ESPI
European Space Policy Institute

In collaboration with the
SPACE POLICY INSTITUTE
ELLIOTT SCHOOL OF INTERNATIONAL AFFAIRS

Security in Outer Space: Perspectives on Transatlantic Relations

Report 66
October 2018

Federal Ministry
Republic of Austria
Transport, Innovation
and Technology

Short title: ESPI Report 66
ISSN: 2218-0931 (print), 2076-6688 (online)
Published in October 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

In the sixty years since the launch of the first satellite in 1957, the global space economy has grown tremendously.[1] Space-based services now bring substantial socio-economic benefits to end-users, across numerous strategic domains and economic sectors.[2] Simultaneously, the increasingly pervasive use of space-based services by governments, businesses and consumers has resulted in a growing dependence of society and economy on space infrastructure. For example, it was recently estimated that a large share of the European Union GDP depends on space assets, and that an incapacitation of these assets would lead to a significant economic loss.[3] Similar proportional impacts could occur in other countries. In the future, the development of new space-based services, in synergy with terrestrial technologies (e.g. 5G networks, precision agriculture, smart energy grids, autonomous vehicles), will increase the benefits of space assets but also deepen the dependence of governments, businesses and consumers on these assets.

In Europe, the significant progress made by Galileo, EGNOS and Copernicus programmes and the introduction of new initiatives in the field of GOVSATCOM have further emphasised the importance of ensuring that all conditions for the delivery of operational space-based services conforming to user needs are met. This is a prerequisite to fostering the uptake of space services and, consequently, maximising the benefits of the space infrastructure. This is also a key area of space policy development in light of the growing dependence of the European economy and society on space assets, including critical infrastructure such as telecommunications, energy and transport. The conditions to ensure an appropriate quality of service include:

- A proven or certified level of performance;
- Long-term availability of services;
- A secure service that can justifiably be trusted.

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. The last encompasses multiple and transverse aspects covering:

- Access to space to ensure an autonomous capacity to deploy space systems safely;
- The integrity of the space segment, including all systems in orbit;
- The ground segment that includes stations and equipment for the operation and delivery of services;
- Downlinks and uplinks used to operate the space system and receive its data.

Each of these components is vulnerable to a range of security concerns. Experts have routinely cautioned governments and space businesses that space is increasingly vulnerable, posing an intensifying challenge to guaranteeing a safe, secure and sustainable environment to deploy, operate and exploit space assets. Rising challenges to the security of the space infrastructure are numerous and include:

- Passive man-made hazards, in particular the proliferation of space debris that jeopardizes the sustainability of space activities and threatens unintentional jamming of signals and equipment;
- Active man-made threats such as Anti-Satellite capabilities and cyber-attacks;
- Natural hazards such as natural debris and space weather events such as geomagnetic storms, solar radiation storms, and disturbances of the ionosphere.

The deteriorating security situation has been acknowledged by the European Union, which made “the protection and resilience of critical European space infrastructure” a flagship objective of the Space Strategy for Europe

1 Space Foundation (2018). The Space Report 2018: The Authoritative Guide to Global Space Activity.
2 European Commission (2017). Dependence of the European Economy on Space Infrastructures: Potential Impacts of Space Assets Loss, (March 2017).
3 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

adopted in October 2016.[4] The strategy underlines the objectives of the EU 1) to enhance the security of its space programme, 2) to ensure the protection and resilience of critical European space infrastructure, in particular through the development of Space Situational Awareness (SSA) capabilities, and 3) to reinforce synergies between civil and security space activities. For these objectives, the European Union stresses the importance of cooperation, first at European level with ESA, EUMETSAT and Member States, but also at international level, in particular with the United States (U.S.). The importance given to space security and international cooperation in this field is shared by the European Union External Actions Services (EEAS) and is addressed in the Global Strategy for the European Union's Foreign and Security Policy, and in the European Defence Action Plan. These elements were again addressed in the draft regulation for the Space Programme of the European Union published in June 2018 by the European Commission in preparation for the next Multiannual Financial Framework (MFF) 2021–2027.[5] This document proposes several provisions in line with the existing strategic framework and recalls that "[Space Situational Awareness] should have regard to cooperation with international partners, in particular the United States of America".[6]

Across the Atlantic, in the United States, space has always had a prominent defence and national security dimension, and securing space assets has long been a strategic priority, as witnessed by the development of an ambitious Space Situational Awareness (SSA) programme by the U.S. Department of Defense (DoD). This programme relies on an extensive and advanced network of surveillance sensors[7] including space and ground-based radars and optical telescopes operated by military and civilian entities, together making up the U.S. Space Surveillance Network (SSN). The outstanding tracking capabilities of this network are expected to be further improved by the end of 2018[8] as part of the U.S. Space Fence programme.[9] Noticeably, the United States has adopted a model of global SSA cooperation with close to 100 unclassified SSA Sharing Agreements with commercial and international partners,[10] which also supports U.S. capabilities by improving the quality and quantity of SSA information. More recently, a major development in the U.S approach to security in outer space was the adoption of Space Policy Directive 3 (SPD-3), which establishes the first "approach to Space Traffic Management (STM) that addresses current and future operational risks."[11] The policy also announced that the U.S. Department of Commerce (DoC) would be responsible for relations with commercial and international partners for STM and SSA, shifting some of the responsibilities now handled by U.S. DoD.

Recent developments in space security in Europe and the United States have reshuffled the cards at strategic, policy and operational levels. In this context, an examination of the new state of affairs on each side of the Atlantic, and of mutual transatlantic relations seems timely. More specifically, this study aims to provide elements of an answer to the following questions:

- What is the state of affairs in space security in Europe, the United States, and in transatlantic relations?
- How might recent developments impact transatlantic relations in the short- to long-term?
- How can partners revisit or reinforce cooperation frameworks for mutual benefit?

4 European Commission (2016). 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
5 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
6 European Commission (2018). 'Establishing the space programme of the Union and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013, (EU) No 377/2014 and Decision 541/2014/EU', COM(2018) 447 final (June 6, 2018).
7 Space Traffic Management: Towards a Roadmap for implementation, IAA Cosmic Study (2017) 80.
8 For completeness, it should be noted that the current Space Fence project is to replace the previous Air Force Space Surveillance System, one of the SSN components active from 2008 to 2013.
9 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
10 U.S. Strategic Command and Norway sign agreement to share space services, USSTRATCOM Public Affairs, April 2017 http://www.stratcom.mil/Media/News/News-Article-View/Article/1142970/us-strategic-command-norway-sign-agreement-to-share-space-services-data/
11 Space Policy Directive-3, National Space Traffic Management Policy, (June 18, 2018).

1.2 Objectives of the Study

The overarching objective of the research is to raise awareness of the key stakes in transatlantic relations in the field of space security by providing useful perspectives on recent and potential future developments in this domain. Specifically, the study aims to achieve the following:

- Review the U.S. and European approaches to address challenges to space infrastructure security, including:
  - Strategic and policy rationales, key priorities and objectives;
  - Activities and capabilities in the field of security in outer space;
- Investigate past and current transatlantic relations in the field of space security and analyse the conditions to reinforce cooperation in this domain;
- Examine the potential implications of ongoing policy developments on future transatlantic relations in space security.

1.3 Research Scope and Key Concepts

The broad concept of space security can be delineated in three conceptual dimensions as shown in Table 1:[12]

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

In this report, 'Space Security' is understood primarily as 'Security in Outer Space' as defined in Table 1. Given the strong interrelation between the three dimensions of space security, 'Outer Space for Security' and 'Security from Outer Space', may be addressed when relevant in this study.

'Security in Outer Space' itself encompasses three areas of action that are investigated in this report and that correspond to three core objectives: 1) monitor the space environment, 2) mitigate threats to space infrastructure, and 3) reduce vulnerability of space infrastructure.

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

Measures directly targeting the source of the threats, such as actions against cybercrime or signal jamming, are not included this report.

Measures that are external to the space sector, such as actions against cybercrime, disarmament policies, and radio spectrum management are not addressed here. By the same token, broader security and defence matters such as strategic stability in outer space, deterrence and space superiority, although exceedingly central in the posture of many space powers, will not be directly covered by the report.

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 a space segment, a ground segment, a user segment, and down-links and up-links to interface between these segments. As the present report focuses on 'Security in Outer Space', the analysis addresses predominantly security challenges to the 'space segment' and, whenever relevant, to the down-link and up-link data. However, the report does not address security challenges specific to ground and user segments, such as Earth natural hazards, physical attacks on facilities, or eavesdropping.

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

The analysis focuses predominantly on challenges to space infrastructure in operation (up to system disposal) but also addresses, whenever relevant, security challenges during other stages of the infrastructure lifecycle including, in particular, challenges related to security-by-design and supply chain security. These challenges are addressed as part of the Space Infrastructure Security (SIS) component:

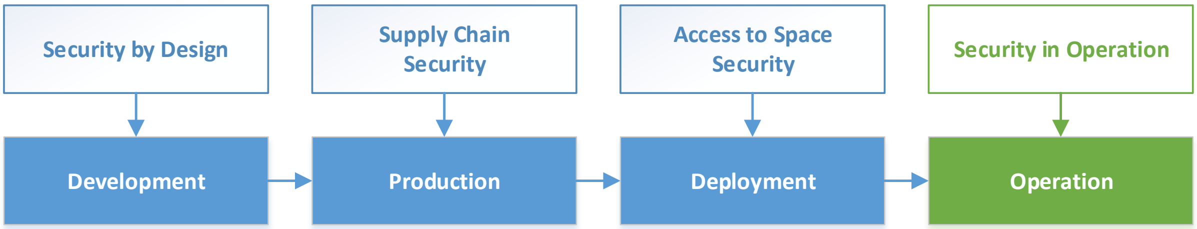

Figure 1: Security challenges throughout the space infrastructure lifecycle

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.

1.4 Methodology

With the objective of providing a common understanding of space security challenges and analysing a potential way forward in transatlantic relations in security in outer space, the study aims to provide:

- An assessment of common space security challenges;
- A common understanding of each partners' priorities;
- Insights on the respective approaches to the issue;
- A sound evaluation of drivers and obstacles to cooperation.

To this effect, the research has followed a methodology based on: a comparative analysis of the European and American approaches to security in outer space; a review of current transatlantic relations in this domain; and the identification of drivers and barriers to a reinforced framework. The research has been supported by an extensive literature review, face-to-face interviews of key stakeholders in Europe and in the United States, and a review of the study's progress by a board of recognised international experts. An overview of the general methodology is provided below:

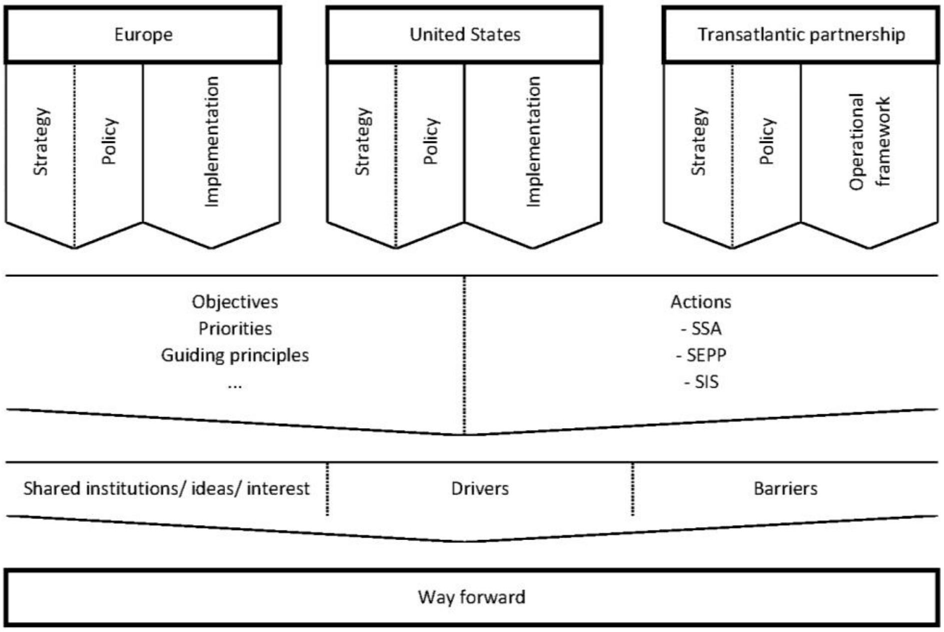

Figure 2: General approach to the problematic

The review of European and U.S. approaches aimed to disentangle the strategy and policy frameworks adopted in this field in Europe and in the United States, in order to identify elements that influence each partner's attitude to cooperation/coordination. The analysis is based on the collection and review of relevant strategy (i.e. general long-term direction), and policy (i.e. statement of position directing responses or actions) documents, upon which activities and decisions are based.

The analysis of strategy and policy frameworks was complemented with a comprehensive overview of implementing activities across the three areas of security in outer space (i.e. Space Situational Awareness, Space Environment Protection and Preservation, Space Infrastructure Security). This overview takes into account three fields of action:

- Capacity-building programmes;
- Legal and regulatory regimes;
- Diplomatic and cooperation frameworks.

For this overview, the study followed the categorization matrix prepared by ESPI for a previous report in order to organise actions and measures related to security in outer space by domain and field of action as shown in the figure below:

Security in Outer Space subdomain	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*
Space Situational Awareness (SSA) *Monitor space environment threats*	Examples: • SST capabilities development • Space weather models development • SSA services delivery	Examples: • Space objects registration obligations and procedures • SSA data policy	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: • Curative 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: • Space Debris Mitigation Guidelines • Long-term sustainability guidelines • International Code of Conduct proposal
Space Infrastructure Security (SIS) *Protect the space infrastructure from threats*	Examples: • Security enhancing technologies development (e.g. secure links) • Resilient system architectures (e.g. fragmented systems)	Examples: • Space programme security rules and procedures • Security and safety standards • Supply chain control processes (e.g. export/import rules, testing procedures)	Examples: • Collision avoidance procedures and coordination • Deterrence through hosted payloads on allies' satellites

Table 2: Examples of 'Security in Outer Space' measures by field and domain category

The analysis of European and U.S. approaches was completed with a review of current transatlantic relations and cooperation frameworks. The analysis then focused on the assessment of space security transatlantic collaboration with the overarching aim of supporting the identification of key areas of reinforced cooperation/coordination. This assessment was performed through:

- An analysis of the integration of transatlantic cooperation in respective approaches to space security;
- A review of the achievements of, and limits to, current transatlantic cooperation frameworks;
- The identification and analysis of drivers of and barriers to reinforced transatlantic cooperation at the strategic, political and operational levels.

