European Space Policy Institute

Security in Outer Space: Rising Stakes for Europe

Report 64
August 2018

Short title: ESPI Report 64
ISSN: 2218-0931 (print), 2076-6688 (online)
Published in August 2018

Editor and publisher:
European Space Policy Institute, ESPI
Schwarzenbergplatz 6 • 1030 Vienna • Austria
http://www.espi.or.at
Tel. +43 1 7181118-0; Fax -99

Design: Panthera.cc

Table of Contents

1. Introduction

1.1 Background and Rationale for the Study

The ecosystem of the space sector has shifted drastically over the past decades with new technical concepts and business endeavours building on a changing institutional and economic environment. Now a pillar of the modern economy and society, the global space infrastructure enables key services across vital sectors, and directly supports public actions to address economic, societal, environmental and security issues at a national and global level. This ever-growing use of space-based data and services by a variety of public and private actors/users has created a virtually invisible dependence on space technologies, which closely relates to Information and Communication Technologies (ICT). As the use of space applications becomes more pervasive, brings more benefits, and becomes part of the business-as-usual routine, dependence on space infrastructure intensifies, which creates new vulnerabilities for the economy and society at large. A disruption or shutdown of space systems - intentional or not - would cause disastrous knock-on effects on other key infrastructures and sectors, leading to possible waves of crises. In the European Union only, at least 10% of the GDP depends to some extent on space assets.[1] Thus, even a partial incapacitation of these assets could lead to a substantial economic loss of up to EUR 50 billion per year, and would put up to 1 million jobs at risk. Other impacts, more complex to measure, would also arise in the fields of environmental protection or security and defence, putting human life at risk of harm or loss.

At the 10th European Space Policy Conference in January 2018, Mrs. Frederica Mogherini, High Representative of the European Union for Foreign Affairs and Security Policy and Vice-President of the European Commission (EC), delivered a keynote speech on the role of space in security and defence matters. Her presence at this high level policy event, for the second consecutive year, along with five other commissioners, holds out the prospect of an even greater political acknowledgement of the socio-economic and strategic significance of space infrastructures within the broad EU perimeter of action, in particular while the EU is increasing its activities in the fields of defence and security.

The growing importance of space infrastructure raises new stakes concerning its protection from harm. Experts routinely caution governments and operators about the rising threats to space infrastructure security, underlining that space is increasingly congested and contested, which poses an intensifying challenge to safely deploying, operating and exploiting space assets. Driven by a variety of trends from inside and outside the space sector, challenges to the security of space infrastructure include the proliferation of space debris, accidental or malicious radio interferences, cyber-attacks, anti-satellite technologies (ASAT), and natural space hazards such as geomagnetic and solar radiation storms.

This deteriorating situation has already been widely acknowledged by European stakeholders including Member States from the European Space Agency (ESA) and the European Union (EU). Recently, the EU identified the reinforcement of 'Europe´s autonomy in accessing and using space in a secure and safe environment' as a top priority of its Space Strategy for Europe.[2] Accordingly, European stakeholders have taken steps in this field. Organised at national, intergovernmental and European level, efforts encompass capacity-building in the field of Space Situational Awareness (SSA), development of technologies and standards, reinforcement of space programmes security architecture, establishment of legal and regulatory regimes but also diplomatic initiatives and cooperation frameworks.

[1] PwC (2017). *Dependence of the European Economy on Space Infrastructures*. Brussels: EU Publications. Retrieved from: http://www.copernicus.eu/sites/default/files/library/Copernicus_SocioEconomic_Impact_October_2016.pdf

[2] European Commission (2016). Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions. Space Strategy For Europe. COM (2016) 705 final. Brussels: https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/COM-2016-705-F1-EN-MAIN.PDF

Despite multiple initiatives, European efforts, in particular in the field of capacity-building, remain limited in comparison with other space-faring nations and especially with the United States. Across the Atlantic, securing space assets has long been a strategic priority as underlined by the development of an ambitious SSA programme by the U.S. Department of Defence. Recent developments, including the launch of the $1.6 billion U.S. Space Fence programme[3] aiming to further increase domestic SSA capabilities and the recent publication of a Space Traffic Management (STM) policy demonstrate the desire of the U.S. government to accelerate its effort in this domain.

As the space security dialogue gains momentum, Europe sits at the crossroads of important decisions with far reaching consequences. Among these decisions, the priorities and budget envelopes of the post-2020 Multi-annual Financial Framework (MFF) will be decisive to shape the role that Europe will play in this field in the coming years.

1.2 Research Objectives and Approach

The European Space Policy Institute ranks space security as a short-term priority for space policy development and considers it one of the key challenges for the future of Europe´s activity in space. In this context, the purpose of this ESPI research project is to provide a comprehensive overview of the state of affairs in the current European approach to space security, and to discuss possible developments. In investigating the rationale for a strong European role in space security and examining European achievements and shortcomings in this field, this report seeks to identify possible pathways to shape a coherent European space security strategy. The overarching objective is to raise awareness about the evolving situation and to contribute to the future of European space security policies.

More specifically the study aims to:

- *Assess the rationale for space security in Europe* by reviewing the key stakes for Europe
- *Provide a comprehensive overview of threats* challenging the security of European space infrastructure
- *Investigate the European approach and effort in the field of space security* and assess achievements and limitations including:
  - European objectives and resources
  - European initiatives (e.g. capacity-building, legal framework, standards)
  - International cooperation and diplomacy
- *Identify and discuss European stakes, ambitions, and means* for short- to long-term space policy developments.

The analysis provided in this report is based on publicly available information and on interviews with stakeholders and experts, under Chatham House rules.

1.3 Research Scope

1.3.1 'Security in Outer Space' and other Dimensions of 'Space Security'

Space Security is defined by the Space Security Index as 'the secure and sustainable access to, and use of, space and freedom from space-based threats'. [4] This definition 'encompasses the security of the unique outer space environment, which includes the physical and operational integrity of man-made assets in space and their ground stations, as well as security on Earth from threats originating in space'.[5] This definition can be expanded further to encompass the crucial role played by space systems in support of defence and security activities on Earth.

Here, three conceptual dimensions of Space Security can be delineated as shown in Table 1. [6]

In this report, 'Space Security' is understood primarily as 'Security in Outer Space' referring to the protection of space infrastructure from threats so that this infrastructure can fulfil its specific functions as expected. In this case, activities in the field of Space Security encompass the set of political, legal, economic and

[3] The Space Fence will utilise S-band ground-based radars. http://www.lockheedmartin.com/us/products/space-fence.html
See also: http://www.airforcemag.com/MagazineArchive/Pages/2017/August%202017/A-Closer-Watch-on-Space.aspx

[4] West, J. *Space Security Index 2017*. Waterloo, Ontario, Canada: Space Security Index.

[5] West, J. *Space Security Index 2017*. Waterloo, Ontario, Canada: Space Security Index.

[6] Mayence J-F (2010). 'Space security: transatlantic approach to space governance', Prospects for transparency and confidence-building measures in space . (ESPI, Vienna, p 35)

technical provisions required to ensure an 'Accessible', 'Affordable' and 'Safe to Operate' space environment.

Security in Outer Space	Outer Space for Security	Security from Outer Space
The protection of the space infrastructure against natural and man-made threats or risks, ensuring the sustainability of space activities.	The use of space systems for security and defence purposes.	The protection of human life and the Earth environment against natural threats and risks coming from space.

Table 1: Complementary dimensions of Space Security

The topics of 'Outer Space for Security' (i.e. the use of space-based capabilities to support security and defence activities), and of 'Security from Outer Space' (i.e. the protection of the Earth against space-based threats), are not directly addressed in this study.

Notwithstanding this, the three dimensions of Space Security are strongly entangled and interdependent. For example, users of space systems for ground security and defence operations have strong requirements in terms of service resilience, which reinforce the need to protect space assets from threats. In this case, it is 'Outer Space for Security' that nurtures the need for 'Security in Outer Space'. Some aspects of 'Outer Space for Security' and 'Security from Outer Space' that have an impact on 'Security in Outer Space' may therefore be mentioned in this report, but special efforts were made to preserve the scope of the study.

1.3.2 Security of the Space Infrastructure

The space infrastructure can be described as a network of space-based and ground-based systems interconnected by communication channels and enabled by access to space capabilities. It includes:

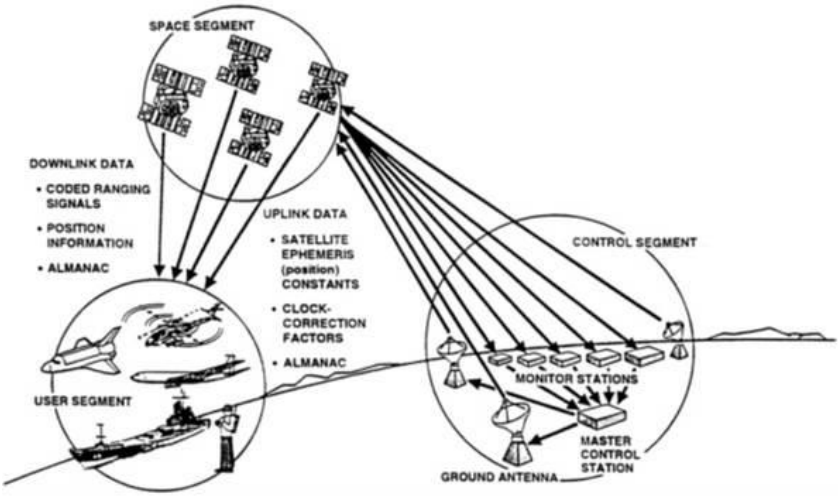

Figure 1: Representation of the GNSS infrastructure components[7]

- *A space segment,* composed of all systems of the infrastructure located in orbit, namely satellites required for the conduct of operations and delivery of intended service;
- *A ground segment*, composed of all systems of the infrastructure located on the surface of the Earth and necessary for the conduct of operations in space and delivery of data and signals (i.e. stations to interface with the space segment, mission control centres to manage operations in space, networks and terminals to connect the different elements of the ground segment between each other and with other ground systems such as internet and mobile networks);
- *A user segment,* sometimes addressed as a sub-part of the ground segment and composed of complementary ground-based systems required for the delivery of full-fledged space services accessible by end-users (i.e. service monitoring cen-

[7] National Research Council. (1995*). The Global Positioning System. Retrieved from National Academies Press*. Retrieved from https://www.nap.edu/read/4920/chapter/9

tres, data processing facilities, user equipment such as terminals or navigation systems);

- *Down-links and up-links* to interface between the space and ground segments (i.e. including users' equipment) and to operate the space system and receive its data.[8] The uplink refers to signals transmitted from the ground to space and the downlink refers to signals received on the ground from space.

As the present report focuses on 'Security in Outer Space', the analysis addresses predominantly security threats and challenges to the 'space segment' of the space infrastructure. Whenever relevant, the report also discusses threats and challenges affecting other components of the space infrastructure, in particular intentional and unintentional threats to down-links and uplinks. The report does not address security challenges specific to the ground segment, such as Earth natural hazards, physical attacks on facilities or eavesdropping (e.g. sabotage).

1.3.3 Security in Operation

From a wider angle, a comprehensive review of space security challenges faced by space infrastructure would require taking into account the entire system lifecycle including development, production, deployment, and operations up to disposition. Indeed, space security is the result of measures applied throughout the infrastructure lifecycle:

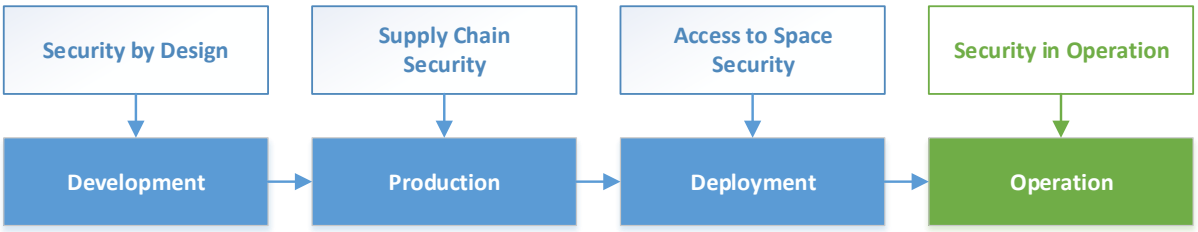

Figure 2: Security challenges throughout system lifecycle

This study focuses primarily on security challenges to space infrastructure in operation, including system disposal. Security challenges at earlier stages of space programmes (e.g. security-by-design, supply chain security) are mentioned whenever relevant but have not been investigated specifically. By extension, the security architecture of space programmes (e.g. Security Accreditation, Threat Response Architecture), which requires to be adapted to the specificities of each infrastructure, is not addressed in this study which focuses on common and external dimensions of security in outer space.

[8] National Research Council. (1995).*The Global Positioning System.* Retrieved from National Academies Press: https://www.nap.edu/read/4920/chapter/9

2. Increasing Need for Space Security in Europe: Policy Drivers

2.1 European Space Infrastructure: a Substantial and Continuous Investment

It is undisputed that today Europe has acquired the status of a full-fledged space power. With a diversity of space programmes for scientific and operational purposes and an autonomous launching capability resulting from substantial and continuous investment, Europe has joined with full-rights the small club of space powers. As a result, Europe is equipped today with a complete and operational space infrastructure, including orbital systems (i.e. spacecraft), ground stations, launchers, spaceports and, in general, all systems and facilities required to develop, manufacture, deploy, operate and exploit space systems.

For the purposes of this study, European space infrastructure is understood as the sum of space and ground assets owned and operated by European public and private stakeholders. Ownership of European space infrastructure, encompassing space and ground components but also access to space facilities, is shared among five main actors:

- The *European Union*, as a supranational institutional actor, owns the space infrastructures of the current flagship programmes Galileo, EGNOS and Copernicus. Development, operation and exploitation of EU space infrastructures are delegated to partner organisations including the European Space Agency, the European GNSS Agency (GSA), EUMETSAT, Frontex, the European Union Satellite Centre (EU SatCen), the European Maritime Safety Agency and other public and private entrusted entities.
- The *European Space Agency*, as an intergovernmental organisation, develops, owns and operates a variety of space systems and ground infrastructures funded from annual contributions by its Member States;
- *EUMETSAT*, as the European operational satellite agency for monitoring weather, climate and the environment, operates a system of meteorological satellites. It relies on ESA for the design and development of its space segment;
- *Member States*[9], who conduct both civil and military programmes and whose national institutions (e.g. space agencies, department of defence) own, operate and exploit national space infrastructures;
- *Commercial Operators,* such as Eutelsat, SES or Inmarsat, own, operate and exploit private space infrastructures for a commercial purpose.

Together, these European actors own and operate a wide space infrastructure comprised of numerous space systems and related ground segments. Focusing on the space component, 219 European satellites, excluding cubesats and other smallsats below 15 kg, were operational as of end 2017. The following figure, extracted from ESPI database, provides an overview of the number of operational European satellites by owner/operator.

[9] Note: Member States include here a broad coverage of European countries active in space and in particular Member States of the European Union and of the European Space Agency.

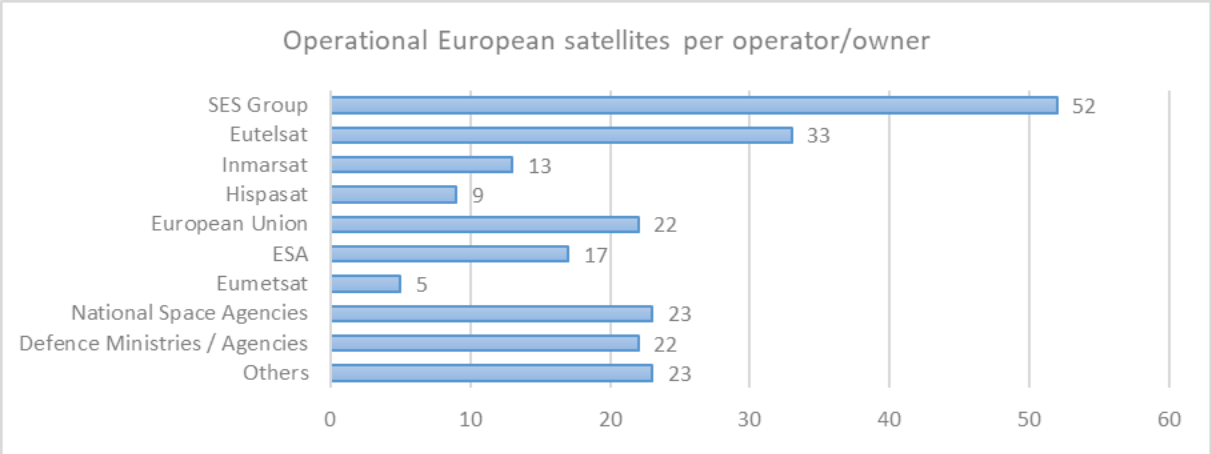

Figure 3: Number of operational European satellites per operator/owner as of end 2017 (source: ESPI database)

Interestingly, in Europe, the number of satellites operated by private entities (124) exceeds the number of satellites operated by public civil and military institutions (95). This is a direct consequence of the leading position occupied by European satellite operators on global markets, in particular for satellite telecommunication. Among key European players, SES, a private telecommunication satellite operator with headquarters in Luxembourg (including several branches: O3b, Astra, AMC, NSS and QuetzSat) operates 52 satellites. Eutelsat, another private satcom operator, with headquarters in France, operates 33 satellites. Other key private operators include Hispasat and Inmarsat operating respectively 9 and 13 satellites.

Satellites operated by European institutions include a total of 44 space systems: 17 operated by ESA (including 5 EU Sentinel satellites), 5 operated by EUMETSAT and 22 Galileo satellites owned by the EU and operated by the GSA with the support of private operators. Satellites operated by national civil and military institutions include 45 space systems: 23 operated by national space agencies (i.e. ASI, CNES, DLR, INTA, UKSA) and 22 by military-related organisations.

The remaining 23 satellites include mostly smaller private operators such as Airbus, Skynet (for the UK Ministry of Defence), Avanti Communications Group, Telenor, Bulsatcom and DMC International Imaging, for example.

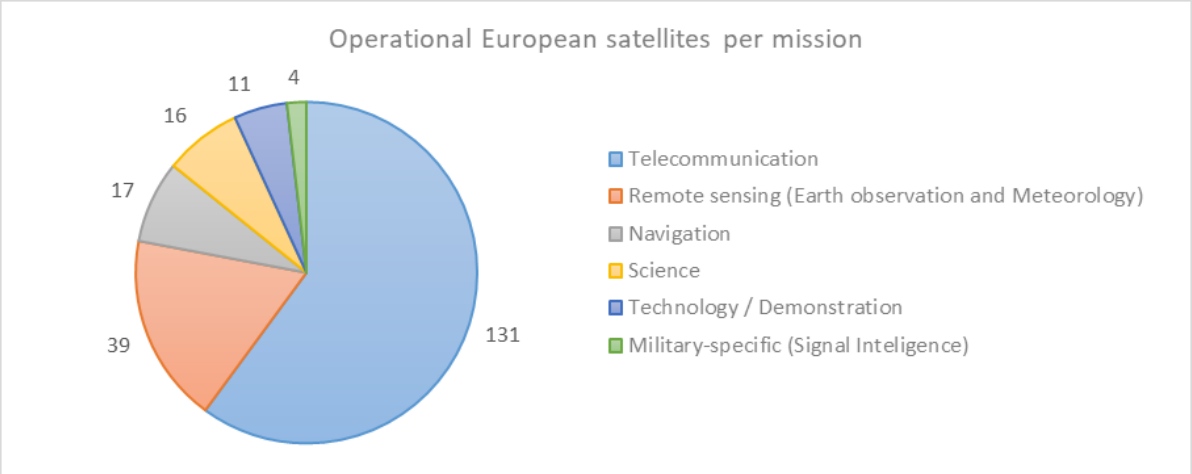

Figure 4: Number of operational European satellites per mission as of end 2017 (source: ESPI database)

With the recent deployment of new systems, in particular Galileo, EGNOS, and Copernicus, European space assets cover a rather large set of scientific and operational missions including telecommunication, Earth observation and science, meteorology, navigation, astronomy and military intelligence, and deliver data and services for a multitude of civil and military applications.

In addition to this orbital component, European actors rely on an extensive ground segment to operate and exploit these satellites and deliver data and services to users. The ground segment includes a large range of stations, positioned across the globe and used for various purposes. For example, the ground segment of Galileo, among the most complex systems, is composed of the following centres:

- Two Galileo Control Centres (GCC), in Fucino Italy (GCC-I) and in Oberpfaffenhofen Germany (GCC-D), each one hosting:
  - A Ground Control Segment (GCS) dedicated to the control of the satellites on-orbit. This manages five Telemetry Tracking & Control (TT&C) stations distributed globally. The GCS handles spacecraft housekeeping and constellation maintenance.
  - A Ground Mission Segment (GMS), dedicated to the Galileo mission and the generation of Navigation and Timing signals. It manages a network of Galileo Sensor Stations (GSS) and 5 Up-Link Stations (ULS) distributed globally.
- Two Launch and Early Orbit Phase (LEOP) Operation Control Centres (LOCC), one hosted by CNES in Toulouse (France), and the other hosted by ESOC in Darmstadt (Germany). The two centres are used alternatively for each dual launch to operate the satellites from launcher separation until reaching the final target orbit. The LOCCs include a dedicated ground station network used for tracking, commanding and controlling the satellites (LEOP TT&C).
- One In Orbit Test (IOT) ground station executes In-Orbit Test campaigns for each satellite to verify the in-orbit performance of the payload signals, ensuring that no degradation has occurred during launch with respect to the signal performances as measured during ground testing. After IOT has been successfully completed, the spacecraft is declared officially operational and transmits its L-band ranging signal.
- The Galileo Data Dissemination Network (GDDN) is a Wide Area Network, connecting the Galileo Ground Stations (GSS, ULS, TT&C) to the GCCs, the LOCCs, and the IOT station.
- Two Galileo Security Monitoring Centres (GSMC), one in Saint-Germain, France, and one in Madrid, Spain, ensure the security of the Galileo infrastructure. The centre monitors and takes action regarding security threats, security alerts and the operational status of systems components and ensures that sensitive information relating to the use of the Public Regulated Service (PRS) is suitably managed and protected.
- The Galileo Service Centre (GCS) in Madrid, Spain, and Galileo SAR Centre provide end-users with additional data for the Open Service, the Commercial Service and the Search-And-Rescue services.

Each individual European space infrastructure comprises ground stations that can be isolated, co-located in hubs, or shared with other systems. Another example of a broad ground segment is that deployed for EGNOS, which includes two Mission Control and Processing Centres (MCC), two Central Processing Facility (CPF), 2 Central Control Facilities (CCF), 40 Ranging and Integrity Monitoring Stations (RIMS), 8 Navigation Land Earth Stations (NLES), and the EGNOS Wide Area Network (EWAN).

Lastly, Europe has an autonomous access-to-space capability comprising the required industrial setup, an operational spaceport, and a broad family of launchers covering small, medium and heavy lift capacities.

The European space infrastructure is the result of a substantial and continuous investment from public and private actors. European institutions (EU, ESA and national governments) mobilize, every year, a sizeable space budget. In 2016, the consolidated European space budget reached € 7,726 million.[10] This consolidated value for the year 2016 encompasses € 6,035 million in civil and military national space budgets, including contributions to ESA budget, and € 1,691 million from the budget of the European Union. The management of this budget comprises a complex multi-layered structure involving various actors in charge of managing a share of this budget to conduct various space programmes.

Figure 5 provides an overview of the European space budget flow with sources and managing entities.

In general, this budget corresponds to the annual investment of public stakeholders to develop, deploy and operate space infrastructure as part of public programmes. Beyond the direct investment in industry for procurement of space and ground systems or launch services, this public budget also encompasses a range of activities to support a competitive and capable European industrial base, in particular through Research & Development programmes such as ESA Basic and General Technology Research Programmes and the EU Horizon 2020 programme. Finally, a part of the budget includes necessary expenditures for programme management and other activities part of agency portfolios.

[10] Lionnet, P. (2017). *(Upstream) economic space data*

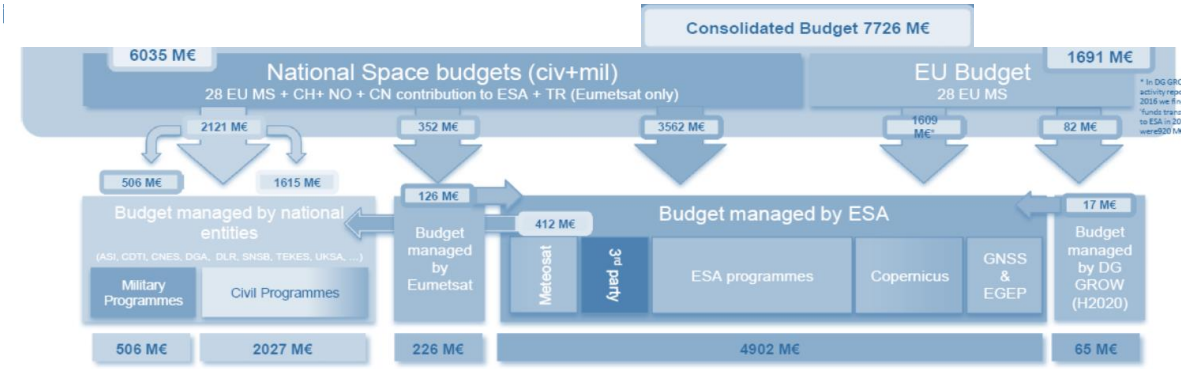

Figure 5: European public space budget sources and management flow[11]

From a top-down perspective, the annual investment of public stakeholders provides a good metric of the value of the European public space infrastructure. This metric is not perfect since it includes a share of activities that are not directly related to the European space infrastructure itself (e.g. investment in the downstream sector, international programmes…) and does not provide for an estimate of the cumulative investment related to the operational infrastructure currently in orbit. This being said, and although the financial value of operational public space infrastructure could be estimated (with considerable analysis effort and access to classified data), it is important to note that such metric would also not provide a complete picture of the total intrinsic value of the infrastructure. From this standpoint it is to be noted that the European space infrastructure as it stands is the result of a long and constant efforts by public stakeholders. These efforts started long ago, with the initial setup of European industrial capabilities, carry on today with current programmes and will endure in the future to ensure programme continuity and further expand European space infrastructure.

Looking into individual programmes of the European Union, for example, the total budget allocated up to 2020 to finance activities related to Galileo and EGNOS programmes amounts to € 10,500 million, including € 3,405 million allocated during the 2007 – 2013 period[12] and € 7,071 million allocated during the 2014 – 2020 period.[13] For the Copernicus programme, a total investment of € 7,500 million[14] is established for the period 2008-2020. In both cases, amounts exclude complementary Horizon 2020 budgets dedicated to supporting R&D efforts related to the programmes. These amounts also exclude expenditures made as part of previous programmes to develop industrial facilities and capacities re-used for these programmes (e.g. clean rooms, vacuum chambers, test-beds, generic technologies, and know-how…). Alongside those considerations, the long-term continuation of EU programmes, a prerequisite to achieving programme objectives, will require further financial support beyond 2020 as proposed by the European Commission in the proposal for a regulation establishing the space policy programme of the European Union for the period 2021-2027.[15]

In addition to public budgets, a substantial investment is also made each year by private operators to deploy, maintain, upgrade and expand the infrastructure they exploit commercially. Estimating this investment is complex exercise. In 2016, Eurospace estimated that sales of space and ground systems from the European space manufacturing industry to European private operators reached € 485 million.[16] This figure excludes an important share of private expenditures such as purchase of systems from third country industry, internal running costs, and complementary expenses

[11] Lionnet, P. (2017). (Upstream) economic space data
[12] European Commission (2011). *REGULATION (EC) No 683/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 July 2008 on the further implementation of the European satellite navigation programmes (EGNOS and Galileo).* Brussels: European Commission. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008R0683&from=EN
[13] European Union (2013). *Regulation (EU) No 1285/2013 of the European Parliament and of the Council*. Retrieved from EUR-Lex: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013R1285
[14] European Commission. (2016). *Copernicus: Market report.* Retrieved from Copernicus. Luxembourg: Publications Office of the European Union: http://www.copernicus.eu/sites/default/files/library/Copernicus_Market_Report_11_2016.pdf
[15] European Commission. (2018). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the space policy programme of the European Union, relating to the European Union Agency for Space and repealing Regulations (EU) No 1285/2013, No 377/2014 and No 912/2010 and Decision 541/2014/EU. Brussels
[16] ASD-Eurospace. (2017). *Facts and Figures press release.* Retrieved from Eurospace: http://www.eurospace.org/Data/Sites/1/pdf/eurospacefactsandfigures2017pressrelease.pdf

for network control centres and teleports, among others.

Europe can therefore rely on a wide space infrastructure comprised of numerous space and ground systems functioning together to provide end-users with a broad range of space-based data and services. When adopting a top-down approach and looking into the financial resources mobilized by public and private stakeholders, it appears quite clearly that this infrastructure is the result of a substantial and continuous effort. Estimating precisely the financial value of the European space infrastructure in terms of investment is not straightforward as the current infrastructure builds upon decades of investment and will require continuous effort for future maintenance, upgrades and evolutions to accommodate new emerging needs. For this reason, estimating the value of the infrastructure at a given moment by summing the cost of each component would not provide a fair assessment of its actual value.

2.2 Socio-Economic Value of the European Space Infrastructure

2.2.1 Considerable Economic Benefits

Another, probably more suitable, way to estimate the value of the European space infrastructure is based on a bottom-up approach, looking into the various benefits arising from the exploitation of this infrastructure. By means of comparison, the intrinsic value of a highway, or of an airport for example, does not lie in the financial resources mobilized to build and operate it but actually in the fulfilment of the infrastructure objective which is, in general, to support the socio-economic development of a region. Infrastructures can also support the achievement of other strategic objectives such as reducing the environmental impact of human activities or improving safety.

The socio-economic and strategic value of the European space infrastructure has already been investigated in the frame of various studies ordered by the European Commission, ESA and EUMETSAT, among others. In general, these studies underline that, driven by the development of space and ground technologies, in particular ICT, the role of space systems has radically progressed. Today, the European space infrastructure provides a broad range of unique capabilities that are essential for a variety of strategic domains and economic sectors.

When looking at the space value chain, models show that the exploitation of space infrastructures has two sequential impacts. First, it fosters the development of a vibrant downstream sector comprising numerous companies specialized in processing raw space data and capabilities to deliver turnkey services to end-users. Then, the use of these space-based solutions, with the emergence of new applications, generates considerable benefits for end-users including institutions and businesses widespread across numerous sectors (i.e. defence, agriculture, energy, insurance, banking…), and a vast majority of European households and citizens that use space-based solutions in their daily lives.

These benefits are complex to estimate at a macro-economic level but specialists tend to point out that space related benefits are often underestimated simply because, at user-level, the use of space infrastructures, although pervasive, is often transparent. It was recently estimated that, thanks to a fertile ecosystem for the development and adoption of space-based solutions, more than 10% of European Union Gross Domestic Product (GDP) depends today, somehow and in different ways, on the space infrastructure.[17] The total economic benefit for the EU is estimated to be as large as € 53.5 billion per year in Gross Value Added, supporting directly and indirectly about 1 million jobs in the European Union. This value includes economic activities in the European space downstream sector and economic benefits (e.g. increased output, reduced intermediate costs, improved productivity) materializing in end-user sectors. Comparatively, this economic impact is highly cost-effective, with limited European spending in comparison to other spacefaring nations (0,1% of European public budgets / €12,5 per European citizen per year). From this perspective, the space infrastructure actively contributes to the economic development of Europe by improving the competitiveness and productivity of numerous European industrial sectors.

The following figure provides a simplified representation of the chain of economic benefits enabled by the European space infrastructure. In this figure additional non-economic benefits (e.g. job creation, environmental impact, digital divide mitigation) are not represented.

[17] PwC (2016). Study to examine the socioeconomic impact of Copernicus in the EU. Report on The socio-economic impact of the *Copernicus programme*. Brussels: European Commission. Retrieved from European Commission: http://www.copernicus.eu/sites/default/files/library/Copernicus_SocioEconomic_Impact_October_2016.pdf

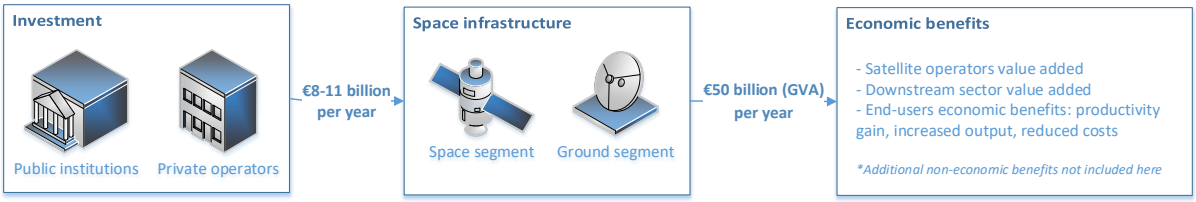

Figure 6: Simplified space infrastructure benefits chain

Focusing on EU programmes, Copernicus, alone, is expected to enable more than € 13,5 billion of cumulated economic benefits in gross value added by 2020. This impact includes the investment impact on the upstream industry, enabled revenues from European downstream actors, and the estimated economic benefits at end users' level, value which is expected to increase significantly as more Sentinels and related services become operational.[18] An ex-ante cost-benefits analysis of EGNOS for the aviation sector[19] estimated that cumulated undiscounted benefits could be as high as € 2.4 billion between 2008-2030 with € 1.1 billion of benefits for commercial and general aviation, € 350 million for airports and air navigation service providers, and € 1 billion for the general public and other sectors. The socio-economic impacts of Galileo have yet to be assessed but, since the programme is not fully operational despite declaration of initial services[20] in December 2016, the potential of Galileo in terms of benefits has not yet been maximised. Nevertheless, given the size of the programme and the fast-growing downstream industry for GNSS services[21] it can already be anticipated that the programme will enable considerable benefits for Europe.

