skilling of downstream space industry, including through the establishment of a new large-scale partnership.

## 5. PARTNERING FOR RESPONSIBLE BEHAVIOURS IN OUTER SPACE

Forging strong external partnerships is essential to promote a common vision for peaceful and responsible behaviours in space, respond to space threats and support the use of space services for security and defence

### 5.1. Promoting norms rules and principles for responsible behaviours in outer space

Avoiding an arms race in outer space and preventing it from becoming an area of conflict is crucial to safeguard the long-term use of the space environment for peaceful purposes.

The 1967 Outer Space Treaty and the principles developed in the United Nations (UN) framework are the cornerstone of the global governance of outer space, together with relevant resolutions adopted by the UN General Assembly.

In complementarity, a non-legally binding, transparency and confidence-building instrument would be an effective tool[36]. Additional measures should supplement the relevant traditional disarmament and arms control tools to address irresponsible behaviours that may lead to escalation, including due to misunderstanding, misinterpretation, or

[36] For example the Hague Code of Conduct (HCoC) against the proliferation of ballistic missiles.

miscalculation. In this regard, the commitment of the United States (US) not to conduct destructive, direct-ascent ASAT missile testing, which has been joined by Germany and France, is a pragmatic, concrete, and measurable step forward. The EU and all its Member States supported the corresponding Resolution[37] approved at the 77th session of the UN General Assembly in October 2022.

### 5.2. Engaging with the United Nations on space and security

The EU will take full benefit of its permanent observer status in the United Nations (UN) to act side by side with its Member States in discussions on outer space. The EU will continue to participate in and actively contribute:

- to the UN Committee on Peaceful Uses of Outer Space (COPUOS) and its subsidiary bodies and to the Special Political and Decolonization Committee (Fourth Committee) of the UN General Assembly for issues pertaining to space safety; and
- to the Conference of Disarmament and the Disarmament and International Security Committee (First Committee) of the UN General Assembly for issues pertaining to space safety and security.

The EU and its Member States support[38] the Open-Ended Working Group on reducing space threats through norms, rules and principles of responsible behaviours (OEWG)[39], as a pragmatic step that helps build a common understanding of what can be considered responsible and irresponsible behaviours.

The main challenge for the EU and its Member States together with likeminded partners is to convince the vast majority of UN member countries of the relevance of a normative approach. The EU and its Member States will work towards broadening international support for their position on outer space.

The EEAS has launched a 'bottom-up' public diplomacy initiative to build support for a Safe, Secure and Sustainable Outer Space (3SOS), promoting a sustainable approach to space by encouraging collision avoidance, reducing the creation of long-lived orbital debris and promoting transparency and confidence-building measures. This will contribute to reducing mishaps, misperceptions, and mistrust.

### 5.3. Partnering with the US on space security and defence

The Strategic Compass recalls that the EU's partnership with the US is of strategic importance for the deepening of EU-US security and defence cooperation in a mutually beneficial way. The US has a privileged relationship with the EU and some of its Member States in this area.

Since 2009, the US and the EU have held a space security dialogue based on close collaboration beyond civilian areas. The discussions have, for example, allowed their respective Global Navigation Satellite Systems to move from perceived competition towards growing complementarity, interoperability, and redundancy.

---

[37] "Destructive direct-ascent anti-satellite missile testing" (document A/C.1/77/L.62).
[38] The EU has made several joint contributions, and several of its Member States have submitted national or cross-regional working papers.
[39] Adopted by UNGA Resolution 76/231

A similar approach can be envisaged for space situational awareness and other areas, where the EU could move from a dependence on US space services to a partnership based on mutual interest.

### 5.4. Dialogue with third countries on space security

Transparent and open communication between different actors in space (including civilian and military) is crucial to avoid conflicts and contributes to confidence building.

A growing number of third countries have reviewed, or are reviewing, their defence organisations and doctrines to recognise the importance of space for security and defence. Several third countries, including allies but also strategic competitors, have developed space security and defence strategies to develop domestic capabilities and foreign partnerships with likeminded countries.

The EU is increasingly addressing space security and defence in its political discussions with third countries. The EEAS and relevant Commission services will set up staff-to-staff dialogues between the EU and the relevant authorities of other third countries, such as Canada and Norway, as is already the case with the US and Japan.

These space security dialogues are an opportunity to engage with partners and allies, discuss their space and security strategies, establish partnerships for the exchange of information, share best practices on how to increase the resilience of space infrastructure and establish norms and standards, identify areas for possible cooperation and coordinate action in multilateral forums.

Space and security dialogues can also be key to promoting EU positions and approaches in multilateral forums. They may constitute a diplomatic channel the EU can activate to de-escalate tensions or convey warning messages to deter further actions –, especially when confronted with irresponsible behaviour in the space domain.

### 5.5. Partnership with NATO on space security and defence

The Strategic Compass sets clear objectives for the EU-NATO strategic partnership - political dialogue and practical cooperation across all agreed areas of interaction, including new work strands such as space.

In the third joint declaration on EU-NATO cooperation of 10 January 2023, the institutional leaders of the EU and NATO confirmed their commitment to expand and deepen their cooperation on space, based on the agreed principles underpinning their strategic partnership.

EU-NATO cooperation continues to rely on mutual openness and transparency, reciprocity and inclusiveness, in full respect of the decision-making autonomy and procedures of both organisations, and without prejudice to the specific character of the security and defence policy of any Member State.

Both organisations are contemplating the evolution of space from a capability in support of military and civilian operations into a strategic domain. The EU's and NATO's responses to space incidents and threats will be complementary and mutually reinforcing.

The two organisations will jointly explore new areas of cooperation in the space domain through regular exchanges, including staff-to-staff talks, cross-briefings and reciprocal

invitations to events. Parallel and coordinated exercises organised by the EU and NATO staff could also include a space domain component.

***Way forward***

- The EU will support multilateral efforts to reduce space threats through norms, rules and principles for responsible behaviours, including through the work of the OEWG established by the UN General Assembly.
- The High Representative together with the Commission will step up the 3SOS public diplomacy campaign for Safety, Security and Sustainability in Outer Space.
- The High Representative and the Commission will deepen cooperation in space security with the US.
- The High Representative and the Commission will develop space security dialogues with like-minded partners and allies, where relevant. In close cooperation with Member States, they will consider dialogue with non-like-minded countries.
- The High Representative and the Commission will develop cooperation with NATO in space security.

## 6. CONCLUSION

Space systems and services in the EU contribute to the strategic autonomy of the EU and its Member States. They are key assets that will contribute to shaping the future competitiveness, prosperity and security of the EU for next generations.

The Space Strategy for security and defence demonstrates the EU's commitment to protect its security interests while preventing an arms race in outer space, and accelerating synergies between space, security and defence.

The EU is committed to strengthening the resilience of the value chains that underpin the space ecosystem and to supporting the innovation and competitiveness of the EU space industry. The Commission and the High Representative will report to the Council on a yearly basis on the progress achieved and potential further actions.