For this last point, an assessment of the way forward was conducted through a significant number of interviews both in Europe and in the United States. The information collected from the interviewees listed below helped shape the findings and later recommendations by identifying potential areas for reinforced cooperation. The results of the previous analytical work and of the discussions with stakeholders across the Atlantic paved the way for the preparation of main takeaways in the context of space security from a transatlantic perspective, and the identification of key areas and potential options for transatlantic cooperation development in the field. The third part of the analysis was therefore to provide recommendations regarding areas of cooperation, and models to enhance bilateral coordination, to policy makers and interested stakeholders in the field of space security.

2. The United States: Consolidating Leadership for National Security

2.1 Legacy of Successive U.S. Space Policies

The current U.S. strategy for security in outer space largely builds on the legacy of previous administrations. Hence, understanding the key tenets and objectives of the incumbent administration's approach to space security first requires an assessment of the policy developments made under the presidencies of George W. Bush and Barack Obama.

The United States entered the 21st century with a rising dependence on space systems, with GPS, alone, enabling 16 of the 18 Critical Infrastructure and Key Resources (CIKR).[13] As a result, the posture of the G.W. Bush administration reflected the fact that space had become an even more important component of U.S. economic security and national security. President G.W. Bush envisioned that the United States would establish "space leadership and ensure that space capabilities are available in time to further U.S. national security, homeland security, and foreign policy objectives".[14] The events of 9/11 and the Second Gulf War further deepened U.S. military reliance on space systems and led to a departure from the approach of the previous administration towards a more assertive stance. More specifically, the military operational and tactical advantages offered by space promoted the idea that the United States ought to take control of the 'ultimate high-ground', by furthering the country's ability to use space for its own purposes while denying it to potential adversaries.[15]

With this sentiment, the administration established the National Space Policy (2006), an overarching national policy that governed the conduct of U.S. space activities and envisioned space activities to strengthen and maintain national security.[16] The document implied the objective of 'dominance and control' in the space domain by prioritising U.S. defence and security above all else. Equally important, the document underscored a patent unilateral attitude to space security issues and characterised the role of U.S. space diplomacy merely in terms of persuading other nations to support U.S. policy.[17]

The year 2007 brought two issues to the top of the security agenda for space: the challenges posed by anti-satellite (ASAT) weapons, and orbital debris. In response to the Chinese ASAT test of 2007, the U.S. government adopted an even more aggressive approach to space security, drafting documents that envisioned a restructuring of military commands and increased funding for research and development of space-relevant technologies, including counter-space developments, improved tracking of space objects and lightweight sensors.

While U.S. leadership in space remained the core focus of the Obama administration (2009-2017), from 2009 the U.S. government shifted away from the unilateral stance of the Bush administration and took a more internationally focused approach, promoting U.S. space security through cooperation where the United States would "lead in the enhancement of security, stability, and responsible behaviour in space."[18,19]

---

13 United States Department of Homeland Security. (2012). GPS Critical Infrastructure Timing Study.

14 National Space Policy. (1996). Presidential Decision Directive/NSC-49/NSTC-8, [September 14, 1996].

15 This ability is generally referred to as space superiority, whereas the set of capabilities or techniques that are used to gain space superiority are referred to as space control or counterspace. "Counterspace capabilities have both offensive and defensive elements, which are both supported by SSA. Defensive counterspace helps protect one's own space assets from attack, while offensive counterspace tries to prevent the adversary from using their space assets. Antisatellite (ASAT) weapons are a subset of offensive counterspace capabilities, although the satellite itself is only one part of the system that can be attacked. Offensive capabilities can be used to deceive, disrupt, deny, degrade, or destroy any of the three elements of a space system: the satellite, the ground system, or the communication links between them" (Weeden & Samson).

16 National Space Policy of the United States of America. (2006).

17 Kaufman, M. (2006). 'Bush Sets Defense As Space Priority'. The Washington Post, [October 18, 2006].

18 Broad, W. & Chang, K. (2010). 'Obama Reverses Bush's Space Policy'. The New York Times, [June 28, 2010].

19 United States National Space Policy (2010).

Influenced by debris producing events, such as the 2007 Chinese ASAT test and the 2009 Iridium-Cosmos collision, the U.S. leadership became increasingly concerned about the multiplicity of hazards to its space capabilities and activities. The principal objective of most space security initiatives became to protect the space environment as well as space infrastructure from natural and man-made risks and threats. Consistently, the concept of space security was broadened to include "space sustainability, stability, safety, and free access to, and use of, space to support vital national interests of all nations."[20]

In terms of policy initiatives, Barack Obama's administration released a National Space Policy in 2010 and a National Security Space Strategy (NSSS) in 2011. These two documents highlighted the current and future space environment. The point stressed by the NSSS was that outer space had become increasingly "*congested*, contested, and *competitive"*[21] and – in contrast to the Bush policy – prioritised orbital debris and space weather as two risks for U.S. space systems.[22]

Overall, through those two documents the Obama administration directed the United States away from the national-security-oriented strategy focused on U.S. "domination and control" of space that had prevailed during the George W. Bush administration, toward a more cooperative, civilian, and commercial-oriented programme overall. In terms of space security strategy, the pre-Bush approach of "strategic restraint" was again favoured, whereby the United States would restrain itself from introducing offensive capabilities, while seeking to moderate the behaviour of both friends and potential foes. Instead, it would focus on technology development in areas such as space situational awareness (SSA) and Space Weather (SWE), two areas where cooperation could also be promoted.

The Obama administration's approach to space security faced a major turning point in May 2013, when China launched a rocket that nearly reached geostationary orbit (GEO), 36.000 kilometres, without any prior announcement. China announced that the launch was for scientific purposes but an assessment by the United States Air Force found China's statement to be false. The rocket did not deploy any objects, which implies the possibility of the test being a test of counterspace related technologies. The launch and destination came as a surprise to the United States, as well as the world, and drew similarities to the Chinese ASAT test of 2007, even without hitting any target.[23] While it is impossible to know the true intentions of China in this case, the test generated worst-case assessments within the American intelligence and security community. They viewed the test as an important new threat to an orbit where many U.S. high-value intelligence satellites reside. In the same year, both Russia and China had also tested manoeuvrable satellites in LEO,[24] a capability previously demonstrated only by the United States. Such developments raised the question of whether Russia and China were trying to catch up to the United States with their space capabilities, and further exacerbated anxieties in the Pentagon and intelligence community.

In 2013, the heightened threat perception renewed fears about a "Pearl Harbour in space", leading policy-makers to openly speak about space being a war-fighting domain. They also compelled President Obama to order the National Security Council to lead a Strategic Space Portfolio Review (SPR) during the summer of 2014.[25] The effort led to changes in force posture, development programs and budgets, toward a more robust U.S. national security space strategy.[26] Following the SPR, the Pentagon and the Air Force began an aggressive public diplomacy effort, notifying potential threatening actors that the United States would respond to threats with force. Such rhetoric was reminiscent of the Bush administration's "domination and control" motif.

20 Rose, F. (2012). Space Sustainability through International Cooperation. U.S. Department of State, [March 01, 0212]. https://2009-2017.state.gov/t/avc/rls/184897.htm

21 United States National Security Space Strategy (2011). It was congested with space debris and new satellites, contested with new threats coming from old and new spacefaring nations, and competitive with the rise of commercial actors.

22 See National Space Policy of the United States of America, (2010). https://www.nasa.gov/sites/.../national_space_policy_6-28-10.pdf

23 Mike Gruss (2015) SpaceNews. https://spacenews.com/pentagon-says-2013-chinese-launch-may-have-tested-antisatellite-technology/

24 Weeden, B. (2014), 'Through a Glass, Darkly: Chinese, American, and Russian Anti-satellite Testing in Space', Space Review.

25 The SPR concluded "there was a need to identify threats in space, be able to withstand aggressive counterspace programs, and counter adversary space capabilities. Following the SPR, senior military leadership began to talk publicly about the inevitability of conflict on earth extending to space and the need for the military to prepare to defend itself in space. There was also increased focus on preparing to "fight a war in space", even though senior U.S. military leaders expressed no desire to start one. A similar shift in tone can also be seen in academic writings from U.S. military journals calling for renewed focus on fighting wars in space and offensive space control. The U.S. Congress also weighed in, calling for a study on how to deter and defeat adversary attacks on U.S. space systems, and specifically the role of offensive space operations."

26 Hitchens, T., Johnson-Freese, J. (2016), Toward a New National Security Space Strategy, Atlantic Council, p.iii.

The United States has maintained a similar stance on space security with the "America First" theme set by the Trump administration. Marked by a strong interest in space and the security dimension of space activities, the agenda for the White House on space policy remains substantial and overarching, from rationalising space launch, to fully integrating new privatised and commercial space capabilities into all national space activities, to fielding new and dominant space deterrence and war-fighting capabilities and doctrine.[27] In order to get a more comprehensive understanding of the current administration's approach to space security, the various policy initiatives undertaken under President Donald Trump's tenure must be outlined.

2.2 New U.S. Policy Framework for Security in Outer Space

2.2.1 U.S. Strategies and Policy Directives Related to Space Security

President Trump's first measure to promote security in Outer Space came on June 30, 2017, when he re-established the National Space Council (NSpC) through an executive order. The National Space Council was last active at the end of the administration of President George H.W. Bush in 1993. The National Space Council's role is to "provide a coordinated process for developing and monitoring the implementation of national space policy and strategy"[28] and review the nation's long-term goals for space activities. The executive order clarifies that the NSpC is "a central hub guiding space policy within the administration" and is responsible for fostering "close coordination, cooperation, and technology and information exchange" among government agencies and the commercial space sector.[29] The council has met three times since its re-institution, first on October 5, 2017, second on February 21, 2018, and third on June 18, 2018.

The re-establishment of the NSpC was a stepping-stone in the development of the administration's posture to space security issues. In part, building on the outcome of the Council's meetings and advice on national security concerns, the administration issued three policy directives, one after each meeting. These documents outline and modify the basic U.S. posture in key areas of outer space activities. A timeline of these policy documents is provided in Figure 3.

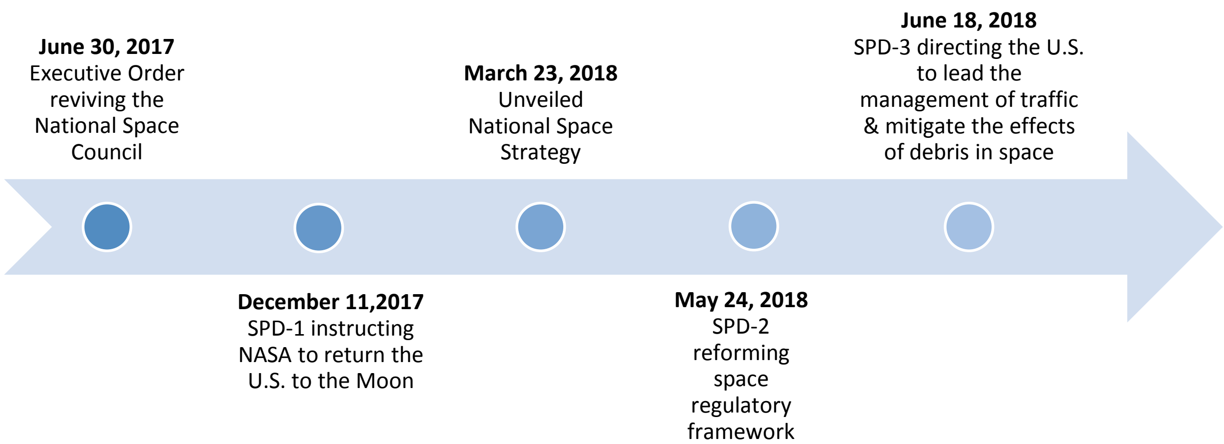

Figure 3: Review of key strategy and policy documents provisions (ESPI)

27 Space News (2017). 'President Trump reestablishes National Space Council'. Available at: https://spacenews.com/breaking-president-trump-reestablishes-national-space-council/, (June 30, 2017).
28 White House (2017). Presidential Executive Order on Reviving the National Space Council, (June 30, 2017). https://www.whitehouse.gov/presidential-actions/presidential-executive-order-reviving-national-space-council/
29 White House (2017). Presidential Executive Order on Reviving the National Space Council, (June 30, 2017).

Space Policy Directive-1

Drawing on the discussions and results of the first NSpC meeting, President Trump issued Space Directive-1 (SPD-1) on December 11, 2017. The policy directs NASA to focus its human spaceflight efforts on return to the Moon, and on to Mars after establishing a long term presence on the Moon.[30] Rather than replacing the National Space Policy (2010) set in place by Obama, the new directive merely modifies and adds to the existing policy. The new direction for space exploration set by SPD-1 draws similarities to President Bush's Vision for Space Exploration of 2004, which envisioned a human return to the Moon by the year 2020.[31,32] The first step in the United States establishing a permanent lunar presence is the Lunar Orbital Platform – Gateway (LOP-G, or Deep Space Gateway), a small human-tended facility in the lunar vicinity that will serve as a technology test bed, enabling human explorers to tackle the challenges and risks of exploration beyond low earth orbit.[33] The LOP-G is to be constructed with the help of a large number of U.S. international partners.

National Security Strategy

A few weeks after the release of the first space policy directive, the Trump administration issued the National Security Strategy (NSS), setting the tone for the administration's national security policy. Space constitutes an integral part of the December 2017 NSS under the third pillar entitled "Preserve Peace through Strength." The pillar highlights the importance of "U.S. leadership in space activities [which] has benefited the global economy, enhanced national security, strengthened international relationships, advanced scientific discovery, and improved way of life."[34] To retain U.S. dominance in space, the strategy lists three priority actions — to "advance space as a priority domain," "promote space commerce," and "maintain leadership in exploration."[35] The document outlines that the United States will seek to achieve these priorities through regulatory reform, public-private partnerships, and by leveraging the National Space Council to develop goals and strategies and promote innovation.

Additionally, the document declares the United States will strengthen its space capabilities through partnerships. The operative language reads as follows: "allies and partners magnify our power. We expect them to shoulder a fair share of the burden of responsibility to protect against common threats." Such language illustrates the administration policy of 'America first but not alone.'[36]

National Defense Strategy

The NSS was followed by the National Defense Strategy (NDS), released on 19 January 2018. The document articulates the U.S. strategy to compete, deter, and win in an increasingly complex security environment defined by rapid technological change and challenges from adversaries in every operating domain. The Strategy acknowledges contested space as a top challenge to be taken up by the U.S. military by stating, "attacks against our critical defence, government, and economic infrastructure must be anticipated" during conflicts.[37] The document also identifies space as war-fighting domain together with cyberspace. In this respect, the U.S. plans to "prioritize investments in resilience, reconstitution, and operations to assure our space capabilities."