2.2.2 Instrumental for Policy Implementation

Beyond measurable economic benefits, the use of space-based solutions also brings noticeable benefits to European society at large, and to the fulfilment of a variety of European Union and Member States governmental objectives. Indeed, space systems are, before all, strategic assets that contribute to many European sectorial policies and support in multiple ways the European effort to tackle modern societal and environmental challenges.

Space capabilities are instrumental for the implementation of key European policies. The space infrastructure can either contribute directly to the implementation of policies (i.e. space-based solutions are used directly by the EU to achieve flagship objectives), or indirectly (i.e. space-based solutions are used by actors of target sectors to improve productivity or reduce the environmental footprint, for example, which supports the achievement of EU objectives).

Examples of space infrastructure contributions to EU sectorial policies include, among others, the EU Digital Agenda to bridge the digital divide in Europe, the Common Fisheries Policy (CFP) to support the sustainable exploitation of fisheries resources, EU Road Safety to enable competitive, sustainable, secure and safe transport services, the Common Agricultural Policy (CAP) to foster agricultural productivity, viable food production, reduction of agriculture environmental footprint and farmers' access to ICT or the Energy Union to give consumers secure, sustainable, competitive, and affordable energy.[22] In the domain of security and defence, the space infrastructure also supports multiple policies and activities within and outside European borders including, among others, civil protection and police mission, maritime security (e.g. traffic monitoring, surveillance of illegal activities, Search & Rescue missions), border surveillance or humanitarian aid.

These are only a few of many examples. In fact, space infrastructure is used or could be used, in a vast majority of EU policy areas that require EU intervention, ranging from border control to sustainable forestry strategy. The magnitude of benefits enabled by space assets varies between policy areas but can be critical

[18] European Commission (2016). *Copernicus: Market report.* Luxembourg: Publications Office of the European Union. Retrieved from http://www.copernicus.eu/sites/default/files/library/Copernicus_Market_Report_11_2016.pdf
[19] GSA (2010). EGNOS Cost Benefit Analysis in Aviation.
[20] European Commission (2011). *Mid-term review of the European satellite radio navigation programmes.* Retrieved from EUR-Lex: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52011DC0005
[21] European GNSS Agency. (2016). *Security Accreditation.* Retrieved from European GNSS Agency: https://www.gsa.europa.eu/security/accreditation
[22] PwC (2016). Study to examine the socioeconomic impact of Copernicus in the EU. Report on The socio-economic impact of the *Copernicus programme*. Brussels: European Commission. Retrieved from European Commission: http://www.copernicus.eu/sites/default/files/library/Copernicus_SocioEconomic_Impact_October_2016.pdf

when space assets provide a particularly efficient, and sometimes irreplaceable, means to achieving policy objectives.

2.2.3 A Promising Future ahead

In the context of the digital revolution, the space sector is undergoing a major transition and seems to have a bright future. In this respect, analysts agree that the socio-economic and strategic value of European space infrastructure is poised to increase, driven by the development of new applications and the integration of space-based data and capabilities in a growing number of ground technologies.

The transition currently being observed in the space sector is usually referred to as *New Space* and encompasses a broad range of diverse, interrelated trends. In a recent study of the rise of private actors in the space sector, ESPI isolated the following trends as drivers of the New Space dynamics:

Figure 7: Key trends driving the New Space sectorial dynamic

- *New entrants* in the space sector, including large Information and Communication Technology (ICT) firms, start-ups, and new business ventures;
- *Innovative industrial approaches* with announcements and initial development of ambitious projects based on new processes;
- *Disruptive market solutions* offering, for example, integrated services, lower prices, reduced lead times, lower complexity or higher performance, among other value proposition features;
- *Substantial private investment* from different sources and involving different funding mechanisms;
- *Innovative public procurement and support schemes* involving new R&D funding mechanisms and costs/risks sharing arrangements between public and private partners;
- *New industry verticals and space markets* such as miniature systems (micro-launchers, cubesats) or in-orbit servicing in the upstream part of the space value chain and global connectivity or near-real time geoinformation in the downstream part;
- *Involvement of an increasing number of space-faring nations* investing in the acquisition of turnkey space capabilities or even in the development of a domestic space industrial base.

Overall, ESPI defines New Space as a disruptive sectorial dynamic featuring various end-to-end efficiency-driven concepts driving the space sector towards a more business- and service-oriented paradigm. This dynamic is embedded in the cross-fertilisation of space technologies with ground technologies. From this perspective, it is anticipated that space data and capabilities will become central components of promising technologies that are part of the on-going digital transformation, such as 5G networks, precision agriculture and forestry, next-generation air traffic management systems, smart energy grids, and autonomous vehicles, to name a few. Investors are confident that the global space economy, estimated in 2016 already at around $350 billion, will continue to grow substantially to reach $1.1 trillion by 2040, according to the financial services firm Morgan Stanley, and possibly up to $3 trillion by 2050, in the view of Bank of America Merrill Lynch estimations.

2.3 2021: A Turning Point for the European Union Space Programme

Beyond the socio-economic rationale, the rising need for space security in Europe is also driven by recent developments in the European space policy landscape and, more specifically, by advancements in EU space programmes and new initiatives, as well as the growing importance of synergies between civil and security related space activities.

2.3.1 Space Security, a Key Component for a 'Service-Driven' Policy

Looking at the substantial progress achieved by EU space programmes since their inception, and at the additional progress expected to be achieved by the end of the current multiannual financial framework, the period 2014-2020 will mark a turning point for the Galileo, EGNOS and Copernicus programmes. Whereas at the beginning of the period, in 2014, programme partners were focusing primarily on ensuring the successful development and deployment of the infrastructure, the spotlight is gradually shifting to the provision of services to end-users and to maximising benefits enabled by the infrastructure.

The European Commission recently published the results of mid-term evaluations of the Galileo, EGNOS and Copernicus programmes,[23,24] which highlight the considerable progression of these programmes, shifting from development to exploitation phases, and underline the new challenges raised by this advancement. In parallel, the EU, in close collaboration with ESA and EDA, is moving forward with the GOVSATCOM initiative that aims 'to ensure reliable, secured and cost-effective satellite communication services for the EU and national public authorities and infrastructure.[25] The challenges that lie ahead of the European Union space programme are multiple but, in accordance with the space strategy for Europe, can be summarised as follows:

- *Further advance* EU space programmes and meet new user needs
- *Encourage the uptake* of space services and data
- *Ensure the protection* and resilience of critical European space infrastructure
- *Reinforce synergies* between civil and security space activities

In other words, the significant progress of EU programmes and the introduction of new initiatives such as GOVSATCOM, have amplified the importance of a service-oriented space policy aimed at ensuring that all conditions for the delivery of operational space-based services conforming to user needs are met, including for users in the security sector. This is a prerequisite to building users' confidence, encouraging the uptake of space services, and consequently maximising the benefits of European space infrastructure for civil and security purposes. As underscored above, this is also a key area of space policy development in light of the growing dependence of the European economy and society on space infrastructure, including critical infrastructure such as telecommunications, energy and transport.

The conditions to guarantee an appropriate Quality of Service (QoS) to meet user needs in the long-term, include:

- *Performance through a proven or certi*fied level of performance
- *Stability* through the long-term availability of services and data
- *Security* through comprehensive protection of the service against threats

From an infrastructure standpoint, these conditions translate into 1) operational capacities that meet user performance requirements, 2) continuity of programmes to ensure infrastructure maintenance and upgrade, and 3) appropriate measures to protect the infrastructure against threats.

2.3.2 'Outer Space for Security' Nurturing the Need for 'Security in Outer Space'

The rising need for space security also lies in the increasing areas of application, in particular in the field of (ground) security. This strategic area encompasses various activities such

[23] European Commission (2017). REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the implementation of the Galileo and EGNOS programmes and on the performance of the European GNSS Agency. Brussels. Retrieved from European Commission: https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-616-F1-EN-MAIN-PART-1.PDF

[24] PwC (2017). *Interim evaluation of Copernicus*. Brussels: European Commission. Retrieved from Publications Europa: https://publications.europa.eu/en/publication-detail/-/publication/86fe47d6-c501-11e7-9b01-01aa75ed71a1/language-en/format-PDF/source-65409384

[25] European Commission (2016). Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions. Space Strategy For Europe. COM (2016) 705 final. Brussels: European Commission. Retrieved from https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/COM-2016-705-F1-EN-MAIN.PDF

as civil protection, police forces, border control, peace keeping, external actions and crisis management, to name a few.[26] Because of the nature of these activities, space-based services users in the security domain have stringent requirements and needs in terms of service availability, reliability, safety, integrity, and confidentiality. Here the concepts of 'Security in Outer Space' and 'Outer Space for Security' cross-fertilize each other, as it is the nature of the use of space infrastructure (i.e. for ground security) that nurtures the rationale to ensure its protection against threats.

In fact, although European countries' investment in military space activities has remained rather limited in comparison to the United States, space infrastructure has always provided services and data to defence and security actors in Europe. Space-based capabilities sought by users in the security sector range from high-resolution imagery to secured telecommunications through signal intelligence and early warning, among others. These services and data can be provided by space assets owned/operated by national military bodies, by commercial companies, or by civil institutions.

Although space infrastructure has long been used for a variety of security-related applications, recent developments in the European foreign, security and defence policy landscape are bringing new challenges and needs to the fore. The institutional setup is also evolving with the European Union taking an increasingly more prominent role in these fields, without undermining the role of Member States. Over recent years, the EU has developed various instruments and policy documents delineating its role, objectives and actions in the field of Security and Defence:

- A *Common Security and Defence Policy (CSDP)* reinforced with new provisions resulting from successive amendments to the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU). The EU CSDP comprises an institutional structure, instruments and agencies to enable the European Union to assume new responsibilities.
- The *European External Action Service (EEAS)*, managing EU's diplomatic relations with third-countries and conducting the EU Common Foreign & Security Policy (CFSP) of which the CSDP is an integral component. For space, the EEAS plays a central role in a number of areas. Among other things, the EEAS is in charge of coordination with Member States, external relations in cooperation with DG GROW and of space policies in relation with security and defence. In the Galileo programme, the EEAS, and especially its Head, the High Representative for Foreign Affairs and Security Policy (HR), have major responsibilities in the management of infrastructure security and emergency response according to the Joint Action defined by Regulation 2014/496.[27] The EEAS has organized itself for these purposes, notably by setting up a GNSS Threat Response Architecture (GTRA) including a group of experts in charge of organising a response in case of security issues related to the functioning of Galileo on a 24/7 basis. In the future, the EEAS will likely be further integrated within the institutional framework of the EU space programme with new responsibilities related to the extension of the Regulation 2014/496 scope to the whole European Union space programme (i.e. Galileo, EGNOS, Copernicus, GOVSATCOM, SSA) and, in general, new roles to support security architectures, synergies with security and defence policies and coordination with other European actors, Member States and third-parties.[28]
- A *European Agenda on Security* setting out European Union priorities for security and underlining how the European Union can bring added value to support the Member States in ensuring security;
- A *European Defence Action Plan*[29] proposing to:
  - Set up a European Defence Fund to support investment in joint research and the joint development of defence equipment and technologies (established in June 2017 – see below)

[26] Darnis, J. P., Veclani, A., & Nones, M. (2011). *Understanding the European Space Policy*. Paris: Fondation pour la recherche stratégique.

[27] European Union. (2014). Council Decision 2014/496/CFSP of 22 July 2014 on aspects of the deployment, operation and use of the European Global Navigation Satellite System affecting the security of the European Union and repealing Joint Action 2004/552/CFSP. Brussels.

[28] European Commission. (2018). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the space policy programme of the European Union, relating to the European Union Agency for Space and repealing Regulations (EU) No 1285/2013, No 377/2014 and No 912/2010 and Decision 541/2014/EU. Brussels

[29] European Commission. (2015). *The European Agenda on Security.* Brussels. Retrieved from European Commission: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

- Foster investments in SMEs, start-ups, mid-caps, and other suppliers to the defence industry
- Strengthen the Single Market for defence

- A *European Defence Fund*[30] to coordinate and increase national investment in defence research and improve interoperability between national forces. The fund was proposed in September 2016 and established in June 2017 with two components
  - Research: €90 million until the end of 2019, and €500 million per year after 2020
  - Development & Acquisition: €500 million in total for 2019-20, then €1 billion per year after 2020

As a result of these developments, security and defence aspects took a noticeable place in the space strategy for Europe endorsed by the European Union.[31] Addressed extensively throughout the document, the European Commission highlighted, in general, that 'space services can strengthen the EU's and Member States' capacity to tackle growing security challenges', that 'most space technologies, infrastructure and services can serve both civilian and defence objectives' and that 'synergies between civilian and defence areas can reduce costs, increase resilience and improve efficiency'. More specifically the strategy explains that 'additional services will be considered to meet emerging needs in specific priority areas, including […] (ii) security and defence to improve the EU's capacity to respond to evolving challenges taking into account 'the need to ensure adequate level of security of the infrastructure and services'. This strategic framework is aligned with the European Union defence action plan, which also highlight space's crucial enabling role for civilian and defence capabilities. Key actions in the field include the GOVSATCOM initiative and efforts to strengthen security requirements when developing EU space systems. This last element includes, or at least builds on, the European Commission objective to 'ensure the protection and resilience of critical European Union space infrastructure'.

These considerations, although made more visible in the latest strategy document, are not new and multiple actions and steps have already been taken in the frame of European Union space programmes.

Starting with Galileo, the system will answer a variety of security needs of European governmental actors, both at a national and European level (e.g. FRONTEX and peace-keeping operations). GNSS systems are already extensively used to support defence and security operations, such as localisation and navigation for troops and vehicles (both on the ground and in the air), mission planning, delivery of cargos, and search and rescue, among others [32]. During a conflict, GNSS-based services can be essential for the guidance of munitions, improving strike effectiveness and avoiding friendly fire, as well as for the navigation of Unmanned Aerial Vehicles (UAV) or for other operations such as rescue and evacuation.[33] Intentional, but also unintentional, interferences with GNSS signals such as jamming or spoofing can have dramatic consequences for defence and security operations. This is true for open and restricted signals that are often used in combination even by users in the security field.[34]

In anticipation, security concerns gave way to several measures within the Galileo programme including in particular the establishment of an independent Security Accreditation Board (SAB) within the European GNSS Agency (GSA). The SAB is in charge of verifying the compliance of the programme with the applicable security rules and regulations established by the Council and the European Commission, and of initiating and monitoring the implementation of security requirements to verify a high, robust and uniform level of security for EU GNSS systems.[35] Galileo Open Service will also will soon provide a Navigation Message Authentication feature, known as the Open Service Navigation Message Authentication (OS-NMA) which will eventually make it

[30] European Commission. (2017). *A European Defence Fund: €5.5 billion per year to boost Europe's defence capabilities*. Brussels. Retrieved from European Commission Press release: http://europa.eu/rapid/press-release_IP-17-1508_en.htm

[31] European Commission (2016). Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions Space Strategy For Europe. COM (2016) 705 final. Brussels: European Commission. Retrieved from https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/COM-2016-705-F1-EN-MAIN.PDF

[32] Mutschler, M. M. (2010). *Keeping Space Safe. Towards A Long-Term Strategy to Arms Control in Space. Frankfurt:* Peace Research Institute Frankfurt.

[33] Sitruk, A., & Plattard, S. (2017). *The Governance of Galileo*. Vienna: European Space Policy Institute. Retrieved from ESPI: https://www.espi.or.at/images/Rep62_online_170203_1142.pdf

[34] Ruegamer, A., & Kowalewski, D (2015). *Jamming and Spoofing of GNSS Signals – An Underestimated Risk?!* Retrieved from FIG: https://www.fig.net/resources/proceedings/fig_proceedings/fig2015/papers/ts05g/TS05G_ruegamer_kowalewski_7486.pdf

[35] European GNSS Agency (2016). *Security Accreditation.* Retrieved from European GNSS Agency: https://www.gsa.europa.eu/security/accreditation

more robust and resistant to jamming & spoofing attacks. Galileo High Accuracy Service will provide additional features to enhance the quality and resilience of the signals and therefore services. Among Galileo services, the Public Regulated Service (PRS) meets even more stringent security needs by providing an encrypted navigation service for governmental authorised users and sensitive applications that require high continuity including in case of malicious interferences such as spoofing (i.e. transmission of counterfeit GNSS signals) and jamming (i.e. intentional interference with GNSS signals). The Galileo infrastructure also includes the Galileo Security Monitoring Centre (GSMC), which is in charge of monitoring and taking action regarding security threats, managing PRS access on system level, implementing 'joint action' instructions in case of crisis, and providing PRS and Galileo security expertise and analysis.

For Copernicus, also, protection supports crucial strategic interests, affecting the implementation of several national and European policies and operations including in the field of defence and security. In fact, from a historical perspective, the Global Monitoring for Environment and Security programme (GMES, renamed Copernicus) was primarily conceived as a strategic asset with the objective of ensuring Europe´s autonomous access to information on its environment and security (i.e. ground situational awareness),[36] and supporting flagship European environmental and security policies.[37] This objective is still current today, and is covered by the numerous services enabled by Copernicus assets (i.e. Sentinel satellites) that are grouped in six main thematic areas:

- *Atmosphere:* Copernicus Atmosphere Monitoring Service (CAMS) provided by the European Centre for Medium-Range Weather Forecast (ECMWF);
- *Marine Environment:* Copernicus Marine Environment Monitoring Service (CMEMS) provided by Mercator Océan (i.e. the French centre for analysis and forecasting of the global ocean);
- *Land:* Copernicus Land Monitoring Service (CLMS) provided by the European Environment Agency (EEA) for the pan-European and local components and to the European Commission Joint Research Centre (JRC) for the global land component;
- *Climate Change:* Copernicus Climate Change Service (C3S) provided by the ECMWF;
- *Emergency Management:* Copernicus Emergency Management Service (CEMS) provided by the European Commission JRC;
- *Security:* Copernicus Security Service (CSS) provided by FRONTEX for Border Surveillance, by the European Maritime Safety Agency (EMSA) for Maritime Security, and by the EU SatCen for Support to External Action.

Copernicus data, through the Copernicus Emergency Management and Security Services, are actively used at all stages of disaster management (i.e. prevention, preparedness, response and recovery) and support a variety of security operations conducted by national and European organisations. In these fields, Copernicus products and services are used to support interventions inside and outside EU borders, for example in the frame of assistance of third countries in situations of crisis, through peacekeeping operations, conflict prevention and resolution activities, as well as in risk assessment of global and trans-regional threats that might bring political destabilisation.[38]

Finally, the upcoming GOVSATCOM initiative to ensure reliable, secure and cost-effective satellite communication services for EU and national public authorities and infrastructure will encompass, by design, a central and strong security dimension. In fact, security needs held a central position in both the 'Study on Satellite Communication to support EU Security Policies and Infrastructures' and in the subsequent 'Study in support of the impact assessment of an EU GOVSATCOM initiative',[39] which investigates various options for the implementation of the initiative. GOVSATCOM

[36] Note: As the Commission stated in the 2008 European Working document (European Space Policy Progress Report): 'European space capacities have become critical information tools in addressing a diversity of environmental, economic and security challenges of a global or regional scale. Autonomous access to information derived from space is thus a strategic EU asset. The EU will need to further strengthen its ability to respond to these challenges, including in the security and defence domains, both through improved coordination and through the development of own capacities'. See: http://ec.europa.eu/transparency/regdoc/rep/1/2008/EN/1-2008-561-EN-F1-1.Pdf

[37] EEAS (2017). *9th Conference on European Space Policy.* Retrieved from European Union External Action: https://eeas.europa.eu/headquarters/headquarters-homepage/19135/9th-conference-european-space-policy_en

[38] Regulation n. 911/2010 of the European Parliament and the Council of the 22nd of September 2010 on the European Earth Monitoring Programme (GMES) and its initial operations (2011 to 2013)

[39] PwC(2016). *Satellite communication to support EU security policies and infrastructures*. Brussels: European Commission. Retrieved from Publications Europa: https://publications.europa.eu/en/publication-detail/-/publication/92ce1a30-0528-11e6-b713-01aa75ed71a1/language-en

will, itself, support security aspects of other components of the EU space programme by providing secure communication links between remote parts of European space systems ground segments. In particular, GOVSATCOM will allow to connect remote sites requiring satellite communication links (e.g. sites located on islands in the Pacific, in the Arctic, etc.) and that are, currently, dependent on capabilities provided by commercial operators, sometimes from third countries.

2.4 European Autonomy and Freedom of Action

2.4.1 Strategic Stakes

Another essential driver is related to the strategic need for Europe to guarantee the security of its space infrastructure autonomously through independent capabilities, in particular for space situational awareness (i.e. systems, data, technologies). European autonomy and freedom of action in the field of security in outer space is a condition to fully achieving the 'independence' objective that initially motivated the launch of programmes such as Galileo.[40] Failing this, dependence on third countries would persist even though there would be a shift from direct dependence on foreign space systems (e.g. GPS) to dependence on foreign capabilities to secure European systems.

This necessity is acknowledged and addressed within the European Union's pillar objective of 'reinforcing Europe's autonomy in accessing and using space in a secure and safe environment'.[41] Although the strategy does not elaborate precisely on the details in the field of security in outer space, the Commission clearly states its intention to 'ensure [Europe's] freedom of action and autonomy'[42] in accessing and using space safely.

Such autonomy is not planned to be sought at the expense of cooperation with third countries, which is actually essential for effective and efficient action in the field of space security. Notwithstanding, Europe must ensure a capacity to control the level of reliance on its partners and to maintain it within acceptable boundaries.

2.4.2 The U.S.: a Leader in Space Situational Awareness Capabilities

Security in Outer Space has long been a strategic interest of the U.S., compelled by the military stakes of the Cold War related to ballistic missiles development and nuclear deterrence. Today, the U.S. SSA system is the most advanced in the world and relies on a wide national infrastructure called the U.S. Space Surveillance Network (SSN), a network of 30 surveillance sensors,[43] including radars and optical telescopes, operated by military and civilian entities.

It is the Joint Force Space Component Command (JFSCC since December 2017 - formerly the Joint Functional Component Command for Space), a component of the U.S. Strategic Command (USSTRATCOM), which, through the Joint Space Operations Center (JSpOC - recently renamed the 18th Space Control Squadron (SPCS)[44], operates the SSN to gather, catalogue and analyse SSA data. The Centre is one of the ten joint command centers of the U.S. Department of Defense (Unified Combatant Commands of the United States Department of Defense, DoD) and is funded by the U.S. military programme.[45] In this regard, the SSN system was originally conceived to detect objects of military significance, even though it quickly moved towards monitoring a diversity of other space objects. With ground-based radars and optical sensors located in 25 sites worldwide, SSN surveillance allows the U.S. to have unmatched mapping of orbiting objects and predict their trajectory, making interventions in advance possible, in case collisions can be predicted, or to foresee the re-entry of a body, as well as to monitor launches led by other states.[46]

Currently, the JSpOC is able to track approximately 22.000 objects about 10 cm in LEO and

[40] Kinnock, Neil. European Strategy for GNSS. SPEECH/98/210 of 20 Oct. 1998. Toulouse.
[41] European Commission (2016). Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions Space Strategy For Europe. COM (2016) 705 final. Brussels: European Commission. Retrieved from https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/COM-2016-705-F1-EN-MAIN.PDF
[42] Ibid
[43] International Academy of Astronautics (2017). *Space Traffic Management: Towards a Roadmap for implementation.* Paris: IAA Cosmic Study
[44] Phillips, C. (2017). *Time for common sense with the satellite catalog.* The Space Review. Retrieved from http://www.thespacereview.com/article/3215/1
[45] B. Weeden, P. Cefola, J. Sankaran (2013). *Global Space Situational Awareness Sensors, paper presented at the Advanced Maui Optical and Space Surveillance Conference*, Maui,p. 13. Retrieved from https://www.researchgate.net/publication/228787139_Global_Space_Situational_Awareness_Sensors
[46] Briani, V. (2011). *La Sicurezza nello Spazio: Risvolti Italiani e Internazionali, in Osservatorio di politica internazionale*, n.29,p. 5. Rome: Istituto Affari Internazionali

1m in GEO. However, these performances are expected to be improved to 200.000 objects including debris as small as 5 cm in LEO [47] with the deployment of the U.S. Space Fence, a $1,594 million programme[48] expected to be operational in 2019.[49] The U.S. Space Fence will cover a large majority of the 500.000 estimated items between 1 and 10 centimetres, which are so far not trackable, and increase the accuracy of payload identifications and risk conjunction predictions.[50] This significant upgrade will bring U.S. capabilities even further ahead of other space powers, including Europe, and will likely play a crucial role in ensuring the safety of space assets in particular thanks to the continuation of U.S. cooperation schemes confirmed by the last 2011 National Security Space Strategy.[51]

2.4.3 U.S. SSA Sharing Agreements

Partial access to American SSA data is granted to selected partners through a worldwide cooperation scheme. The American approach to cooperation was updated, formalised and expanded in 2004 by the Commercial and Foreign Entities (CFE) Pilot Program and gave way, in 2009, to a full-fledged SSA Sharing Program under the responsibility of the USSTRATCOM. Today, the U.S. has more than 70 unclassified SSA Sharing Agreements with commercial and institutional organisations. These SSA Sharing Agreements aim to support transparency on operations in outer space, promote cooperation for security and safety, enhance the availability of information among the partners, and improve the quality of U.S. SSA information.[52,53] In practice, SSA sharing agreements provide selected organisations, which are not affiliated to the Federal government, including foreign institutions and private operators, with free access to authorised data stemming from SSN sensors.

A vast majority of European public and private operators resort to this opportunity to meet their own needs. As a result, a share of European capabilities relies/depends on a series of Sharing Agreements with the U.S. signed by European intergovernmental organisations (i.e. ESA and EUMETSAT), Member States institutions (i.e. France, Germany, UK, Italy, Spain, Belgium) and a number of European commercial satellite operators and launch service providers.

JSpOC provides different levels of access to SSN data as shown in the following graph:

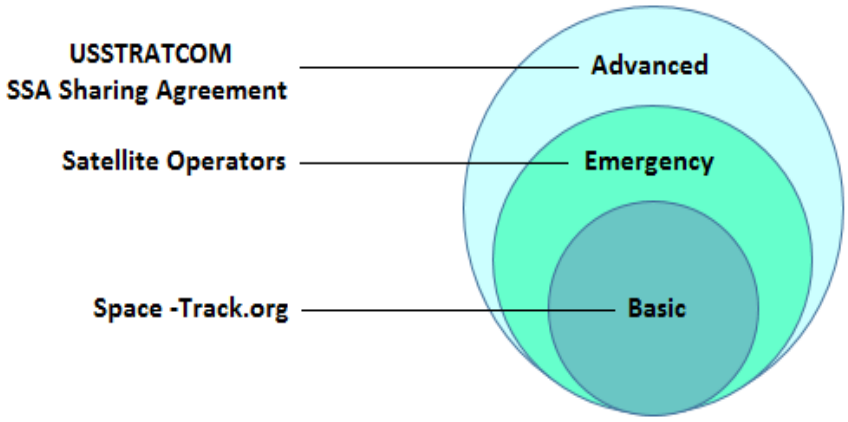

Figure 8: Data access to the U.S. SSA System

http://www.parlamento.it/application/xmanager/projects/parlamento/file/repository/affariinternazionali/osservatorio/note/Nota_29_IAI_Spazio.pdf

[47] Gruss, M. (2016). *Good (space) fences make for good (orbital) neighbors*. Retrieved from http://space-news.com/good-space-fences-make-for-good-orbital-neighbors/

[48] GAO (2015). *Defense Acquisitions Assessments of Selected Weapon Programs*. United States Government Accountability Office
Report to Congressional Committees: Washington. Retrieved from https://www.gao.gov/assets/670/668986.pdf#page=133

[49] Note: Just for needs of completeness, it should be noticed that the current Space Fence project goes to replace the previous Air Force Space Surveillance System, one of the SSN components active from 2008 to 2013.

[50] NASA (2010). *What Is Orbital Debris?* Retrieved from https://www.nasa.gov/audience/forstudents/5-8/features/nasa-knows/what-is-orbital-debris-58.html

[51] Department of defense, Office of intelligence of national intelligence (2011). *National Security Space Strategy*. Retrieved from https://www.hsdl.org/?view&did=10828

[52] Helms, S. (meeting of June 3, 2010) Space Situational Awareness. Power Point presentation for the United Nations Committee on Peaceful Uses of Outer Space (COPUOS).

[53] USSTRATCOM Public Affairs (2017). *U.S. Strategic Command, Norway sign agreement to share space services, data*. Retrieved from U.S. Strategic Command Peace is our Profession. Retrieved from http://www.stratcom.mil/Media/News/News-Article-View/Article/1142970/us-strategic-command-norway-sign-agreement-to-share-space-services-data/

JSpOC regularly tracks 22.000 objects in space and, comparing these predictions with other information, feeds a catalogue of about 16.000 of those objects, made available publicly and free of charge on the Space Track Platform accessible online at www.space-track.org. The Space Track catalogue provides the orbital position of space objects through the Two-Line Element sets (TLEs), the Satellite Catalogue data and the Satellite Decay & Re-entry Data. This constitutes the 'Basic service' offered by JSpOC. The 'Emergency notification service' seeks to identify close approaches for active payloads in orbit (between 20 and 30 per day) and to notify operators about the risk, through e-mails or Conjunction Summary Messages (CSMs). Last, the 'Advanced service' requires the setup of an SSA sharing agreement and involves two-way information exchange for a variety of activities including conjunction assessment, anomaly resolution, electromagnetic interference investigation, and support to launch, disposal, deorbit and re-entry.[54]

The U.S. also recently set up a series of partnerships with companies involved in commercial SSA data collection (e.g. ExoAnalytic Solutions Rincon, Lockheed Martin, LeoLabs) and in SSA value adding services (e.g. Analytical Graphics Inc., Boeing, Schafer Corp., Applied Defence Solutions).

Lastly, the U.S. has made an outstanding move toward the establishment of a civil space traffic management framework that will be entrusted to the Department of Commerce (DoC) instead of the Federal Aviation Administration (FAA) as was expected.[55] Although "space situational awareness and space traffic management are distinct concepts with different technical requirements and policy implications",[56] they are entangled in a number of ways and the construction of such a civil STM framework will imply a partial and progressive transfer of responsibility, not yet determined, between the U.S. DoD and DoC. This transfer of responsibility and overall governance change will likely impact cooperation agreements, including with European partners, and will open the market for SSA data and added-value services to private companies.[57]

2.4.4 European Autonomy and American Leadership

Cooperation on security in outer space is unavoidable for the overall success and efficiency of a variety of actions and measures including, in particular, the development of advanced SSA capabilities and safety of operations in outer space. From this standpoint, transparency, data sharing and coordination between international partners bring clear benefits for all, ranging from improved monitoring capacities (e.g. quantity of objects tracked, precision of measurements) to enhanced security (e.g. collision avoidance, monitoring of proximity operations).

From a strategic perspective however, cooperation with third countries, as beneficial as it may be, cannot become the sole corner stone. In other words, although access to foreign SSA data and services is a relevant way to augment domestic SSA capabilities. Such access, even deemed unrestricted, free and guaranteed, cannot constitute a critical input on which they depend. Assessing the criticality of U.S. SSA data and services for European stakeholders is challenging as there is no clear threshold identifying a minimum, required, level of capabilities that would be strategically acceptable. Notwithstanding, the discrepancy between European and American capabilities in the field of SSA, expected to increase substantially with the deployment of the U.S. Space Fence, somehow creates a situation of reliance/dependence for European stakeholders and an imbalance in cooperative arrangements.

Beyond this general strategic principle, this state of affairs also brings the following issues, including:

- *SSA data and service restrictions:* Even though JSpOC grants access to SSN-based data and services to commercial and foreign partners, restrictions exist. Because of its intrinsic military nature, a lack of transparency or a delay in information provision can occur for a variety of motives related to U.S. national security.[58] Although open, Brian Weeden of the Secure World Foundation notes that ´the SSA sharing strategy unveiled by the

[54] Major Courtland B. McLeod. *Space Situational Awareness (SSA) Sharing.* United States Strategic Command Space Policy. Retrieved from http://www.unoosa.org/pdf/pres/stsc2012/tech-40E.pdf

[55] White House. (2018). Space Policy Directive-3, National Space Traffic Management Policy. Washington. Retrieved from *https://www.whitehouse.gov/presidential-actions/space-policy-directive-3-national-space-traffic-management-policy/?mc_cid=c4111beda6&mc_eid=8b6815cdba*

[56] Nightingale, Bhavya, Weeden, Picard, Eisenstadt (2016). *Evaluating Options for Civil Space Situational Awareness (SSA).* Washington: scienc e & technology policy institute. Retrieved from https://www.ida.org/idamedia/Corporate/Files/Publications/STPIPubs/2016/P-8038.ashx

[57] INFRASTRUCTURE & TECHNOLOGY (2018). *Remarks by Vice President Pence at the 34th Space Symposium, Colorado Springs, CO*. Colorado. Retrieved from WhiteHouse.gov. Retrieved from https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-34th-space-symposium-colorado-springs-co/

[58] Specifically, the DoD resistance to open SSA data sets, algorithms, and processes to external review and scrutiny

USSTRATCOM in 2014 has led to removal of more SSA data from public access, including data on the estimated size of space debris objects in the public satellite catalogue, and limitations on what data is provided privately to satellite operators, due to national security concerns´.[59]

- *Reliability and accountability:* Although advanced, the U.S. system is not flawless and may provide wrong information due to measurements or processing errors, in particular for smaller objects that Europe cannot track.[60] Sharing agreements discharge U.S. organisations of any liability for the information provided, which raises the necessity for Europe to be able to verify the data that are provided or to find itself fully exposed to errors of foreign systems.
- *Uncertainty on future access:* The U.S. Government holds the right to terminate the user account at any time for any reason, to limit both access duration and data amount for *any* user, to deny access to SSA data and information, and to change or modify the terms and conditions at any time, and without prior notification.[61] The U.S. Government also has the option to change the 'free access' policy and to start charging SSA services.[62] Yet, the involvement of the U.S. Government in the field of civil SSA is being challenged and the current open policy may progressively and partially give way to commercial agreements based on services offering by public agencies, or, more likely, by private providers.[63]

In a nutshell, although cooperation is a necessity in the field of space security, and Europe benefits greatly from the open policy of the U.S., it should not be relied upon at the expense of European autonomy and freedom of action. From this perspective the current state of affairs does not provide a sustainable solution for Europe.

results in the uncertainty of the data and in possible false positive rates. See: https://www.ida.org/idamedia/Corporate/Files/Publications/STPIPubs/2016/P-8038.ashx

[59] Weeden, B. (2016). *Time for the U.S. military to let go of the civil space situational awareness mission.* Retrieved from SpaceNews: http://spacenews.com/time-for-the-u-s-military-to-let-go-of-the-civil-space-situational-awareness-mission/

[60] Froeliger, J. L. (2017). *Greater Industry Cooperation Needed to Avoid Space Collisions.* INTELSAT http://www.intelsat.com/news/blog/greater-industry-cooperation-needed-to-avoid-space-collisions/

[61] Space-Track. *User agreement.* Retrieved from https://www.space-track.org/documentation#/user_agree

[62] Ibid

[63] Nightingale, Bhavya, Weeden, Picard, Eisenstadt (2016). Evaluating Options for Civil Space Situational Awareness (SSA). Washington: scienc e & technology policy institute. Retrieved from https://www.ida.org/idamedia/Corporate/Files/Publications/STPIPubs/2016/P-8038.ashx

3. Rising Threats to the European Space Infrastructure Security

To build a comprehensive picture of space security challenges to the European space infrastructure, the following section seeks to characterize the threats affecting the safety of space infrastructures and the long-term sustainability of space activities.

These threats are grouped in three categories:

- *Passive man-made threats*, including unintentional man-made hazards to space infrastructures such as space debris or unintentional interferences to signals;
- *Active man-made threats,* including intentional attacks on space infrastructures such as anti-satellite capabilities, malicious interferences and cyberattacks;
- *Natural threats,* including space weather hazards such as geomagnetic storms, solar radiation storms or disturbance of the ionosphere.

Security challenges specific to the ground segment, such as Earth natural hazards, physical attacks on facilities or eavesdropping (e.g. sabotage) were not included in this overview.

3.1 Passive Man-Made Threats: an Increasingly Congested Space Environment

3.1.1 Space Debris

Among rising threats to an accessible and safe to operate space environment, the growing number of space debris and the resulting congestion of some orbits has become a central topic raising major concerns in the space community. In various venues, experts routinely caution governments and operators about the escalating threat of space debris to space operations, which, if not addressed properly and timely, could seriously jeopardize the long-term sustainability of space activities.

Space debris, also known as orbital debris, are defined by the Inter-Agency Space Debris Coordination Committee (IADC) as 'all man-made objects, including fragments and elements thereof, in Earth orbit or re-entering the atmosphere, that are non-functional'[64]. Although measures can be taken to mitigate the creation of these non-functional elements, space debris remain, first, a natural by-product of space exploration and exploitation activities. Today, it is estimated that 29,000 objects larger than 10 cm are orbiting the Earth along with 750,000 objects from 1 to 10 cm and roughly 166 million from 1 mm to 1 cm.[65]. Debris include launcher upper stages, inoperative spacecraft, mission-related debris - such as paint fracks or parts of release mechanisms - and fragmentation debris stemming from explosions or collisions. These last events, that can happen intentionally, for example during anti-satellite technology tests, or unintentionally, when satellites collide, are rare but have dramatic consequences, creating hundreds or thousands of debris.

The following figure shows the evolution of the space debris population regularly tracked by the U.S. Space Surveillance Network (>10cm on Low Earth Orbit and >1m in other orbits). Only the largest debris are counted here which represents a small portion of all debris in orbit.

On the graph, the continuous and steady evolution of rocket bodies, inoperative spacecraft and mission-related debris can be explained by the fact that these objects are direct consequences of regular space activities. Spikes in recent years are the results of two major events in 2007 and 2009 – respectively, a Chinese ASAT kinetic test on the decommissioned weather satellite Feng Yun 1C and a collision between the Russian satellite Cosmos 2251 and the American satellite Iridium 33. Together, these two events increased the space debris population by 40%. The collision between Cosmos 2251 and Iridium 33 created 1,366 pieces larger than 10 cm set to remain

[64] Inter-Agency Space Debris Coordination Committee (2013). *Key Definitions of the Inter-Agency Space Debris Coordination Committee IADC.* Retrieved from http://www.iadc-online.org/Documents/IADC-2013-02,%20IADC%20Key%20Definitions.pdf

[65] ESA (2017*). Space debris*. Darmstadt: ESA's Space Debris Office at ESOC. Retrieved from European Space Agency: http://www.esa.int/Our_Activities/Operations/Space_Debris/Space_debris_by_the_numbers

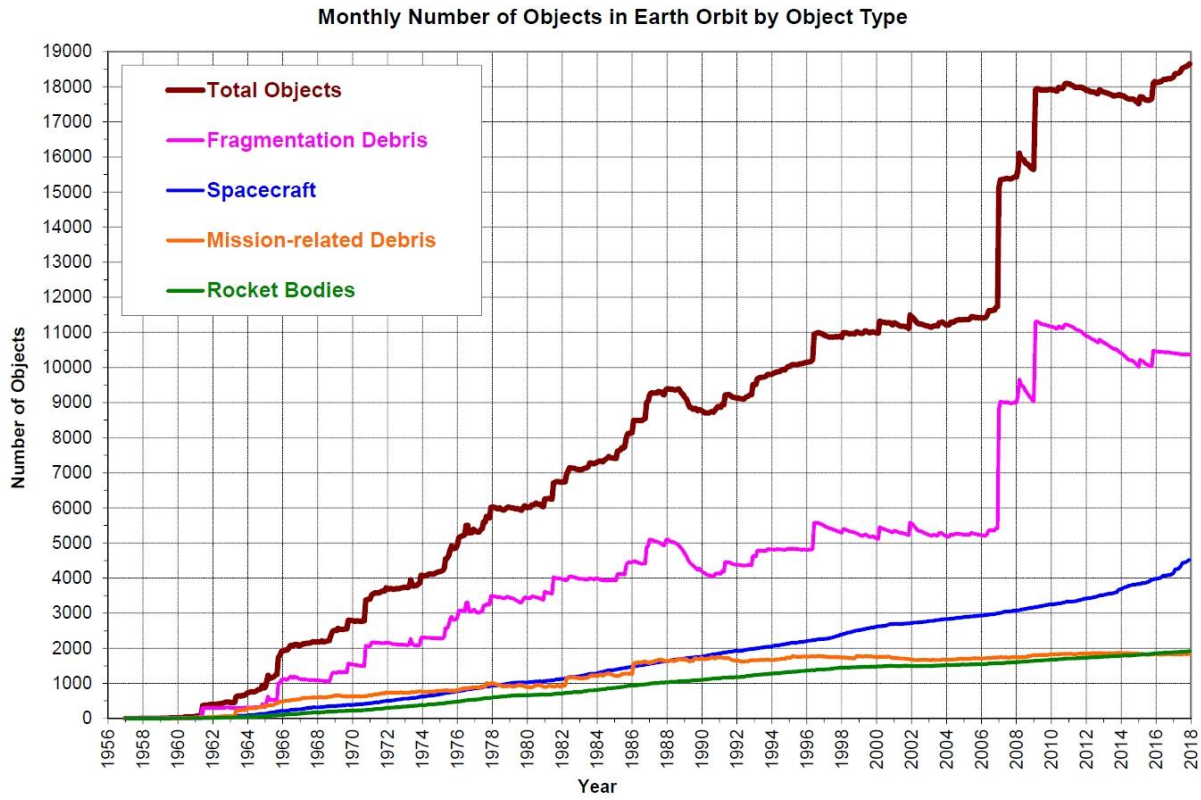

Figure 9: Count evolution by object type between 1957 and 2017 (Source: NASA)

in orbit for 20 to 100 years.[66] In 2017, and despite growing efforts to mitigate space debris creation, the number of space debris reached an all-time high.

Although large objects account for the vast majority of the total debris mass and present an obvious threat, they are simpler to track and account for a very small share of the overall debris population. Smaller fragments of satellites or launchers are, in contrast, much more numerous and difficult to track, creating a more persistent threat that is difficult to detect. Regardless of the debris size and mass, the consequences of a collision with a space debris for an operational satellite can be dramatic: when orbiting at high velocity, even the smallest piece of debris can have devastating consequences as it can reach a relative speed of 27,000 km/h.[67] An object as small as 5 mm can disrupt or even completely incapacitate a satellite.[68] This means that each debris is a serious hazard to operational systems in orbit, and also to astronauts. In 2014, for example, the International Space Station performed an emergency avoidance manoeuvre because of a 14cm chunk of space debris.[69]

Although congestion of the space environment by orbital debris is a broad concern affecting all systems in orbit, space infrastructures are not equally threatened by space debris. Indeed, a number of factors must be taken into account to assess the threat more precisely. For example, all orbits are not impacted by space debris in the same way according to the altitude (i.e. which impacts the re-entry time of space debris, for example), the intensity of the activity on the orbit, and the efforts in maintaining the orbit free from orbital debris (e.g. satellite end-of-life requirements). Low Earth Orbit, which is the region of space with the most intense activity but also the region of space where collisions and explosions have occurred, counts the largest share of orbital debris. In this region, which includes a variety of orbits below 2,000 km of altitude, specific orbits can be more affected than others. The

[66] (Kelso, 2009). It should be added that it is after this accident that the U.S. Strategic Command put in place a new programme called Space Situational Awareness (SSA) Sharing. See: https://armedservices.house.gov/legislation/hearings/hearing-space-posture-review-and-fy2011-national-defense-authorization-budget

[67] Moon, M. (2017*). The Space Domain and Allied Defence Report*. Brussels: Sub-Committee on Future Security and Defence Capabilities, NATO Parliamentary Assembly.

[68] Bonnal, C. (2016). IAA Situation on Space Debris. International Academy of Astronautics. Paris: International Academy of Astronautics (IAA). Retried from *http://www.iaaweb.org/iaa/Scientific%20Activity/sg514finalreport.pdf*

[69] Pigoni, L. (2015). *Space: The New Frontier of Security Policy'.* CSS Analysis in Security Policy. Retrieved from https://www.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse171-EN.pdf

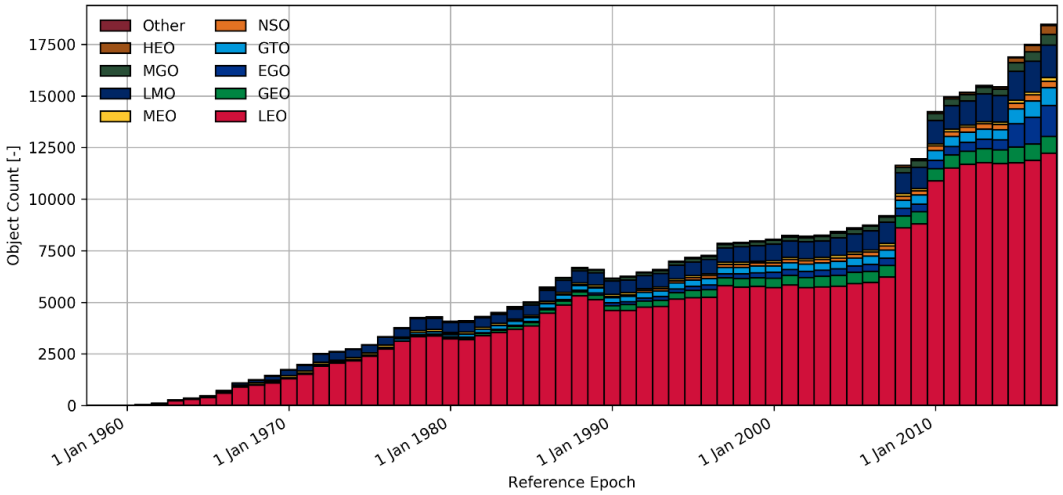

Figure 10: Count evolution by object orbit between 1957 and 2017 (Source: ESA)[70]

following figure, extracted from ESA's DISCOS database (Database and Information System Characterizing Objects in Space) shows the distribution of space debris by orbit.

The multiplication of space debris is raising growing concerns among experts for many reasons: it is unavoidable, indiscriminate, and uncontrollable, especially in very crowded orbits such as LEO.

On the longer-term, sustainability of space activities could be seriously jeopardized, notably by the intensification of space activities and by the so-called 'Kessler syndrome', the former aggravating the latter. Theorized by NASA scientist Donald Kessler in 1978, the Kessler syndrome predicts a cascading effect on the space debris population.[71] As the number of space debris grows, the risk of collisions also increases. Therefore, as space debris beget space debris, further collisions between debris would create evermore debris eventually rendering orbital slots impossible to use. Yet space activity, both in terms of launches and satellites in orbit, is expected to increase very rapidly in the coming years as suggested by FAA's forecast provided below, making the problem of space debris more pressing. This is explained by several factors including the growing popularity of smallsats, in particular cubesats, new concepts such as LEO mega-constellations and, in general, growing investment in the space sector.

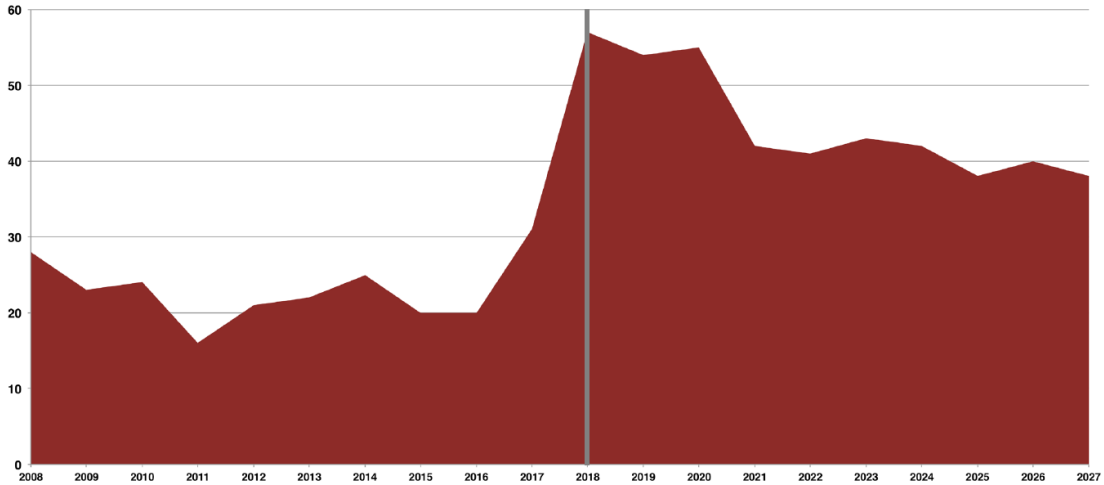

Figure 11: Historical and projected number of commercial orbital launches
(Source: FAA Commercial Compendium of Space Transportation 2018)

[70] Orbits: GEO (Geostationary Orbit); IGO (Inclined Geosynchronous Orbit); EGO (Extended Geostationary Orbit); NSO (Navigation Satellites Orbit); GTO (GEO Transfer Orbit); MEO (Medium Earth Orbit); GHO (GEO-superGEO Crossing Orbits); LEO (Low Earth Orbit); HAO (High Altitude Earth Orbit); MGO (MEO-GEO Crossing Orbits); HEO (Highly Eccentric Earth Orbit); LMO (LEO-MEO Crossing Orbits); UFO (Undefined Orbits); ESO (Escape Orbits)

[71] Kessler, D., & Cour-Palais, B. (1978). *Collision Frequency of Artificial Satellites:* The Creation of a Belt Debris. Journal of Geophysical Research vol.83, 2638-2648. Retrieved from Webcharter: http://webpages.charter.net/dkessler/files/Collision%20Frequency.pdf

3.1.2 Accidental Interferences

The radio frequency spectrum is an essential component of space activities. Indeed, a vast majority of satellites use a fraction of it to communicate with the ground or other satellites. The radio frequency spectrum is used by space infrastructures for two main functions:

- *Telemetry, Tracking and Control (TT&C):* By using long, medium, short, ultra-, and micro-waves, satellites can receive instructions from the ground-controller (*up-link)* and return information to the ground-controller (*down-link)*.
- *Satellite payload mission:* Space systems, such as telecommunication and navigation satellites among others, use the radio spectrum as part of their mission to receive and transmit signals (e.g. PNT signals, broadcast channels…).

Although it is a crucial element of the space infrastructure, that spectrum can be altered by so-called Radio Frequency Interferences (RFI). RFI can be defined as events or activities which disturb or disrupt communication channels. While 'permissible or accepted interferences' are normal, expected, and tolerated, in the frame of nominal satellite operations, "harmful interference', however, can 'endanger the functioning of a radio navigation service or of other safety services or seriously degrades, obstructs, or repeatedly interrupts a radio communication service operating'[72]. Such RFI can have severe consequences both at user level, temporarily affecting the quality of space-based services including for critical applications such as air traffic management, and at system level, causing long-term degradation of services.[73] A variety of RFI exist, stemming from natural causes (e.g. space weather events or Earth atmosphere effects), or from human activity in space and on the ground. In the latter case, interferences can be intentional (malicious) or unintentional (accidental).

Looking into unintentional and accidental interferences (i.e. natural and malicious interferences are addressed later in this chapter), a variety of sources exist: technical and planning errors (e.g. uplink personnel mistakes), equipment (e.g. bad installation of devices, poor equipment, equipment failure…), adjacent satellite interference, and terrestrial service interference on shared bands[74]. Accidental interferences account for almost 90% of satellite interference (i.e. a majority arises from technical errors) and pose a threat to space infrastructures in multiple ways.

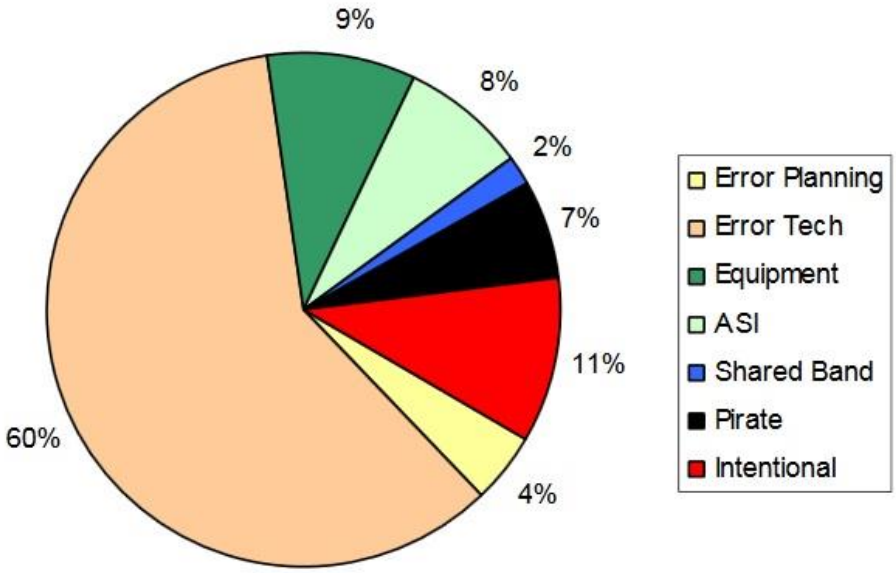

Figure 12: Share by type in interferences

[72] Matas, A., (2016). CONFLICTS RELATED TO RADIO FREQUENCY INTERFERENCE ABUSE OF ITU REGULATORY PROCEDURES

[73] Canzian, L., & al. (2017). Interference Localization from Space.

[74] Öz, I. (2013). *Harmful Interference: Regional Security Consequences*. Astana: Turksat. Retrieved from UNIDIR: http://www.unidir.ch/files/conferences/pdfs/harmful-interference-regional-security-consequences-en-1-933.pdf

Although the vast majority of accidental interferences are part of business-as-usual and result from the efforts of operators to continuously improve the quality of their service, the growing number of Adjacent Satellite Interferences (ASI) is, however, a direct result of the increasing congestion of the space environment. Every satellite into orbit has the potential to cause ASI and the multiplication of objects in space therefore irremediably leads to a growing threat of ASI[75].

Intelsat's Galaxy 15, or 'Zombiesat', is a famous example.[3] In 2010, Intelsat lost contact with this satellite in GEO preventing the company from performing manoeuvres. The satellite started drifting past other working satellites in that orbital region. As Galaxy 15 onboard equipment was still operational, the satellite could still receive and re-broadcast signals meant to be received by other functioning satellites. Eventually, Intelsat managed to re-establish contact with Galaxy 15 thanks to the cooperation of other satellite operators. Another example of that problem happened in 2002 when a poorly installed CCTV camera on the Isle of Man (Douglas) blocked the GPS signal within a kilometre. Unintentional interference was reported by the Engineering section of the Stanford University campus in 1999. The GPS signal went missing in that area with a radius of 1 kilometre, also affecting helicopters transporting severe cases to Stanford Hospital.[76] The designers of the offending device were not aware of their capability to disrupt the GPS signal.

Comparable to space debris, interferences, and in particular accidental ones, pose a persistent threat to space infrastructures in general as most spacecraft are equipped at least with TT&C subsystems. However, systems using the radio spectrum for payload operations can be more vulnerable than others. For example, Global Navigation Space Systems (GNSS) such as Galileo, which involve numerous up-link and down-link channels for continuous signal corrections and global broadcast of signals.

3.2 Active Man-Made Threats: an Increasingly Contested Space Environment

Comparable to other critical infrastructures, space systems are strategic targets for a range of actors including governments, military and intelligence agencies, armed groups and terrorists, but also individuals such as hackers. For a variety of motivations, these organisations and individuals can seek to incapacitate, exploit or take control of space assets with the objective of disrupting space-based services or accessing protected information. Such attack against space infrastructure can have a range of potentially dramatic consequences. These threats, referred to in this report as 'man-made active threats', are not limited to military space assets in the event of open conflicts and on theatres of operations. Although the threat may vary in intensity according to systems or geopolitical conditions, it remains ubiquitous and inclusive, menacing any system, anywhere, anytime.

Here, civil and military dimensions coexist with concerns over assets protection shared by governmental, military and commercial stakeholders who may, however, perceive threats differently and pursue different objectives. The overarching objective to protect national space infrastructure remains, nevertheless, with governments as part of national security and defence strategies. From this standpoint, the integration of space infrastructures as assets of interest in defence and security strategies is not new, as space activities have always had strategic implications. However, as space-based capabilities gain in importance for the economy, society and security, space infrastructure becomes an increasingly central component and its protection a growing concern. This has led to the development of doctrines, capabilities, and technologies around the concept of space control, which encompasses both defensive (i.e. capacities to protect space assets) and offensive (i.e. capacities to strike space assets) dimensions with the ultimate objective to gain 'space superiority'[77]. The concept of 'space warfare', which was dominant during the Cold War but lost significance after that, is currently being rehabilitated. In August 2017, Gen. John 'Jay' Raymond, commander of the U.S. Air Force Space

[75] Intelsat General Corporation (2015). *Battling Satellite Interference — A View from the Front Lines.* Retrieved from SpaceNews: http://spacenews.com/battling-satellite-interference-a-view-from-the-front-lines

[3] SWF (2015). *Radio Frequency Interference*. Retrieved from Secure World Foundation: https://swfound.org/space-sustainability-101/radio-frequency-interference/

[76] Pullen, S., Gao, G., Tedeschi, C., & Warburton, J. (2017). *The Impact of Uninformed RF Interference on*. Retrieved from citeseerx: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.224.6672&rep=rep1&type=pdf

[77] Hostbeck, L. (2015). *Space Weapons´ Concepts and Their International Security Implications*. In K. U. Schrogl, Handbook of Space Security (pp. 955-983). New York: Springer.

Command summarized the situation by explaining that, today, 'space is a war-fighting domain just like air, land and sea'[78].

In a nutshell, with the growing importance of space systems, two complementary dynamics have recently gained momentum[79, 80]:

- The development of offensive capabilities to attack space systems
- The development of defensive capabilities to detect and act against such attacks

Offensive means, i.e. man-made active threats from a space security standpoint, include three main categories:

- *Anti-Satellite Weapons,* including means to physically incapacitate space systems;
- *Malicious interferences***,** including means to interrupt or disturb radio uplinks and downlinks;
- *Cyberattacks,* including means to breach space infrastructure networks and systems software, including taking control of one and/or several satellites simultaneously[81].

3.2.1 Anti-Satellite Weapons

Several military technologies able to strike assets in space (i.e. 'space denial' or 'counter-space' capabilities) have been developed by various governments since the Cold War. As of today, the United, States, Russia and China,[82] have reportedly tested counter-space capabilities which could already, or soon, translate into full operational capacity to make direct attacks against space assets.[83,84]

Counter-space capabilities that could potentially be used against European space assets include:

- Ground-based kinetic weapons are 'weapons that use kinetic energy, or energy of motion, to kill an object.'[85] Instead of using explosive material, the energy released by high-speed collision neutralizes the space asset. This method is considered as relatively low tech. ASAT testing reached a peak in 2007 when China, Russia, and the United States all performed tests in real conditions. The People's Republic of China, after two non-destructive tests in 2005 and 2006, intentionally destroyed one of its old non-operational weather satellites, Fengyun-1C, with a land-based ballistic missile –the SC-19 direct-ascent antisatellite missile. Before that event, the last ASAT test dated back to 1985 and was performed by the United States.[86] Even though a great number of space debris were created during the explosion, the legitimacy of the test *per se* was not questioned. In February 2008, the destruction of the defunct satellite USA 193, described as a public safety measure motivated by the danger posed by the toxic hydrazine stocked in the fuel tank,[87] was presumably an ASAT test. This latter, however, was conducted under safer and less polluting parameters. In 2010, 2013,[88] and 2014, China conducted land-based interception tests[89] that the U.S. considered to be ASAT tests, using the same missile.[90] This time, fortunately, the missile was on a suborbital trajectory, causing less pollution than the explosion

[78] Fabey, M. (2017). *U.S. Space Command develops operational concepts for waging war in orbit*. Retrieved from SpaceNews: http://spacenews.com/u-s-space-command-develops-operational-concepts-for-fighting-war/
[79] Pasco, X. (2015). *Various Threats of Space Systems.* In K.-U. S. al., Handbook of Space Security (pp. 673-674). New York: Springer.
[80] Weeden, B. (2013). *Radio frequencies Spectrum, Interference and Satellites Fact Sheet*. Retrieved from Secure World Foundation: https://swfound.org/media/108538/swf_rfi_fact_sheet_2013.pdf
[81] Note: Malicious interferences and cyberattacks overlap to some extent as rogue signals can be used as a mean to access the space infrastructure network, in particular systems in space to conduct cyberattacks.
[82] Weeden, B. (2014). *Through a glass, darkly: Chinese, American, and Russian anti-satellite testing in space*. Retrieved from The Space Review: http://www.thespacereview.com/article/2473/1
[83] Johnson-Freese, J. (2014). Space Warfare in the 21st Century: Arming the Heavens. New York: Routledge.
[84] *Under Trump, GOP to Give Space Weapons Close Look.* Retrieved from Roll Call: http://www.rollcall.com/news/politics/trump-gop-give-space-weapons-close-look
[85] Office of Technology Assessment. (2014). *Strategic Defenses: Two Reports by the Office of Technology Assessment*. New Jersey: Princeton University Press.
[86] Weeden, B. (2014). *Through a glass, darkly: Chinese, American, and Russian anti-satellite testing in space.* Retrieved from The Space Review: http://www.thespacereview.com/article/2473/1
[87] National Research Council. (2011). Limiting Future Collision Risk to Spacecraft: An Assessment of NASA's Meteoroid and Orbital Debris Programs. Washington D.C.: National Academies Press
[88] Wright, D. *How High Did China's May 2013 Launch Go?* Retrieved from Union of Concerned Scientists: http://allthingsnuclear.org/dwright/how-high-did-chinas-may-2013-launch-go
[89] Gertz, B. (2015). *China Tests Anti-Satellite Missile New ASAT interceptor threatens U.S. spy satellites.* Retrieved from The Washington Free Beacon: http://freebeacon.com/national-security/china-tests-anti-satellite-missile/ See also: Vasani, H. (2017). *How China Is Weaponizing Outer Space.* Retrieved from The Diplomat: http://thediplomat.com/2017/01/how-china-is-weaponizing-outer-space/
[90] Rose, F. (2015). *Written Remarks Delivered to the Federation of American Scientists*. Washington D.C: Bureau of Arms Control, Verification and Compliance.

of Fengyun-1C.[91] Russia joined the race in 2016 – the Soviet Union already had several ASAT R&D programmes during the Cold War, using the direct ascent anti-satellite missile A-235 Nudol,[92] but without destroying any target.[93]

- Ground-based non-kinetic weapons, or soft weapons, do not involve the destruction of the space asset but are used to incapacitate them and therefore do not generate space debris. A handful of states are pursuing the development of such capacities. These threats mainly consist of direct energy weapons (DEW) using a laser beam against the target, and Radio Frequency Weapons (RFW) using microwave techniques. They can produce three types of effects (organized by intensity of the threat)[94]:
    - *Jamming effect,* when the disturbance is limited in time and stops when the weapon is not focusing the target;
    - *Disruption effect,* when the disturbance is permanent - even though there is no definitive destruction - and an external intervention or reset is required to repair the system;
    - *Destructive effect,* when there is a definitive disruption requiring external intervention.

  DEW have an impact on receivers or specific kinds of sensors, their effects depending on their functionalities.[95] DEW, directing concentrated energy towards a target on a line-of-sight trajectory, can almost instantly disrupt or destroy equipment and facilities. When set at low energy level, they can blind or damage satellites' optical sensors; when set at high energy level, they can cause physical damage. RFW can damage or destroy electronic components of satellites by overheating or short-circuiting them. [96] While existing DEW are mostly ground-based (i.e. placing them into orbit being too expensive and representing a bigger technical challenge), RFW can be ground-based, space-based or fitted on missiles, posing a more serious threat than laser beams. It is believed that China fired a high-powered laser at a U.S. satellite in 2006, with the intent to either locate or blind it, temporarily degrading the satellite's functionality.[97]

- *Space-based weapons,* involve manoeuvrable spacecraft (i.e. spacecraft equipped with advanced mobility sub-systems – propulsion, attitude and orbit control) used for ASAT purposes through:
    - *Deliberate Collision* with a target satellite, resulting in a total, or partial, destruction of the two objects. Such operations can be conducted by spacecraft specifically designed and deployed for this purpose but could also be hypothetically conducted by standard satellites hijacked and directed to collide with another spacecraft.
    - *Hostile Proximity Operations (RPO)* disrupt a target satellite in close distance through the use of devices such as blinding laser beams or jammers. Various cases of passive hostile RPO have been reported recently, but general uncertainty remains with regards to the goals being pursued (i.e. passive observation and intelligence, technology tests and demonstration…). So far, a handful of space-faring nations such as China, Russia, and the United States, have displayed an interest in developing such technology as part of their deterrence strategies.[98]

  From a technical standpoint, a parallel can be made between such ASAT capabilities and the on-going development of technologies such as on-orbit servicing or Active Debris Removal, which build on comparable key technologies. This suggests that, in the future, such technologies could become more and more available on the

[91] U.S.-China Economic and Security Review Commission. (2015). *China's Space and Counterspace Programs*. Washington: USCC. Retrieved from https://www.uscc.gov/sites/default/files/Annual_Report/Chapters/Chapter%202%2C%20Section%202%20-%20China%27s%20Space%20and%20Counter-space%20Programs.pdf

[92] Lewis, P., & Livingstone, D. (2016). *What to Know About Space Security*. Retrieved from Chatham House: https://www.chathamhouse.org/expert/comment/what-know-about-space-security

[93] Gerty, B. (2016). Retrieved from Washigton Free Bacon: http://freebeacon.com/national-security/russia-conducts-fifth-test-new-anti-satellite missile/?utm_content=buffer94877&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer%20See%20also:%20http://www.washington-times.com/news/2016/dec/21/russia-test

[94] Pasco, X. (2015). Various Threats of Space Systems. In K.-U. S. al., Handbook of Space Security (pp. 673-674). New York: Springer.