As a matter of continuity in this new environment, the administration has increased the military budget for space programs by 14 percent. The new strategy stresses the importance of sustained, long-term investment in the modernization of key capabilities. Figure 4 (below) illustrates the long-term budget forecast to reinforce such capabilities through fiscal years 2019-2023.

30 The White House (2017). Presidential Memorandum on Reinvigorating America's Human Space Exploration Program. Available at: https://www.whitehouse.gov/presidential-actions/presidential-memorandum-reinvigorating-americas-human-space-exploration-program/.
31 NASA (2017). 'New Space Policy Directive Calls for Human Expansion Across Solar System', NASA Release 17-097. Available at: https://www.nasa.gov/press-release/new-space-policy-directive-calls-for-human-expansion-across-solar-system, (December 11, 2017).
32 National Aeronautics and Space Administration (2004). The Vision for Space Exploration.
33 NASA (2018). 'The Global Exploration Roadmap' https://www.nasa.gov/sites/default/files/atoms/files/ger_2018_small_mobile.pdf
34 National Security Strategy of the United States of America (2017).
35 Ibid.
36 http://thehill.com/homenews/administration/344531-administration-policy-is-america-first-its-not-america-alone
37 National Defense Strategy of the United States of America (2018).

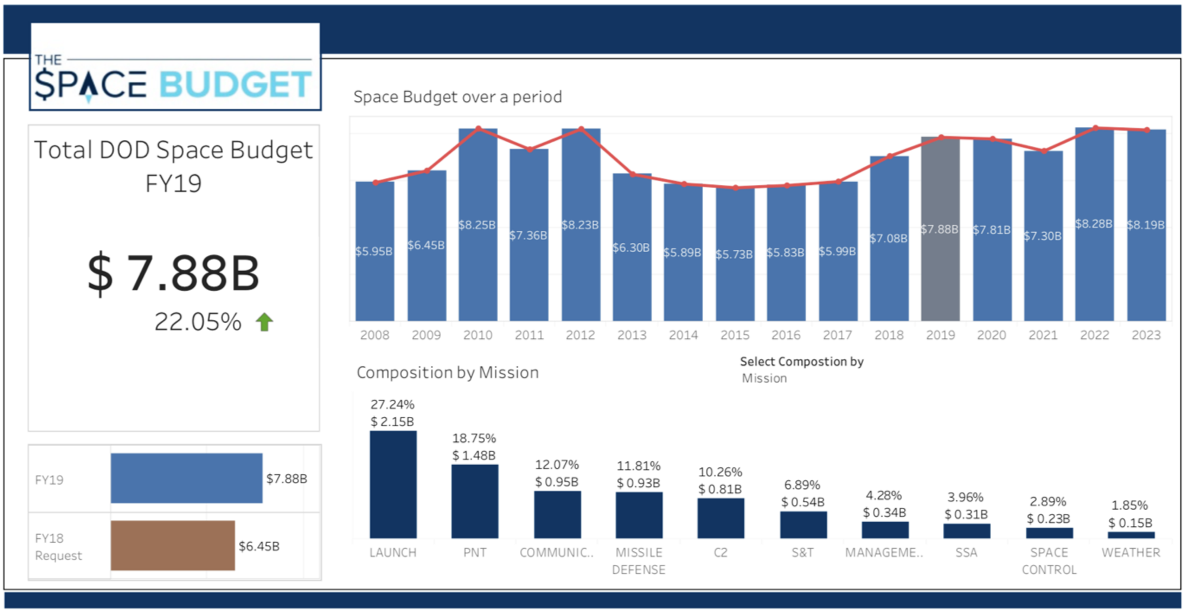

Figure 4: Overview of DoD Space budget[38]

As the National Defense Strategy notes, "investments will prioritize ground, air, sea and space forces that can deploy, survive, operate, manoeuvre, and regenerate in all domains while under attack." The U.S. space investments include:

- 5 Evolved Expendable Launch Vehicles - $2.0 billion;
- Global Positioning System - $1.5 billion;
- Space Based Infrared System - $0.8 billion.

Like the National Security Strategy, the National Defense Strategy stresses the need to strengthen alliances and attract new partners. By working together with allies and partners, the United States recognises that when pooling "resources and sharing responsibility for our common defence, our security burden becomes lighter. Our allies and partners provide complementary capabilities and forces along with unique perspectives, regional relationships, and information that improve our understanding of the environment and expand our options."[39]

National Space Strategy

Soon after the NSS and NDS documents, President Trump unveiled a new National Space Strategy in March 2018. The new strategy is meant to fit into the "America First" theme of the Trump administration, seeking to protect American interests in space through revised military space approaches and commercial regulatory reform.[40] The document reinforces the broader motifs set by the National Security Strategy, emphasising peace through strength in the space domain:

- Protect the U.S. vital interest in space – to ensure unfettered access to, and freedom to operate in space, in order to advance America's security, economic prosperity, and scientific knowledge;
- Affirm that any harmful interference with or attack upon critical components of U.S. space architecture that directly affects this vital interest will be met with a deliberate response at a time, place, manner, and domain of our choosing;
- Recognize that their competitors and adversaries have turned space into a war-fighting domain;
- Seek to deter, counter, and defeat threats in the space domain that are hostile to the national interests of the United States and their allies.[41]

The strategy also features four "essential pillars" that constitute a "whole-of-government" approach to United States leadership in space, in close partnership with the private sector and allies. Three of those pillars are related to national security activities in space, including a shift to more resilient space architectures, strengthening deterrence and war-fighting options in space, while the fourth pillar is devoted to developing "conducive" environments for working with commercial and international partners.

38 SagasIT Analytics. (2018). The Space Budget.
39 National Defense Strategy of the United States of America (2018).
40 Mike Wall (2017). SpaceNews. https://www.space.com/40700-trump-space-policy-private-spaceflight-deregulation.html
41 National Space Strategy of the United States of America (2018).

Finally, the strategy backs cooperation with international partners as done in previous policies, however emphasising that international agreements need to "put the interests of American people, workers, and businesses first."[42] This refers to the strong economic protection promoted by the United States for the space industry.

Space Policy Directive-2

In line with his Administration's priority to bolster the space economy, the President released the Space Policy Directive-2 (SPD-2) in May 2017. SPD-2 instructs the Secretary of Transportation to devise a new regulatory regime for launch and re-entry activities, and to consider requiring just a single license for all such commercial operations.[43] With this policy, the administration is "committed to ensuring that the federal government streamlines the process and helps private enterprise in supporting the economic success of the United States."[44] Space Policy Directive 2 then directly instructs the Commerce Department to consolidate its various space responsibilities into a "one-stop shop" regulatory office.

Space Policy Directive-3

Continuing from SPD-2, and also coming at the recommendation of the National Space Council, President Trump signed a third Space Policy Directive (SPD-3) on June 18, 2018. The primary focus of SPD-3 is on space traffic management,[45] which is a highly critical issue to ensuring the security of operation of U.S. private actors in space. The House Science Committee reinforced the position of the President with the approval of the American Space Situational Awareness and Framework for Entity (SAFE) Management Act, on June 27, 2018.[46] The bill tasks the Commerce Department to provide space traffic management services, such as collision warnings, to civil and commercial satellite operators within one year of the bill's enactment.[47] Development of a regulatory framework for STM has become a top priority as more actors join the space domain, furthering the challenges of the congested space environment. The overarching goals of the new Directive are:

- Advance SSA and STM Science and Technology;
- Mitigate the effect of orbital debris on space activities;
- Encourage and facilitate U.S. commercial leadership in S&T, SSA, and STM;
- Provide U.S. Government-supported basic SSA data and basic STM services to the public at no cost;
- Improve SSA data interoperability and enable greater SSA data sharing;
- Develop STM standards and best practices;
- Prevent unintentional radio frequency (RF) interference;
- Improve the U.S. domestic space object registry;
- Develop policies and regulations for future U.S. orbital operations.

SPD-3 shifts responsibility for disseminating space situational awareness (SSA) data to satellite operators from the Department of Defense to the Department of Commerce (DoC), by directing the DoC to provide a basic level of space situational awareness "free of direct user fees."[48]

The Directive instructs the DoC "to develop stronger relationships with private organizations to more easily share SSA data."[49] To facilitate greater data sharing with satellite operators and enable the commercial development of enhanced space safety services, the Directive tasks the DoC to "be responsible for the publicly releasable portion of the DoD catalogue and for administering an open architecture data repository."[50] The DoC is also instructed to develop standards and best practices for pre-launch risk and on-orbit collision assessments.

NASA was given the responsibility of leading efforts in updating the U.S. Orbital Debris Mitigation Standard Practices (ODMSP), "but also incorporate sections to address operating practices for large constellations, rendezvous and proximity operations, small satellites, and

42 Ibid.
43 Mike Wall (2018). SpaceNews. https://www.space.com/40700-trump-space-policy-private-spaceflight-deregulation.html
44 U.S. Government. (2018). Space Policy Directive-2, Streamlining Regulations on Commercial Use of Space .
45 U.S. Government. (2018). Space Policy Directive-3, National Space Traffic Management Policy, (June 18, 2018). Note: "Space Traffic Management shall mean the planning, coordination, and on-orbit synchronization of activities to enhance the safety, stability, and sustainability of operations in the space environment."
46 H.R. 6226, the American Space Situational Awareness and Framework for Entity Management Act is yet to be voted on by the House.
47 Foust, J. (2018). 'House Science Committee approves space traffic management bill', SpaceNews, (June 27, 2018).
48 U.S. Government. (2018). Space Policy Directive-3, National Space Traffic Management Policy, (June 18, 2018). (Sec. 5. (a)(ii)).
49 Ibid.
50 Ibid.

other classes of space operations."[51] The Department of Transportation (DoT) will then work with the Commerce Department and the FCC to incorporate the updated debris mitigation standards into their respective licensing processes.

2.2.2 Disentangling Key Tenets and Objectives of the United States

A comprehensive assessment of the various policy documents released during the first 18 months of President Trump's tenure illustrates the key tenets and objectives of the administration posture vis-à-vis space security. These can be depicted under a 'triad' of concepts corresponding to technical, martial and diplomatic measures, as detailed in Figure 5.

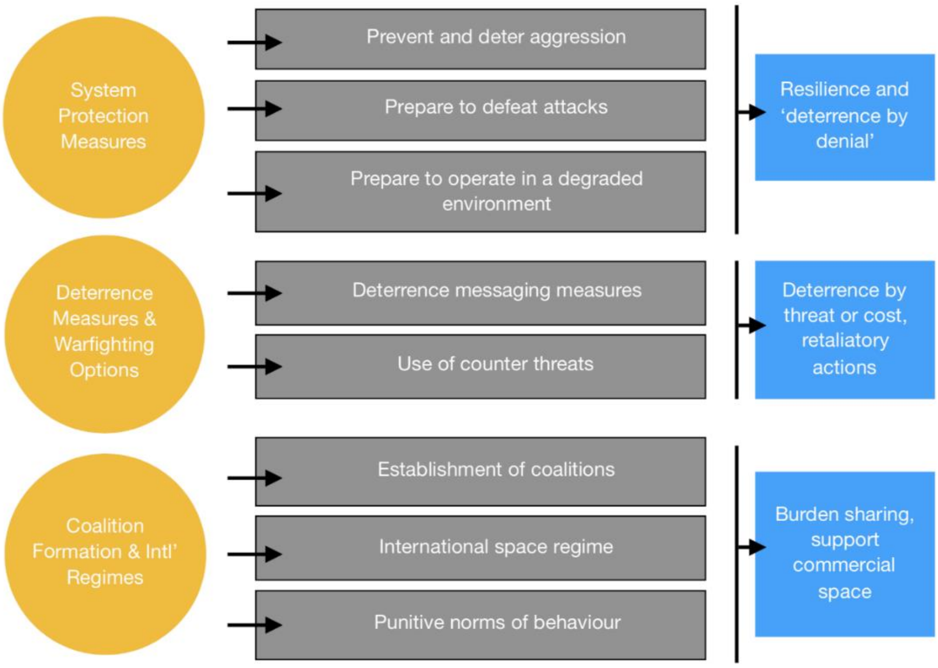

Figure 5: Elements of Defending the U.S. National Space Assets[52]

System Protection Measures and the Role of Commercial Space

The first element, system protection measures, includes activities that serve the security objectives of preventing and deterring aggression, defeating attacks and operating in a degraded environment. These are primarily technological solutions to enhance the safety and survivability of space systems. System protection involves upgrading current systems where possible, and constructing future systems to be more survivable and thus less vulnerable to collision, interference, or attack.[53]

What is also noteworthy about the U.S. posture is the ever-growing prominence of commercial space. For the United States, private space entities will play a significant role in the future, including in the security domain (e.g. through military-commercial partnerships for meeting some military necessities in various fields). The National Space Strategy holds that teaming up with commercial firms is a strong way to improve System Protection Measures and enhance the resiliency of the U.S. space architecture. This is not surprising considering that the lines between military, civil and commercial assets are increasingly blurred (see Figure 6), and the United States is gradually becoming more reliant on commercial space for national security (e.g. the DoD relies on commercial satellite communications systems for more than 40% of its communications needs).[54]

51 U.S. Government. (2018). Space Policy Directive-3, National Space Traffic Management Policy, (June 18, 2018). (Sec. 5. (a)(iii)).
52 Adapted from U.S. Space Strategy (2018) and inspired by the triad model build in National Security Space Defense and Protection: Public Report (2016).
53 National Security Space Defense and Protection: Public Report (2016), p.25-29.
54 Department of Defense, Chief Information Officer, "Satellite Communications Strategy ReportAugust 14, 2014.