[95] Ibid

[96] US-China Economic and Security Review Commission (2015). *Report to Congress of the US-China Economic and Security Review Commission*. Washington: US Government Printing Office.

[97] Ibid

[98] Note: As a matter of fact, manoeuvrability of spacecrafts is not only limited by fuel availability, but especially in case of non-cooperative targets, the rendezvous success also requires precise orbit data and trajectory calculations.

market and that operators will increasingly need to be able to detect and identify the intentions of manoeuvring objects thanks to 'optical tracking, [the] interpretation of ground communication data and [the] interception of the payload's telemetry signals'[99]. When hostile manoeuvres are detected, protecting the asset against this threat will likely be as important as identifying the source of the threat (i.e. spacecraft operator or owner).

3.2.2 Malicious Interferences: Satellite Signals Jamming and Spoofing

Among RFI techniques, malicious interferences include all intentional disruptions or deceptions of uplink or downlink signals aiming to disturb space systems' operations and/or delivery of space-based services[100]. Even though this kind of interference makes up only 11% of all reported interferences, it is becoming more frequent. Motivations behind such obstruction or misinformation attempts are multiple, ranging from governmental censorship to deny a population access to satellite-based information services, to logistics professionals seeking to block or deceive the monitoring of their position. Malicious interferences are also a growing component of warfare with opponents seeking to deny or exploit satellite support to ground operations (e.g. positioning and navigation, telecommunication).

Malicious interferences include two main categories of threats: Jamming and Spoofing.

Jamming is a type of signal-based attack that aims to disrupt authorized radio communication signals. From a technical perspective, malicious interferences usually involve the emission of rogue radio signals that disrupt a target signal by decreasing its signal-to-noise ratio. Jamming can be done at any point of the communication channel: at both ends, in space, or on the ground, by directly targeting satellites, ground stations or user equipment communication sub-systems (i.e. antennas, receivers, emitters, transponders…) and by interfering locally with radio signals at any point between space and ground systems.

Numerous examples of satellite jamming have occurred in recent years. For example, in 2010, the UN leading communication agency called on Iran to end jamming of satellite broadcasts[101]. During the Arab Spring in 2010-2012 satellite jamming rose dramatically in quantity and duration, targeting news agencies notably BBC Middle East, France 24, Deutsche Welle and the Voice of America,[102] and GPS signals were regularly under siege during the Crimean crisis in 2014[103]. These are only a few notable examples among many others. Overall, there were 75 times more jamming cases in 2011 than in 2010, in particular because of the various geopolitical conflicts at the time.

Spoofing is a type of signal-based attack (i.e. software-based spoofing is addressed later as a type of cyberattack) that aims to deceive a receiver by broadcasting incorrect signals structured to resemble genuine signals, or by re-broadcasting genuine signals captured at a different location or time. Spoofed signals target the receiver part of the communication channel, which can include satellites in the case of spoofed uplink signals or, more commonly, ground stations and user equipment in the case of spoofed downlink signals.

One of the most notable examples of spoofing took place in the Black Sea when the U.S. Maritime Administration reported 20 affected ships near the coast of Novorossiysk[104]. Another manifestation of such activity targeted the popular location-based applications PokemonGo and Uber in Moscow. Several areas of spoofing around the Kremlin have been reported, with users being wrongfully geo-localised in the city´s Domodedovo airport instead of the Kremlin.[105] The spoofing system in the Kremlin area is believed to be intended to prevent the use of unauthorised drones relying on

[99] Bhalla, P. (2014). *Weaponisation of Space*. New Delhi: KW Publishers Pvt Ltd.
[100] Eutelsat. (2013). *Satellite Interference: an Operator's Perspective*. Retrieved from ITU: https://www.itu.int/en/ITU-R/space/workshops/2013-interference-geneva/presentations/Ethan%20Lavan%20-%20Eutelsat.pdf
[101] Nebehay, S. (2010). *U.N. tells Iran to end Eutelsat satellite jamming*. Retrieved from Reuters: https://www.reuters.com/article/us-iran-jamming-itu/u-n-tells-iran-to-end-eutelsat-satellite-jamming-idUSTRE62P21G20100326
[102] Director General's Office. (2012). *EBU Deplores Middle East SAtellite Jamming.* Retrieved from EBU: https://www.ebu.ch/contents/news/2012/10/ebu-deplores-middle-east-satelli.html
[103] Pomerlau, M. (2016). *Threat from Russian UAV jamming real, officials say*. Retrieved from C4isrnet: https://www.c4isrnet.com/unmanned/uas/2016/12/20/threat-from-russian-uav-jamming-real-officials-say/
[104] Hambling, D. (2017). *Ships fooled in GPS spoofing attack suggest Russian cyberweapon.* Retrieved from New Scientist: https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/
[105] Oliphant, R. (2016). *Is Kremlin cyber warfare behind Moscow GPS quirk sending Uber cars and Pokemon Go players to strange destinations?* Retrieved from The Telegraph: Is Kremlin cyber warfare behind Moscow GPS quirk sending Uber cars and Pokemon Go players to strange destinations?

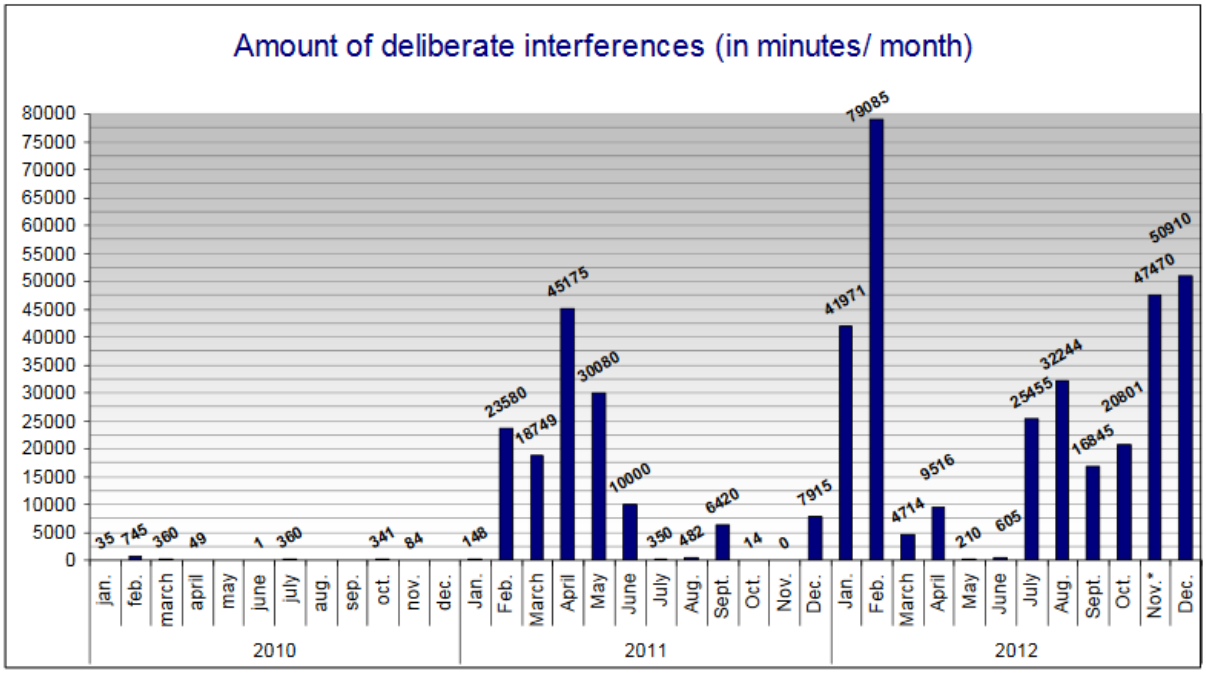

Figure 13: Number of deliberate interferences (Source: Eutelsat)

GNSS signals for flight guidance. Another example is the disruption by North Korea of PNT signals used by South Korean aircrafts and ships. The most acute attacks occurred in March 2016 when more than 1,000 aircraft and 700 ships were affected. Interestingly, these repeated attacks influenced the recent decision of South Korea to invest in a national positioning system.[106]

From a legal standpoint, both jamming and spoofing are a violation of the ITU Convention. However, loopholes in enforcement mechanisms make it difficult to either prevent or punish them[107]. While production, commerce and/or use of jamming and spoofing devices are illegal in various countries, reports suggest that these devices are becoming increasingly simple to procure via dedicated websites, very often Chinese made, and use. GNSS and satcom signals appear to be the two main targets of jamming and spoofing attacks but, in general, any communication channel between space and ground can be vulnerable to such hazards. These threats can seriously affect the quality of space-based services and therefore lead to substantial impacts on operations dependent on these services such as road, rail, air, and water transport, and civil protection among many others. Here again, the threat is ubiquitous and inclusive.

The EU recently funded the STRIKE3 project through Horizon 2020 with the objective to improve awareness of existing and continuously increasing threats to GNSS signals, develop and validate new international standards for the monitoring and reporting of GNSS signal attacks and eventually mitigate the criminal use of jammer technology.

3.2.3 Cyberattacks

Comparable to other infrastructures relying on ICT to operate, space infrastructure can be the target of cyberattacks, which include a range of offensive manoeuvres against computer and information systems to steal, disrupt or destroy a specified target (e.g. data, service, system) by hacking into the network. Cyberattacks can be led by governments, organisations, groups or individuals for a variety of motivations and objectives, and can be run from the outside or the inside. Here it is important to note that an overlap exists between malicious interferences and cyberattacks, with rogue signals being used as a means to access the space infrastructure network. This happened in October 2007 and July 2008, when LandSat-7 and Terra AM-1, two earth observation satellites operated by NASA, were hacked, possibly by China's military, via a

[106] Kim, J., & Saul, J. (2016). *South Korea revives GPS backup project after blaming North for jamming.* Retrieved from Reuters: https://www.reuters.com/article/us-shipping-southkorea-navigation/south-korea-revives-gps-backup-project-after-blaming-north-for-jamming-idUSKCN0XT01T

[107] Jakhu, S. (2013). *Satellites: Unintentional and Intentional Interference.* Retrieved from Secure wold foundation: https://swfound.org/media/108687/jakhu-satellite%20interference%20and%20space%20sustainability%20(17jun13).pdf

rogue signal sent by a satellite station located in Norway.[108]

In recent years, both the level of magnitude of cyberattacks and their occurrence have been raising concern across ICT reliant sectors, including the space sector. This unprecedented level of threat is driven by increasingly sophisticated cyberattacks from a growing number of cyber-capable entities. In January 2018, John Drzik, President of Global Risk and Digital at Marsh, evaluated the aggregate cost of global cyberattacks at USD 1 trillion per year and subsequent economic losses at USD 300 billion, comparing them to natural catastrophes in scale.[109] In the World Economic Forum´s Global Risks report of 2018, cyberattacks ranked as the third most likely global threat this year.[110]

In a recent report on space cybersecurity, Chatham House, the Royal Institute of International Affairs, evaluated that 'the intersection of space security and cybersecurity is not a new problem, but it has remained largely unrecognized as a potentially significant vulnerability [and] remains unaddressed in practical mechanisms'.[111] This situation is not specific to the space infrastructure as 'even outside the space domain, cybersecurity cultures across national and international communities are immature and inconsistent in their development'.

From a practical perspective, cyberattacks targeting space infrastructure include a variety of possible manoeuvres in pursuit of the general objective to 1) steal information (e.g. data, communications) and/or 2) disrupt space infrastructure (e.g. systems, operations, capabilities, services). Threats also include cyberattacks that do not target directly the space infrastructure but rather exploit its vulnerabilities as a means to reach other infrastructures and systems. Cyberattacks can be grouped in the following categories, with the most sophisticated attacks resulting from a combination of different types of attacks:[112]

- *System Compromise,* to obtain temporary control of a system and consequently the capacity to execute arbitrary commands or to gain a foothold in the network to carry out other attacks;
- *Service Disruption,* to prevent a system from performing as expected with consequences ranging from reduced quality of service to total system failure;
- *Data Exfiltration,* to steal sensitive information from a target for reconnaissance, strategic intelligence, theft, or to expose secret information;
- *Bad Data Injection,* to submit incorrect data (e.g. erroneous TT&C data) to a system without detection with a range of possible consequences;
- *Advanced Persistent Threat (APT),* to gain extended access to a system and get permanent and undetected capacity to access system information or take control of the system.

From a more general perspective, the Chatham House report classifies cyber threats against space-based systems as follows:[113]

- States setting out to create military advantages in space, or seeking to steal strategic quantities of intellectual property and having sufficient computing power to crack encryption codes;
- Well-resourced organized criminal elements seeking financial gain;
- Terrorist groups wishing to promote their causes, even up to the catastrophic level of satellite collisions with space debris including a cascade of collisions denying the use of space for all actors;
- Individual hackers who simply want to prove and fanfare their skills;
- Any combinations of the organizations and individuals above.

The report also underlines the following potential methods:[114]

[108] Wolf, J. (2011). *China key suspect in U.S. satellite hacks: commission.* Retrieved from Reuters: https://www.reuters.com/article/us-china-usa-satellite/china-key-suspect-in-u-s-satellite-hacks-commission-idUSTRE79R4O320111028

[109] Strategic Risk. (2018). *Global Risks Report 2018: Cyber risk growing faster than mitigation efforts, says John Drzik.* Retrieved from Strategic Risk Europe: https://www.strategic-risk-europe.com/analysis/global-risks-report-2018-cyber-risk-growing-faster-than-mitigation-efforts-says-john-drzik/1426075.article

[110] World Economic Forum. (2018). *The Global Risks Report 2018, 13th Edition. Geneva: World Economic Forum*. Retrieved from World Economic Forum: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

[111] Livingstone, D., & Lewis, P. (2016). Space, the Final Frontier. London: Chatham House.
Lu, M. (2014). *Types of Cyber Attacks*. Retrieved from TCIPG: https://tcipg.org/sites/default/files/rgroup/tcipg-reading-group-fall_2014_09-12.pdf

[112] Lu, M. (2014). *Types of Cyber Attacks.* Retrieved from TCIPG: https://tcipg.org/sites/default/files/rgroup/tcipg-reading-group-fall_2014_09-12.pdf

[113] Livingstone, D., & Lewis, P. (2016). Space, the Final Frontier. London: Chatham House.
Lu, M. (2014, September 12). Types of Cyber Attacks. Retrieved from TCIPG: https://tcipg.org/sites/default/files/rgroup/tcipg-reading-group-fall_2014_09-12.pdf

[114] Ibid

- Attacks on satellites, by targeting their control systems or mission packages, perhaps taking control of the satellite to exploit its inherent capabilities, shut it down, alter its orbit (perhaps thereby 'weaponizing' it), or 'cook' or 'grill' its solar cells through deliberate exposure to damaging levels of highly ionizing radiation;
- Attacks on the ground infrastructure, such as satellite control centres, the associated networks and data centres, leading to potential global impacts (for example on weather forecasting systems, which use large quantities of space-derived data).
- Hacking attacks on, for example, communication networks, by using space infrastructure;

A few examples of noteworthy cyberattacks can already be provided. In 2002, a SinoSat satellite was hacked to broadcast contents promoting the cult of Falun Gong, forbidden in China, on national television for four hours.[115] In 2007, the Sri Lankan terrorist group, Tamil Tigers, managed to broadcast on TV and radio in Europe and Asia through Intelsat satellite transponders.[116] The Russian speaking Turla Group, a notorious group developing Advanced Persistent Threats (APT), have been exploiting satellite links on stealth mode by using hijacked satellite IP addresses belonging to well established companies such as Telesat, Teleskies, Skylinks Satellite Communications Limited, Lunasat, Emperion, SkyVision Global Networks, Orioncom, Intrasky, IABG GmbH and Sky Power International, to conduct cyberattacks since at least 2007 with their main targets being diplomatic and military stakeholders in the United States, Europe, Middle East and Central Asia.[117] Other hacker groups such as HackingTeam, Xumuxu Group, and Rocket Kitten ATP group, resort to the same procedure.

Vulnerabilities of space infrastructures to cyberattacks can arise from a variety of factors throughout the system lifecycle including during development and production. Indeed, loopholes in some satellite hardware (e.g. electronic components) or software can be intentionally added and/or exploited by offenders to conduct cyberattacks. This technique is referred to as ´back doors´. For this reason, experts underline the importance of controlling the provenance of software, firmware and components as part of a comprehensive cybersecurity strategy.[118] These aspects are addressed as part of a cybersecurity-by-design approach.

Space infrastructure must be also protected after its deployment, during operations. Bob Gourley, a leading cybersecurity expert, explains that 'the most modern platforms have a high degree of security engineered into them [but] operate with legacy systems that are very vulnerable, especially to a well-resourced adversary'. He also explained that 'ground stations have a mixed degree of protection'. This situation will persist, even with new systems safeguarded from cyber threats by design. Indeed, the level of cybersecurity of any system tends to decrease during its operational lifetime as the nature of cyber threats develops with new, more sophisticated attacks.

3.3 Natural Threats, Space Environment Hazards

Besides intentional and unintentional man-made threats, the space environment *per se* can pose serious hazards to the safety of space objects and space activities. These natural hazards, which can be more intense during specific events such as geomagnetic storms, solar radiation storms or disturbances of the ionosphere, are commonly referred to as 'space weather'. According to ESA, space weather can be defined as 'the environmental conditions in Earth's magnetosphere, ionosphere and thermosphere due to the Sun and the solar wind that can influence the functioning and reliability of space-borne and ground-based systems and services or endanger property or human health'.[119]

Studying and monitoring space weather involves the examination of ambient plasma, magnetic fields, radiation or particle flows in space and their influence on the outer space environment and effects on man-made systems. Space weather can have severe consequences on space assets, potentially deteriorating satellite components - such as sensitive

[115] Hogg, C. (2004). *HK probes Falun Gong 'hacking'.* Retrieved from BBC News: http://news.bbc.co.uk/2/hi/asia-pacific/4034209.stm
[116] McCoy, J. (2007). *Intelsat Shuts Down Transponder Hijacked By Terrorists.* Retrieved from Via Satellite: http://www.satellitetoday.com/uncategorized/2007/04/26/intelsat-shuts-down-transponder-hijacked-by-terrorists/
[117] Nakashima, E. (2015). *Russian hacker group exploits satellites to steal data, hide tracks*. Retrieved from The Washington Post: https://www.washingtonpost.com/world/national-security/russian-hacker-group-exploits-satellites-to-steal-data-hide-tracks/2015/09/08/c59fa7cc-5657-11e5-b8c9-944725fcd3b9_story.html?utm_term=.f8ab230f1530
[118] Wood, P. (2012). *Cyber Attacks: An Emerging.* Retrieved from Swri: http://flightsoftware.jhuapl.edu/files/2012/FSW12_Wood.pdf
[119] ESA. (2018). *About space weather. Retrieved from European Space Agency:* http://swe.ssa.esa.int/what-is-space-weather

electronic equipment or solar panels, their communication network, performances, and reliability, which ultimately will have a negative impact on their operational lifetime.[120] In turn, these effects can pose a serious threat to space-based services such as telecommunication, broadcasting or PNT signals. Even though in principle space weather does not directly affect our planet as the Earth's natural magnetic field protects us from solar and radiation phenomena, some extreme events can also affect some ground systems, such as electrical power grids or radio communication infrastructures. Although important, these effects are not addressed here.

The results of a study recently conducted by ESA and PwC[121] provide an overview of the cascading effect and potential socio-economic impact of space weather events on space infrastructure. This cost-benefit analysis compares a 'do nothing' with a 'do ESA SSA programme' scenario (i.e. focusing on the space weather element of the programme)[122] and investigates the chain of effects of a selection of space weather perturbations on space systems and space-based services in economic sectors. The study addresses three main space weather events:

- *Geomagnetic storms,* resulting from coronal mass ejection and high-speed solar winds
- *Solar radiation storms,* resulting from solar energetic particle events
- *Ionosphere disturbances,* resulting from solar flares

The study investigates the impact of these events on space systems, the resulting disruption of space-based services, and ensuing socio-economic impacts in selected economic sectors.

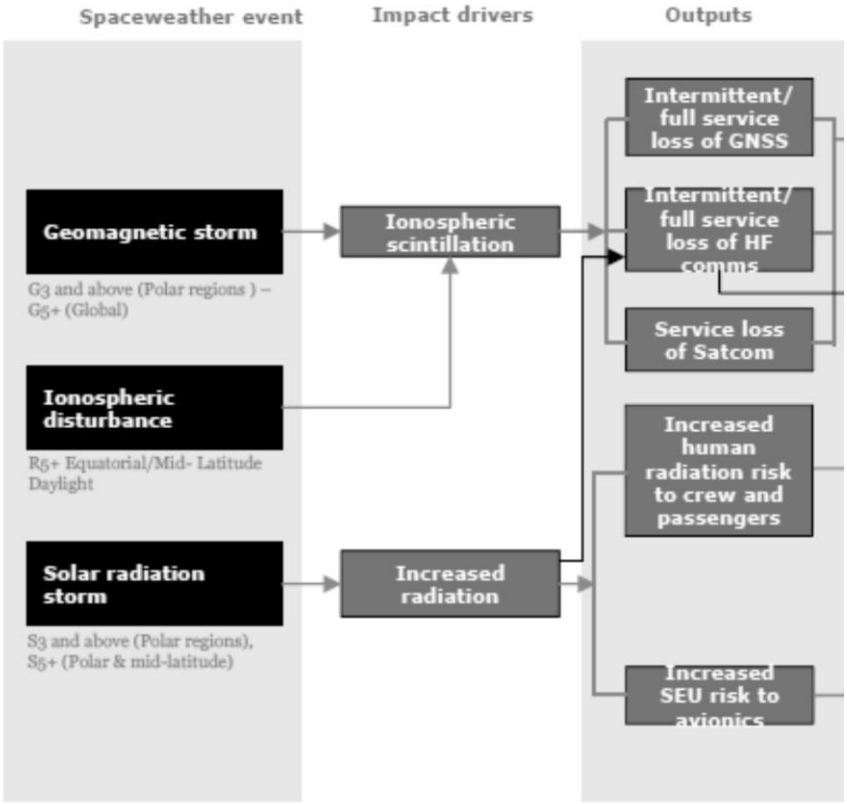

Figure 14: Extract of cascading impact of space weather events on space systems and services (ESA)[123,124]

[120] Eastwood, J., & al, e. (2017). *The Economic Impact of Space Weather: Where Do We Stand?* Risk Analysis: An international journal, 206-2018.
[121] Luntama, J.-P. (2017). *Report on the ESA Space-Weather.* Retrieved from NOAA: https://www.swpc.noaa.gov/sites/default/files/images/u33/%281130%29%20Session%202%20Luntama%20SSA%20SWE%20CBA%20Study.pdf
[122] Ibid
[123] Del Monte, L. (2017). *Ex-ante cost benefit analysis of the Space Weather.* Retrieved from UNOOSA: http://www.unoosa.org/documents/pdf/psa/activities/2017/ISWI%20Boston/ISWIBostonDay1/05.pdf
[124] SEU: Single Event Upset is a change of state caused by one single ionizing particle (ions, electrons, photons...) striking a sensitive node in a micro-electronic device. The resulting error in device output or operation is called an SEU or a soft error.

Cost/Benefit	'Do nothing' Scenario (€M)	'Do ESA' Scenario (€M)	Value added of ESA services (€M)
User domain benefits			
Satellite operations	- 293	- 267	26
Launch operations	- 0.3	- 0.1	0.2
Resource exploitation	- 327	- 135	192
Power grid operations	- 5,771	- 4,546	1,225
Aviation	- 3,312	- 3,066	246
Logistics/Road transport	- 3,432	- 2,888	544
Investment benefits			
GDP impact	None	- 952	952
Total benefits	- 13,135	- 9,950	3,185
Programme costs	None	- 529	- 529
Total net benefits	**- 13,135**	**- 10,479**	**2,656**

Table 2: Cost/Benefit analysis of ESA space weather programme (adapted from ESA)

As shown in the table above, the implementation of a space weather component in the frame of a full-fledged SSA programme can contribute to mitigating, at least partially, the consequences of space weather events with a net benefit estimated around €2.7 Billion for a €529 Million programme.

3.4 Key Takeaways

The review provided above underlines that security challenges and threats faced by the European space infrastructure are:

- *Multiple and diverse* in nature and origin and as a consequence require a set of different mitigation and protection measures. Although this report focuses on 'Security in Outer Space', and therefore on threats in orbit, it can be established that a share of space infrastructure vulnerabilities during operations in space can result, at least partially, from earlier stages (e.g. system development and production).
- *Interrelated and interdependent,* with space infrastructure being vulnerable to some hazards that have the potential to create new threats. For example, vulnerability to cyberattacks aiming to take control of a satellite to weaponize it (e.g. by commanding it to collide with another satellite) can create new ASAT threats. Similarly, challenges and threats to space security depend on the approach of all space stakeholders, underlining the relevance of the OSCE's underlying premise that, comparable to other security domains, space security is indivisible.[125]
- *Ubiquitous and inclusive,* although some systems are less exposed or vulnerable to specific threats.
- *Intensifying,* driven by endogenous and exogenous trends including:
- Increasing space activity in terms of the number of launches and objects in orbit but also in the number of governmental and commercial actors owning and operating space systems;
- New concepts, technologies and capabilities;
- An ever more connected space infrastructure, including with other ground networks and systems;
- The increasing importance of space infrastructure, which makes it a key target for a variety of actors pursuing different objectives;
- The rehabilitation of a 'space warfare' doctrine encompassing activities to develop 'space control' capabilities.

To conclude, space is an increasingly congested and contested resource. This situation, expected to further deteriorate in the future, results from a variety of factors consistent with the growing strategic and socio-economic significance of space infrastructure, as discussed previously. From this standpoint, the pervasive dependence on space systems suggests that rising threats to the space infrastructure mean, ultimately, potential risks for the modern economy, society, security and, more generally, modification of the geopolitical scene.

[125] OSCE. (2009). *The OSCE Concept of Comprehensive and Co-operative Security.* Vienna: OSCE Secretariat. Retrieved from OSCE: https://www.osce.org/secretariat/37592?download=true

4. European Approach to Space Security

4.1 Securing the European Space Infrastructure: a Multi-Fold Challenge

4.1.1 Core Components of the 'Security in Outer Space' Challenge

From a general standpoint, ensuring 'Security in Outer Space' is a multi-fold challenge encompassing three main areas.

Ensuring 'Security in Outer Space' therefore requires a variety of measures targeted to 1) monitor the space environment, 2) mitigate threats to space infrastructure, and 3) reduce vulnerability of space infrastructure:[126]

- *Space Situational Awareness (SSA)* encompasses all means and measures to monitor, detect, predict and inform about man-made and natural, intentional and unintentional, threats to operations in space (i.e. threats originating from the space environment). More specifically, SSA includes three main components:
  - *Space Surveillance and Tracking (SST)* of man-made objects including operational systems and orbital debris;
  - *Space Weather* to study, monitor and predict natural events which can affect space-borne systems or even ground infrastructure;
  - *Near Earth Objects (NEO)*, i.e. asteroids or comets, to monitor, predict and assess potential threats to life and property on Earth and eventually issue warnings to mitigate damages.

  With a wider scope, including 'Security from Outer Space', SSA can also be used for Near-Earth Objects (NEOs) and space weather events.
- *Space Environment Protection and Preservation (SEPP)* through means and measures to prevent and mitigate the effect of human activity on the space environment and ensure it remains safe on the long-term. In the context of 'Security in Outer Space', this line of action includes measures to promote, facilitate or enforce the responsible behaviour of organisations conducting activities in space (i.e. governmental and commercial operators, launch service providers…), and in particular to limit debris generation but also the development of solutions to make the space environment safer to operate (e.g. Active Debris Removal).

Security in Outer Space

1- Space Situational Awareness (SSA)	2- Space Environment Protection and Preservation (SEPP)	3- Space Infrastructure Security (SIS)
Current and predictive knowledge and understanding of the outer space environement including space weather and location of natural and manmade objects in orbit around the Earth.	Preventive and curative mitigation of negative effects of human activity in outer space on the safety and sustainability of the outer space environment.	Assurance of the infrastructure ability to deliver a service that can justifiably be trusted despite a hazardous environment.

Table 3: Core components of the 'Security in Outer Space' challenge

[126] Note: Complementary measures targeting directly the source of the threats such as actions against cybercrime, space disarmament policies or radio spectrum management are not included here.

- *Space Infrastructure Security (SIS)* to reduce vulnerabilities of space systems to intentional and unintentional threats. This includes protection measures aimed at guaranteeing systems dependability and resilience. 'Dependability' is defined here as a measure of a system´s availability, reliability, safety, integrity, confidentiality and maintainability. 'Resilience' is defined as the persistence of system dependability when facing functional, environmental, or technological changes. SIS includes two main components:
    - *Security-by-design:* Implementation of appropriate measures during system development and production. This encompasses systems and supply chain compliance with security requirements and procedures;
    - *Security in operation:* Implementation of appropriate measures during system operations. This encompasses a variety of procedures and capabilities to detect, characterize, and respond to threats to ground and in orbit systems operations.[127]

Some complementary measures, involving activities beyond the space sector or focused on military objectives, (e.g. actions against cybercrime, disarmament policies, radio spectrum management) are not addressed here.

4.1.2 Main Fields of Action

The implementation of this set of measures requires a variety of actions across multiple domains.

The initial and overarching action is the elaboration and endorsement of a comprehensive space security strategy and policy framework including clear objectives and associated actions supported by a coherent governance framework and the allocation of appropriate resources.

Key space security actions include:

- *Capacity-building programmes:* Setting up technical capabilities required for the implementation of space security measures. Capacity-building covers the entire lifecycle from research & development to operations and delivery of service, through acquisition, deployment, and upgrade of assets. In the field of security in outer space, key technologies and capacities include:
    - *Space Surveillance & Tracking capabilities,* including networks of ground- and/or space-based assets (radar, telescope, laser, spacecraft, data processing facilities…) providing the range of technical capabilities required to detect and monitor objects in space as well as prediction tools and services to identify potential threats to operations in space;
    - *Space Weather capabilities,* including scientific models of space weather events and of their potential impact on space (and ground) systems, space weather monitoring assets, and prediction and forecasting tools and services;
    - *CleanSpace technologies,* including technologies to enable environment-friendly space systems supporting Space Environment Protection and Preservation. This includes, for example, the development of effective and affordable solutions for space systems end-of-life control and debris removal.
    - *Security enhancing technologies,* including technologies to improve space infrastructure dependability and resilience. Such technologies include, for example: secure links (encryption, robustness…), debris shielding materials, autonomous collision avoidance, and fault-tolerant electronic components.
- *Legal and regulatory regimes:* Preparation, ratification and application of a set of laws, regulations, rules, procedures and standards supporting space operations security and space environment protection and preservation. Such framework, which aims to foster the implementation of diverse security-related rules, is the result of actions conducted at international, regional and national level. For this reason, initiatives in this field often overlap with measures in the field of "diplomacy and operational collaboration". It includes in particular:
    - Binding space legislation
    - Non-binding guidelines and rules
    - Standards and procedures
- *Diplomacy and cooperation frameworks:* Setting up of co-operative political and

[127] Note: The detection and characterization of threats originating from the space environment is covered by Space Situational Awareness. However, additional capabilities may be required for ground-based threats such as malicious interferences.

operational frameworks supporting a collective approach to space security through:

- *Multilateral discussions* between governments, and with commercial stakeholders, to raise awareness and promote a common understanding and assessment of space security challenges;
- *Collective engagements* to tackle security challenges through common approaches and frameworks (e.g. transparency measures, international guidelines);
- *Cooperation agreements* to provide the foundations for multilateral actions including, for example, information and data sharing, or coordinated space operations procedures.

4.1.3 Security in Outer Space: Action Matrix

The following table, based on a categorization matrix applied to security in outer space, provides a list of examples of actions and measures related to 'Security in Outer Space' organised by domain and field of action.