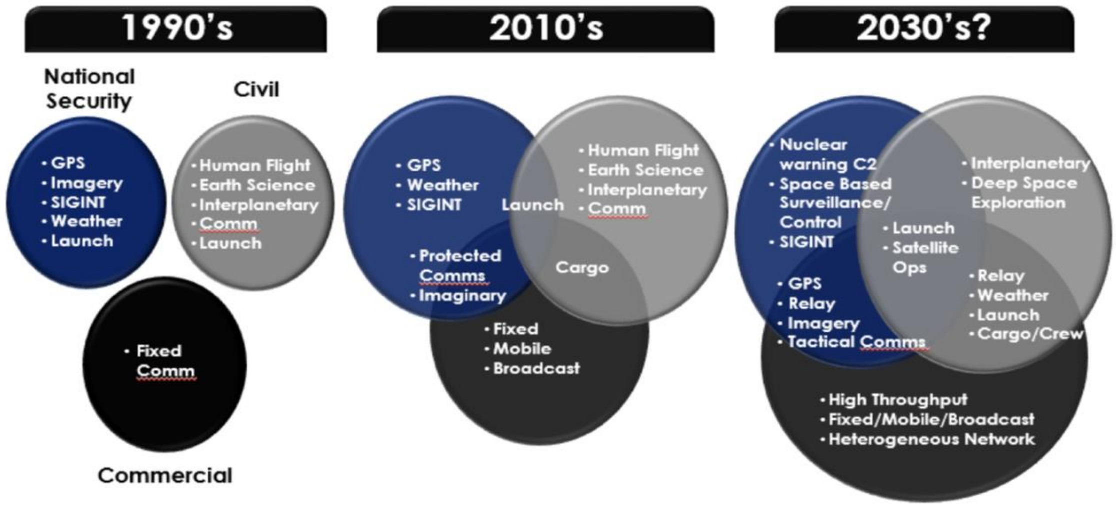

Figure 6: Growing convergence of sectors, products, and services[55]

While opening new options for U.S. national security, military-commercial partnerships also bring new vulnerabilities, as commercial assets can also become targets of potential attacks from adversaries. It is in that vein that the administration is also considering extending national security protections to government private sector partners as needed. To address their vulnerabilities, commercial actors are required to evaluate the information security recommendations of the Defense Department, National Institute of Standards and Technology and the International Organization for Standards.[56] Fleet operators such as Inmarsat, Intelsat, SES and Eutelsat follow extensive requirements included in government regulations and government contracts, ranging from encryption of spacecraft commands to protecting ground stations from cyber and physical intrusion.[57] Another way companies improve the security of their assets is by sharing information with one another and with government agencies, including the Department of Homeland Security and the Defense Department.[58]

Deterrence and Space as a Warfighting Domain

The second key tenet in the U.S. approach to space security is deterrence: discouraging adversaries from interfering with or attacking U.S. space systems either because there is no value in doing so or the actual or threatened cost of doing so is too high. Through the 2018 National Space Strategy, the United States makes clear that it is ready to retaliate to attacks in any necessary and proportional response, but not necessarily solely in space as deterrence measures draw upon the full array of elements of national power, including diplomatic, intelligence, military, and economic tools.

What is noticeable about the current U.S. approach is the token consideration given to the military aspects of deterrence. The administration openly envisions space as a warfighting domain, placing an increased focus on the topic of space superiority and on preparing to 'fight a war in space', thereby challenging long-standing maxims on the need to avoid space confrontations because of the high risks of escalation. There have been explicit suggestions on focusing on how to fight a "limited" space war. Even though senior U.S. military leaders have expressed no desire to start one.[59] In addition, as a recent report by Secure World foundation reported, a similar shift in tone can also be seen in academic writings from U.S. military journals calling for renewed focus on fighting wars in space and offensive space control. The U.S. Congress has also weighed in, calling for a study on how to deter and defeat adversary attacks on U.S. space systems, and specifically the role of offensive space operations.[60]

55 National Security Space Defense and Protection: Public Report (2016), p. 15.
56 Werner, D. (2018). 'Satellite communications firms remain vigilant as cyber threats evolve', SpaceNews, (February 20, 2018).
57 Ibid.
58 Ibid.
59 Elbridge Colby, From Sanctuary to Battlefield, Center for New American Security, January 27, 2016. https://www.cnas.org/publications/reports/from-sanctuary-to-battlefield-a-framework-for-a-us-defense-and-deterrence-strategy-for-space
60 U.S. Congress. (2018). https://www.congress.gov/bill/113th-congress/house-bill/3979/text

Early indications are that the overt development of space weapons will be pursued, although only a small amount of funding has been allocated to space control in the public DoD budget. In addition, the United States "continues to hold annual space war games and exercises that increasingly involve close allies and commercial partners." It is under this "space control" tenet that the present administration has been also considering the establishment of a "Space Force" within the Defense Department.

Diplomacy and Regime Formation

The third tenet of the space security triad is coalition formation and international regimes. Cooperation in space security is perceived as unavoidable for the overall success and efficiency of a variety of actions and measures, including in the development of advanced SSA capabilities and safety of operations in outer space.

In January 2018, U.S. Vice President Pence declared that, even though his policies always aim to put America first, this "does not mean America alone." With specific respect to space security, the various strategic documents released under the Trump presidency all mention the need to strengthen alliances and attract new partners to provide complementarity to "improve our understanding of the environment and expand our options." To this end, U.S. space security actors intend to establish partnerships with commercial, governmental, and international organizations in the field of SSA, space environment protection, and space infrastructure security. More specifically, the benefits of alliances and partnerships contribute to the four lines of effort described in the implementation plan for the National Space Strategy, namely:[61]

- Mission assurance
- Deterrence and war-fighting
- Organisational support
- Creating conducive domestic and international environments for U.S. space objectives.

Each of these lines of effort can be strengthened with the involvement of allies and partners. Thus, "America first does not mean America alone" is a meaningful phrase for the future of space collaboration in the United States. While the National Defence strategy backs cooperation with international partners, it also emphasizes that the United States will do so only on terms the administration deems favourable. "The new strategy ensures that international agreements put the interests of American people, workers, and businesses first". In short, it can be argued that the basic American strategy for dealing with space security challenges at the diplomatic level is to bring other states that are willing to team-up with the United States into a coalition that would be able to set rules and standards for the enhancement of security, stability, and responsible behaviour in outer space. As under the Obama administration, partnering with like-minded states continues to be given more prominence than working with international organisations, which may lessen U.S. bargaining power.

2.2.3 Preparing a National Approach to Space Traffic Management

The most important stakeholder in civil SSA is currently the Department of Defense but, as discussed above, the United States has shifted many SSA responsibilities to the Department of Commerce. The recent Space Policy Directives have placed a focus on Space Traffic Management, which is becoming a key area of relevance for promoting space infrastructure security. The development of a Space Traffic Management (STM) framework that can be applied internationally is part of the "soft power" strategy of creating coalitions and proposing regulations. Through a series of key policy documents and meetings, the current administration is laying the ground work for global STM. With the SPD-3, the United States aims to remain a leader in providing a safe and secure environment as commercial and civil space traffic increases. The policy reads:

"To maintain U.S. leadership in space, we must develop a new approach to space traffic management (STM) that addresses current and future operational risks. This new approach must set priorities for space situational awareness (SSA) and STM innovation in science and technology (S&T), incorporate national security considerations, encourage growth of the U.S. commercial space sector, establish an updated STM architecture, and promote space safety standards and best practices across the international community."[62]

According to the SPD-3, the Department of Transportation and Department of Commerce will assist in working toward developing STM standards and best practices. This includes "technical guidelines, minimum safety stand-

61 Assistant Secretary of Defense Kenneth Rapuano in his testimony to the House Armed Services Subcommittee on Strategic Forces [March 2018].

62 White House (2018), Space Policy Directive-3, National Space Traffic Management Policy.

ards, behavioural norms, and orbital conjunction prevention protocols related to pre-launch risk assessment and on-orbit collision avoidance support services."[63] Moreover, the State Department is instructed to lead discussions with international partners to develop non-binding guidelines on how to increase international transparency for STM (see Annex 6).

The State Department was instructed to lead discussions with international partners to develop non-binding guidelines on how to increase international transparency for STM. This could potentially pave the way to new international cooperation with key partners, while enhancing U.S. global leadership in space. The authority of the Department of Defense to provide space situational awareness data to commercial and foreign entities will terminate on January 1, 2024.[64] International cooperation can also be driven by larger policy objectives and be part of a strategy to advance foreign policy, innovation, or trade policy goals.

2.2.4 U.S. Strategy and Policy Rationales for Security in Outer Space in a Nutshell

The US has made major strides in embedding space as a core component of the political, economic, and national security framework. The new policies have simply reorganized and restructured the space infrastructure into a new framework. This can be seen from the start of the 21st century to today. Though there have been multiple administration changes, the overall rationales that drive U.S. space security policy have remained consistent. The rationales are as follows:

- **Military superiority**: space assets are critical for U.S. military operations; hence space assets must be secured. This is a component of the resilience of national assets. For decades, Administrations have adopted the idea of "peace through strength" by outspending and out-developing the rest of the world in space technologies. Deterrence from attack and mitigating vulnerabilities currently found in the U.S. space infrastructure are currently a top priority across all space actors within the nation. The proposed Space Force is a way to reinforce the deterrence measures of the nation while also reorganizing current military space capabilities to possibly react and counter any threats U.S. space infrastructure might face. The United States wants to be the only country in the world with certain capabilities and has the tendency to panic when other, potentially hostile, nations develop the same capabilities, such as satellite manoeuvring.
- **National security**: The United States has and will prioritize its national security. The notion is comparable to military superiority, however, it considers the notion of 'country, defence, and security' rather than domination and power in the field. It stresses the gathering of data and intelligence (knowing what others are doing in view of monitoring and detecting a threat). With such a large infrastructure in place, the United States logically has huge strategic stakes in space activities. In addition, as the uptake of space services is further integrating in the economy, growing reliance on the space infrastructure becomes highly critical, but increasingly vulnerable.
- **Foster Commercial Space**: The United States views its commercial space sector as the key to its future success in its space security infrastructure. The United States has taken a hands-off regulatory approach in nurturing the development of the commercial space industry. This approach has seen a boom in innovation and development of new space capabilities. This is most notably seen in the recent Space Policy Directives; rather than prohibiting commercial actors, the Directives are meant to streamline the regulatory process, making it easier for commercial actors to operate. As such, the Directives have been met with near universal praise from commercial actors. The goal is to nurture companies and even individual projects beyond public programs in order to increase competitiveness within the budding space economy. Competitiveness between these actors has brought tremendous innovation to the U.S. industrial base while having a positive impact on the economy. While commercial actors are not necessarily pillars of the space security infrastructure, they are set to play a major role in the future of space security. Some of the greatest innovations in debris mitigation, satellite servicing, and satellite capability development are coming from the commercial sector. Additionally, companies such as Analytical Graphics, Inc. (AGI) have become hugely important to the processing of SSA data.
- **Global leadership in space:** Leadership in the space security domain (e.g. capabilities, best practices, standards…) has

63 U.S. Government. (2018). Space Policy Directive-3, National Space Traffic Management Policy, (June 18, 2018). (Sec. 6. (f)).

64 House Armed Services Committee (2018), Section 1603 of the chairman's bill, "Space Situational Awareness Services and Information."

become a key lever for global leadership in the space sector at large. The U.S is leveraging its space capabilities and political power to utilize the concept of 'soft leadership' where it leads by example. The general stance of the United States is that it considers space as a strategic high ground, where the preservation of the U.S. technological edge has been deemed necessary to promote national security and maximise the country's overall international power. However, it also recognises the need for international partnerships for strengthening geopolitical relationships, redundancy, and collaboration. Without these partnerships, United States space security infrastructure would be nowhere near where it is today. This stance will be further expanded on in the next chapter.

2.3 Overview of U.S. Activities and Capabilities

To prevent a loss or disruption of its space capabilities from occurring, the U.S military is charged with protecting the space infrastructure from harm and ensuring reliable space operations. However, many civilian entities also participate in the protection of the U.S. space infrastructure, notably federal agencies, NGOs, and even commercial companies. Six main actors – both public and private – can be considered as having major roles in the security of U.S. space activities. They are as follows:

- **The Department of Defence (DoD),** which plays a highly strategic role in the field of space security, as it operates the US SSA system through the US Strategic Command and was, until recently, the official interlocutor for fostering cooperation schemes with international partners. DoD also funds many projects related to Space Security. The Defense Advanced Research Projects Agency (DARPA) is an agency of the DoD that conducts fundamental R&D for the government. DARPA's scope of research also covers key areas in Space Security, such as launchers and Space Situational Awareness;[65]
- **The Armed Forces** are the primary role in defence and security matters related to outer space. Within the U.S. Armed Forces, most space activities are funded through the Air Force budget. The Air Force Space Command provides military focused space capabilities;
- **The National Aeronautics and Space Administration (NASA)**, which is actively involved in Space Security at operational level as it operates its own satellites, sometimes in collaboration with other federal agencies, designs and manages a number of projects with security dimensions. NASA dedicates more than 15% of its USD 18.1 billion budget to safety and security programmes;[66]
- **The Federal Aviation Administration (FAA)** oversees the issuing of launch licenses for launch providers;
- **The National Oceanic and Atmospheric Administration (NOAA)**, which is under the responsibility of DoC, operates and exploits weather monitoring satellites;
- **The Federal Communications Commission (FCC)** issues licenses for satellite constellations for which requirements have been produced;
- **Commercial Operators**, such as Intelsat, Orbcomm, Globalstar, which operate and exploit their own fleet and have already gained experience in participation in space security-related activities, are funded through the DoD.

United States space security is primarily viewed as a subset of security policies, measures aimed at enhancing the protection of space assets have been implemented in accordance with U.S. national security strategies. Notably, these have guided a wide range of technical, legal, military and diplomatic actions intended to both advance the resiliency of U.S. space systems and to deter possible aggression while also promoting norms of responsible behaviour in space.

Consistent with the space security components outlined in the previous chapter of this report, this next section focuses on current U.S. activities in the field of Space Situational Awareness (SSA), Space Environment Protection and Preservation (SEPP) and Space Infrastructure Security (SIS).

2.3.1 Space Situational Awareness

Over the past two decades, the United States has had growing concerns over the increase in the number of space objects and the development of ASAT capabilities by adversaries.

65 Foust, J. Space News. (2015) https://spacenews.com/darpa-space-efforts-address-u-s-reliance-on-space/

66 https://www.faa.gov/about/office_org/headquarters.../2018_AST_Compendium.pdf

These concerns have elevated the importance of space surveillance as a tool for measuring the increase in space debris and other potential security challenges posed to operational satellites. Space situational awareness (SSA) indicates that the focus is not just on tracking space objects but also on generating information about the entire space environment, including space weather, Near-Earth Objects and radio frequency interference (RFI).[67]

Space Surveillance and Tracking

The U.S. orbital tracking 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, including radars and optical telescopes operated by military and civilian entities.[68] The DoD, including U.S. Strategic Command (USSTRATCOM), NASA, the FAA Office of Commercial Space Transportation and NOAA, are the federal organisations currently involved in the provision of civil SST services. Figure 7 shows the activities covered by civil and military SST in the United States.