The list is intended to be illustrative rather than comprehensive:

		Field of action		
		Capacity-building programmes *Develop and deploy operational capacities to ensure security in outer space*	**Legal and regulatory regimes** *Establish a reference framework to conduct space activities in compliance with space security requirements*	**Diplomacy and cooperation frameworks** *Harmonise and coordinate space security efforts among stakeholders*
Security in Outer Space subdomain	**Space Situational Awareness (SSA)** *Monitor space environment threats*	Examples: • SST systems acquisition • Space weather models development • SSA services delivery	Examples: • Space objects registration obligations and procedures	Examples: • SSA data sharing agreements • Transparency and Confidence-Building Measures
	Space Environment Protection and Preservation (SEPP) *Keep the space environment safe to operate in*	Examples: • CleanSpace technologies development (e.g. active debris removal solutions)	Examples: • Space law (e.g. end-of-life obligations) • Standards for space environment-friendly satellite design (e.g. passivation devices)	Examples: • Endorsement of Space Debris Mitigation Guidelines • Code of Conduct negotiations
	Space Infrastructure Security (SIS) ☐*Protect the space infrastructure from threats*	Examples: • Security enhancing technologies development (e.g. secure links) • Security-by-design know-how	Examples: • Space programme security rules and procedures • Security standards • Supply chain control processes (e.g. export/import rules, testing procedures)	Examples: • Collision avoidance procedures and coordination

Table 4: Examples of 'Security in Outer Space' measures by field and domain category

In a nutshell, the concept of 'Space Security' actually encompasses diverse objectives and challenges. Guaranteeing secure and sustainable access to and use of space also requires the implementation of a broad range of measures spread across political, diplomatic, operational and legal dimensions. The various aspects of space security can be viewed as interconnected and interdependent, which underlines that an effective approach to space security should be:

- *Comprehensive:* covering a broad and multidimensional scope;
- *Coherent:* following consistent principles and building on synergies between the different actions;
- *Co-operative:* structured around, and contributing to, a multilateral approach.

This chapter provides an overview of the European approach to space security on the basis of this matrix organisation and for each key stakeholder: Member States, the European Space Agency and the European Union.

4.1.4 The Case of Space Traffic Management

Several definitions of Space Traffic Management (STM) exist. A common definition is "the set of technical and regulatory provisions for promoting safe access into outer space, operations in outer space and return from outer space to Earth free from physical or radio-frequency damage".[128]

In this study, and taking into account exclusively civil space activities, space traffic management is understood as an operational and organisational concept encompassing systems assisting operators for safety of operations in orbit, practices ensuring the sustainability of the use of outer space (e.g. regulations, standards, procedures, protocols), and frameworks governing the exploitation of these systems and the implementation of these practices.

Space traffic management is therefore a concept covering part of the elements included in the space security matrix (e.g. SSA systems, collision avoidance procedures, system standards, international regulations…) and bringing them together, under a common-roof.

The U.S. is taking initial steps toward a national civil space traffic management framework. U.S. VP Mike Pence's declaration at the 34th Space Symposium in Colorado Springs clearly demonstrated the intention of the U.S. to move fast in this direction to promote American leadership, ensure national security, and promote commercial solutions. More specifically, the new policy "directs the Department of Commerce to provide a basic level of space situational awareness for public and private use, based on the space catalog compiled by the Department of Defense, so that military leaders can focus on protecting and defending national security assets in space"[129] and to "encourage the commercial space industry to partner with the government to develop data-sharing systems, technical guidelines, and safety standards to apply domestically and be promoted internationally that will help minimize debris, avoid satellite collisions during launch and while in orbit."[130]

A possible international approach to STM is also regularly discussed, looming over the horizon. Nevertheless, space traffic management is still at a very early stage, including in Europe, and the boundaries of this concept are still undefined, making it complex to analyse practically today. For this reason, space traffic management is not addressed directly in the overview and analysis of the European approach to space security.

4.2 Countries: the Core Actors of Space Security in Europe

4.2.1 A National Defence and Security Domain

Historically, activities in the field of security in outer space have been primarily organised at national level, comparable to other security and defence domains, and in close relations with military space programmes. Here again, 'Outer Space FOR Security' remains the predominant driver for 'Security IN Outer Space', which has led the most active countries in the field of military space (i.e. France, Germany, Italy, United Kingdom, Spain) to also engage in a variety of actions in the field of space security.

In these countries, security in outer space is being addressed, first, as a national security strategy domain. In France, for example, space security is addressed in multiple occasions in the White Paper on Defence and National Security (2013),[131] declaring that 'with the multiplication of debris in space and the emergence of potential direct attacks on satellites, the protection of outer space is now a major challenge given the importance of the services and missions carried out by spacecraft.'[132] These concerns were echoed in the 2016 report on the future of the French space sector of Mrs. Fioraso, former French minister for higher education and research.[133] Germany also extensively addresses space security in the White Paper on German Security Policy and the Future of the Bundeswehr (2016).[134] In this document, the German Federal Ministry

[128] International Academy of Astronautics (2017). *Space Traffic Management: Towards a Roadmap for implementation.* Paris: IAA Cosmic Study

[129] Infrastructure & Technology (2018). Remarks by Vice President Pence at the 34th Space Symposium, Colorado Springs, CO. Colorado. Retrieved from WhiteHouse.gorv: *https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-34th-space-symposium-colorado-springs-co/*

[130] Ibid

[131] Ministère de la Défence. (2013). *Defence And National Security.* French White Paper. Retrieved from https://www.defense.gouv.fr/content/download/215253/2394121/White%20paper%20on%20defense%20%202013.pdf

[132] Ibid

[133] Fioraso, G. (2016). L´*Overture Comme Réponse Aux Défis De La Filiére Spatiale.* Open Space. Retrieved from http://www.gouvernement.fr/sites/default/files/document/document/2016/07/rapport_vf_- _remise_du_rapport_de_genevieve_fioraso_sur_lavenir_du_secteur_spatial.pdf

[134] Germany Federal Government (2016), White Paper on German Security Policy and the Future, Retrieved from: http://www.gmfus.org/publications/white-paper-german-security-policy-and-future-bundeswehr

of Defence explains that 'Germany's security policy […] expressly includes space'[135] and underlines that 'space security is becoming a key issue', concluding that 'Germany must therefore work towards ensuring the unhindered use of […] space.'[136] These documents also set the direction for activities in this field including, among others, support to international initiatives promoting sustainable exploitation of space, development of space surveillance capabilities to preserve an independent assessment of the situation in space, and promotion of confidence-building measures for transparency in the use of space.

Although prevalent, the national security dimension is not the only one in the space security domain. The convergence of interests between defence, science, space and non-space domains has actually given rise to a variety of national governance models across European countries involving a number of ministries and organisations concerned by space security matters among which, of course, are national space agencies. The cross-domain aspect of space security is best illustrated by the United Kingdom's National Space Security Policy (2014),[137] which resulted from cooperation between the Ministry for Universities and Science, the Ministry for Defence Equipment, Support and Technology, the Ministry of State, and the Ministry for Immigration and Security.

The following table provides a summary of strategy documents addressing space security:

	France	Germany	Italy	United Kingdom	Spain
National space agency or research organisation	Centre national d'Etudes Spatiales (CNES)	Deutschen Zentrums für Luft- und Raumfahrt (DLR)	Agenzia Spaziale Italiana (ASI)	UK Space Agency (UKSA)	Centro para el Desarrollo Tecnologico Industrial (CDTI)
Last space policy / strategy document	French Space Strategy (2012)	The Space Strategy of the German Federal Government (2010)	ASI Strategic Vision Document 2016-2025 (2016)	UK National Space Policy (2015)	Strategic Plan for the Space Sector 2007-2011 (2006)
Other policy / strategy document addressing space security	White Paper for Defence and National Security (2013)	White Paper on German Security Policy and the Future of the Bundeswehr (2016)	White Paper for International Security and Defence (2015)	UK National Space Security Policy (2014)	National Security Strategy (2013)
Authority for space security matters	Ministry of the Armed Forces	Ministry of Defence	Ministry of Defence	Foreign & Commonwealth Office, Ministry of Defence, UK Space Agency, Home Office	Department of the National Security

Table 5: Selected national strategy documents for Security in Outer Space and organisations involved

4.2.2 Between Sovereignty and Cooperation

More concretely, security in outer space, which has been recognised as a key component of national security by a handful of European countries, has given way, since the early 2000s, to a variety of actions in the fields of 1) capacity-building, 2) legal and regulatory framework and 3) diplomacy and cooperation. Efforts in the field of space security remain unequal among countries with a few countries that are active in military space programmes having made a more substantial effort, in particular in the field of SST capacity-building.

[135] Ibid
[136] Ibid
[137] HM Government (2014). *National Space Security Policy.* Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/307648/National_Space_Security_Policy.pdf

4.2.2.1 National Capacity-Building Programmes

National governments are the owners and operators of the main European SST systems. ESA also funded the development of complementary systems as part of its SSA programme (addressed later in this report) such as a space debris test radar located in Spain and designed to test new methods for finding orbital debris.[138]

In France, the GRAVES radar (Grand Réseau Adapté à la Veille Spatiale) is operated by a special military division of the CDAOA (Commandement de la Défense Aérienne et des Opérations Aériennes). Designed by the French Aerospace Lab (ONERA) and operational since 2005, this bistatic radar relies on two ground stations located in France (i.e. near Dijon and on the Albion plateau) and covers a database of over 2,000 orbiting objects. In Germany, the TIRA (Tracking and Imaging Radar) system is operated by the Research Establishment for Applied Science (FHR) in Wachtberg, near Bonn. TIRA can track objects in L and Ku Band and its imaging capability ably complements the French system by contributing to the identification of objects spotted by GRAVES. The French Monge ship, equipped with five radars including ARMOR, which was designed for missile tracking, is occasionally used to provide more precise data on objects in LEO.

The British Chilbolton Facility for Atmospheric and Radio Research, operated by the Rutherford Appleton Laboratory, can also support the characterization of orbital objects thanks to a 25-meter steerable parabolic dish meteorological S-band radar called the CAMRa. Other systems include the Starbrook wide-field telescope based in the Royal Air Force Troödos station in Cyprus, funded by the UK Space Agency and the EISCAT (European Incoherent Scatter Scientific Association) system, featuring a monostatic VHF radar in Tromsø with two reception stations in Sweden (Kiruna) and Finland (Sodankylä) able to monitor orbits, especially polar ones.

Additional optical capabilities complement this list with, among others (non-exhaustive list), the French systems SPOC (Système Probatoire d'Observation du Ciel), ROSETTE and TAROT (Télescope à Action Rapide pour les Objets Transitoires) and the British PIMS (Passive Imaging Metric Sensor) using a telescope at Herstmonceux in the United Kingdom, another in Gibraltar and a third one in Cyprus, which have the potential to contribute to space tracking. The astrometric telescope Zimlat in Switzerland, whose main mission is laser telemetry, can be used to monitor GEO and produce precise trajectography. The ZIM SMART telescope of the University of Bern, is used to identify orbital elements in GEO, GTO and MEO. The Italian system Croce del Norte, ASI´s multistatic radar system, was built to detect debris and Near Earth Objects (NEO). The TFRM telescopes at the Montsec Astronomical Observatory and the Sagra Sky of the Observatory of Mallorca can be used for the same purposes. The nature of organisations involved in space security, for example for SST systems, underlines the importance of cooperation between military and scientific communities but also between Member States.

These national SST systems (non-exhaustive list) are operated in very different ways according to the nature of ownership (civil/military) and to their purpose (scientific/operational). The diverse data they produce are also handled according to different protocols and data policy. A substantial effort of networking has been conducted by a consortium supported by the EU that is addressed later in this report with elements on the overall SST capability achieved as a result.

National efforts in the field of capacity-building for security in outer space are not limited to SST capabilities. In the context of military, dual-use, and to a more limited extent, civil space programmes, national space agencies, in collaboration with industry, develop advanced technologies, standards, procedures and other measures to continuously improve dependability and resilience of space infrastructures and operations (e.g. resilient architectures, secure links and electronics…). National space agencies may also proactively promote or support similar developments in the field of space environment protection and preservation (e.g. space environment-friendly design, de-orbiting technologies…).

4.2.2.2 National Legal and Regulatory Regimes

Other noticeable undertakings by European countries include the ratification of national space legislative regimes governing activities in space.

A number of European countries have recently adopted national space laws, such as Belgium (Act on the Activities of Launching, Flight Operation or Guidance of Space Objects of 2005), the Netherlands (Space Activities Act of 2007), France (Act on Space Operations of 2008),

[138] ESA. (2012). ESA deploys first orbital debris test radar in Spain. Retrieved from http://www.esa.int/Our_Activities/Operations/Space_Situational_Awareness/ESA_deploys_first_orbital_debris_test_radar_in_Spain

Austria (Outer Space Act of 2011), and Denmark (Danish Outer Space Act of 2016). [139]

Based on different rationales and approaches, among other things, these legal regimes set the requirements, conditions and restrictions for licenses authorizing organisations to conduct launch and space operations. Some of these legal regimes contain provisions that contribute actively to space environment protection and preservation through obligations in the domain of space objects registration, space debris mitigation or space systems re-entry. [140]

4.2.2.3 Diplomacy and Cooperation Frameworks

Although autonomy remains an important component of national space security strategies (as it does for all defence and security domains), this objective is not pursued at the expense of coordination and cooperation, in particular with other European countries.

From this standpoint, national approaches to space security have been flanked, since the early stages, with the development of a number of bi- and multi-lateral agreements for data sharing, resources pooling, technology transfer, operational coordination, and development of an international framework comprising legally-binding treaties, Transparency and Confidence-Building Measures (TCBMs) and best practice guidelines.

Incentives to develop diplomatic and cooperative initiatives in the field of security in outer space are numerous including:

- *Share efforts and results* between partners to enhance efficiency and performance;
- *Coordinate actions* among partners to ensure coherence and complementarity;
- *Converge on best practices* to conduct activities in outer space;
- *Share information* to build confidence among actors and foster regional and global stability.

On the international scene, European countries proactively contribute to a range of multilateral discussions and activities related to space security taking place under the aegis of international committees such as the Inter-Agency Space Debris Coordination Committee (IADC), the United Nations Committee on the Peaceful Uses of Outer Space (UN COPUOS), and the Conference on Disarmament (CD) or the Committee on Space Research (COSPAR), among others. Focused on promoting international diplomacy and cooperation frameworks, these international engagements address a variety of space security topics (i.e. Space Situational Awareness and Space Traffic Management, Space Infrastructure Security, Space Environment Protection and Preservation) with viewpoints on capacity-building and on legal and regulatory regimes.

Among international agreements to which European countries actively contributed to, the report of the Group of Governmental Experts (GGE) on Transparency and Confidence-Building Measures (TCBMs) in Outer Space Activities certainly represents a noticeable achievement. This initiative, launched in 2011 by the UN General Assembly, brought together a small group of experts (15 international experts nominated by Member States[141]) with the objective to improve international cooperation and reduce the risks of misunderstanding, mistrust, and miscalculations in outer space activities. In addition to internal discussions, the GGE also consulted with the UN COPUOS, the UN CD, other international organisations such as the International Telecommunication Union (ITU and with other relevant entities such as the European External Action Services (EEAS).

The final report of the GGE, which was endorsed at the 68th session of the UN General Assembly in late 2013, outlines the need for TCBMs in space as "means by which governments can share information with an aim of creating mutual understanding and trust, reducing misperceptions and miscalculations and thereby helping both to prevent military confrontation and to foster regional and global stability." The report also proposed TCBMs for consideration and implementation on a voluntary basis:

- Information exchange on national space policy and goals, and exchange of information on military space expenditures;
- Information exchange on activities in outer space, including orbital parameters, possible conjunctions, natural space hazards, and planned launches;
- Notifications on risk reductions such as scheduled manoeuvres, uncontrolled high-risk re-entries, emergency situations, intentional orbital breakups; and

[139] Froehlich, A., Seffinga, V. (2018). *National Space Legislation*. Vienna: European Space Policy Institute (ESPI). Springer.
[140] Ibid

[141] Note: Representatives of China, France, Russia, the United Kingdom and the United States as permanent members of the UN Security Council and representatives of Brazil, Chile, Italy, Kazakhstan, Nigeria, Romania, South Africa, South Korea, Sri Lanka and Ukraine.

- Voluntary visits to launch sites and command and control centres, and demonstrations of space and rocket technologies.

Overall the GGE stressed the importance of international dialogue and received a strong support from the international community.

Another important work in progress is conducted within the Working Group on the Long-term Sustainability of Space Activities (WG-LTS), established by the UN COPUOS in 2010, with the objective to examine and propose measures to ensure the safe and sustainable use of outer space for peaceful purposes and for the benefit of all countries. The expected result of this Working Group is the production of a report providing voluntary best-practice guidelines in this field. The document will be finalised and provided for review and endorsement at the occasion of the 61st session of the COPUOS in June 2018. If successful, this report will be the result of a long diplomatic process initiated by France when Mr. Gérard Brachet, former director of CNES, was chairing the COPUOS. Along this process, France and other European countries actively contributed to the progress of the WG-LTS and to the promotion of international dialogue around long-term sustainability of space activities.

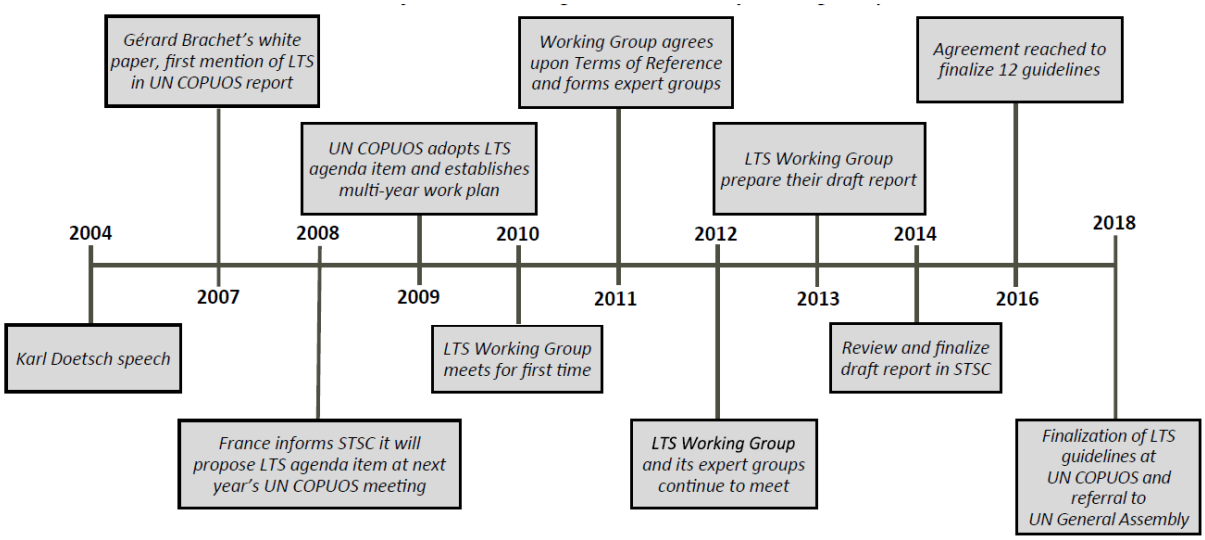

Figure 15: Timeline of UN COPUOS Long-Term Sustainability Working Group (source: Secure World Foundation)[142]

On the European scene, dispositions to cooperate stem from a geopolitical environment promoting cooperation between European countries but also from practical considerations concerning the capacity of countries to conduct, alone, ambitious space security programmes.

Current national strategies highlight a growing readiness and willingness of European countries to build further upon European cooperation in space security. France has declared, in this regard, that 'a European approach to this topic of mutual interest will be promoted, taking advantage of existing resources and developing new concrete projects'[143] and has affirmed that 'France and Germany possess the resources that could serve as a basis to develop a European space surveillance capability.'[144]

The step-up of European institutions in the field of space security, namely the European Union and the European Space Agency, has also given a new dimension to European cooperation, beyond ad-hoc bi-lateral agreements. Two main drivers can be identified here: the rise of security as an integral component of engagement in space, including for supranational and intergovernmental actors, and the growing relevance and legitimacy of the European Union in the areas of defence and security.

[142] Secure World Foundation, (2017), The UN COPUOS Guidelines on the Long-term Sustainability of Outer Space Activities Fact Sheet, Retrieved from https://swfound.org/media/205929/swf_un_copuos_lts_guidelines_fact_sheet_july_2017.pdf

[143] Ministère de la Défense. (2013). Defence And National Security. French White Paper. Retrieved from https://www.defense.gouv.fr/content/download/215253/2394121/White%20paper%20on%20defense%20%202013.pdf

[144] Ibid

4.3 ESA: a Key Actor of Space Security Capacity-Building

4.3.1 Space Security in the ESA Portfolio

According to its convention, ratified in 1975, 'the purpose of [ESA] should be to provide for and to promote, for exclusively peaceful purposes, cooperation among European States in space research and technology and their space applications, with a view to their being used for scientific purposes and for operational space applications systems'.[145] The Agency's scope did not completely hinder activities in the field of security and safety in and from outer space, but rather confined ESA undertakings to a scientific and research dimension with limited connection to national defence and security strategies.

Since then the role of the Agency has progressively evolved, first in the domain of space environment protection and preservation with the adoption of a resolution on the protection of the space environment in 2000 by ESA Council. The resolution established a task force, coordinated by ESOC (European Space Operations Centre) in Darmstadt, with the objective of working on the definition of standards for the safety of orbiting satellites. The task force brought together ESA and national agency representatives and in 2002 introduced preventive measures covering the entire space activities lifecycle and the principle of orbit protection.

Focusing on scientific and operational considerations, ESA funded a feasibility study in 2005 for a space surveillance mission based on secondary optical payloads on board spacecraft in LEO and GEO to detect small debris.[146] A report on space surveillance, ´Europe´s eyes on the sky´[147], was also produced by the European Coordination Group on Space Debris, composed of members from BNSC, ESA, CNES and DLR, using studies presented by the Space Surveillance Task Force in 2006. The report exposed that Europe had no systematic operational capability in the field of space surveillance and heavily relied on non-European sources of information. The findings were endorsed by the ESA Council in November 2008, leading to the establishment of ESA's Space Situational Awareness (SSA) Programme. Through this optional programme, counting on the financial participation of 19 ESA Member States, ESA aims to support the development of an independent European capability to assess space-based threats to systems in orbit or on the ground. Focused on research and development activities, the programme complements and supports coordination of European national capabilities in various ways. In addition, the Agency also established the CleanSpace initiative in 2012 which supports and promotes space environment protection and preservation through the development of an eco-friendly approach to space activities.

ESA involvement in space security is not limited to these two initiatives and actually encompasses a variety of other contributions, such as participation in the IADC, activities in the field of cybersecurity, development of standards for space sustainability (i.e. ECSS U Branch) and other activities directly embedded within space programmes managed by ESA. Notwithstanding, with the endorsement of an SSA programme by its Member States, ESA has become an official operational actor of the European approach to space security, giving a pan-European dimension to the domain.

From a general standpoint, and as highlighted in a paper describing elements of ESA's policy on space and security, the Agency "has evolved to conduct security related projects and programmes and to address the threats to its own activities". [148] Concretely this evolution has been marked by the setting up of a comprehensive regulatory framework including ESA's Security Agreement and Security Regulations and implementing procedures and facilities. As a result, ESA has developed a capability to receive, store, and produce classified information and exchange classified information with third parties such as the EU Council, marking a step forward in the role that the Agency could play in the field of space security in the future.

4.3.2 ESA Capacity-Building Programmes

4.3.2.1 ESA Space Situational Awareness Programme

Approved in November 2008 by the ESA Ministerial Council, the SSA programme officially

[145] ESA (2003). *Convention For The Establishment Of A European Space Agency & ESA Council Rules Of Procedure.* The Netherlands: ESA Publications Division. Retrieved from http://www.kosmos.gov.pl/download/ESA_Convention.pdf

[146] Flohrer T., Krag H., Klinkrad H., Schildknect T. *Feasibility of performing space surveillance tasks with a proposed space-based optical architecture.* Advances in Space Research, Volume 47, Issue 6, p. 1029-1042.

[147] "Europe's eyes on the Skies. *The proposal for a European Space Surveillance System.* ESA Bulletin n° 133 - February 2008, p. 42-48.

[148] Giannopapa. C, Adriaensen. M, Antoni. N, & Schrogl. K-U. (2018). *Elements of ESA's policy on space and security*. Acta Astronautica 147 (2018) 346–349

kicked-off in 2009.[149] The objective of the programme is ´to support the European independent utilisation of, and access to, space for research or services, through the provision of timely and quality data, information, services and knowledge regarding the space environment, the threats and the sustainable exploitation of the outer space surrounding our planet Earth.´[150] In developing such capabilities, the SSA programme aims to strengthen the reliability, availability and security of European space assets, produce critical data on the status of highly strategic orbits, create opportunities in the industry, and develop Europe's role on the international scene with independent data channels.[151]

The programme is optional and has been funded by 19 ESA Member States through 2020 at approximately €200 million for the period 2009-2020. A total budget of €95 million was allocated on the period 2017-2020 alone. This budget is dedicated to a variety of capacity-building projects including research and technology, set-up and operation of data and coordination centres, and systems development and procurement. Notwithstanding, ESA is primarily building on existing capabilities, from ESA itself but also from European and international stakeholders, working on enhancing and integrating these capabilities. The SSA Programme is coordinated from ESOC in Darmstadt (Germany) but various ESA centres are actively working on the programme, such as ESRIN and ESTEC, in collaboration with industry. Between 2009 and 2016, the programme gave way to over 100 industrial contracts.

The ESA SSA Programme includes three main segments:

- *Space Surveillance & Tracking (SST):* The programme aimed to develop European SST capabilities in close collaboration with ESA Member States. The core activity of the SST segment is the maintenance of a data catalogue documenting orbiting space objects. Following a series of discussions with ESA Member States this component was scaled down to focus on R&D and operational activities were transferred to an intergovernmental consortium supported by the EU (addressed later in this report).
- *Space Weather (SW):* The programme seeks to enhance European capabilities to monitor solar activity by producing critical information from various observation angles, and ensure the dissemination of that data to relevant stakeholders in a timely manner. Recent developments are building on a solid foundation of already existing assets and expertise producing high quality scientific output in both the public and private sector.
- *Near-Earth Objects (NEO):* The programme aims to provide data on NEOs (asteroids or comets with a size ranging from one meter to tens of kilometres whose orbitography takes them close to the Sun and, more importantly, to Earth), make impact likelihood estimations, assess the consequences of such impact, and develop deflection methods. A rough estimate of their number, from existing databases, is about 17 000, while the total number of asteroids in the solar system is estimated at around 700,000. However, the Chelyabinsk incident in Russia in 2013, where an unknown object with a velocity of 66,000 km per hour and a 20-meter diameter exploded above the city damaging infrastructure and causing multiple injuries in the region, highlighted the need for an enhanced catalogue with regular updates.

ESA SSA activities include the coordination of centres and data integrity processes, studies on the deployment of hosted payloads, asteroid impact mitigation-related studies, sensor development studies – notably for Lagrange point space weather missions, and similar related activities. Part of the programme budget goes to developing new infrastructure such as databases, software tools, applications, and also hardware such as optical survey telescopes and radars. The possibility of including dedicated satellite missions is being discussed. A few examples of noteworthy results of the SSA programme are provided below:

- Funding for preliminary studies of a future space weather satellite monitoring solar activity was approved by the 2016 Ministerial Council,
- Two new radars were built, respectively, in Spain (monostatic test radar) and France (bistatic test radar) to support future SST for civilian purposes,
- ESA´s Proba-2 solar observatory satellite was incorporated into the SSA programme,

[149] ESA. Space Situational Awareness. https://www.esa.int/Our_Activities/Operations/Space_Situational_Awareness

[150] Luntama, J. P.,(2011). *ESA SSA Services Helping to Mitigate the Risks of Space Weather Events.* Madrid: ESA. Retrieved from http://www.proteccioncivil.es/documents/20486/4c58f134-cb8e-41fc-a473-960568bf9b31

[151] Suzuki, K. *Space Security: Is Europe a Credible Diplomatic Actor?* Hokkaido University / Princeton University. Retrieved from https://swfound.org/media/91262/suzuki_kazuto.pdf

- Establishment of the ESA Space Security and Education Centre (ESEC) at Redu, including a space weather data centre,
- Establishment of the Space Surveillance and Tracking Data Centre at European Space Astronomy Centre (ESAC) in Madrid,
- New coordination centres were inaugurated – notably at Space Pole in Brussels, for space weather, and at ESRIN in Frascati (Italy) for NEOs, as well as another at ESOC in Darmstadt (Germany),
- Test-bed optical telescopes were installed at ESA´s ground station in Cebreros (Spain) and are being installed at La Silla in Chile. These will be used for observation software and techniques testing,
- An initial automated telescope called 'FlyEye' with high tech European optical hardware will be deployed in 2018 that will constitute the core technology of a global asteroid survey system that will be updated on a daily basis.

In the frame of this programme, ESA works closely with European and international partners. ESA coordinates its efforts with European Member States, interacting with ministries of defence, space agencies and other national institutions, as well as with foreign institutions, in particular in the U.S., such as NASA and NOAA.

4.3.2.2 R&D and Standards: ESA CleanSpace Initiative

The main objective of the ESA CleanSpace Initiative is to promote an eco-friendly and sustainable approach to space activity through the development of industrial materials, processes and technologies that are both Earth and space environment-friendly.

Established in 2012, the initiative addresses the entire lifecycle of space systems from conceptual design to end of life, and up to removal of debris. With the objective of covering all aspects of the environmental footprint of space activities, CleanSpace comprises three branches:

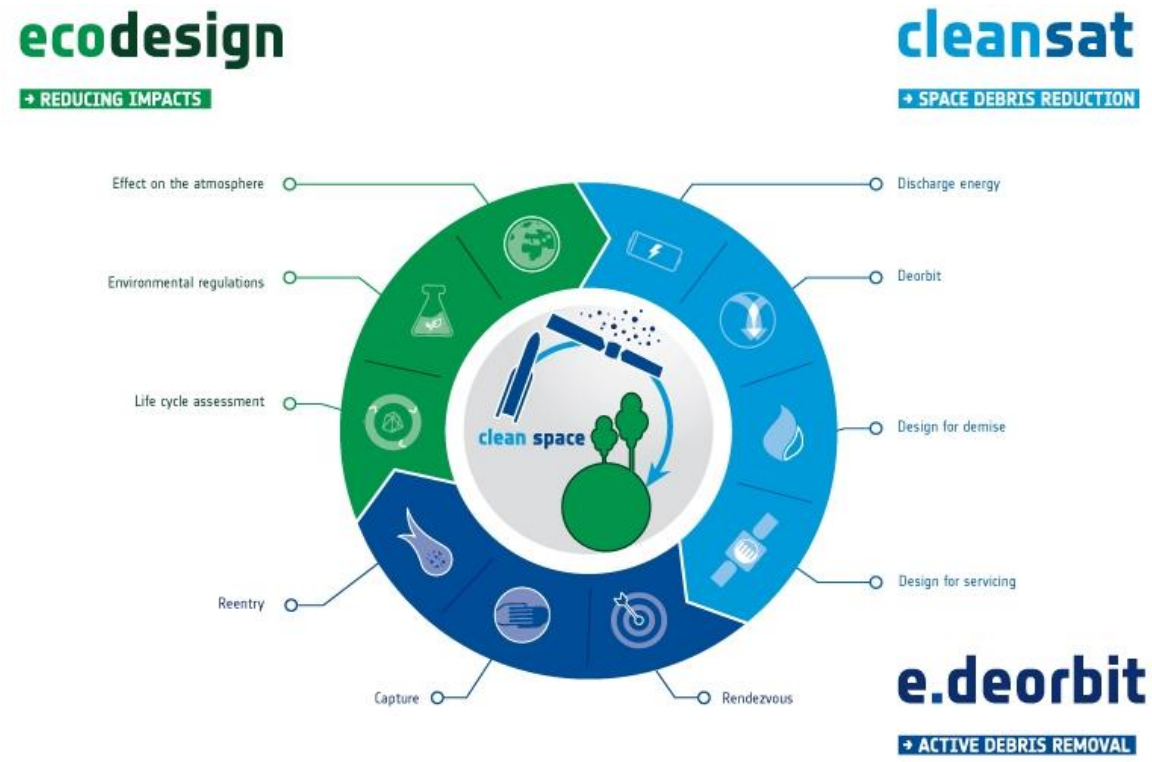

Figure 16: Overview of the CleanSpace Initiative activities (source: ESA)

- *EcoDesign:* designing to address environmental impacts and foster green technologies

Through the establishment of a common ecodesign framework for the European space sector, ESA is seeking to develop tools and systems to evaluate and mitigate the environmental impact of space programmes and also to verify and ensure compliance with existing laws and regulations. Focused on mitigating the impact of space activities on human health and Earth environment, this segment is not related to "Security in Outer Space". However,

the approach of ESA to EcoDesign and the tools developed to evaluate environmental impact (e.g. Life Cycle Assessment) and compliance with legal frameworks (e.g. RoHS directive, REACH regulation) constitute interesting practices that could be expanded to equivalent activities for security in outer space.