Figure 7: Division of Labour between Civil and National Security SSA Data[69]

The authority in charge of the SST system is the U.S. Strategic Command (USSTRACOM), part of the Joint Functional Component Command for Space, which operates the SSN through the Joint Space Operations Center, referred to as JSpOC or 18th Space Control Squadron (SPCS).[70] The initial purpose of JspOC was to track artificial objects in Earth orbit for military purposes but was extended in 2005 to monitoring and cataloguing objects for public use. The SSN is composed of ground-based radars and optical sensors that produce orbiting objects' ephemeris, or approximate location, and allow the US military to monitor global launch activity on an unprecedented scale.[71] The U.S. budget for SST efforts averages about $ 1.0 billion per year for fiscal years 2015 through 2020.

Currently, the U.S. system has the capability of tracking approximately 22,000 objects about 10 cms in LEO and 1m in GEO. However, the deployment of the U.S. Space Fence, a $1.594 million programme[72] expected to be operational in 2019,[73] will drastically improve these performances, as the new system, once operational, will be able to track 500.000 objects between 1 and 10 centimetres and 200.000 objects as small as 5 centimetres. This large-scale project is also going to increase the accuracy of payload identifications and risk conjunction predictions.[74] A future second site is planned to go online in 2021.[75]

JspOC also maintains unclassified versions of SST data sets and generates warnings in the form of Conjunction Data Messages (CDMs) that are sent out to operators around the world. In addition, JspOC provides deorbit, reentry, and disposal/end-of-life support. The U.S. stance on SSA cooperation has evolved over time. The Commercial and Foreign Entities (CFE) Pilot Program formalised and streamlined the U.S. cooperation approach to SSA sharing in 2004, and was upgraded into a full-fledged SSA Sharing Program managed by the USSSTRATCOM in 2009. More than 70 agreements of this kind have been signed with primarily commercial operators, such as launch providers, etc., and institutional actors. The main objective of entering into these agreements pursued by the United States is indeed to promote international security and safety cooperation among allies, to promote

67 Evaluating Options for Civil Space Situational Awareness, IDA (2016).
68 International Academy of Astronautics. (2017). Space Traffic Management: Towards a Roadmap for implementation. Paris: IAA Cosmic Study
69 Weeden (2014).
Notes: Civil SSA data includes those data that are essential to providing safety of space flight services. National Security SSA data builds upon the civil SSA data and includes data essential to characterizing actions and behaviour in space and assessing potential threats.
70 Phillips, C. (2017). Time for common sense with the satellite catalog. The Space Review. Retrieved from http://www.thespacereview.com/article/3215/1
71 Briani, V. (2011). La Sicurezza nello Spazio: Risvolti Italiani e Internazionali, in Osservatorio di politica internazionale, n.29,p. 5. Rome: Istituto Affari Internazionali
72 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
73 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.
74 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
75 Lockheed Martin, (2018). Space Fence.

the transparency of outer space activities, and last but not least, to enhance the quality of the U.S. service delivery system.[76,77] Three service delivery levels can be identified:

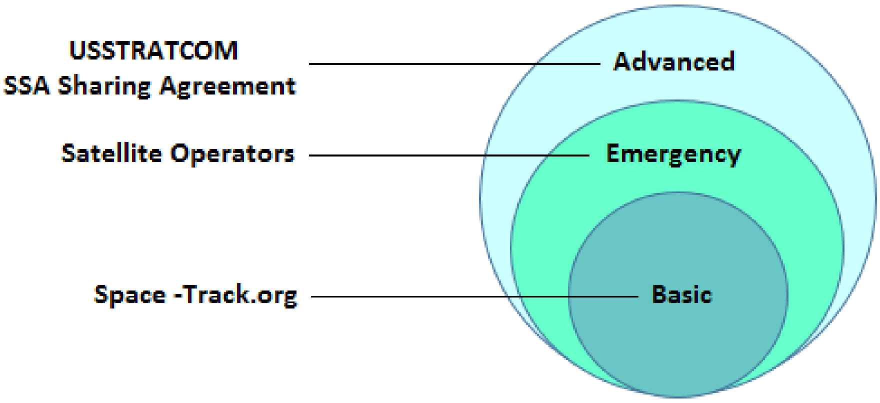

Figure 8: Data access to the U.S. SSA System

SpOC provides three different levels of access to SSN data as shown in the above graph. At the 'Basic' level, the Space-Track Platform is accessible online at www.space-track.org and offers a catalogue of about 16,000 objects. The Space Track catalogue provides the orbital ephemeris of space objects through the Two-Line Element sets (TLEs), the Satellite Catalogue data and the Satellite Decay & Re-entry Data. In addition to that service, the 'Emergency notification service' is aimed at identifying close approaches for active payloads – 20 to 30 warnings to operators through e-mails and Conjunction Summary Messages (CSMs) are issued every day. Finally, the 'advanced service' involves the establishment of a full-fledged SSA sharing agreement that includes information exchange such as conjunction assessment, anomaly resolution, electromagnetic interference investigation, and support to space activities.[78] Recently, based on guidance in Space Policy Directive-3 to support the Department of Commerce's transition as the lead U.S. authority for Space Traffic Management, Space-Track.org began to receive additional data about some space objects that was not previously available.

Notwithstanding that U.S. SST capabilities are unmatched, the United States has also placed continuous emphasis on the upgrading of its SST system so as to tackle the lengthy acquisition timelines and keep pace with the ever-growing tracking requirements. In 2015, the Air Force Space Command announced three unclassified Air Force programmes in the field: the Space Fence, a next-generation space surveillance system; the Space Based Space Surveillance satellite follow-on; and the Joint Space Operations Center Mission System, a three-phase hardware and software upgrade intended to improve the precision and timeliness of space situational awareness information.[79]

In addition to these programmes, the Defense Advanced Research Projects Agency (DARPA) has contributed to the creation of capabilities for realising space domain awareness in real-time. Two DARPA projects are particularly relevant in this regard:

- Hallmark, for integrating real-time space domain command and control (C2) capabilities for the U.S. space enterprise;
- OrbitOutlook (O2), for improving the SSN through real-time detection using live data feeds incorporated from seven SSA data providers.

These two programmes envision unprecedented, real-time command, control, detection, and tracking of space assets. DARPA's envisioned system could fuse information from diverse sources, allowing potential actions to be simulated and effects determined in advance, and vastly reduce the overall time required to make and execute decisions and observe results.[80] Such technologies are therefore not only valuable to the military, but to the space community as a whole.

76 Helms, S. (meeting of June 3, 2010). Space Situational Awareness. Power Point presentation for the United Nations Committee on Peaceful Uses of Outer Space.
77 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/
78 Major Courtland B. McLeod (2012). Space Situational Awareness (SSA) Sharing. United States Strategic Command
Space Policy. Retrieved from http://www.unoosa.org/pdf/pres/stsc2012/tech-40E.pdf
79 Gruss M. (2015). 'U.S. Spending on Space Protection Could Hit $8 Billion through 2020', referring to the words of Gen. John Hyten, SpaceNews. (July 2, 2015).
80 DARPA (2018). 'Hallmark'. Available at: https://www.darpa.mil/program/hallmark.

Regarding the civil side of SSA, NASA is both a provider and consumer of SSA data and is heavily invested in and integrated into the current JspOC system. NASA's Conjunction Assessment Risk Analysis (CARA) mission at Goddard Space Flight Center is responsible for the safety of NASA robotic missions along with selected robotic missions from other civil and commercial customers, and engages in conjunction assessment risk analyses for these missions.

NASA's Conjunction Assessment Risk Analysis (CARA) is primarily concerned with the safe operations of the International Earth Observing Constellations at the 705 km orbit. The CARA team works closely with the United States Air Force's JspOC to assess the risk of predicted potential close approaches between NASA and International Earth observing assets and other space objects. If a potential threat from a secondary space object is detected, CARA notifies the affected mission team. This is a three-step process between the JspOC, the CARA team, and the mission Owner/Operators (O/O):

- Identification of close approaches (i.e. Conjunction Assessment);
- Screening to determine the risk posed by a given conjunction event (i.e. Conjunction Assessment Risk Analysis); and
- Planning and execution of any risk mitigation strategies (i.e. Collision Avoidance).

NOAA is also both a provider and consumer of SSA data and is increasingly integrated into the current JspOC system. As a provider, NOAA's activities mainly focus on Space Weather phenomena. Together with NASA and NOAA, and consistent with the current U.S. posture, commercial companies are becoming involved in the JspOC system. In 2018, JspOC conducted a commercial-military cooperation pilot programme: the Commercial Integration Cell (CIC).[81] The CIC aimed at building synergies between DoD and commercial space operators in the space sector for more coordination, timely responses to critical space operations and resiliency needs. The project was enabled by Cooperative Research and Development Agreements (CRADAs) approved by the Air Force Research Laboratory (AFRL). Within the framework of that project, JspOC collaborated with Intelsat General Corp, SES-Government Solutions, Eutelsat-America, Iridium, Inmarsat, and Digital Globe.[82] Daily exchange with operators facilitated information sharing at operational level, bringing commercial perspectives to the table – such as technical solutions, concerns, and best practices. Cooperation areas included theatre support, SSA, resiliency, threat mitigation and exercises including conjunction assessment and space object catalogue maintenance, rapid identification, diagnosis, resolution. Satellite operators participated in the definition of the concept of operations (CONOP) through the establishment of relationships between stakeholders, procedures, and joint contingency plans for space.

The involvement of commercial operators in DoD's activities is beneficial not only for the enhancement of the U.S. SSA system but also for strengthening interrelationships with them, especially in case of attack. Many satellite operators view JspOC's Conjunction Summary Messages as sufficient for their mission needs, but some commercial and governmental operators with more investment in space have seen the need to protect their assets by joining the Space Data Association (SDA) or purchasing services from SSA companies.[83] The DoD estimates that more than 350 potential SSA sensors exist outside of the SSN.[84] Many satellite operators view JspOC's Conjunction Summary Messages as sufficient for their mission needs, but some commercial and governmental operators with greater investments in space have seen the need to protect their assets by joining the Space Data Association (SDA) or purchasing services from SSA companies.

81 See Intelsat website: https://www.intelsatgeneral.com/blog/inside-the-commercial-integration-cell-project/http://www.stratcom.mil/Portals/8/Documents/JSpOC%20Fact-sheet%20FINAL%20CAO.pdf?ver=2018-04-12-134128-903

82 Buck, D. J. (2017), Statement before the House Armed Services Subcommittee on Strategic Forces on Fiscal Year 2018 Priorities and Posture of the National Security Space Enterprise https://docs.house.gov/meetings/AS/AS29/20170519/105974/HHRG-115-AS29-Wstate-BuckD-20170519.pdf

83 The Space Data Association (SDA) is a membership-based organization of satellite owner/operators that want more accurate and up-to-date collision avoidance data. The analytical core of the SDA is the Space Data Center (SDC), run by Analytical Graphics, Inc. (AGI), and it provides the ability to ingest many different types of owner/operator positional data and manoeuvre plans. The Commercial Space Operations Center (ComSpOC) fuses satellite tracking measurements from a global network of commercial sensors. ComSpOC is tracking 5,000+ total space objects, 75% of all active global GEO satellites and 100% of all active GEO satellites over the continental U.S. Network of globally distributed optical, radio frequency, radar and space-based sensors. ComSpOC has more than 28 optical sensors and one radar site. See: SSA Services - Current and Future US Capabilities, IDA (2018)

84 Government Accountability Office (2015).

Space Weather

Together with object tracking, Space Weather has received increased attention in the United States. The Obama administration released a dedicated policy for Space Weather Events in 2015.[85] The document coordinated interagency efforts to improve the nation's ability to prepare, avoid, mitigate, respond to, and recover from the potentially devastating impacts of space weather events. These efforts included the establishment of the interagency Space Weather Operations, Research, and Mitigation (SWORM) Task Force in 2014. The goal of the SWORM Task Force was to unite the national and homeland security enterprise with the science and technology enterprise to formulate a cohesive vision to enhance national preparedness to face space weather hazards. The strategy also invited other countries around the world to collaborate to improve situational awareness, and forecasting.

NASA is active in providing a better understanding of space weather. Under its *Living With a Star* programme (LWS), the Agency is developing several missions on space weather in cooperation with European partners.[86]

The space weather forecast is delivered by the Space Weather Prediction Center (SWPC) of the National Oceanic and Atmospheric Administration (NOAA). The NOAA Space Weather Prediction Center monitors and provides forecasts, alerts, and warnings to a broad user community spanning the public and private sectors for space weather phenomena (e.g. solar flares and geomagnetic storms) that could have a negative impact on technological systems on the Earth's surface or in orbit. This forecasting and warning service is important both for satellite launch and operations, and for human space flight. NOAA's first space weather satellite, DSCOVR, has been operational since 2016, replacing NASA's aging research satellite, the Advanced Composition Explorer (ACE). In 2017, the U.S. Senate passed the Space Weather Research and Forecasting Act. The legislation directs NOAA to propose options to replace solar imaging data provided by NASA's Solar and Heliospheric Observatory (SOHO) spacecraft. NOAA requested $1,414,263, but the space weather program actually received $5 million, double the amount in NOAA's original request.[87] The Space Weather Follow On satellite will launch by 2024.

Near Earth Objects

A focus of U.S. SSA activities is Near Earth Objects (NEOs). In January 2016, the National Science and Technology Council (NSTC) convened to define, coordinate, and oversee the goals and programmatic priorities of Federal science and technology activities related to potentially hazardous near-Earth objects (NEOs). The primary goal of the Interagency Working Group on Detecting and Mitigating the Impact of Earth-bound Near-Earth Objects (DAMIEN) was to develop a National NEO Preparedness Strategy and Action Plan to improve capabilities for prediction (detection, characterization, and monitoring) and National preparedness (protection, mitigation, response, and recovery).

In 2016, the Obama administration released the National Near-Earth Object Preparedness Strategy and the National Near-Earth Object Preparedness Action Plan, which identified goals and activities to "enhance the understanding of risk from, and national preparedness for, NEO impacts."[88] In June 2018, the Trump administration released its National Near-Earth Object Preparedness Strategy and Action Plan. The strategy improves U.S. preparedness to "address the hazard of NEO impacts by leveraging and enhancing existing national and international assets and adding important capabilities across government."[89]

Operationally, the NASA Center for Near Earth Object Studies (CNEOS) computes high-precision orbits for Near-Earth Objects in support of NASA's Planetary Defense Coordination Office. The NEO Observations Program supports NEO surveys that contribute to a sustained and productive campaign to find and track NEOs, collecting data of sufficient precision to allow accurate predictions of the future trajectories of discovered objects. In addition, the Program devotes a limited amount of funding to research into NEO impact mitigation and deflection strategies and techniques.

2.3.2 Space Environment Protection and Preservation

NASA and the Department of Defense have been directed to pursue research and development of technologies and techniques to mitigate and remove on-orbit debris, reduce hazards, and increase the understanding of the current and future debris environment.

85 The White House. (2015). Coordinating Efforts To Prepare the Nation for Space Weather Events.
86 National Aeronautics and Space Administration. (2014). Global Reach.
87 Wolfe, (2018), 'FY19 Budget Request: 20% NOAA Cut Targets Research, Forecasters', American Institute of Physics, (February, 2018).
88 Interagency Working Group (IWG) for Detecting and Mitigating the Impact of Earth-bound Near-Earth Objects (NEOs) (DAMIEN), (2016). https://obamawhitehouse.archives.gov/.../9.25A%20Drew%20A..p...
89 U.S. government (2018). National Near-Earth Object Preparedness Strategy and Action Plan.

Debris Mitigation

Since 1988 the official policy of the United States, as with most space faring nations, has been to minimize the creation of new orbital debris. The most recent National Space Policy (2010) addresses the importance of preserving the space environment, including orbital debris mitigation. A set of U.S. Government Orbital Debris Mitigation Standard Practices was developed in 1997 and approved in 2001. Major focuses of the practices are the control of debris released during normal operations, minimizing debris generated by accidental explosions, limiting the probability of on-orbit collisions, and the post-mission disposal of space structures.[90] The standards set in place remain the foundation for specific debris mitigation requirements issued by individual U.S. Government departments and agencies.[91]

The FCC requires a debris mitigation plan to be included in every license application. It must address measures to limit operational debris, collision risk, and avoidance of accidental explosions for both during and after mission completion. Included in this requirement are an end-of-life disposal plan and a 25-year maximum disposal time for a single satellite.[92,93] With the establishment of SPD-2 and 3, the licensing process is set to face a large overhaul and will see significant changes in the near future. The NASA Orbital Debris Program Office has taken the international lead in conducting measurements of the environment and in developing the technical consensus for adopting mitigation measures to protect users of the orbital environment. The Inter-Agency Space Debris Coordination Committee (IADC) grew out of the NASA-ESA coordination meetings and was set up as a formal organization in 1993. The role of the Inter-Agency Committee is to coordinate research on space debris between NASA and other space agencies. This resulted in the creation of the 2007 IADC Space Debris Mitigation Guidelines, which were subsequently endorsed by the United Nations in 2008.[94]

Active Debris Removal

NASA and the Department of Defense have also been directed to pursue research and development of technologies and techniques to mitigate and remove on-orbit debris, reduce hazards, and increase the understanding of the current and future debris environment. While there is a great deal of effort to limit new debris in orbit, very little attention is being paid to eliminating the debris already there. Within Obama Administration's 2010 National Space Policy, the Department of Defense, and NASA were tasked to jointly research and develop technologies and techniques for debris remediation. But NASA plans for active debris removal are tied to other planned projects, such as Restore-L, RRM3 and Raven. The idea is that technologies developed for refuelling satellites — robot arms, grapple tools, and software — could also be eventually applied to clean-up the NEO environment (see Annex 4).[95]

In parallel to these 'in-house' missions, NASA has held two Satellite Servicing Technology Transfer Industry Days, to nurture the growth of commercial satellite servicing actors. Utilizing the capabilities of U.S. based space companies is a key component in NASA's plan for making satellite servicing ubiquitous over time. The current focus is the Transfer of servicing technologies to interested U.S. commercial actors, in tandem with development. From this, NASA hopes to foster the growth of a robust satellite servicing industry within the United States.[96] The growth of the commercial industry could lead to a cleansing of the crowded space environment through debris removal, servicing, or repurposing. Some major U.S. space companies, such as NanoRacks and Orbital ATK, have begun testing and operations in this field (see Annex 4).

2.3.3 Space Infrastructure Security

Due to the reliance the United States has on space systems, the National Space Policy of 2010 and the policies of the Trump Administration state that the protection of all critical

90 U.S. Government Orbital Debris Mitigation Standard Practices (2001)
91 UNOOSA (2017), Space Debris Mitigation Standards Adopted by States and International Organisations, See: http://www.unoosa.org/documents/pdf/space-law/sd/Space_Debris_Compendium_COPUOS_6_-April-2017.pdf
92 Aerospace Corporation, (2017), Commercial Space Activity and Its Impact on U.S. Space Debris Regulatory Structure. https://aerospace.org/paper/commercial-space-activity-and-debris-regulation
93 Kensinger, K. (2016), U.S. Small Satellite Licensing and the Federal Communications Commission, FCC, ITU Symposium and Workshop on small satellite regulation and communication systems, Santiago de Chile, Chilehttps://www.itu.int/en/ITU-R/space/workshops/2016-small-sat/Documents/Kensinger%20ITU%20Small%20Sat%20Symposium-110716.pdf
94 United Nations Office for Outer Space Affairs, (2010). Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space.
95 National Aeronautics and Space Administration, (2018). Mission: Restore-L. https://sspd.gsfc.nasa.gov/restore-l.html
96 NASA (2018), NASA to Hold Second Satellite Servicing Technology Transfer Industry Day, https://www.nasa.gov/feature/goddard/2018/nasa-to-hold-second-satellite-servicing-technology-transfer-industry-day

space systems and supporting infrastructure needs to be bolstered. To this effect, investments are being made throughout the supply-chain to enhance Space Infrastructure Security (SIS), thereby boosting the resilience of satellites.[97] In parallel, efforts have been directed to tackling the space security challenge by enhancing the redundancy of space infrastructure (e.g. small satellites mega-constellations) and by introducing a set of policies enabling Space Traffic Management (STM).

Resilience to Harmful Interferences

The U.S. government recognises the security challenge posed by malicious or accidental radio-frequency jamming, spoofing and cyber operations to its space systems. According to the 2018 National Security Strategy, the United States "considers unfettered access to and freedom to operate in space to be a vital interest. Any harmful interference with or an attack upon critical components of our space architecture that directly affects this vital U.S. interest will be met with a deliberate response at a time, place, manner, and domain of our choosing."

Due to the increased government and military reliance on commercial systems, the United States has been encouraging commercial actors to manage their supply chain and develop a security by design approach. Commercial actors do not currently have the same level of protection as the government, thus making the U.S. government increasingly vulnerable to attack as reliance on commercial space increases.[98] In 2010, the National Space Strategy called on all U.S. Departments to "engage with industrial partners to improve processes and effectively manage the supply chains." The Trump administration too, in the National Security Strategy, has highlighted the need to improve critical infrastructure cyber security, addressing security threats to space operations.[99]

As mentioned above, security by design is based on the idea of making systems as free of vulnerabilities as possible through measures such as continuous testing, authentication safeguards and adherence to best programming practices.[100] As a result, to support the demands of military and government users, many satellite operators are already complying with various controls, checklists, and certifications – including DoD Information Assurance requirements, international standards, and other criteria.[101]

The Department of Defense creates and adopts standards for materials, facilities, and engineering practices to improve military operational readiness and reduce ownership costs and acquisition cycle time. To meet DoD standards, owners of space assets must carefully manage their supply chains, verifying that their suppliers are trustworthy and effective in their own security protocols, to ensure that defective or compromised components are not introduced.

Along with its role in the market as a regulator, the government exerts considerable influence in SIS through its role as a customer. The government is increasingly utilising public-private partnership-based approaches to engage the private sector. When doing so, the United States allocates a certain amount of funding, while specifying some basic requirements.[102] The U.S. Department of Commerce has a well-practiced approach for investigating the industrial base of high-technology sectors. This approach includes widely disseminated surveys that seek to uncover potential vulnerabilities from the perspective of U.S. competitiveness and national security.[103]

To mitigate some existing vulnerabilities, support has been given to the development of advanced technologies, such as the optical beam, which could bring the cyber risk close to zero. The size of an RF beam pattern transmitted from LEO is around 100 kilometres wide. In comparison, the width of a laser beam from an identical altitude would be just 300 meters. This technology also enables data rates way over the RF domain, making it extremely attractive to operators of telecommunications satellites. It is expected that NASA will greatly benefit from laser optical communication to address its RF issue.[104]

97 Agence France-Presse (2017). 'The US military is preparing for war without GPS', AFP, (December 20, 2017).
98 See National Space Policy 2017.
99 See National Security Space Strategy (2017).
100 Dougherty, C. et al. (2009). "Secure Design Patterns." CMU.
Strict quality control is therefore essential to the manufacturing of space hardware because the system cannot easily be repaired or maintained once delivered to orbit.
101 CSRIC (2015). CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES WORKING GROUP 4: Final Report (March 2015).
102 Logan, T. (2018), 'The U.S. must secure its supply chain in the face of anti-satellite weapons', C4isrnet.
103 Bryce Space and Technology (2017), New kids on the block: How New Start-Up Space Companies Have Influenced the U.S. Supply Chain.
104 ViaSat's next-gen satellite's security infrastructure will feature "distributed cybersensors, visualization techniques, and greater automation of attack response." "Many things are occurring at machine time, and people can't respond quickly enough to the threats. So there's a lot of research going on to figure out better ways to handle it."Potential security threats are among the reasons that the engineers working on Lockheed Martin's Advanced Extremely High-Frequency (AEHF) satellite communications designed it to be one of the world's most resilient satellite communications systems. AEHF serves not only the U.S., but also

Space Infrastructure Security by Redundancy

Another measure the United States has adopted to promote SIS is through space systems redundancy. The National space strategy of 2010 urged to "implement, as necessary and appropriate, redundant and back-up systems or approaches for critical infrastructure, key resources, and mission-essential functions." Redundancy is the duplication of critical functions with the intention of increasing reliability and actual system performance. To reach redundancy, the United States is taking the following measures:

- Deployment of a larger quantity of satellites;
- Improving launch responsiveness;
- Partnering with foreign actors.

Achieving more operational availability by increasing redundancy requires greater complexity and development costs. Since deploying large satellites can be costly, the United States has supported the development of large swarms of small satellites as they are cheaper to launch and cheaper to develop, rather than one large satellite. Redundancy allows for satellites to go out of service without having a major impact on the space infrastructure. An example of this is the GPS constellation, which consists of more than 30 satellites in six orbital planes. Potential attackers would have to successfully disable at least six GPS satellites to meaningfully impact U.S. performance.

Additionally, the United States relies heavily on commercial launch companies for space launch. This market is developing rapidly. The annual number of launches by the three primary providers in the U.S. market (United Launch Alliance, SpaceX, and Orbital ATK/Northrup) and new entrants (Blue Origin and Virgin Galactic) is continuing to increase.[105] By utilizing multiple launch providers, the United States reinforces its own industrial base while strengthening its economy through competition.

partner nations Canada, the Netherlands, and the United Kingdom. See http://mil-embedded.com/articles/military-communications-capacity-evolving-rapidly/

105 Beyer, B. (2018). 'A new governance model to grow U.S. space launch capability', SpaceNews, (April 30, 2018).

3. Europe: Rising Space Security Stakes and Ambitions

This chapter provides an adapted synthesis of information presented in ESPI Report 64 "Security in Outer Space: Rising Stakes for Europe". A more thorough analysis of the European approach to security in outer space can be found in this report which is available for download on ESPI website (www.espi.or.at).

3.1 Strategy and Policy Rationales

The growing importance awarded to security in European space policies is driven 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.

3.1.1 Protect the Value of the European Space Infrastructure

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. However, 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 if space assets were to be incapacitated, even partially. With the intensification of challenges to the security of space systems, the need to protect space assets to safeguard the benefits they enable can be considered, alone, as a reasonable argument for Europe to position security at the top of the space policy agenda.

The elaboration of increasingly sophisticated space policies, involving a growing number of actors and sectors is driven by the political willingness to *fully exploit the socio-economic value of the European space infrastructure*. The thriving downstream space sector processes and exploits space-derived data derived from that infrastructure in increasingly innovative ways. More and more turnkey services are available to end-users – households, companies, and public actors – which are increasingly disseminating them through their business models in the form of new applications. As a result, the exploitation of space services stimulates growth and generates considerable benefits for the European economy. More than 10% of the EU GDP depends on space infrastructure.[106] The European GNSS system, Galileo, now has more than 200 million users[107] and its full potential has yet to be reached. Financial assessments investigating the downstream sector and economic benefits to end-user sectors conclude that the total economic benefit is around € 53.5 billion per year in Gross Value Added, supporting 1 million workers directly or indirectly. The European Earth Observation programme, Copernicus, is expected to generate more than € 13, 5 billion of cumulated economic benefits in gross value added by 2020. The European space infrastructure is also a critical asset for the implementation of governmental policies benefiting society and the environment at large. The uptake of space-based solutions for EU sectoral policies is already a reality for the

106 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

107 https://www.numerama.com/politique/386721-galileo-le-gps-europeen-compte-200-millions-dutilisateurs-dans-le-monde.html

EU Digital Agenda dealing with the digital divide, the Common Fisheries Policy (CFP), and the Common Agricultural Policy (CAP) for natural resources management or the Energy Union's policies.[108] The role of space systems is also critical for defence and security policies dealing with traffic monitoring, border surveillance, and humanitarian aid. Additionally, the uptake of space technology plays a huge part in Innovation Policy, laying the groundwork for the development of new services in Europe. In this context, NewSpace is defined by ESPI as a disruptive sectoral dynamic featuring various end-to-end efficiency-driven concepts driving the space sector towards a more business- and service-oriented paradigm, laying the foundations for the cross-fertilisation of space technologies with ground technologies is indeed important to allow the on-going digital transformation to move forward, in which space systems are likely to be key enablers for 5G networks, precision agriculture, forestry, air traffic management, smart energy grids, and autonomous vehicles.

3.1.2 Contribute to a "Service-Oriented" Policy

The rising need for enhanced space security in Europe also lies in the significant progress of EU programmes (i.e. Galileo, EGNOS, Copernicus) and in the potential introduction of new initiatives such as GOVSATCOM. These developments are amplifying the importance of a service-driven policy to build user confidence, encourage the uptake of space services, and consequently maximise the benefits of the European space infrastructure. Such policy encompasses 1) operational capacities meeting user performance requirements, 2) continuity of programmes to ensure infrastructure maintenance, upgrade and evolution, and 3) appropriate measures to protect the infrastructure against threats. These requirements are even more stringent for governmental and defence and security users that the EU seeks to support to 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.