- *CleanSat:* designing to reduce the production of space debris

CleanSat deals with the development of technical solutions and standards to mitigate the production of space debris by future satellites in line with regulations, guidelines and requirements. Concretely, 'CleanSpace investigates technologies that enable, simplify and make the mission compliance with mitigation requirements more efficient, and oversees efforts to comply with mitigation objectives, seeking to plug current technological gaps in this area.'[152]

A variety of solutions is being investigated as part of CleanSat:

- *End-of-life passivation:* to avoid spacecraft break-ups, the passivation of propulsive systems and power systems must be considered – that is to say ´the action to permanently deplete or make safe all onboard sources of stored energy in a controlled way in order to prevent break-ups´;[153]
- *Design for Demise*: an engineering process allowing the disassembly, by design, of a given spacecraft once it enters the Earth´s atmosphere to prevent harm to people or property on Earth;[154]
- *Space debris environmental modelling:* this involves studying the behaviour of the space debris population and developing technical means to measure man-made objects between 1mm and a few centimetres in diameter (invisible to current detection methods).

CleanSat is the leading programme of ESA in the field of capacity-building for Space Environment Protection and Preservation.

- *eDeorbit:* removing a large piece of space debris from orbit

Complementing CleanSat, the eDeorbit branch aims to develop solutions for Active Debris Removal covering technologies and research in the fields of target characterization, capture mechanisms and disposal methods.

More specifically, CleanSpace is studying a mission called e.deorbit that will capture an ESA-owned derelict satellite in low orbit and then safely burn it up in a controlled atmospheric reentry. Two concepts are being considered: using a net or a robotic arm. The mission is expected to take place in 2023 and will be the world's first active debris removal mission, attempting an automated capture and deorbit of an uncooperative object.

Beyond the development of ADR capabilities, this capacity-building effort is also expected to support the European space industry to develop new concepts, such as in-orbit servicing using non-cooperative rendezvous, capture, and control of large objects. Moreover, spin-offs from such technological developments could give Europe a clear competitive advantage in the ADR market that is expected to develop in the coming years.

4.3.3 Additional ESA Activities: Regulatory and Cooperation Frameworks

ESA also leads or contributes to several other activities closely related to the field of security in outer space. Additional activities include, among others:

- Setting up a framework (Security Agreement, Security Regulations and Implementing Procedures and Facilities) building a capability to receive, store, and produce classified information and exchange classified information with third parties;
- Development of standards for space project management, assurance, and system engineering. For example, a branch related to space sustainability was added to the ECSS set of standards incorporated in ESA projects;
- Establishment of the European Space Security and Education Centre at Redu (ESEC) as a centre of excellence for space cyber security services;
- Contributions to security aspects of EU space programmes such as Galileo and Copernicus;

[152] ESA. *Clean Space: Cleansat*. Retrieved from ESA: http://www.esa.int/Our_Activities/Space_Engineering_Technology/Clean_Space/CleanSat

[153] Austin J., Ferreira I., Gernoth A., Goody N., Soares T. (2017). *System impacts of propulsion passivation*. Retrieved from ESA: https://indico.esa.int/indico/event/181/session/1/contribution/42/material/slides/0.pdf

[154] Peter M.B. Waswa , Michael Elliot, Jeffrey A. Hoffman (2012). *Spacecraft Design-for-Demise implementation strategy 3 & decision-making methodology for low earth orbit missions.* ScieVerse Science Direct. Retrieved from Scinece Direct: https://aiaa.kavi.com/apps/group_public/download.php/4546/Design%20for%20Demise%20JASR_11188_PRINT.pdf

Lastly, ESA also plays an important role in the promotion of outer space security and sustainability at the international level by being particularly proactive in international forums that work in different ways on security in outer space including the International Astronautical Congress (IAC), Committee on Space Research (COSPAR), IADC, IAA, and UNCOPUOS of which ESA became an observer in 1972.

Noticeable international activities include participation in the IADC, with other European national space agencies (i.e. ASI, CNES, DLR, UKSA), 'to exchange information on space debris research activities between member space agencies, to facilitate opportunities for cooperation in space debris research, to review the progress of ongoing cooperative activities, and to identify debris mitigation options.'[155] IADC Space Debris Mitigation Guidelines formed the basis of the *Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space* that were endorsed by the UN General Assembly on December 22nd 2007.

4.4 EU: Cross-Fertilization of Security and Space Policies

4.4.1 A Domain at the Crossroad of the EU's Growing Engagement in Space and Security

The interest and role of the European Union in space security has grown within a broader and more political context, as the result of cross-fertilization between, on the one hand, developments in the EU mandate in the space domain, and on the other, in the security and defence domain. In this regard, the Lisbon Treaty (2009) was a stepping stone for both domains, establishing shared competences between Member States and the European Union.

In fact, the EU had started considering these domains long before the Lisbon Treaty. At the crossroad of these two domains, space security progressively grew in importance within European Union priorities. In 2007, the European Commission's European Space Policy (ESP) outlined goals for space programmes, enhanced coordination, and promoted free and independent access to space. The use of European space assets for the fulfilment of security missions, confirmed by the Council of the EU's meeting on 'Taking forward the European Space Policy', led to the conclusion that the "economy and security of Europe and its citizens are increasingly dependent on space based capabilities which must be protected against disruption."[156] It is this underlying principle that fostered a natural expansion of the EU perimeter, initially focused on 'Outer Space for Security', to also encompass 'Security in Outer Space' as shown in table 6.

In this frame the European Union launched several actions including, among others:

- *Support to Research & Development,* with projects funded under FP7-Space Area 9.2.3 'Research into reducing the vulnerability of space assets' (e.g. SPA.2013.2.3-01: Space-weather events and SPA.2013.2.3-02: Security of space assets from in-orbit collisions)[157] and under H2020-Space 'Secure and safe space environment' (e.g. SU-SPACE-22-SEC-2019: Space Weather).[158]
- *Support to European operational cooperation,* with the establishment of a Space Surveillance and Tracking (SST) Support Framework in 2014[159] to support the networking and operations of SST assets owned by EU countries and provide EU SST services with the EU Satellite Centre acting as front-desk and interface with users.

Diplomacy and international cooperation, with EU proposal to establish an International Code of Conduct for Outer Space Activities in 2008 aiming to enhance safety and security in outer space through the development and implementation of transparency and confidence-building measures and with additional activities in international fora.

[155] Krag, H. *An overview of the IADC annual activities*. Retrieved from: http://www.unoosa.org/pdf/SLW2016/Panel4/1._Krag_IADC-16-03_UNCOPUOS_Space_Law_Workshop.pdf

[156] Official Journal of the European Union (2007*). Communication from the Commission to the Council and the European Parliament, COM(2007) 212.* Retrieved from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52008AE0260

[157] European Commission C (2013). *Work Programme 2013 Cooperation Theme 9 Space.* Retrieved from https://ec.europa.eu/research/participants/portal/doc/call/fp7/common/1567643-9._space_upd_2013_wp_27_june_en.pdf

[158] European Commission (2017). *EN Horizon 2020 Work Programme 2018-2020 5.iii. Leadership in Enabling and Industrial Technologies – Space.* European Commission Decision C (2017)7124. Retrieved from European Commission: http://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-leit-space_en.pdf

[159] DECISION No 541/2014/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 April 2014 establishing a Framework for Space Surveillance and Tracking Support. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014D0541&from=en

European space policy topics	1988	1992	1996	2000	2003	2007	2011	2016
Space capacity foundation – upstream sector								
R&D activities	●	●	▪	●	●	●	●	●
Launchers and launch services	▪	●	●	●	●	●	▪	●
Space industry	●	▪	●	●	●	●	●	●
Space applications – downstream sector								
Telecommunications	●	●	●	●	●	●	●	●
Earth observation	●	●	●	●	●	●	●	●
Satellite navigation		▪	●	●	●	●	●	●
Space science and exploration		●		●	●	●	●	
International cooperation		●	●	●	●	●	●	●
Defence and security								
Space for security issues		▪	▪	●	●	●	●	●
Defence and dual-use		▪	●	●	●	●	●	●
Secured space infrastructures							●	●
Other aspects								
Training/careers in space sector activities	●		▪		●	▪		▪
Financing the space sector			▪		●	●		●
Regulation for the space sector	●	▪		▪	●	●		▪
Governance of European space sector	▪	▪	▪	▪	●	●	●	

Data source: Elaboration on European Commission documents. ● = key priority ▪ = mentioned area

Table 6: European space policy priorities in Commission communications [160]

More recently, the Space Strategy for Europe (2016) highlighted the central place that the EU now gives to space security.[161] In this document, references to space security are made transversely across the five EU strategic pillars, but are addressed more specifically in the frame of the EU objective to 'reinforce Europe's autonomy in accessing and using space in a secure and safe environment'. From this standpoint, the European Union aspires to develop EU SST services further so that they could evolve into a more comprehensive space situational awareness service to 'ensure the protection and resilience of critical European space infrastructure'. The EU aims to conduct these activities in close cooperation with Member States and European partners such as ESA and EUMETSAT, taking into account international cooperation frameworks, in particular with the U.S.

4.4.2 Capacity-Building through EU Research and Innovation Programmes

EU R&D framework programmes have progressively supported the development of technologies in the field of 'Security in Outer Space'.

Although the FP7 work programme 2007-2008 did not include specific calls related to 'Security in Outer Space', it already stated the intention of the EU to support projects to 'reduce the vulnerability of space assets' through 'techniques for the identification, inventory, monitoring and early warning of events that could affect the space assets' as part of that future work programmes.[162,] This being said, and although not directly called for, in 2007 the EU funded a €5 million project called SOTERIA, which aimed to provide new data from ground based and space-borne observations and models crucial for space weather forecasting.[163] The 2009 work programme gave further details of 'external events', by listing risks such as 'space debris, hostile laser

[160] Official Journal of the European Union (2007*). Communication from the Commission to the Council and the European Parliament, COM (2007) 212.* Retrieved from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52008AE0260
[161] European Commission (2016). Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions Com(2016) 705 Final. Brussels. Retrieved from EURO-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0705
[162] European Commission (2007). *Work Programme 2007-2008 Cooperation Theme 9 Space.* European Commission C (2007)2460 of 11 June 2007. Retrieved from http://ec.europa.eu/research/participants/data/ref/fp7/88321/j_wp_200702_en.pdf
[163] European Commission (2008). *Solar-TERrestrial Investigations and Archives.* Retrieved from European Commission: https://cordis.europa.eu/project/rcn/89460_en.html

or Anti SATellite systems (ASAT), jamming, viruses, natural or man-made electro-magnetic disturbances.'[164] The FP7 work programme 2010 eventually covered 'Security from and in Outer Space'. Concretely, the work programme opened calls for 'security of space assets from space weather events' and for 'Security of space assets from on-orbit collisions', thus supporting fifteen R&D projects.

Since then the EU has almost continuously[165] included calls for projects aimed at enhancing the security of space infrastructures, covering successively different areas of 'Security in Outer Space,' including Near Earth Objects (NEOs), as part of FP7 work programme 2011[166], and space weather and space debris as part of FP7 work programme 2013. Following FP7, Horizon 2020 continued to support R&D activities related to space security with a specific line for 'Protection of European assets in and from space' (H2020-PROTEC) in the work programme 2014-2015[167], and for 'Secure and safe space environment' in the work programme 2018-2020[168]. H2020 calls focused on supporting projects in the field of space weather, space debris, and in funding the Space Surveillance & Tracking support framework, which is addressed in more detail later in this chapter.

Interestingly, FP7-SPACE and H2020-SPACE are the only instruments that have supported projects in the field of 'Security in Outer Space'. Complementarily, some projects have also been funded under other focus areas that are not specific to space. Within FP7, some space security projects can be found under the 'PEOPLE' programme, which provides individual grants for training and career development of researchers (e.g. SpaceDebEMC project for Space Debris Evolution, Collision risk and Mitigation / STARDUST, the Asteroid and Space Debris Network[169]). Within Horizon 2020, the SME Instrument, designed to enable small and medium industries to competitively take part to R&D calls, also includes a space security project.

To conclude, since 2010, the EU has almost continuously supported R&D projects directly linked to 'Security in Outer Space' as part of FP7-SPACE and H2020-SPACE, but also through other non-space instruments. In total, the EU has supported at least 35 R&D projects in this domain for a total of €66 million over 7 years (i.e. excluding funding to the EU SST support framework). These projects have covered a wide scope of activities including topics such as space debris mitigation, in-orbit collision avoidance, and space weather.

The evolution of the EU contribution to 'Security in Outer Space' projects is provided in the figure below. A spike in EU contributions can be observed in 2010 corresponding to financial support to a number of large projects. It is important to note that since 2014, the EU has also funded the SST support framework (roughly for around €28 million per year) through H2020-SPACE and H2020-SECURITY grants, and also through funds allocated to Copernicus and Galileo programmes. Contributions to the SST support framework are not included in this figure. The decrease observed since 2013 actually indicates that EU support has switched from R&D projects to operational capacity-building.

A list of projects supported by EU R&D frameworks between 2007 and 2017 is provided as Annex C of this report.

[164] European Commission (2008). *Work Programme 2009 Cooperation Theme 2 Food, Agriculture and Fisheries, and Biotechnology*. European Commission (2008)4598 of 28 August 2008. Retrieved from European Commission: http://ec.europa.eu/research/participants/data/ref/fp7/88711/b_wp_200901_en.pdf

[165] Note: FP7 work programme 2012 did not include specific calls in the area 9.2.3 'Research into reducing the vulnerability of space assets'

[166] European Commission (2010). *Work Programme 2011 Cooperation Theme 10 Security.* European Commission C(2010)4900 of 19 July 2010) Retrieved from http://ec.europa.eu/research/participants/data/ref/fp7/89287/k-wp-201101_en.pdf

[167] European Commission (2016). *EN Horizon 2020 Work Programme 2016 - 2017 5 iii. Leadership in Enabling and Industrial Technologies – Space*. European Commission Decision C (2016)4614. Retrieved from European Commission: https://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-leit-space_en.pdf

[168] European Commission (2018). *EN Horizon 2020 Work Programme 2018-2020 5.iii. Leadership in Enabling and Industrial Technologies – Space.* European Commission Decision C (2017)7124 of 27 October 2017. Retrieved from European Commission: http://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-leit-space_en.pdf

[169] See Annex for projects list

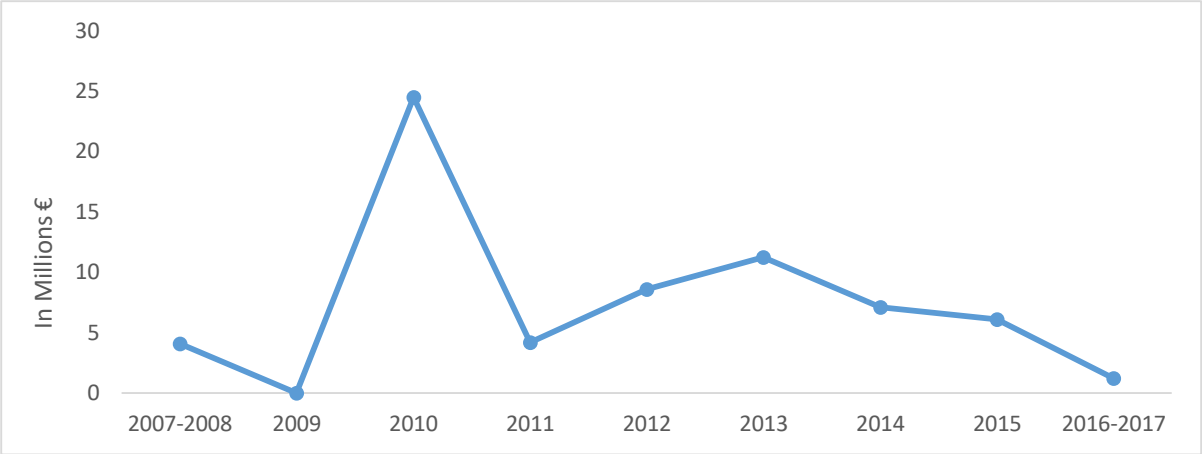

Figure 17: EU contribution to 'Security in Outer Space' R&D projects - FP7 and Horizon 2020

4.4.3 EU Initiatives in the Field of Diplomacy and Cooperation

EU actions in the field of security in outer space also integrate a variety of legal and diplomatic initiatives, with the aim of asserting its role in the international framework for space activities.

The EU has established a number of Space Policy Dialogues with key partners including the United States, Russia, China, Japan and South Africa to address a number of civilian and security issues such as GNSS interoperability, partnerships in the field of Earth Observation, research and development agenda or cooperation in the domains of security in outer space and space for security. The EU also actively contributes to the work (including activities related to security in outer space) of international organisations and committees such as the International Telecommunication Union (ITU), the International Committee on Global Navigation Satellite Systems (ICG) and the UN COPUOS.

Over the past decade, the leading action of the European Union has been the preparation, negotiation and tentative adoption by third countries of an International Code of Conduct for Outer Space Activities (ICoC). As a non-legally binding and voluntary-based complement to the existing legal framework regulating outer space activities, the purpose of the Code is 'to enhance the safety, security, and sustainability of all outer space activities' and to 'establish transparency and confidence-building measures, with the aim of enhancing mutual understanding and trust and helping both to prevent confrontation and foster national, regional and global security and stability'.[170] With these overarching objectives, the Code provides a set of rules and measures to be followed by subscribing states in the field of 'Outer Space Operations and Space Debris Mitigation', 'Notification of Outer Space Activities', 'Information on Outer Space Activities' and a 'Consultation Mechanism'.[171] More concretely, measures promoted by the Code have the following objectives:[172]

- Promoting space safety and sustainability;
- Pursuing strategic stability;
- Minimizing the risk of accidents, collisions, and harmful interference in space;
- Refraining from deliberate damage or destruction of spacecraft, unless in self-defence or to mitigate debris;
- Taking appropriate measures such as prior notification and consultations to minimize collision risks
- Improving adherence to and implementation of the International Telecommunications Union (ITU) regulations;
- Minimizing the creation of long-lived space debris and implementing the United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS) Space Debris Mitigation Guidelines.

The preparation of the Code started as early as 2007, as a first exercise at the crossroads of the new responsibilities given to the EU by

[170] Code of conduct Working Document 21 (2014). *Draft International Code of Conduct For Outer Space Activities*. Retrieved from https://eeas.europa.eu/sites/eeas/files/space_code_conduct_draft_vers_31-march-2014_en.pd f

[171] Ibid

[172] Johnson, C. (2014). *Draft International Code of Conduct for Outer Space Activities Fact Sheet.* Retrieved from Secure Word Foundation: https://swfound.org/media/166384/swf_draft_international_code_of_conduct_for_outer_space_activities_fact_sheet_february_2014.pdf

the Lisbon Treaty in space and foreign and security policies. A first draft, based on the input of EU Member States, was released to the international community in December 2008 to solicit feedback from non-EU countries and to negotiate the adoption of an international code. Multiple expert meetings took place, and the code was amended several times, with the latest draft produced in March 2014.

Although the Code has received support from a large number of countries, others, including emerging space-faring nations and established space powers, have expressed concerns about the negotiation process and the lack of involvement of non-EU countries in the production of the Code. Some countries have also openly criticised the contents of the Code and, in particular, the lack of definitions, the level of restrictions, and the scope of the document in addressing both civil and military space activities. The latest draft of the Code was intended to be negotiated at the United Nations in New York in July 2015, outside the official UN structure, but the meeting that had been organised by the EU, and to which representatives from over 100 countries were invited, was cut short by procedural moves.[173]

This failed exercise highlighted the complexity of diplomatic procedures in the field of security in outer space, the discrepancy of views in the international community, and the unsolved ambiguity between civil and military aspects. On the international scene, the EU and its Member States have demonstrated their readiness and willingness to move forward with more restrictive frameworks promoting security, safety, and sustainability for the conduct of space activities. This is, however, not the case with a number of other countries, including major space powers reluctant to agree on a limitation of their freedom of action in outer space, in particular for military purposes, and emerging space-faring nations concerned by additional obligations that could hamper their access and use of outer space.

Today, the European Union engagement in the advocacy of responsible behaviour in the conduct of outer space activities continues, in close collaboration with its Member States. Noticeable activities include, among others:[174]

- Recognition and support to UN COPUOS activities such as the Working Group on Long Term Sustainability of Outer Space Activities (WG-LTS);
- Contribution to the Group of Governmental Experts (GGE) on Transparency and Confidence-Building Measures in Outer Space Activities (TCBMs), and support to their adoption;
- Support to UN General Assembly Resolution 71/42 regarding the Prevention of an Arms Race in Outer Space (PAROS) and contribution to the GGE on PAROS that will be kicked-off in July 2018;
- Negotiations with third countries regarding draft treaties and initiatives in the field of 'Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects' (PPWT) and 'No First Placement of Weapons in Outer Space' (NFP);
- Promotion of initiatives such as the Principles of Responsible Behaviour for Outer Space (PORBOS), which provides a set of principles 'preventing an arms race in outer space and preventing outer space from becoming an area of conflict to safeguard the long-term use of the space environment for peaceful purposes.'[175]

4.4.4 EU Space Surveillance & Tracking Support Framework

4.4.4.1 Genesis

In 2012, at the end of the Preparatory Phase of the ESA SSA programme, several Member States decided to withdraw or reduce their contribution to the programme component related to SST, with the objective of managing it through a consortium, under the aegis of an EU framework. The two other domains, space weather and NEOs observation, remained under the responsibility of the European Space Agency, with a preponderant budgetary focus on space weather.

The main reason behind this decision was related to the prominence of military and operational aspects in this field and the limited capacity of ESA, an R&D agency, to properly manage security aspects. In this regard, some Member States expressed concerns about

[173] Listner, M., J., (2015). The International Code of Conduct: Comments on changes in the latest draft and post-mortem thoughts. Retrieved from Space Review: http://www.thespacereview.com/article/2851/1

[174] EEAS (2016). *Conference on Disarmament – Working Group of the "Way Ahead*". Geneva. Retrieved from European Union External Action: https://eeas.europa.eu/headquarters/headquarters-homepage/28329/conference-disarmament-working-group-way-ahead-eu-statement-prevention-arms-race-outer-space_en

[175] EEAS (2017). *Conference on Disarmament - Working Group on the "Way Ahead" - EU Statement on the Prevention of an Arms Race in Outer Space.* Retrieved from European Union-External Action: https://eeas.europa.eu/headquarters/headquarters-homepage/28329/conference-disarmament-working-group-way-ahead-eu-statement-prevention-arms-race-outer-space_en

compliance with defence and security requirements. Indeed, many systems used for SST are owned or operated by military organisations and SST data to be processed, exchanged or distributed may be classified, requiring all entities involved to comply with specific requirements and to follow strict procedures. The prominence of military aspects also raised some concerns related to national sovereignty and some Member States, especially France and Germany, stressed the importance for them of maintaining control over their assets and data produced by these assets.

To tackle this situation, German and French military organisations negotiated and prepared a non-paper submitted to the Commission in December 2012. The document requested the establishment of a new mechanism at EU level with a specific governance scheme where Member States could maintain control over their assets while cooperating in SST activities. The objective pursued by Germany and France was to promote a framework that would foster pan-European cooperation and improve cost-efficiency (e.g. by avoiding duplication of efforts) to deliver EU SST services while complying with national concerns resulting from the specific nature of SST systems and data. Well-suited to the Lisbon treaty regime of shared competences between the European Union and Member States in the field of security and space, the framework promoted by France and Germany would also enable transference to the European Union of a share of the financial burden of SST operation and coordination activities.

Accordingly, in 2013 the Commission published a first communication mentioning its intention to ´come forward with a proposal sketching the organisational framework for the setting up and operation of a European SST service in partnership with Member States building on their existing assets and expertise´.[176] The Space Working Party in Brussels started to negotiate the contents of what became Decision No 541/2014/EU of the European Parliament and of the Council of 16 April 2014 establishing a Framework for Space Surveillance and Tracking Support.[177]

Today, the SST component of the ESA SSA programme still exists but is disconnected from the EU SST Consortium.[178] The programme now focuses mostly on the Space Weather component with around 50% of the budget allocated to it.[179]

4.4.4.2 General Presentation

On 16 April 2014, after two years of discussion, the European Parliament and the Council of the European Union adopted Decision No 541/2014/EU. The document outlines the following: [180]

- *Purpose:* The general purpose of the support framework is to ensure the long-term availability of the European and national space infrastructures, services and facilities and to contribute to ensuring the peaceful use and exploration of outer space. Specific goals include:
  - Assess and reduce the risks of collision to enable operators to carry out and plan mitigation measures;
  - Reduce risks related to launches;
  - Survey uncontrolled re-entries of space objects to Earth atmosphere;
  - Prevent the proliferation of space debris.
- *Objective:* The objective of the support framework is to pool and network national and European assets to provide SST services.
  - These services should be driven by civilian user requirements defined in the 'European space situational awareness high-level civil-military user requirements' working paper;
  - These services should be complementary to research activities related to the protection of space-based infrastructure carried out under Horizon 2020;

[176] European Commission (2013). Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions EU Space Industrial Policy. COM (2013) 108 final. Brussels: European Commission https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013DC0108&from=EN

[177] European Commission (2014). *DECISION No 541/2014/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 April 2014 establishing a Framework for Space Surveillance and Tracking Support.* Retrieved from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014D0541&qid=1535031889695&from=en

[178] ESA. *7th European Conference On Space Debris*. *Space Surveillance and Tracking in ESA's SSA programme*. Retrieved from https://conference.sdo.esoc.esa.int/proceedings/sdc7/paper/242

[179] ESA. *Space Situational Awareness.* Retrieved from http://swe.ssa.esa.int/

[180] European Commission (2014). *DECISION No 541/2014/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 April 2014 establishing a Framework for Space Surveillance and Tracking Support.* Retrieved from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014D0541&qid=1535031889695&from=en

- The development of new sensors or the upgrading of existing sensors operated by Member States should be encouraged afterwards;
- Cooperation with international partners, in particular the United States of America, should be addressed to avoid collisions in space and to prevent the proliferation of space debris.

- *Activities:* The activity is organised around three project lines: the Sensor Function, the Processing Function and the Service Provision Function.[181]
  - The establishment and operation of a sensor function consisting of a *network of* Member States and European ground and space-based *sensors* to survey and track space objects, creating then a *database;*
  - The establishment and operation of a *processing function* to process and analyse SST data (at national level) in order to produce SST information, i.e. processed data readily meaningful to the recipient;
  - Set up a function to provide *SST services* of civilian nature, i.e. services of collision avoidance, fragmentation and re-entry, to users including all Member States, the European Commission and Council, the EEAS, public and private spacecraft owners and operators and public authorities concerned with civil protection.

The EU SST Consortium (http://www.eusst.eu/) outlines that to establish, operate, and evolve these three functions, EUSST consists of three incremental projects:

- *Initial Service Delivery (1SST):* Based on current operational national SST assets within the SST Consortium, early SST services are provided to European users in cooperation with the EU SatCen.
- *Service Provision (2SST):* To consolidate SST Services, a European SST network is constructed that connects national sensors to national operations centres (NOCs) and NOCs between each other.
- *Sensor Development (3SST):* To understand the evolution and future performance of EUSST, a roadmap lays out R&D actions for prioritizing, upgrading, and developing new sensor assets (radars, telescopes, laser stations).

According to the report from the European Commission to the European Parliament and the Council on the implementation of the Space Surveillance and Tracking (SST) support framework (2014-2017) published in May 2018, "a total of EUR 167.5 million has been allocated for 2015-2020 through various grants financed by the Copernicus, Galileo and Horizon 2020 programmes, out of which around EUR 70.5 million to implement the actions of the SST Decision (1SST and 2SST grants) and EUR 97 million for the sensors' upgrades (3SST)."[182]

In this framework, Member States are directly responsible for the operation of their sensors and the processing of data, as well as for the implementation of the data policy in cooperation with the EU SatCen. The role of the Commission is to manage the SST Support Framework, as well as monitor and ensure its implementation. For this purpose, a first report on the implementation of the SST Support Framework is expected by the European Parliament and the Council by July 1st 2018. The Commission also defines the general guidelines for the governance of the SST Support Framework and facilitates the broadest participation of Member States. The EU SatCen cooperates with the consortium and acts as the EU SST Front Desk, providing SST services to SST Users.

In March 2015, five Member States (i.e. France, Germany, Italy, Spain and the United Kingdom) represented by a national entity (i.e. respectively CNES, DLR, ASI, CDTI and UKSA) were deemed compliant with the criteria for participation in the SST support framework and designated national entities to make up the SST Consortium. In line with the ambition to develop a broad European SST capability benefiting all Member States, the Consortium is open to enlargement. In this regard, applicant states, after having presented their national assets to the Consortium, have to

[181] Note: The Sensor Function consists in a network of the five member States ground-based sensors, survey ing and tracking space objects and feeding, for the moment, a national database thereof; The Processing Function consists of processing and analysing the SST data at national level, producing SST information and services for transmission to the SST Service Provision Function; The Function to provide SST Services consists of providing, on the basis of the SST data, collision avoidance, fragmentation and re-entry services.

[182] European Commission. REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the implementation of the Space Surveillance and Tracking (SST) support framework (2014-2017). Retrieved from: http://eur-lex.europa.eu/resource.html?uri=cellar:fbafc703-4eb8-11e8-be1d-01aa75ed71a1.0021.02/DOC_1&format=PDF

submit a formal application to the Commission, demonstrating their compliance with the two following criteria:

- Applying states must *own or have access to adequate SST sensors*, already available or under development, as well as to the human resources to operate them.
- Applying states must *establish and present an action plan* for the implementation of the objectives set out in the Decision including the modalities of cooperation with other Member States.

To date, Romania, Portugal and Poland have already submitted their applications to join the consortium, and a growing number of countries has expressed their interest in joining the consortium.

4.4.4.3 Governance

The governance scheme in which the Consortium currently operates is outlined by the Consortium Agreement among the five Member States.[183] The Consortium governance system is segmented in three layers: the decision-making level, the management level and the operational working level. A broader description of that working scheme is provided below.

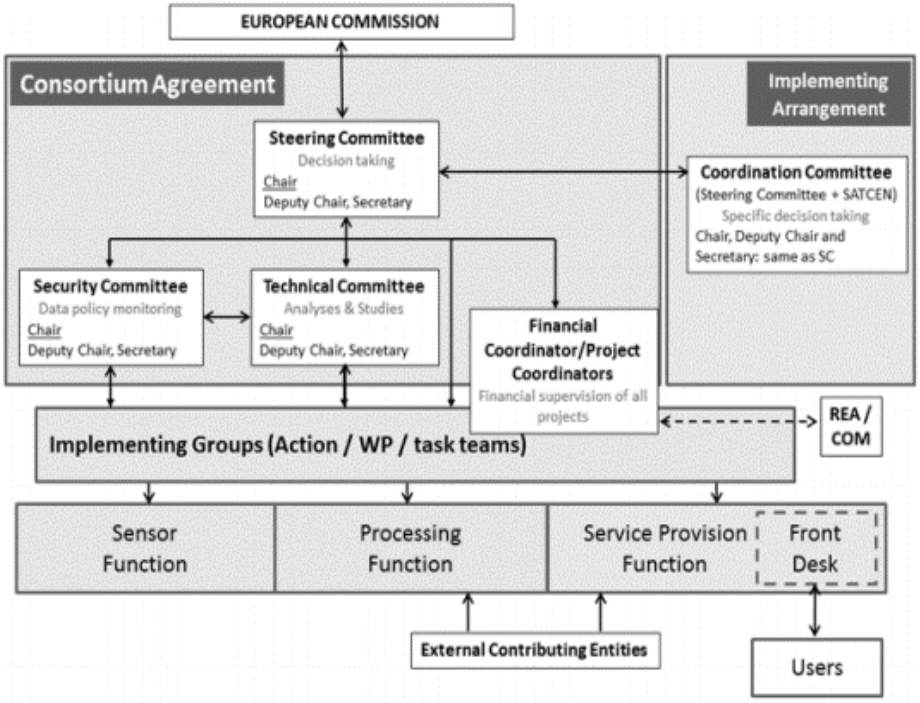

Figure 18: EU SST support framework governance

The decision making level provides for the normalisation of the relationship between the Consortium and the EC, notably the Directorate-General for Internal Market, Industry, Entrepreneurship, and SMEs (DG GROW) and Member States. Decision-making processes are ruled by the *Consortium Agreement*, the formal agreement that governs cooperation and the action of the Member States, and the *Implementing Arrangement*, which governs the interaction of the five Member States and the SatCen. Currently, decisions are taken on a consensus basis, which means that one veto can potentially stop the entire decision process. The decision-making layer includes *the Chair of the Steering Committee, the Steering Committee itself, the Coordination Committee* and *the Technical and Security Committees*.

- The *Steering Committee* is the organisation that takes the main decisions, at present chaired by France. Germany was the first country to be in charge. The Steering Committee has to meet other committees at least 4 times per year, not including its working meetings.
- The *Technical Committee* is involved in all the technical aspects of the Consortium, mainly producing technical analyses and studies. This committee reports to the Steering Committee.

[183] ASI (2015). SST Consortium agreement signed Signature of the EU initiative to guarantee the long-term availability of space structures for the security of EU citizens, along with a national ASI-INAF-Defence agreement. Retrieved from http://www.asi.it/en/news/sst-consortium-agreement-signed

- The *Security Committee* is in charge of monitoring all the security data and information policies. This committee reports to the Steering Committee.
- The *Coordination Committee* is chaired by the Chair of the Steering Committee and gathers delegate from SatCen and the Steering Committee. It coordinates the collaboration schemes of Member States and with SatCen.[184] The Commission and, if relevant, aspiring Member States who want to join the Consortium, participate to the Steering Committee as observers.

The management level refers to the coordination of projects and encompasses the three main projects undertaken by the Consortium, reflecting the three budgetary lines that fund the EU SST Support Framework. Each project includes six work packages, each of which has from 5 to 6 specific tasks executed by the working group of each state or SatCen.[185] Finally, each project has a lifetime of 18 months, after which the Consortium must develop new applications for projects and new projects within the three core areas to move forward with. The advancement and the outlining of projects must include reporting to the EC to justify the use of funds. In this regard, it could be argued that the EC intervention currently mainly lies in the budgetary dimension of the SST initiative.

The operational working level refers to the management of the sensor function and the national operational centres that produce SST data. This level constitutes the foundation of the Consortium architecture.

4.4.4.4 From Networking to Delivery of SST Services

So far the evolution of the EU SST System Architecture (operational phase) has mainly been segmented in three phases:

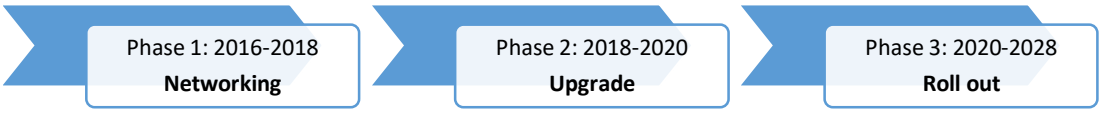

Figure 19: Phases of the EU SST System Architecture

- *Networking (2016-2018):* The Consortium has been working on networking national sensors and operational centres with a view to delivering services through its front-desk, namely SatCen. So far there is no service entirely based on European indigenous SST data and most services are based on U.S. data complemented with data generated from national capabilities. At the start of the current phase, the Consortium and SatCen have already achieved the first milestone - the delivery of initial services. By the end of 2018 it is expected to have improved services, and the basis for a shared European database.

An Action Plan, proposed by the European Commission (under negotiations), building on the assessment and gap analysis of the current European SST capabilities will lay the steps forward - in terms of capacity building, geographical coverage and budget allocation - to achieve maximum risk reduction by the end of the next multi-annual financial framework (2021-2027). After that, the decision on the level of autonomy to reach among the different Member States will be left up to them.

- *Upgrade (2018-2020):* Along with pursuing sensor networking objectives, the Consortium will incorporate new Member States and create the nucleus of a Shared European Catalogue – aside from U.S. data based services, to support the American catalogue.
- *Roll out (2020-2027):* The Consortium will create an integrated EU – U.S. catalogue of space objects and deliver regular services based on this Shared European Catalogue.

Depending on the time, budget, technical challenges, system performances and reliability, as well as user satisfaction, the consortium has structured possible pathways ahead with an incremental approach to reach an appropriate SST capability. Key parameters are the budget, the upgrade of sensors, the development of new sensors, and the signing of new Sharing Agreements.

Current capacities (2017) and expected capacities (2021) of the sensor function are provided in the table below:[186]

[184] European Satellite Union. *Space Situational Awareness (SSA)*. Retrieved from The EU Satellite Centre: https://www.satcen.europa.eu/services/ssa

[185] Note: In total, there are about 70 to 80 different tasks to be performed by the Consortium.

[186] European Commission (2018). REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the implementation of the Space Surveillance and Tracking (SST) support framework (2014-

	2017 (initial architecture)		2021 (expected architecture)	
MS architecture (orbit and object size)	Total observed (%)*	Total well -observed (% of the total) **	Total observed (%)*	Total well -observed (% of the total)**
LEO (> 7 cm)	19%	14%	35%	19%
LEO (> 50 cm)	79%	72%	95%	80%
LEO (> 1 m)	96%	95%	98%	97%
MEO (> 40 cm)	18%	7%	62%	7%
GEO (> 50 cm)	40%	30%	66%	42%

* Observed objects are objects that were observed at least once during the 14-day period of the simulation.
** Well-observed objects are those observed objects that were observed every day in LEO and every three days in MEO/GEO

Table 7: Estimated level of coverage by size of object and orbit of the initial architecture (2017) and expected architecture (2021)

4.4.4.5 Achievements and Challenges

On the basis of a documentation review, stakeholders' consultations (including member states, users and other public stakeholders) and with the support of independent experts, the European Commission identified the following key achievements of the support framework: [187]

- *availability of the EU SST services* (i.e. collision avoidance, in-orbit fragmentation and re-entry services) since July 1st 2016, through the EU SST portal to all European institutional users and spacecraft owners and operators free of charge and on a 24/7 basis;
- *outreach to users* including identification of potential users, documentation of their needs and awareness raising of space risks and the need to protect space infrastructure;
- *cooperation and collection of shared know-how* with the establishment of regular communication between NOCs and increased cooperation between national experts through working groups;
- *mapping and pooling of European assets* with 33 sensors contributing to the initial EU SST operations, a complete mapping of national and European sensors and beginning of national sensors upgrades;
- *outreach to other Member States* to collaborate with or to join the SST Consortium.

Stakeholders interviewed by ESPI unanimously acknowledged the multiple achievements of the consortium so far, particularly for the complex systems networking and the initial steps towards a full-fledged European Union SST service, while complying with both civil and military frameworks. An important achievement of the consortium, difficult to measure but often praised by consortium partners, has been the reinforcement of European coordination and the confidence-building among partners. Achieving consensus among France, Germany, Italy, Spain and the UK – which speak today with a clear and unified voice – has been a challenge that the consortium successfully took on. Today, EU Member States established national databases and are currently building a common European database of unclassified data. The consortium also continues its efforts to promote the exchange of classified data through bilateral agreements and the construction of a secure data sharing exchange network. From this standpoint the consortium is certainly achieving its purpose.

Nevertheless, stakeholders also underline that various issues remain and that serious challenges lie ahead of the consortium to take a more prominent role, and achieve more ambitious objectives in line with the rising space security stakes in Europe. Key stakes ahead of the consortium identified by the European Commission assessment include: [188]

- *effectiveness and European added-value optimisation* to avoid duplication of efforts and support an efficient development of EU SST capabilities;
- *achievement of an acceptable level of European autonomy* based on further networking and development effort in line with a level of ambition to be decided by the European Union and with, as a first step, the delivery of a common EU database of orbital objects building on national data;

2017). Retrieved form EUR-Lex: https://eur-lex.europa.eu/resource.html?uri=cellar:fbafc703-4eb8-11e8-be1d-01aa75ed71a1.0021.02/DOC_1&format=PDF

[187] Ibid
[188] Ibid

- *development of EU SST services in compliance with users' needs* requiring additional outreach effort to raise awareness and collect feedback but also the development of common operational procedures and standards;
- *synergies with other components of security in outer space* to cover the range of space hazards over the entire space mission lifecycle;
- *governance optimisation* to accommodate a broader Member State participation, an enhanced role of the European Commission for guidance and monitoring at the strategic, policy and organisational levels and to explore of the role of EU SatCen as EU SST services front-desk.

With regards to financial management, other issues will have to be addressed by future arrangements revision including:

- simplification of funding sources to avoid unnecessary burdens affecting the results achieved by the consortium and
- budget allocation, to adapt current rules (i.e. sharing on an equal base between the members of the consortium, independently from their current capabilities) to the enlargement of the consortium.

These challenges, and other short- and long-term stakes identified as a result of ESPI analysis, are discussed in more details in the following chapter on the way forward for an enhanced role of Europe in Security in Outer Space.

5. Way Forward for an Enhanced Role of Europe in Security in Outer Space

5.1 Rising Stakes for Europe

5.1.1 Short-Term Policy Rationales

The value of the European space infrastructure, which is the result of a continuous and substantial investment by public and private actors, lies first and foremost in the substantial socio-economic benefits it enables across a multitude of economic and strategic sectors for Europe. Recent studies have captured the sizeable impact of space infrastructure on the European economy and society. This already considerable socio-economic value can reasonably be expected to increase in the future. Indeed, fostered by the digital revolution, and stimulated by a transition of the space sector characterised by intense innovation and considerable private investments, new space applications are being continuously developed, also contributing to promising terrestrial technologies.

Interestingly, benefits enabled by the space infrastructure can be looked at from another angle: as the use of space-based solutions becomes more pervasive and part of business-as-usual, the dependence of governments, businesses and individuals on space infrastructure grows, creating new risks. Incapacitation, even partial, of space assets could lead to a dreadful chain of impacts for the European economy and society. From this standpoint, the socio-economic rationale (i.e. secure the space infrastructure to protect the benefits it enables) can be considered, alone, as a reasonable argument for Europe to position security at the top of the space policy agenda.

In fact, 'Identify and mitigate risks associated to dependence on critical space assets' is the first recommendation of a PwC study conducted for the European Commission on the dependence of the European Economy on Space Infrastructures.[189] The study identifies three main options:

- *Space infrastructure security:* continue, consolidate and further enhance the European effort to ensure the security of the space and ground components of space infrastructures;
- *Alternative solutions and redundancy:* consider different approaches to reduce the risks of relying on a single system, for example ground-based complements or substitutes;
- *Crisis management and Emergency Response:* guarantee access to satellite services during crises and emergency situations, at least for relevant governmental actors.

In line with these concerns and in the field of GNSS, the European Commission published in March 2018 the first edition of the European Radio Navigation Plan, which aims to identify and mitigate risks associated to dependence on GNSS.[190]

The significant progress of EU programmes over the period 2014-2020 is also amplifying the importance of a service-oriented space policy to build user confidence, encourage the uptake of space services, and consequently maximise the benefits of the European space infrastructure. In the future, the potential introduction of new initiatives such as GOVSATCOM will further amplify this need.

Conditions to guarantee an appropriate quality of service include 1) operational capacities meeting user performance requirements, 2) continuity of programmes to ensure infrastructure maintenance, upgrade and evolutions, and 3) appropriate measures to protect the infrastructure against threats. Such requirements are even more stringent for governmental and defence and security users that the EU seeks to support to reinforce and leverage synergies between the civil and defence domains. To do so, protecting the space infrastructure and meeting the most stringent security requirements is a prerequisite.

[189] PwC (2017). *Dependence of the European Economy on Space Infrastructures*. Brussels: EU Publications. Retrieved from: http://www.copernicus.eu/sites/default/files/library/Copernicus_SocioEconomic_Impact_October_2016.pdf

[190] European Commission (2018). *European Radio Navigation Plan*: https://ec.europa.eu/docsroom/documents/28325/attachments/1/translations/en/renditions/native

Europe also needs to guarantee the security of its space infrastructure autonomously through independent capabilities (i.e. systems, data, technologies). From this perspective, although cooperation with third countries is essential in the field of space security, Europe must ensure a capacity to control the level of reliance on its partners and to maintain it within acceptable boundaries.

To conclude, the rising need for enhanced space security in Europe is driven in the short-term by four key policy rationales:

- *Secure the results of the continuous and substantial investment* made by public and private actors;
- *Protect the European economy and society* against risks related to its pervasive and sizeable dependence on the space infrastructure;
- *Contribute to a service-oriented policy* by assuring the ability of the infrastructure to deliver a service that can justifiably be trusted, in particular for users in defence and security;
- *Guarantee European autonomy and freedom of action* in the field of security in outer space, and in the space domain at large.

5.1.2 Long-Term Strategic Stakes

Beyond these short-term policy stakes, the need for a reinforced approach to space security is also driven by longer-term considerations stemming from the strategic ambition of Europe to "promote its position as a leader in space, increase its share on the world space markets, and seize the benefits and opportunities offered by space."[191] In many ways, the level of European engagement in the space security domain will be a determining factor in the position that Europe can expect to hold in the global space arena in the future.

First, space security now holds a central position in space diplomacy. To be recognised as a leader in space, Europe must therefore play a prominent role in international dialogues and negotiations, as a promoter of a clear, united and consistent "European way". In this respect, European activities and initiatives on the international scene, and in particular the elaboration of a Code of Conduct for Outer Space Activities and subsequent international diplomatic efforts, have demonstrated Europe's willingness to work with the international community on space issues. The exercise has positioned the European Union and its Member States as the principal advocates of the preservation of a safe and secure space environment and of the peaceful use of outer space. The unsuccessful outcome, however, has revealed the need for Europe to reinforce bilateral and multilateral relations with international partners on this matter, including both established space powers and emerging spacefaring nations.

Second, building European autonomy and authority in the field of space security will also be essential to foster European leadership on the global scene. Today, Europe acts as a trailblazer in the adoption of best practices for Space Environment Protection and Preservation (e.g. legislation, standards) and in the development of related technologies (i.e. passive de-orbitation, active debris removal), but lags behind in the field of Space Situational Awareness with a gap that is poised to grow in the next decade if Europe does not make a more substantial effort in this field. From this perspective, equipping Europe with a system providing comprehensive and independent SSA capabilities is a priority to position Europe as a credible interlocutor on the international scene; hence capacity-building alike in SSA. Such effort is also essential in view of the development of a civil space traffic management framework. Stakes for Europe are high to develop its own approach to STM and play a prominent role in the construction of an international framework taking into account that, in the long run, 1) the globalization and intensification of space activity will make the development of an international STM framework necessary, and 2) that the U.S. is already moving forward with preliminary steps. From this standpoint, equipping Europe with advanced SSA capabilities, compulsory to fully monitor operations in orbit, would be a prerequisite to build the required credibility and capacity to participate to the development of rules and norms of an international STM framework.

Last but not least, space security will play an increasing role in commercial space markets:

- *Commercial SSA data and value-added services:* the growing need for SSA data and services of public and private satellite operators is a formidable business opportunity that a handful of private actors are already trying to seize. Supporting the

[191] European Commission (2016). Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions. *Space Strategy For Europe*. COM (2016) 705 final. Brussels: European Commission. Retrieved from https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/COM-2016-705-F1-EN-MAIN.PDF

emergence of European champions, offering solutions to European and foreign users, is an important parameter for consideration.

- *Competitive bias:* the implementation of new practices (e.g. laws, regulations, standards, procedures) promoting space security but constraining the way space activities are conducted inevitably creates competitive bias:
  - Between industries that are constrained and those that are not;
  - Between industries that are prepared to implement such constraints and those that are not.

  Supporting the preparation of the European space industry for the impact of space security practices on international competition is another important parameter for consideration.

The Space Data Association (SDA) is an interesting case study. Described as a ´formal, non-profit association of civil, commercial and military spacecraft operators that supports the controlled, reliable and efficient sharing of data that is critical to the safety and integrity of satellite operators´[192], the association was founded in 2009 as a response to the limitations of JSpOC. SDA was originally launched as an initiative of Inmarsat, Intelsat, and SES, which, together with Eutelsat, are currently its Executive Members. The Association has 35 members with 279 GEO satellites as part of the network, making up 70% of all active commercial GEO satellites.[193] In 2010, SDA established the Space Data Centre (SDC) - its own automated SSA system designed and operated by Analytical Graphics, Inc. It became fully operational in April 2011. SDA and AGI will soon launch an upgraded Space Data Centre (SDC 2.0) Space Traffic Management (STM) Service, powered by ComSpOC, as announced in March 2017. SDC 2.0 will independently supply a highly accurate catalogue of space objects, gathered by ground-based telescopes, radars, and potentially space-based optical sensors,[194] to include objects larger than 20 cm in GEO – the current capability being 1 m.[195]

Developing a fruitful cooperation framework with private industry (consultation, partnerships, distribution of responsibilities…) based on mutual benefits should be a central axis of development on the long-term.

5.2 Way Forward: Key Elements for Consideration

Security in Outer Space is intrinsically a complex issue because of the diversity of potential threats to the various European space infrastructures and to the provision of associated services, as well as of the complexity of mitigation or remediation measures.

As far as Europe is concerned, the multiplicity of stakeholders brings an additional layer of complexity. In one way or another, this issue impacts all European space actors. Therefore, they would undoubtedly benefit from sharing experiences and concerns, as well as from pooling resources to, at the minimum, cope with the security challenges that are transverse to all space systems, such as the proliferation of space debris or space weather hazards. This encompasses:

- Private operators and public bodies,
- Civil and military entities,
- National agencies, intergovernmental and supranational organisations.

What is first at stake is the capacity of Europe to efficiently mobilize the substantial resources required to deal with this complex issue, which implies:

- Reaching a broad political consensus on the objectives to be set for a "joint" European Security in Outer Space policy. Such policy should be based on a joint overarching threat analysis and on internationally recognised standards;
- Devising, accordingly, technological roadmaps for the development and the maturation of required technologies and systems, at affordable conditions, and with the appropriate level of European autonomy;
- Assessing the associated programmatic provisions and schedules in all available or potential sources of funding (MFF, Security Fund, national and ESA programmes, private funding);
- Achieving a sufficient level of coordination of activities among various stakeholders in order to avoid gaps and useless duplication of efforts.

[192] The Space Data Association (SDA). *SDA Overview.* Retrieved from SDA: http://www.space-data.org/sda/about/sda-overview/

[193] Rawlins, M. (2017). *IAA Space Debris Committee*. Retrieved From SDA: http://iaaweb.org/iaa/Scientific%20Activity/debrisminutes031711.pdf

[194] Froeliger, J., L. (2017). *Greater Industry Cooperation Needed to Avoid Space Collisions*. Retrieved from INTELSAT: http://www.intelsat.com/news/blog/greater-industry-cooperation-needed-to-avoid-space-collisions/

[195] Dickinson, M. *Preparing for Congested Space. An SDA Focus*. Retrieved from Sat Magazine: http://www.satmagazine.com/story.php?number=1486837251

Second comes the implementation of such policy, which implies the definition of agreed governance schemes building on the existing areas of expertise readily available throughout Europe, as well as on the integration of established best practices and respective competencies of key stakeholders. These governance schemes shall, for each system concerned, propose an appropriate organisation and provide for the breakdown of responsibilities among the various entities in the processes, aimed at ensuring:

- The definition of security requirements based on specific threat analysis,
- The setting up and implementation of risk management schemes,
- The elaboration and implementation of operational procedures,
- The monitoring of compliance of operations,
- The coordination of the various entities.

A central challenge for these governance schemes will be to find the appropriate mechanism to accommodate a more prominent European leadership for which the European Union is the most suitable candidate, further building on the existing centres of expertise, and the need for Member States to maintain control over national systems and data. Notwithstanding the considerable progress achieved by Europe in both Space and Security & Defence domains over the period 2014-2020, an in-depth reassessment of stakeholders' views, in particular with regards to the respective roles of Member States and the EU in space-related matters, would be timely and opportune in order to move further.

With a view to building a reinforced, comprehensive, coherent and cooperative European approach to security in outer space, various sensitive issues are at stake:

- Capacity-building for SSA (integrating all related components: SST, SWE and NEO),
- Space environment protection and preservation including, in particular, relevant technology developments, common standards and guiding principles for diplomacy and international cooperation,
- Space programme security architecture and risk management procedures for European space programmes.

The success of the European approach to security in outer space will rely on key enabling factors:

- *Setting up consensual European leadership* in a domain that, so far, has been driven primarily by Member States. For that, two scenarios can be envisaged:
  - *Bottom-up approach* building on existing intergovernmental frameworks (in particular ESA and the EU SST consortium) and seeking a progressive enlargement of partners and scope toward, first, a comprehensive SSA framework and, ultimately, the construction of a European Space Traffic Management structure;
  - *Top-down approach* with the introduction of a full-fledged programme establishing the European Union as the main owner and operator of European civil SSA capacities with the necessary reinforcement of security protocols and risk management.
- *Development and distribution of key industrial capacities and adequate involvement of industry* as a core contributor to capacity-building in the following strategic areas of activity. (i.e. such involvement would require the setting up of stringent security protocols and should be conditioned on the expected benefits in terms of cost savings, improved competitiveness and business development, including on international markets):
  - *Data production,* relying on privately-operated sensors and processing capabilities and reinforcing/substituting governmental capacities in carefully selected fields of a lesser sensitivity such as the GEO orbit, space weather or NEO.
  - *Value-added services,* elaborating on publicly available data, possibly complemented by private data, for governmental and commercial users. Ultimately, such services could be embedded in an EU programme to augment SSA services, including for security and defence governmental users.
  - *Standards,* for in-orbit operations and spacecraft design supporting a European approach to the preservation of a safe and secure space environment.
- *Sharing of clearly identified ambitions* to achieve European autonomy and freedom of action in space and, subsequently, mobilisation of the required resources. As the crux of every political issue, the level of funding allocated by the different stakeholders including the European Union, Member States and ESA will be a determining factor of Europe's capacity to meet the rising challenges in the field of security in outer space. Here, two aspects shall be considered:

- *Use of complementary public funding* including, in particular, the new European Defence Fund which is a particularly appropriate mechanism to support EU and national efforts for development and acquisition of systems.
- *Leverage private investment,* provided that more prominent involvement of private actors is sought.

- *International diplomacy and cooperation,* in synergy with European efforts in other areas, for both:
  - Operational concerns about the way forward to an international space traffic management framework (e.g. data sharing, in-orbit operations, SWE and NEO warnings)
  - Fostering of a global approach to space activities in line with Europe's vision on the preservation of a safe and secure space environment and for the peaceful use of outer space.

5.3 Toward a New Framework for 2021-2027

5.3.1 European Commission's draft regulation

An important step toward the preparation of a renewed European framework for security in outer space lies in the current preparation of the future Multiannual Financial Framework 2021–2027 of the European Union, which will set a number of important parameters for mid-term developments in this domain including ambitions, means and organisation.

To provide a baseline for negotiations with Member States, the European Commission issued in June 2018 a draft regulation for the Space Programme of the European Union.[196] When finalised and adopted,[197] the new regulation will repeal previous decisions for EGNOS/Galileo, Copernicus and the SST support framework covering the period 2014-2020 and provide a legal basis for activities on the period 2021-2027.

Stakes are high.

From a general standpoint, the draft regulation proposes the integration of the different space programmes of the EU into a single EU programme with several components (governed by a single regulation), the horizontal extension of GSA mandate to cover executive and security activities for all components of the integrated programme (GSA to become the EU Agency for the Space Programme) and an increase of the overall programme budget to EUR 16 Billion (segmented as follows: EGNOS/Galileo: EUR 9.7 billion, Copernicus: EUR 5.8 billion, SST and GOVSATCOM: EUR 0.5 billion).

The regulation establishes that "the Commission shall implement the Union space policy and shall assume responsibility for the Union space programme, *including in the field of security*. It shall determine the overall objectives and priorities of the programme and shall supervise its implementation, in particular in terms of costs, timetable and results, including over the funds and tasks it entrusts to other entities." [198] This general provision clarifies that, although tasks related to security (e.g. accreditation, SSA, rules and standards implementation…) can be entrusted to other entities such as ESA, Member States or agencies of the EU, the European Commission is ultimately accountable for the security of the EU space programme. This responsibility encompasses:

- The protection of infrastructure, both ground and space, and of the provision of services, particularly against physical or cyber-attacks;
- The control and management of technology transfers;
- The development and preservation within the Union of the competence and know-how acquired;
- The protection of sensitive non-classified and classified information.

5.3.1.1 Space Infrastructure Security

The draft regulation provides a number of provisions related to the security architecture of the EU space programme (Title V) including security activities and governance (Chapter I), security accreditation (Chapter II) and management of classified information (Chapter III). Overall, the draft regulation establishes that the EC shall determine policy measures to ensure a high degree of security for each component of the EU space programme and stresses the importance of building on Member States experience and expertise in this field.

[196] European Commission. (2018). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the space policy programme of the European Union, relating to the European Union Agency for Space and repealing Regulations (EU) No 1285/2013, No 377/2014 and No 912/2010 and Decision 541/2014/EU. Brussels

[197] Note: at the time of this report publication, the draft regulation is still under negotiation with member states.

[198] Ibid

Here, the most substantial proposed evolution with regards to the 2014-2020 framework is related to the reinforcement of security accreditation procedures, in particular with regards to independence from operational functions of the programme and to the enlargement of GSA role across all components of the programme (so far limited to Galileo and EGNOS programmes).

Noticeably, measures to organise a European response to military threats or deliberate attacks are not addressed by the regulation. At this point in time, such move would be quite premature since it implies some pre-requisites, including a European space defence doctrine or a formal governance scheme to deal with such issues. This shall be addressed in the framework of the further development of the EU's Foreign and Security Policy and European Defence Action Plan.

5.3.1.2 Space Environment Protection and Preservation

Space Environment Protection and Preservation is not directly addressed in the draft regulation with concrete measures and activities (e.g. standards, technology developments…), however, a number of mentions delineate the vision of the European Commission in this field:

- Consistency with existing space hazards mitigation measures and with an initiative leading to a non-legally binding instrument to be negotiated within the framework of the United Nations, as a way to foster increased international cooperation, establishing standards of responsible behavior across the full range of space activity, strengthening commitments to non-interference in the peaceful exploration and use of outer space, facilitating equitable access to outer space and increasing transparency of outer space activities.
- Monitoring of international initiatives and developments in the area of the space traffic management to be taken into consideration in the context of the mid-term review of the MFF.
- Synergies of SST with initiatives of active removal and passivation measures of space debris with a view to reducing risks of collision.

With these mentions, the regulation highlights the importance of these topics for Europe but does not elaborate on the ways to ensure that EU will be in a position to weigh in space-related international negotiations in order to effectively contribute to future potential initiatives in the field of space diplomacy (United Nations instrument), Space Traffic Management (monitoring of international developments) and active/passive debris removal.

5.3.1.3 Space Situational Awareness

Space Situational Awareness is proposed as a component of the EU space programme supporting "a global approach towards the main space hazards" and includes activities in the field of SST, Space Weather and NEOs. This SSA component aims:

- "to enhance SST capabilities at the EU level, reduce the risks of spacecraft collisions during all its operational phases from the launch to the decommissioning, survey uncontrolled re-entries of spacecraft or space debris in order to provide early warnings to mitigate damage to EU citizens and terrestrial infrastructure and seek to prevent proliferation of space debris;"
- "to monitor the relevant observational parameters related to space weather events" and
- "to establish and inventory of NEO European capacities, to network them with an aim of supporting the exchange of NEO data and information;"

The introduction of an SSA component within the EU space programme with a dedicated budget (corresponding to a share of the 500M€ allocated to GOVSATCOM/SSA) represents a substantial step towards a more ambitious and integrated capacity-building effort. This new SSA component will build on past activities in the field of SST (essentially on the EU SST support framework) and in the fields of Space Weather and NEOs (essentially on Space Weather prediction services for GNSS, H2020 grants for R&D in these fields and on a number of complementary activities).

With regards to SST, the cornerstone of SSA and main capacity pillar of the European approach to security in outer space, a few changes are proposed. The most noticeable change lies in the enlargement of the scope to encompass a financial support to the development of new sensors (i.e. today, the SST support framework should only "encourage" the development of new sensors and financial support should be addressed either nationally or through a European research and development programme). The SST component shall, now, "support the establishment, development and operation of a network of ground- and/or space-based sensors of the Member States, including sensors developed through ESA and EU sensors nationally operated". The notion of "EU sensors nationally operated" is further developed in the introduction of the

draft regulation: "in case new assets are financed by the programme, the Union should be co-owner of these assets with due consideration of various ownership and governance models". The possibility of co-owned sensors and of EU sensors operated by Member States are the main steps forward in the direction of a more prominent role of the EU in this field. European leadership could also be supported by the 7-year multi-annual plan mentioned in the draft regulation and which will probably have to be validated by the EC as well as by additional changes in the governance structure that could arise from future arrangements revision.

5.3.2 Proposed further developments in light of ESPI conclusions

In its current state, the proposed regulation does not introduce radical changes in the domain of security in outer space but still makes some noticeable steps towards the consolidation of a European programmatic approach. Although much is left to implementing arrangements to be established or revised accordingly by the different stakeholders, the regulation certainly provides for a more cohesive framework in a number of important areas.

Overall, the increasing importance awarded to security features of the EU space programme is striking. In this regard, the draft regulation fits well within the strategy framework set forth by the European Union in both space (Space Strategy for Europe) and security and defence sectors (Global Strategy for the European Union's Foreign and Security Policy, European Defence Action Plan) which call for further developments in the domain of security in outer space. However, if the current strategy clearly sets a number of key principles, it does not provide for concrete objectives. In this respect, setting up a comprehensive European policy in the domain of space security seems a necessary step to ensure smooth and controlled implementation.

Such policy should clarify the approach to a number of pressing issues.

- ***European ambitions and means***

First, the policy should establish clear, measurable, objectives to be achieved in the short-medium- and long-term. In particular, it should:

- clarify the notion of "European autonomy and freedom of action";
- set the required level of autonomy for Europe in these matters;
- set relevant standards applicable to civil and military systems respectively;
- and prioritise the associated developments of critical capabilities.

Accordingly, the overall effort to achieve these objectives should be translated into a broadly agreed roadmap allowing for budget planification and phased scheduling of developments. Actually, roadmapping of activities is necessary to avoid a "Go As You Pay" approach, which is not appropriate for a controlled deployment of capacities.

Considerations for the next MFF
• The introduction of a multiannual plan defining clear objectives for the SST component is an important feature of the proposal. Eventually, the European Commission shall endorse this plan as part of its responsibility over the security of the EU space programme. • The level of budget included in the EC proposal for the period 2021-2027 will increase available resources. However, additional funding from Horizon Europe (i.e. FP9) and other instruments, such as the European Defence Fund, will be essential to reach the level of funding necessary to progressively bridge the capability gap through the deployment of additional EU sensors. • Avoid unnecessary duplication of efforts and foster complementarity should be set as a core principle in order to optimise budget efficiency.

- ***Governance***

The governance scheme that has been set through the Consortium has allowed to accommodate the requirements of different communities by recreating the conditions of an intergovernmental model within the supranational framework of the EU. In such governance scheme the role of the European Commission is rather limited, even though it is the sole funding source and holds the responsibility over the security of the EU space programme.

In essence, the intergovernmental model is meant to mitigate two conflicting objectives:

- On one hand, leverage cooperation among the most motivated Member States to foster a regional approach for the sake of the protection of the European Union space assets,

- On the other hand, preserve national interests by safeguarding national sovereignty over capabilities development and control over SST systems and data.

The argument for an intergovernmental model also lies in the inherent dual nature of SST and in the discrepancy between Member States' capabilities and strategic interests across Europe. Indeed, the model promotes cooperation between capable states and use/upgrade of existing national capabilities (systems, know-how, facilities) resulting from prior investments of a handful of European countries to protect, first and foremost, their national/military space assets. This situation, which cannot be overlooked, is at the core of the governance debate which eventually boils down to the question of the weight of national concerns and interests against European added-value and to the sharing of responsibilities between Member States and the EU.

The draft regulation proposes to maintain this model, seeking enlargement of contributing Member States and progressive reinforcement of the EU role through co-ownership of new sensors, along with revision of the governance scheme and the introduction of a multi-annual plan monitoring key performance indicators. Although these are necessary steps forward on the way to a more prominent European leadership, such intergovernmental scheme might reach its limits with specific risks of:

- *Divergence of interests among stakeholders*, hindering the capacity to implement a coordinated policy in the field of security in outer space;
- *Duplication of efforts and reduced cost-effectiveness*, if motives to develop specific national capabilities surpasses the willingness (and readiness) to focus on distribution and complementarity across Europe.

To tackle these issues, and with the announced objective to involve more contributing states (including some with limited SST capacities or that may not operate satellites, but have a national space agency, or a security protocol of data processing and sharing), there is a pressing need to build further on EU added-value and reinforce European leadership, management and coordination. This might imply the introduction of some supranational provisions giving mandate to the EU in specific areas, in particular to negotiate international arrangements.

Interestingly, SST is not the only domain where EU Member States seek improved cooperation within the Union framework and new instruments such as the Permanent Structured Cooperation on Defense (PESCO) introduced in 2017 may provide new ways to better accommodate national interests and EU added-value.

Anyhow, getting close to the 2020 turning point, a reassessment of Member States concerns and of the role that the EU intends to play in the field of space security would be timely. Such discussion should take into account the substantial progress:

- of EU space programmes;
- of confidence-building among consortium partners;
- SST systems networking and service delivery;
- of the most appropriate institutional framework (including GSA, ESA, national agencies, etc…);
- and of the developing mandate and new instruments of the EU in Security & Defence.

Considerations for the next MFF

- Working on a clear identification of each parties' concerns and requirements would certainly support the identification of an appropriate solution accommodating national/European and military/civil perspectives.
- An enhanced role of the EU, with specific mandates, could be considered to reinforce European leadership, in particular on the international scene.
- A permanent structured cooperation for security in outer space, supported by the European Defence Fund and allowing future participation of third-states (e.g. United Kingdom, U.S.) could be considered.