From this standpoint, four main challenges were identified for Europe, namely: 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, and reinforce synergies between civil and security space activities. As a matter of fact, the security needs of the EU are growing, inasmuch as common foreign, security and defence policy objectives are increasingly being incorporated into the agenda and DNA of the European Union. The EU's role in such matters was reinforced and institutionalised by a number of policy documents which are briefly described below:

- The **Common Security and Defence Policy (CSDP),** which defined an institutional structure for the EU to assume its new role in the field of security and defence;
- The **European Agenda on Security,** which defined EU priorities and its role as a support for Member States' own activities in the field of security;
- The **European Defence Action Plan,**[109] which proposed the establishment of a European Defence Fund to promote interoperability and support R&D in defence, foster investments in SMEs, mid-caps, and other suppliers, and to create a Single Market for defence. The European Defence Fund was enacted in June 2017 budgeting € 90 Million until the end of 2019, €500 Million per year after 2020 for research, and for development and acquisition, € 500 Million for 2019-2020, then € 1 Billion per year after 2020.[110]

These recent developments indicate the growing importance of security in EU Policy.[111] The European GNSS System Galileo will play a pivotal role in the implementation of national and European security policies for localisation and navigation for troops and vehicles, mission planning, delivery of cargos, and search and

108 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

109 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

110 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

111 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

rescue.[112] GNSS-based services are also key in case of conflict for guidance, strikes, and other related operations.[113] The Copernicus programme will provide critical data for policies related to the atmosphere, marine environment, land, climate change, emergency management, and security. The new GOVSATCOM initiative aimed at ensuring reliable, secure and cost-effective satellite communication services for EU and national public authorities will also elaborate on security aspects.

3.1.3 Reinforce European Autonomy and Freedom of Action

From a strategic perspective, Europe also seeks to guarantee the security of its space infrastructure autonomously through independent capabilities (i.e. systems, data, and technologies). Here, and 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.

That policy rationale is acknowledged in the Space Strategy for Europe stating that 'reinforcing Europe's autonomy in accessing and using space in a secure and safe environment' is a pillar objective.[114] Elaborating further, the EC seeks to 'ensure [Europe's] freedom of action and autonomy.'[115] Such strategic goals are not being pursued at the expense of cooperation, however, as cooperation in this field is a necessity (i.e. data sharing, efficiency of measures, transparency, and coordination). The level of reliance European seeks to achieve remains an open question, as there is no well-defined level of strategically acceptable capabilities. At the moment, Europe relies on U.S. data for its operational SSA needs. This position underscores a number of rising issues. First, are the SSA data and service restrictions that mean that the United States does not grant full access to its database because of its intrinsic military nature.[116] Additionally, the U.S. system has its own technical limitations (i.e. unverified warnings) and cooperative agreements do not accommodate accountability mechanisms.[117] And last but not least, the U.S. government has the right to terminate the user account, to limit both access duration and data amount, to deny access to SSA data and information, and to change or modify the terms and conditions at any time for any reason and without prior notification.[118]

3.1.4 Long-Term Stakes for Europe's Position on the International Space Scene

Beyond short-term policy stakes, the need for a reinforced approach to space security in Europe 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."

As space security now holds a central position in space diplomacy, playing a prominent role in international dialogues and negotiations in this field, and promote a clear, united and consistent 'European way', will be essential to build European leadership in the global space sector at large. Taking this into account, equipping Europe with a comprehensive and independent capability to protect its space infrastructure is a priority to position Europe as a credible interlocutor on the international scene.

Last but not least, space security will play an increasing role in commercial space markets. First, the implementation of new practices (e.g. laws, regulations, standards, procedures) promoting space security and impacting the way space activities are conducted will inevitably create a competitive bias for the industry. Second, space security may open up a business opportunity for private industry seeking to enhance public capabilities with commercial data and value-added services. For these two reasons, Europe must contribute actively to future developments in the field of space security to support the competitiveness

112 Mutschler, M. M. (2010). Keeping Space Safe. Towards A Long-Term Strategy to Arms Control in Space. Frankfurt: Peace Research Institute Frankfurt.
113 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
114 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
115 Ibid
116 Specifically, DoD resistance to open SSA data sets, algorithms, and processes to external review and scrutiny, 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
117 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/
118 Space-Track. User agreement. Retrieved from https://www.space-track.org/documentation#/user_agree

of its industry and reap the benefits of new potential markets.

3.2 Overview of European Activities and Capabilities

3.2.1 Space Situational Awareness

The field of Space Situational Awareness (SSA), which encompasses all activities aimed at monitoring space environment threats, constitutes the bulk of activities in the field of Security in Outer Space.

In Europe, just as in many parts of the world, interest in SSA data is growing to meet the challenges of the space environment. Several countries are implementing various national SSA programmes, although the main stakeholders – France, Germany, Italy, Spain, and the UK – still rely on data sharing agreements for their operational needs. This subsection provides an overview of European SSA capabilities. However, assessing the operational needs of European end-users on the basis of open source documents is a challenging task. In investigating national SSA capabilities, the research team focused mainly on the five most involved countries in the field. Organisational culture is diverse, although one can see that in most cases, the military plays a predominant role in SSA activities, highlighting the strategic stakes for the military. Indeed, European states pursue SSA development strategies that involve updating existing systems, funding complementary software able to double check data, and others. However, that very data is still required for manoeuvres and making well-informed decisions. Two tables in Annex 4 present European Space Security strategies in a synthesised manner.

In the field of Space Security, the development of national sensors was the first step when securing space assets first emerged as a national security priority. However, in an attempt to create synergies between European countries and avoid duplication of efforts, the European Space Agency was considered as the most competent body to manage consolidation efforts. The agency today is especially active in the field of space debris, in which it develops software to incorporate raw SSA data into databases, and collision assessment algorithms.[119] As part of its engagement in Space Security, in 2009 ESA launched an SSA programme aimed at supporting '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.'[120] The objectives of the programme were to produce an independent database, support R&D in industry, and strengthen the accuracy of available data through greater focus on European space assets. [121] For the period 2009-2020, € 200 Million was budgeted, including the contributions of 19 Member States. The programme covers R&D, the creation of data and coordination centres, systems development and procurement. The programme has awarded over 100 industrial contacts. ESA is building on the solid base of existing capabilities, relying on the expertise of European and international actors (e.g. the United States), and seeks to actively contribute with additional data to strengthen them. The SSA Programme is coordinated from ESOC in Darmstadt (Germany), but also other centres such as ESRIN and ESTEC.

ESA has developed its SSA programme around three major areas, which are:

- **The Space Surveillance & Tracking (SST) Segment**: which aims at maintaining a data catalogue up to date. Funding allocated to that segment has been reduced and part of ESA activities have been transferred to the EU SST Consortium;
- **The Space Weather (SWE) Segment**: which aims at developing the European ability to monitor solar activity in a timely matter and inform the main stakeholders – public and private – by enhancing existing capabilities;
- **The Near-Earth Objects (NEO) Segment**: which aims at generating data on NEOs – asteroids or comets, making impact likelihood assessments and developing deflection methods. There are estimated to be around 17,000 threatening NEOs that require monitoring.

Part of ESA's mandate in Space Security deals not only with the management of centres and data integrity processes, but also the conduct

119 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

120 ESA. Space Situational Awareness. https://www.esa.int/Our_Activities/Operations/Space_Situational_Awareness

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

of studies on hosted payload and sensor development deployments, and asteroid impact mitigation studies. Funding is also allocated to developing new infrastructure such as databases, software tools, applications, and hardware (optical telescopes and radars). Several achievements illustrate ESA's SSA Programme objectives: funder of preliminary studies of a future space weather satellite, two new radars built in Spain and France to support SST for civilian uses, ESA's Proba-2 solar observatory satellite, the establishment of the ESA Space Security and Education Centre (ESEC) in Redu (Belgium), the Space Surveillance and Tracking Data Centre at ESAC in Madrid, three coordination centres both at Space Pole in Brussels for space weather and at ESRIN in Frascati (Italy) for NEOs, and one at ESOC in Darmstadt. Test-bed optical telescopes were installed in Cebreros (Spain) and are being installed at la Silla (Chile). The project 'FlyEye', which is an initial automated telescope with high-tech European optical hardware, will be deployed by 2018 and is expected to contribute to a global asteroid survey system to be updated every day. ESA's involvement in Space Security also requires constant interactions with the operational entities dealing with SSA at national levels, where ESA actively participates in the coordination of efforts. In the field of Security in Outer Space, ESA fuses data from various sources, primarily from the U.S. SSA System, to provide them to European stakeholders. In this sense, ESA acts as an SSA-providing platform for European users.

ESA is also actively involved in the field of Space Weather (SWE). It coordinates a European network SWE Expert Service Centres (ESCs). Additionally, the agency is conducting a mission at the Lagrangian point L5 (LGR) in cooperation with the United States expected to take place after 2019.

In the field of NEOs, ESA is maintaining its work in developing the field-of-view 'Fly-Eye' telescope, conducting daily sky surveys for objects from 15 meter up to 30 meter. The Consortium in charge is led by OHB. The recently proposed Hera mission will aim at testing planetary defence mechanisms and will be complementary to the NASA DART mission whose objective is to destroy an asteroid.[122] The Hera mission will be instrumental in investigating the kinetic effects of such explosion.[123]

The emergence of the European Union as a major player in Space Security is one of the most important developments of European Space Policy as a whole. As the European Union does not have to deal with institutional constraints, such as ESA in several areas, especially those with strong security dimensions, the EU has more agency to implement programmes in this respect. The European Union funds projects related to 'Security in Outer Space' under the umbrella of large R&D programmes. The FP7 work programme 2007-2018 already included the EU's objective 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'.[124] In 2007, the EU funded a space weather forecasting project called SOTERIA with € 5 Million.[125] The 2009 FP7 work programme of 2009 included a list of external events including 'space debris, hostile laser or Anti SATellite systems (ASAT), jamming, viruses, natural or man-made electro-magnetic disturbances.'[126] The work programme of 2010 supported 15 R&D projects. While the 2011 work programme included NEOs,[127] space debris and weather were respectively covered in 2013. Horizon 2020 included a section on 'Protection of European assets in and from space' (H2020-PROTEC) in the 2014-2015 work programme,[128] and a section called 'Secure and safe space environment' in the work programme 2018-2020.[129] Within FP7, additional financial contributions were allocated to the

122 ESA. (2018) Earth's first mission to a binary asteroid for planetary defence. Retrieved from: https://www.esa.int/Our_Activities/Space_Engineering_Technology/Hera/Earth_s_first_mission_to_a_binary_asteroid_for_planetary_defence

123Jeff Foust. (2018) ESA plans second attempt at planetary defense mission. Retrieved from: https://spacenews.com/esa-plans-second-attempt-at-planetary-defense-mission/

124 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

125 European Commission (2008). Solar-TERrestrial Investigations and Archives. Retrieved from European Commission: https://cordis.europa.eu/project/rcn/89460_en.html

126 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

127 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

128 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

129 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

PEOPLE Programme distributing grants for training and career development, under which the SpaceDebEMC (Space Debris Evolution, Collision risk and Mitigation), and the STARDUST (the Asteroid and Space Debris Network), benefited.[130] The EC SME Instrument also rewarded a Space Security initiative.

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. A spike in EU contributions can be observed in 2010 corresponding to financial support for a number of large projects. It is important to note that since 2014, the EU has also funded the SST support framework (roughly at around €28 million per year) through H2020-SPACE grants, and also through funds allocated to the 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.

In addition to initiatives funded through programmatic investments, the EU has launched the EU Space Surveillance and Tracking Support Framework (http://www.eusst.eu/) aimed at supporting the long-term sustainability of space activities of European stakeholders.[131] The overarching purpose of the Consortium is to leverage the networking of already existing national capabilities to deliver European SST services. To achieve that goal, the Consortium is expected to produce services driven by civilian user requirements, complementary to R&D activities conducted within Horizon 2020, to engage with international partners, particularly with the United States, and to promote the update of capabilities after the networking phase.

In 2018, the European Commission and the European Parliament published a report on the implementation of the EU SST Framework Programme for the 2014-2017 period comparing the capabilities of the sensor function as of today and in 2021:[132]

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

from European Commission: http://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-leit-space_en.pdf
130 See Annex for projects list from ESPI (2018). ESPI Report 64 "Security in Outer Space: Rising Stakes for Europe"
131 Official Journal of the European Union (2014). Decision No 541/2014/Eu Of The European Parliament And Of The Council. Retrieved from EUR-Lex: https://eur-lex.europa.eu/eli/dec/2014/541(1)/oj
132 European Commission (2014). Decision No 541/2014/Eu Of The European Parliament And Of The Council. Retrieved form EUR-Lex: https://eur lex.europa.eu/resource.html?uri=cellar:fbafc703-4eb8-11e8-be1d-01aa75ed71a1.0021.02/DOC_1&format=PDF

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:[133]

- *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:[134]

- *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;
- 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.

A more comprehensive description of the EU SST Consortium and associated stakes and challenges is provided in ESPI Report 64 "Security in Outer Space: Rising Stakes for Europe".[135]

133 Ibid
134 Ibid

135 European Space Policy Institute (2018). Security in Outer Space: Rising Stakes for Europe, Report 64 August 2018. Retrieved from: https://espi.or.at/publications/espi-

3.2.2 Space Environment Protection and Preservation

Space Environment Protection and Preservation (SEPP) is another subdomain of Security in Outer Space. This encompasses all undertakings aimed at keeping the space environment safe to operate in and proactively promoting its preservation.

European Countries

Several Member States are adopting national legislation aimed at regulating space activities. In seeking to establish a legal framework for their activities, Member States have developed requirements, conditions and restrictions for licenses facilitating entities that are eager to engage in space activity.[136] Several jurisdictions also include enforcement mechanisms, actively contributing to Space Environment Protection and Preservation. Already, Austria, Belgium, France, Germany, Luxembourg, Norway, Sweden, and the United Kingdom have passed such laws, a list of which is at Annex 2.[137]

In international fora, a handful of European states have been vocal about the need for greater coordination on Space Security. Good examples are the Inter-Agency Space Debris Coordination Committee (IADC), the United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS), the Conference on Disarmament (CD) and the Committee on Space Research (COSPAR). Among other major initiatives, European states actively contributed to the report of the Group of Governmental Experts (GCE) on Transparency and Confidence-Building Measures (TCBMs). On the occasion, several experts appointed by European states elaborated a strategy towards promoting mutual understanding, and reducing risks of mishaps in outer space.[138] The GGE was adopted at the 68th session of the UN General Assembly in late 2013, and advocated information exchange not only on national space policies and strategies, but also on ongoing space activities and their parameters – launches, natural space hazards, and scheduled manoeuvres. The document also made the case for the use of notifications for risk reduction, emergency situations, high-risk reentries, and intentional break-ups. Lastly, the report restated the value of accommodating visits to launch sites, command and control centres, and technology demonstrations.