- ***Exploitation***

Smooth and efficient exploitation of such sophisticated and critical systems requires a number of conditions:

- Adequate and stable budget properly assessed according to clearly identified operational objectives,
- Pooling of expertise available either at national or European institutional level. This raises in particular the question of the involvement of ESA, which has invested for its own needs in these matters and has gained substantial internal expertise. It remains to be seen how such capabilities could be exploited in a closely military-related environment and how it might intercact with the proposed enlargement of the GSA.

- ***Role of the private sector***

Another important consideration is the involvement of the private sector as a user and provider of SSA capabilities but also as an industry whose business and competitiveness is impacted by developments in the field of security (e.g. standards, regulations).

With the intensification of global space activity and an expected growth of the space economy, the provision of SSA data and services will likely become a new sizeable commercial market. This trend is marked by a growing number of SSA private providers. For example ExoAnalytic solutions, Rincon, Lockheed Martin, LeoLabs or ArianeGroup sell data produced by private sensors and Analytical Graphics, Boeing, Schafer Corp., Applied Defence Solutions use commercial SSA data to develop and sell value-added services to governmental and commercial operators.[199]

So far, and despite noticeable national developments (e.g. integration of ArianeGroup's GEOTracker service by France), the involvement of industry in space security matters does not seem to be perceived as a priority in Europe. In the meantime, the U.S. adopted a policy encouraging the involvement of private companies. The rationale behind this move is to:

- give way to a potentially promising commercial market,
- foster competitivess from supposedly more cost-effective economic agents,
- avoid diverting valuable public assets from their strategic missions.

Such approach supposes a strict delineation of the limits of the respective roles of public (military) actors focusing on strategic security-related activities and of the private actors providing services on a commercial basis in a number of less-sensitive areas.

From this perspective, on the European side, the elaboration of a comprehensive space-security policy is probably a prerequisite to a clear identification of the potential role of the European industry in the domain of security in outer space, taking into account the impacts of future developments (e.g. SSA services, security standards, STM…) on business.

However, advanced reflections should be initiated given the short-term risk of emergence of a *de facto* US industry monopoly on these services, or the creation of parallel SST data channels, making EU efforts redundant. From this standpoint, involving the private sector is at the crossroads of space security and industry competitiveness objectives.

Considerations for the next MFF

- In the short-term, a first step to favour a greater involvement of private actors could consist in the establishment of an enhanced dialogue with commercial stakeholders for example in the frame of the preparation of the SSA multiannual plan with the objective to:
  - map European private capabilities,
  - evaluate business opportunities and challenges in this domain and,
  - in general, assess the needs and views of private industry on potential future developments in this domain.

[199] Weeden, B. (2017). Space Situational Awareness *Fact Sheet.* Retrieved form Space World Foundation: https://swfound.org/media/205874/swf_ssa_fact_sheet.pdf

Annex

A.1 Risk Management Concepts

Risk management is the process of identifying, quantifying and prioritizing the risks that assets face. The following chart introduces a basic risk management model that brings together various security-related concepts and highlights the relationship between them:

The different concepts included in this model are defined more thoroughly below:

- *Threat* is defined as 'any circumstance or event with the potential to adversely impact operations or assets'. A threat can lead, purposefully or unintentionally, to the alteration or destruction of the asset and/or of its operations.
- *Vulnerability* is defined as 'a weakness in a system, security procedures, internal controls or implementation that could be exploited by a threat source'. Vulnerability is a characteristic of a system that must be identified, and then eliminated, limited or protected against.
- *Likelihood* is defined, here, as 'a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability'. This notion 'combines an estimate of the likelihood that the threat event will be initiated with an estimate of the likelihood of impact'.
- *Impact* is defined as the magnitude of harm that can be expected to result from the consequences of a threat exploiting a vulnerability.

Risk, as a combination of the above, is therefore defined as the likelihood of potential loss or damage resulting from the exposure of a system to a threat. This model, initially applied to information systems,[200] shows that risk, which is the essential variable that space security activities aim at mitigating, is the product of three specific factors: threat, vulnerability and consequence (or impact). Risk mitigation can therefore be performed through a variety of actions targeted toward threat reduction, vulnerabilities protection or impact mitigation. A preliminary step in risk management is risk assessment, which implies the identification of threats and vulnerabilities, together with the possible ensuing impact in case of damage.

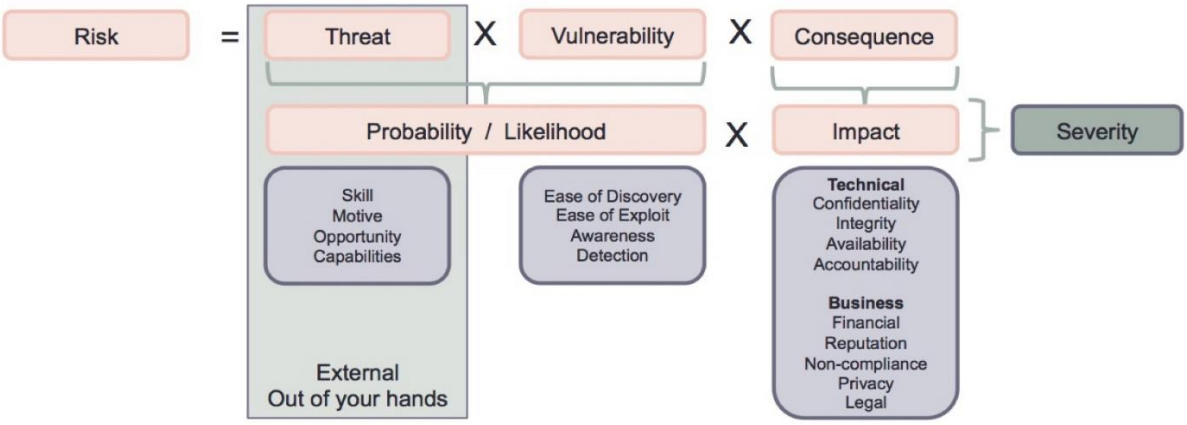

Figure 20: Security-related concepts and the relationship between them[201]

[200] National Institute of Standards and Technology (2012). *NIST Special Publication800-30*, *Revision 1*. Retrieved from NIST: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[201] Van Impe, K. (2017). *Simplifying Risk Management. Retrieved from Security Intelligence*. Retrieved from https://securityintelligence.com/simplifying-risk-management/

A.2 Space Security Concepts

Concept	Definition
Space Infrastructure	A network of spacecraft and ground stations interconnected by communication channels.
Ground Segment	The ground segment architecture of a satellite includes all the elements on the ground necessary to control the spacecraft and ensure its good functioning.
Uplink and Downlink	The satellite link is a radio link between a transmitting Earth station and a receiving Earth station through one satellite. Satellite link comprises one up-link and one down-link.
Space Segment	The space segment is composed of all the assets of the space architecture located in space, namely the satellites in orbit and any other spacecraft required to the completion of space operations.
Access to space capability	That segment is composed of the required launch infrastructure including spaceports – launch pad, integration facilities, and protection fences – but also the shipping facilities and vehicles.
Space Security	The secure and sustainable access to, and use of, space and freedom from space-based threats.
Security in Outer Space	The protection of space assets and systems against natural and man-made threats or risks, ensuring the sustainability of space activities.
Outer Space for Security	The use of space systems for security and defence purposes.
Security from Outer Space	The protection of human life and the Earth environment against natural threats and risks coming from space.
Main lines of action in Security in Outer Space	
Space Situational Awareness (SSA)	Means and measures to monitor, detect and inform about man-made and natural, intentional and unintentional, threats to operations in space.
Space Environment Protection and Preservation (SEPP)	Means and measures to reduce short- to long-term impacts of human activity in outer space and in particular impacts constituting a threat to operations in space. When taking a longer-term perspective, this concept is referred as 'Space sustainability'.
Space Infrastructure Security (SIS)	Means and measures to ensure space systems' availability, reliability, safety, integrity, confidentiality and maintainability and to prevent unwanted, be it intentional or unintentional, disruption of intended operations or access to system information.
Space Traffic Management (STM)	Operational and organisational concept encompassing systems assisting operators for safety of operations in orbit, practices ensuring the sustainability of the use of outer space (e.g. regulations, standards, procedures, protocols) and frameworks governing the exploitation of these systems and the implementation of these practices
Other risk management concepts	
Safety	The risk of a system of being harmed, damaged, destroyed or compromised. A system is safe when it is in the condition of not being harmed or the risk of a system of being harmed has been sufficiently mitigated.
Dependability	Ability of a system to deliver a service that can justifiably be trusted. Dependability is a measure of a system´s availability, reliability, safety, integrity and maintainability.
Resilience	The ability of a system to withstand the harmful impact of unexpected negative events, such as system failure, environmental challenges or adversary conditions, while mitigating damage and enabling the rapid recovery of original functionality. The notion itself can be divided in several sub-elements as such: Disaggregation, Distribution, Diversification, Protection, Proliferation, and Deception.

A.3 Threats to Space Infrastructure

Source: Schrogl, K.-U., Hays, P.L., Robinson, J., Moura, D., & Giannopapa, C. (Eds.) (2015). *Handbook of Space Security: Policies, Applications and Programs*. Vienna: Springer.

Threat	Type of threat (ESPI categories)	Hazard	Mitigation measures	Priority
Space segment				
Space debris	Passive man-made threat	Physical damage	TCBMs, hardening, shielding, SST	High
Space weather	Natural threat	Bugs, damage	SSA, software, EEE components, monitoring	High
Unknown space phenomena	Natural threat	Failure	Redundancy, hardening, resilience, R&D	Medium
KEW/ASAT	Active man-made threat	Partial/Total destruction	International law, ITAR, rules, TCBMs, deterrence	Very low
EMP (h alt nuc.)	Active man-made threat	Destruction, Van Allen	International law, ITAR, rules, TCBMs, deterrence	Low
DEW (energy)	Active man-made threat	Signal disturbance, mechanical destruction	Various	Medium
Laser-based ASAT	Active man-made threat	Sensors/mechanical damage	Classified	High
HPM ASAT (mcrw)	Active man-made threat	Sensors blinded, receivers and electr. Degr.	Self-protecting devices	Medium
EW (E-war)	Active man-made threat	Signal loss, satellite control loss	Various	Very high
Jammers	Active man-made threat	Radarsat/satcom incapacitation	Waveforms, nulling antennas, beamforming, jam	Very high
Cyberattacks	Active man-made threat	Transponder hijack, sat degr, info loss	Cryptography, secured software, process standard	Very high
Ground segment				
Natural disaster	Natural threat	Loss of com w/sat, ground segment disrupt	Redundancy, hardening, physical security measures	Medium
Physical attacks	Active man-made threat	Loss of com w/sat, ground segment	Redundancy, hardening, physical security measures	Medium
Sabotage	Active man-made threat	Loss of com w/sat, ground segment	Hardening	Medium
Cyberattacks	Active man-made threat	Denial of service, info stolen/comprised	Cryptography, authenf. Proced., integrity check	Very high
Back doors	Active man-made threat	Info compromised	Cryptography, authenf. Proced., integrity check	High
Data Links				
Interference	Passive man-made threat	Denial of service/comms/radar systems	Radio-frequency coord. at national/international, null ant, wvfrm	Medium
Jamming	-Active man-made threat	Denial of service/comms/radar systems	Radio-frequency coord. at national/international, null ant, wvfrm	High
Spoofing	-Active man-made threat	Wrong information provided	Cryptography, authenf. Proced., integrity check	Medium
Cyberattacks	-Active man-made threat	Denial of service	Cryptography, secure software	Very high
Interception	-Active man-made threat	Information compromised	Cryptography, specific waveforms	High
Technology/Industry capabilities – not addressed in this report				
Tech transfer	Not addressed in this report	3rd party space progr competition	Coordinate export control, space industrial policy	High
Supply shortage	Not addressed in this report	No system deployed	Space industrial policy	High
Lack of launch opportunities	Not addressed in this report	Satellite grounded	European launch policy, framework contracts	Medium
Loss of industry know-how	Not addressed in this report	No system deployed	Space industrial policy, space R&D programmes	Medium
Loss of spectrum and orbital resources	Not addressed in this report	No system deployed	Coordinated European position at European and ITU levels	High
Firmware, supply chain under stress	Not addressed in this report	Hack	Industrial policy	?

A.4 Projects Related to 'Security in Outer Space' Supported by EU R&D Support Frameworks

*The following list of projects is not exhaustive

Frame-work	Project title	Project coor-dinat.	Project cost (EUR)	EU contrib. (EUR)	Research Aim
2007-2008					
FP7-SPACE-2007-1	SOlar-TERrestrial Investigations and Archives (SOTERIA)[202]	Katholieke Universiteit Leuven, Belgium	5.161.155	3.922.966	Provide new and existing data from ground based and space-borne observations and models crucial for space weather forecasting
FP7-Adhoc-2007-13 (FP7-Space)	International Conference Space and Security 2010 (EUSPACE2010)[203]	Centro para el Desarollo Tecnologico Industrial (CDTI), Spain	154 600	150 000	Aim to facilitate a structured dialogue amongst all actors involved in security-related Space matters embedded in two main programmes: GMES and SSA
2010					
FP7-SPACE-2010-1	Reducing the Vulnerability of Space Systems (ReVus)[204]	Astrium SAS, France	3 191 059	1 971 271,75	Define and assess different satellite architecture solutions to minimise the impacts of small debris on satellites
FP7-SPACE-2010-1	Prediction, Protection & Reduction of OrbiTal Exposure to Collision Threats (P2-PROTECT)[205]	Onera, France	2 933 485,60	1 995 781	Calculate the risks that space debris poses for Europe's satellite infrastructure, and proposes new means to mitigate such risks
FP7-SPACE-2010-1	Propellant-less deorbiting of space debris by bare electrodynamic tethers[206]	Universidad Politécnica de Madrid, Spain	2 337 317,40	1 772 801	Developing an efficient deorbit system for future spacecraft
FP7-SPACE-2010-1	Alignment of Capability and Capacity for the Objective of Reducing Debris (ACCORD)[207]	University of Southampton, UK	560 744,60	425 114,21	Provide a coherent and rigorous mechanism for communicating the efficacy of current debris mitigation practices and opportunities for strengthening European capability
FP7-SPACE-2010-1	Support to Precursor SSA Services (SPA)[208]	European Union Satellite Centre, Spain	735 600	500 000	Studies the tracking of space objects, preparing the way for a European system for SSA
FP7-SPACE-2010-1	Small debris removal by laser illumination and complementary technology (CLEANSPACE)[209]	CILAS , Compagnie Industrielle des Lasers, France	2 882 883,80	1 976 440	Develop a concept allowing for removal of small-sized space waste
FP7-SPACE-2010-1	De-Orbiting of Satellites using Solar	University of Surrey, United Kingdom	2 830 728,40	1 997 342,75	Develop and tests a novel device for de-orbiting of

[202] Project ID: 218816
[203] Project ID: 262587
[204] Project ID: 262156
[205] Project ID: 262820
[206] Project ID: 262972
[207] Project ID: 262824
[208] Project ID: 262930
[209] Project ID: 263044

	Sails (DEORBITSAIL)[210]				Low Earth Orbit space-craft
FP7-SPACE-2010-1	Advanced Forecast For Ensuring Communications Through Space (AFFECTS)[211]	University of Göttingen, Germany	2 550 245	1 999 893	Provide advanced early space weather warning to protect communication systems
FP7-SPACE-2010-1	Advanced Thermosphere Modelling for Orbit Prediction (ATMOP)[212]	DEIMOS Space S.L.U., Spain	2 217 243,16	1 563 980,36	Creation of a new thermosphere model, enabling more precise space weather forecasts
FP7-SPACE-2010-1	Coronal Mass Ejections and Solar Energetic Particles: forecasting the space weather impact (COMESEP)[213]	Institut d'Aéronomie Spatiale de Belgique, Belgium	2 518 021,40	1 798 718	Develop new tools to mitigate the negative impacts of geomagnetic storms and solar energetic particle events
FP7-SPACE-2010-1	European Risk from Geomagnetically Induced Currents (EURISGIC)[214]	Finnish Meteorological Institute, Finland	1 561 175,40	1 056 184	Develop 30-60 minute forecast warnings of geomagnetically induced currents (GIC) threatening critical infrastructure
FP7-SPACE-2010-1	Protecting space assets from high energy particles by developing European dynamic modelling and forecasting capabilities (SPACECAST)[215]	British Antarctic Survey, United Kingdom	2 539 991,31	1 965 071,25	Deliver a European space weather forecasting capability
FP7-SPACE-2010-1	Space Weather Integrated Forecasting Framework (SWIFF)[216]	Katholieke Universiteit Leuven, Belgium	1 991 474,08	1 559 005,56	Develop a physics-based simulation basis for space of the space weather forecasting
FP7-SPACE-2010-1	A new, ground based data-assimilative modelling of Earth's plasmasphere – a critical contribution to Radiation Belt modelling for Space Weather purposes (PLASMON)[217]	Eötvös Loránd University, Hungary	2 626 262,80	1 972 049,75	Measure plasmaspheric electron and mass densities to monitor the changing composition of the plasmasphere
FP7-SPACE-2010-1	Data Services and Analysis Tools for Solar Energetic Particle Events and Related Electromagnetic Emissions (SEPServer)[218]	Helsingin yliopisto, Finland	2 484 125,80	1 932 172,70	Establish an integrated web-based interface to solar energetic particle data and analysis tools
2011					
FP7-SPACE-2011-1	Solar and Heliospheric Collisionless Kinetics: Enabling Data Analysis of the	Queen Mary and Westfield College,	2 602 739,60	1 998 104	Improve the knowledge of the Sun to Earth plasma environment

[210] Project ID: 263248
[211] Project ID: 263506
[212] Project ID: 261948
[213] Project ID: 263252
[214] Project ID: 260330
[215] Project ID: 262468
[216] Project ID: 263340
[217] Project ID: 263218
[218] Project ID: 262773

	Sun to Earth Plasma System with Kinetic Modelling (SHOCK)[219]	University of London, United Kingdom			using kinetic computer simulations
FP7-SPACE-2011-1	Monitoring, Analysing and Assessing Radiation Belt Loss and Energization (MAARBLE)[220]	National Observatory of Athens, Greece	2 845 504,37	1 995 042,90	Aim at shedding light on the ways the dynamic evolution of the Earth's radiation belt is influenced by ultra low frequency electromagnetic waves in geospace
FP7-PEOPLE-2011-IEF	Space Debris Evolution, Collision risk, and Mitigation (SpaceDebEMC)[221]	Politecnico di Milano, Italy	185 763,60	185 763,60	Investigate the orbital dynamics of space debris through semi-analytical models of their motion under the effect of orbit perturbations
2012					
FP7-SPACE-2012-1	First European Comprehensive SOLar Irradiance Data exploitation (SOLID)[222]	Physikalisch-Meteorologisches Observatorium Davos / World Radiation Center, Davos, Switzerland	2 579 598,40	1 994 373,60	Provide a complete and consistent time series of solar spectral radiation incident on the Earth's atmosphere
FP7-SPACE-2012-1	Solar system plasma Turbulence: Observations, inteRmittency and Multifractals (STORM)□[223]	Belgian Institute for Space Aeronomy, Belgium	2 655 900	1 998 200	Develop and apply a full package of advanced analysis methods on plasma data
FP7-SPACE-2012-1	Support for the development of a European SSA capability (STEP)[224]	European Union Satellite Centre, Spain	746 772	500 000	Support action contributes from a technical perspective to the development of a Data Policy for a future European SSA capability
FP7-PEOPLE-2012-ITN	Stardust-The Asteroid and Space Debris Network (STARDUST)[225]	University of Strathclyde, UK	4 049 908,72	4 049 908,72	Develop new tools to better understand the motion and orbit of space objects
2013					
FP7-SPACE-2013-1	Improving Low Earth Orbit Security With Enhanced Electric Propulsion (LEOSWEEP)[226]	SENER Ingeneria y Sistemas S.A, Spain	2 905 380,41	1 999 447	Demonstrate technological feasibility of a first active removal mission to "kick-start" large-scale active debris removal activities
FP7-SPACE-2013-1	A Low Cost Active Debris Removal Demonstration Mission (REMOVEDEBRIS) [227]	University of Surrey, UK	15 321 258,79	6 999 867	Aim to demonstrate key technologies for ADR three main domains by performing in-orbit demonstrations representative of an ADR mission
FP7-SPACE-2013-1	Modelling space weather events and mitigating their effects on	Natural Environment Research Council, UK	2 544 144,52	1 981 301,49	Assess the impact of space weather and develop mitigation strategies

[219] Project ID: 284515
[220] Project ID: 284520
[221] Project ID: 302270
[222] Project ID: 313188
[223] Project ID: 313038
[224] Project ID: 312249
[225] Project ID: 317185
[226] Project ID: 607457
[227] Project ID: 607099

	satellites (SPACESTORM)[228]				
FP7-PEOPLE-2013-IEF	Merging lie perturbation theory and Taylor Differential algebra to address space debris challenges (HOPT)[229]	Universitad de la Rioja, Spain	230 036,60	230 036,60	Merge lie perturbation theory and DA and TM techniques with the goal of applying the resulting methodology to practical problems in SSA
2014					
H2020-PROTEC-2014	Prediction of Geospace Radiation Environment and solar wind parameters (PROGRESS)[230]	University of Sheffield, UK	2 359 235	2 358 230,50	Develop an accurate and reliable forecast system for space weather
H2020-PROTEC-2014	High Energy Solar Particle Events foRecastIng and Analysis (HESPERIA)[231]	National Observatory of Athens, Greece	1 208 956,25	1 101 456,25	Produce two novel operational forecasting tools based upon proven concepts (UMASEP, REleASE)
H2020-PROTEC-2014	Flare Likelihood And Region Eruption Forecasting (FLARECAST)[232]	Academy of Athens, Greece	2 416 651,25	2 416 651,25	Develop an advanced flare prediction system that is based on automatically extracted physical properties of the active region
H2020-SMEINST-2-2014	First European System for Active Debris Removal with Nets (ADR1EN)[233]	STAM SRL, Italy	1 730 000	1 211 000	Aim to validate by testing and qualify for space a scaled-up demonstrator of ADR1EN
2015					
H2020-PROTEC-2015	Technology for Self Removal of Spacecraft (TeSeR)[234]	Airbus Defense and Space GMBH, Germany	2 840 490,75	2 840 490,75	Propose a universal post mission disposal module to be carried into orbit by any S/C to ensure its proper disposal after ending its service lifetime
H2020-PROTEC-2015	Revolutionary Design of Spacecraft through Holistic Integration of Future Technologies (ReDSHIFT)[235]	Consiglio Nazionale della Ricerche, Italy	3 230 295	3 230 294	Provide a complete debris mitigation analysis of a mission, using existing debris evolution models and lessons learned from theoretical and experimental work
2016-2017					
H2020-COMPET-2017	Space Weather Atmosphere Model and Indices (SWAMI)[236]	DEIMOS Space Sociedad Limitada Unipersonal, Spain	1 198 363,75	1 198 363,75	Develop a unique new whole atmosphere model, by extending and blending the Unified Model (UM), and the Drag Temperature Model (DTM)

[228] Project ID: 606716
[229] Project ID: 627111
[230] Project ID: 637302
[231] Project ID: 637324
[232] Project ID: 640216
[233] Project ID: 666758
[234] Project ID: 687295
[235] Project ID: 687500
[236] Project ID: 776287

A.5 Overview of European Actions in the Field of Space Security

The following table, based on the ESPI security in outer space matrix, provides a list of European actions and measures related to 'Security in Outer Space' organised by domain and field of action. The list is intended to be illustrative rather than comprehensive:

		Field of action		
		Capacity-building programmes *Develop and deploy operational capacities to ensure security in outer space*	**Legal and regulatory regimes** *Establish a reference framework to conduct space activities in compliance with space security requirements*	**Diplomacy and cooperation frameworks** *Harmonise and coordinate space security efforts among stakeholders*
Security in Outer Space subdomain	**Space Situational Awareness (SSA)** *Monitor space environment threats*	Examples: • ESA SSA programme (SST, SWE and NEO components) • EU FP7 and H2020 grants (research into space-weather events, security of space assets from in-orbit collisions) • EU SST Support Framework (sensor, processing and service delivery functions) • Member state SST systems development and upgrade	Examples: • Compliance with space objects registration obligations and procedures	Examples: • SSA data sharing agreements
	Space Environment Protection and Preservation (SEPP) *Keep the space environment safe to operate*	Examples: • ESA CleanSpace initiative (EcoDesign, CleanSat and eDeorbit components) • ECSS standards – Branch U (space sustainability) • EU FP7 and H2020 grants (research into secure and safe space environment)	Examples: • National space legislation in European Member States (e.g. end-of-life obligations)	Examples: • ESA and national space agencies contribution to IADC and vote on space debris mitigation guidelines • European Union proposal for an International Code of Conduct for Outer Space Activities • Contribution to UNCOPUOS and Conference on Disarmament initiatives (LTS guidelines, PAROS, GGE, PORBOS) • Space debris mitigation guidelines endorsement
	Space Infrastructure Security (SIS) *Protect the space infrastructure from threats*	Examples: • EU FP7 and H2020 grants (research into reducing the vulnerability of space assets, security of space assets from in-orbit collisions) • Development of technologies, standards and procedures by a range of stakeholders (ESA, national space agencies, commercial operators, industry and non-space governmental actors)	Examples: • European space programme security rules and procedures (e.g. independent Security Accreditation, Galileo Security Monitoring Centre) • Supply chain control processes (e.g. export/import rules, testing procedures)	Examples: • Collision avoidance procedures and coordination with foreign agencies and operators

A.6 List of Interviewees

Name	Organisation	
Asbeck, Frank	European External Action Service (EEAS)	Former Principal Advisor for Space and Security Policy
Bobrinsky, Nicolas	European Space Agency (ESA)	SSA Programme Manager
Braun, Gerald	German Space Agency (DLR)	Head of SSA Department
Buenneke, Richard H.	U.S. Department of State	Senior Space Policy Advisor
Delsaux, Pierre	European Commission (EC)	Deputy Director General at DG Internal Market, Industry, Entrepreneurship and SMEs
Dickinson, Mark	Space Data Association (SDA)	Chairman
East, Alastair	UK Space Agency (UKSA)	UKSA Delegate to the EU SST Consortium
Faucher, Pascal	EU SST Consortium	Chairman
Gerard, Brachet	GGE Report	Space Policy Consultant
Legai, Pascal	European Union Satellite Centre (SatCen)	Director
Pasco, Xavier	Fondation Pour la Recherche Stratégique (FRS)	Director
Peldszus, Regina	German Space Agency (DLR)	DLR Delegate to the EU SST Consortium
Pellegrino, Massimo	United Nations Institute for Disarmament (UNIDIR)	Research Fellow
Portelli, Claudio	Italian Space Agency (ASI)	Dirigente Tecnologo
Rivasseau, Francois	European External Action Service (EEAS)	Director for Security and Space Policy
Robinson, Jana	Prague Security Studies Institute (PSSI)	Space Security Programme Manager
Weissenberg, Paul	European GNSS Agency (GSA)	Senior Advisor to the Executive Director

List of Acronyms

Acronym	Explanation
A	
ACCORD	Alignment of Capability and Capacity for the Objective of Reducing Debris
ADR	Active Debris Removal
AFFECTS	Advanced Forecast For Ensuring Communications Through Space AFFECTS
APT	Advanced Persistent Threat
ARMOR	Advanced Radar for Meteorological and Operational Research
ASI	Agenzia Spaziale Italiana (Italian Space Agency)
ATMOP	Advanced Thermosphere Modelling for Orbit Prediction
C	
CAMRa	Chilbolton Advanced Meteorological Radar
CD	Conference on Disarmament
CDAOA	Commandement de la Défense Aérienne et des Opérations Aériennes
CFPS	Common Foreign & Security Policy
CNES	Centre Nationale D'Etudes Spatiales (French Space Agency)
ComSpOC	Commercial Space Operations Center
UN COPUOS	United Nations Committee on Peaceful Uses of Outer Space
COSPAR	Committee on Space Research
CSDP	Common Security and Defence Policy
CSMs	Conjunction Summary Messages
D	
DEW	Direct Energy Weapons
DG GROW	Directorate-General for Internal Market, Industry, Entrepreneurship, and SMEs
DLR	Deutsches Zentrum für Luft- und Raumfahrt (German Space Agency)
U.S. DoC	United States Department of Commerce
U.S, DoD	United States Department of Defense
E	
EC	European Commission
ECSS	European Cooperation for Space Standardization
EDA	European Defence Agency
EEAS	European External Action Services
EGNOS	The European Geostationary Navigation Overlay Service
ESA	European Space Agency

Acronym	Explanation
EU	European Union
EU SST	European Union support framework for Space Surveillance & Tracking
F	
FAA	Federal Aviation Administration
G	
GDP	Gross Domestic product
GEO	Geostationary Orbit
GGE	Group of Governmental Experts
GRAVES	Grand Réseau Adapté à la Veille Spatiale
GSMC	Galileo Security Monitoring Centre
GTRA	GNSS Threat Response Architecture
GVA	Gross Value Added
H	
H2020	Horizon 2020
HEO	Highly Eccentric Earth Orbit
I	
IADC	Inter-Agency Space Debris Coordination Committee
ICoC	International Code of Conduct for Outer Space Activities
ICT	Information and Communication Technologies
ITU	International Telecommunications Union
JFSCC	Joint Force Space Component
JSpOC	Joint Space Operations Center
L	
LEO	Low Earth Orbit
M	
MEO	Medium Earth Orbit
MFF	Multi-annual Financial Framework of the European Union
N	
NASA	National Aeronautics and Space Administration
NEO	Near Earth Objects
NFP	No First Placement of Weapons in Outer Space
O	
OSCE	Organization For Security and Co-operation
P	
PAROS	Prevention of an Arms Race in Outer Space
PNT	Positioning, Navigation and Timing
PORBOS	Promotion of initiatives such as the Principles of Responsible Behaviour for Outer Space
PPWT	Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects

Acronym	Explanation
PRS	Public Regulated Service
PSSI	Prague Security Studies Institute
QoS	Quality of Service
R	
RFI	Radio Frequency Interferences
RFW	Radio Frequency Weapons
RPO	Rendez-vous and Proximity Operations
S	
SAB	Security Accreditation Board
SatCen	European Union Satellite Centre
SDA	Space Data Association
SDC	Space Data Centre
SEPP	Space Environment Protection and Preservation
SES	Société Européenne des Satellites
SIS	Space Infrastructure Security
SPCS	Space Control Squadron
SPOC	Système Probatoire d'Observation du Ciel
SSA	Space Situational Awareness
SSN	U.S. Space Surveillance Network
SST	Space Surveillance and Tracking
STM	Space Traffic Management
SWAMI	Space Weather Atmosphere Model and Indices
SWIFF	Space Weather Integrated Forecasting Framework
T	
TAROT	Télescope à Action Rapide pour les Objets Transitoires
TCBMs	Transparency and Confidence-Building Measures in Outer Space Activities
TeSeR	Technology for Self Removal of Spacecraft
TEU	Treaty on European Union
TIRA	Tracking and Imaging Radar
TLE	Two-Line Element sets
TT&C	Telemetry, Tracking and Control
U	
UKSA	United Kingdom Space Agency
ULS	Up-Link Stations
UNIDIR	United Nations Institute for Disarmament Research
UNOOSA	United Nations Office for Outer Space Affairs
USSTRATCOM	U.S. Strategic Command
W	
WG-LTS	Working Group on the Long-term Sustainability of Space Activities

About ESPI

The European Space Policy Institute (ESPI) is an association ruled by Austrian Law, based in Vienna, funded at its inception (2003) by the Austrian Space Agency and ESA, and now supported by 17 members that include European national space agencies, the European Commission, and main European space services companies and manufacturers.

The Institute provides decision-makers with an informed view on mid-to-long-term issues relevant to Europe's space activities. In this context, ESPI acts as an independent platform for developing positions and strategies.

ESPI fulfils its objectives through various multidisciplinary research activities leading to the publication of books, reports, papers, articles, executive briefs, proceedings and position papers, and to the organisation of conferences and events including the annual ESPI Autumn Conference. Located in the heart of Vienna, the Institute has developed a privileged relationship with the United Nations Office for Outer Space Affairs and with a network of researchers and experts in Europe and across the globe.

More information on ESPI is available on our website: www.espi.or.at

About the Authors

This report was prepared with contributions from the following ESPI researchers:

(in alphabetical order)

- Sebastien Moranta, Coordinator of Studies
- Giulia Pavesi, Research Intern
- Lisa Perrichon, Research Intern
- Serge Plattard, Senior Resident Fellow
- Martin Sarret, Research Fellow

Publicly available data and information were completed with stakeholders and expert interviews. The list of interviewees is provided in Annex to this report.

ESPI is grateful to the many stakeholders that accepted to be interviewed and provided substantial information for this report.

Mission Statement of ESPI

The European Space Policy Institute (ESPI) provides decision-makers with an informed view on mid- to long-term issues relevant to Europe's space activities. In this context, ESPI acts as an independent platform for developing positions and strategies.

www.espi.or.at