Additionally, the Working Group on the Long-term Sustainability of Space Activities (WG-LTS) was setup by the UN COPUOS in 2010 to investigate possible measures to ensure the safe and sustainable use of outer space for peaceful purposes and for the benefit of all countries. The final product of that work was to compile best-practice guidelines and to have them endorsed at the 61st session of the UNCOPUOS in June 2018. Unfortunately, consensus was not reached. Work on WG-LTS guidelines was initiated under the chairmanship of France. However, moving forward within the UN framework remains a major challenge as no enforcement mechanisms are foreseen and there are major discrepancies in the way states see the implementation of guidelines.

The role of states in Security in Outer Space is pivotal to addressing sustainability issues, and the need for cooperation among countries is frequently restated in policy documents. In this respect, the French Ministry of Defence declared that 'a European approach to this topic of mutual interest will be promoted, taking advantage of existing resources and developing new concrete projects.'[139]

European states also conduct national feasibility studies, research projects and experiments on possible technologies that can contribute to space sustainability. Among others, the UK is particularly active on these matters. The University of Surrey coordinates the RemoveDEBRIS project, which is an international consortium aimed at developing deorbiting and capturing solutions for space debris.[140] Consortium members include Airbus Defence and Space (France, Germany, and UK), ArianeGroup (France), SSTL (UK), ISIS (Netherlands), CSEM (Switzerland), Inria (France), and Stellenbosch University (South Africa). Prior to that, the University completed the DeOrbitSail project aimed at developing wind sails to redirect satellites into the atmosphere for disposal.[141] The Defence Science and Technology Laboratory (DSTL) launched the Daedalus project that will be tested in 2019 and has similar objectives.[142] The British company

public-reports/send/2-public-espi-reports/371-security-in-outer-space-rising-stakes-for-europe
136 Ibid
137 Lucien Rapp. (2018) Space lawmaking. Retrieved from:
http://thespacereview.com/article/3523/1
138 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.
139 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
140 https://www.surrey.ac.uk/surrey-space-centre/missions/removedebris
141 https://www.surrey.ac.uk/surrey-space-centre/missions/deorbitsail
142 The IET. (2017). https://eandt.theiet.org/content/articles/2017/07/satellites-to-be-fitted-with-sails-to-take-them-out-of-orbit-and-prevent-space-junk/

Clyde Space has its own deorbiting project called AEOLDOS (Aerodynamic End-of-Life De-Orbit System). The Italian company D-Orbit is developing debris removal solutions.[143] Other European legacy companies are also looking into these services at conceptual level.

However, as in any field, pooling national resources into budgets allocated at European level remains the top line of action for greater coordination. As such, European institutions are also active in that domain.

European Institutions

The European Space Agency is significantly contributing through the development of more sustainable standards and technologies.[144] ESA's CleanSpace initiative is 'a technology project aiming at developing the necessary technologies to support the compliance of future satellites with Space Debris Mitigation (SDM) requirements'. The overarching goal is to develop an eco-friendly and sustainable approach to space activities through the development of industrial materials, processes and technologies that limit the environmental impact of space activity by addressing weaknesses and shortages in the entire lifecycle of space systems from conceptual phase to end of life and disposal. ESA's CleanSpace revolves around three main core activities: EcoDesign, CleanSat, E.Deorbit.

- **EcoDesign:** deals with environmental impact assessments (e.g. Life Cycle Assessment), compliance with legal frameworks (e.g. RoHS directive, REACH regulation), and the development of green technologies.
- **CleanSat:**[145] deals with the development of technical solutions and standards to mitigate space debris proliferation. This includes several solutions such as end-of-life passivation, design for demise, [146] and space debris environmental modelling. CleanSat is the leading programme of ESA in the field of Space Environment Protection and Preservation.
- **E.Deorbit:** deals with Active Debris Removal and associated capabilities such as target characterisation, capture mechanisms, and disposal methods. One major output aim of this project section is to capture an ESA-owned defunct satellite in LEO by 2023 and make it re-enter the atmosphere. Two concepts for this are being studied: a net or a robotic arm.

International cooperation is continuing, mainly under the UN Committee on the Peaceful Uses of Outer Space (UN-COPUOS) and through the European Space Weather Week conference organised annually. ESA has also been chairing the Space Missions Planning Advisory Group (UN- SMPAG) and co-organised the Planetary Defence Conference. Finally, the Space Debris Conference 2017 also organised by ESA provided an excellent opportunity to address the very closely-related SST aspects.

In Brussels, the European Union's political discussions on how to sustain a safe to operate in space environment have been growing steadily in recent years. When the European Union became an active actor in space, developing a strategy at global level for Space Security appeared to be the next necessary step.

In this respect, the most sophisticated diplomatic initiative was the ill-fated International Code of Conduct for Outer Space Activities (IcoC), a non-legally binding and voluntary-based document aimed at regulating outer space activities. More specifically, the Code sought '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'.[147] Areas of focus included 'Outer Space Operations and Space Debris Mitigation', 'Notification of Outer Space Activities', 'Information on Outer Space Activities' and a 'Consultation Mechanism'.[148,149] The Code benefited from a certain level of support, but was criticised at organizational level for the negotiation process and the lack of non-EU countries participation in the drafting, and at content level for lacking clear definitions, re-

143 http://www.deorbitaldevices.com/
144 Jessica. (2017) The clean space blog. Retrieved from ESA: http://blogs.esa.int/cleanspace/2017/02/03/cleansat-an-exciting-opportunity-for-the-european-space-industry/
145 ESA. Clean Space: Cleansat. Retrieved from ESA: http://www.esa.int/Our_Activities/Space_Engineering_Technology/Clean_Space/CleanSat
146 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
147 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
148 Ibid
149 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

striction methods, and the scope of the document. This resulted in a failure to adopt the latest draft outside the official UN framework, as procedures became the showstoppers of that project.[150]

The EU has played an important role in other diplomatic initiatives that include WG-LTS negotiations at UNCOPUOS, the GGE, the UN General Assembly Resolution 71/42 regarding the Prevention of an Arms Race in Outer Space (PAROS), projects related to the '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), and the Principles of Responsible Behaviour for Outer Space (PORBOS) that are also designed to prevent an arms race in outer space[151] among others.[152]

Interestingly, the European approach to SEPP comprises different strategies that interact with each other for greater efficiency. Moreover, these activities are also complemented by a series of measures in the field of Space Infrastructure Security.

3.2.3 Space Infrastructure Security

The focal point of Space Infrastructure Security is the protection of the space infrastructure from threats that diminish its proper functioning. More precisely, it covers the exploitation of space systems' vulnerabilities and can be unintentional or intentional. Space Infrastructure Security includes security-by-design, program security architecture, and supply chain security covering the field of engineering, safety standards, and regulations.

As European approaches to Space Security first developed at national level, Member States all have their own objectives and ambitions for the protection of their assets. In the field of Space Infrastructure Security, a number of small projects are conducted by national space agencies. A few can mentioned such as the upgrading of the French Syracuse telecom satellites that include an anti-jamming system.[153] More anecdotic projects can also be mentioned such as the Robusta programme that is a student led nano satellite project aimed at studying the effects of solar flares on bipolar electronic components.[154]

Member States are also playing a role in Space Infrastructure Security through the involvement of their industries. Indeed, defining security standards and requirements is also to a large extent determined at industry level, although the standardisation of these requirements has not yet been reached. For instance, Leonardo, an Italian aerospace company, was selected for a data security project on the Galileo constellation.[155]

In developing security protocols and technical standards, ESA has played an important role in Security in Outer Space. ESA's involvement in Security in Outer Space includes:

- Definition of a workable regulatory framework encompassing security agreement, security regulations, and implementing procedures and facilities to receive, store, and produce classified information to set up a regulatory framework (Security Agreement, Security Regulations and Implementing Procedures and Facilities), to build 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 the security aspects of EU space programmes such as Galileo and Copernicus;
- ESA's participation in international fora (IADC, IAC, COSPAR, IADC, IAA, UNCOPUOS).

ESA is also supporting R&D in the field of Security in Outer Space through the funding of projects.

150 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
151 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
152 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
153Retrieved from CNES (2018): https://syracuse4.cnes.fr/fr/syracuse-4
154Retrieved from CNES: https://robusta.cnes.fr/fr/ROBUSTA/Fr/index.htm
155Leonardo. (2017) Press release: http://www.leonardocompany.com/en/-/esa-galileo-cyber

Similarly, the European Union funds a great number of research projects in that field but also conducts its own Space Security activities, mostly related to the EU flagship programmes. A good example is the establishment of an independent Security Accreditation Board (SAB) within the European GNSS Agency (GSA) to verify the compliance of the programme with applicable security protocols and regulations.[156] Additionally, the Galileo Open Service will soon feature an Open Service Navigation Message Authentication (OS-NMA) option to address jamming and spoofing attacks, and a Galileo High Accuracy Service to enhance the quality and resilience of signals and the Open Service. The European Union is actively supporting Space Infrastructure Security through the funding of R&D projects in that subdomain in member states. Considerations regarding resilience are seriously treated by the European Union, for which space resilience is a key objective. Its role can be expected to evolve with the greater integration of the Galileo system into the European economy. In this respect, the European Commission recently issued a proposal for the setting-up of a new EU Agency for the Space Programme. Accordingly, an increased budget share will be dedicated to defence spending on R&D and procurement, which also means more opportunities to strengthen the EU's involvement in that particular field.

Security in Outer Space is being addressed in Europe at different levels. The Member States are actively conducting R&D activities in the field of SSA, SEPP, and SIS to protect their space assets. These efforts are to be considered in a broader context, as a significant share of national budgets is being invested in European endeavours. ESA, acting as an intergovernmental body, is pooling such efforts under the umbrella of its SSA programme but also remains a proactive player in the field of SEPP and SIS. The agency's scope of action is also up for further interpretation, should the institution take on a more prominent role in these matters. Additionally, the European Union, as a supranational actor, is becoming increasingly involved in Space Security, as it operates its own constellations. Other policy developments indicate the EU's willingness to increasingly incorporate security policy considerations in its strategy and will likely take a more instrumental role in conducting security related projects for that reason.

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

4. Transatlantic Relations: State of Affairs

4.1 A Privileged Partnership

4.1.1 Relations between Europe and the United States

The singularity of transatlantic relations lies in their extraordinary steadiness throughout the decades. Since the United States has historic ties to Europe, transatlantic cooperation comes across as a logical follow-up of a long-shared history and value-based proximity between state subjects from North America and their counterparts in Europe. The emergence of close inter-regional bonds has a strong historical foundation and many formal and informal ties. Despite this internal strength, the relationship is presently facing turbulent political developments that are shaping the future development of the transatlantic partnership.

Exceptionally close transatlantic cooperation emerged as a consequence of broader political dynamics following the Second World War and related wartime and post-war developments. The current result is the many formalised cooperative frameworks between the partners on different shores of the Atlantic Ocean (on multiple political levels and across various sectors). Although diplomatic relations between the United States and European Union were established already in the early 1950s, the formalization of general political cooperative ties between the transatlantic partners took place only at the end of the 20th century. The following table summarises the relevant formal cooperative frameworks. Some other additional initiatives (such as TAFTA or TTIP talks) underline that the challenging nature of international collaborative efforts does not automatically lead any given initiative to a successful conclusion in a short timeframe.

Year	Item	Note
Since 1949	North Atlantic Treaty Organization	Political military alliance currently with 29 member states, based on the principle of collective defence.
1995	New Transatlantic Agenda	First official document of the two partners after the EU and CFSP were established in 1993 with the Treaty of Maastricht, calling for joint action in 4 thematic priorities.
1998	Transatlantic Economic Partnership	Initiative aimed at providing impetus for further transatlantic cooperation in the field of trade and investment.
2007	Transatlantic Economic Council	Formal body established to direct EU – U.S. economic relations, meets at least once a year.

Table 4: Selected formalised collaborative instruments in transatlantic relations

Interestingly, historical analysis of the transatlantic cooperation suggests that transatlantic ties have been going through periods of ups (reconstruction of post-war Europe, collapse of the Soviet Union, aftermath of 9/11 terrorist attacks…) and downs (Vietnam War, environmental agenda, current tensions…) relatively frequently. The cyclical nature of such developments calls for a proper evaluation of these trends with regards to the historical patterns. Following up on specific developments in several politically sensitive topics or particular events that have taken place over the last 60 years, it can be argued that fundamental aspects of transatlantic cooperation have not yet been fatally wounded by cyclical events of a deteriorating nature. The recent challenging developments within the realm of transatlantic relations have momentarily changed the overall perception of the state of play in general ties between the two sides of this partnership. Explicit recognition of Europe as a trade foe by the U.S. administration[157] or strong assertive criticism of allied defence spending and the future of military alliance[158] are developments that display unprecedented tensions.[159] Despite their unprecedented impact, the operational aspects of long-lasting EU-US partnerships (in particular in trade, defence or science

157 Trump calls European Union a "foe" of the USA on trade, Euronews, (July 15, 2018).
158 Trump presses Nato allies to lift defence spending to 4% of GDP, Financial Times (July 11, 2018).
159 On the other hand, some warming of relations have been recently recorded – a meeting between U.S. President Donald Trump and European Commission President Jean-Claude Juncker, on July 25, 2018, resulted in a declared ceasefire in U.S.-EU trade rules tensions.

and innovation) do not seem to be diminishing, and this conveys the important message of the stability of the transatlantic bonds.

Security and Defence

With regards to the security aspects of transatlantic ties, the primary platform of cooperation is the NATO framework in the form of a political and military alliance of 29 member states across the Atlantic in the northern hemisphere. Recently NATO has added more eastern European countries, thus forming an alliance with substantial regional reach within the European continent, it remains valid today as it adjusts to the new security environment with emerging threats coming from state as well as non-state actors. No other relevant multilateral transatlantic cooperative frameworks in security and defence (comparable in size and scope to the NATO) have emerged, though it is not rare to see European countries cooperate with the United States on a bilateral basis. Some smaller multilateral cooperative frameworks applicable in this section include the EU-U.S. Security and Development Dialogue since 2010 and a framework agreement on U.S. participation in EU crisis management operations signed in 2011. Recent developments in Europe could also lead to EU member states taking greater responsibility for security outside NATO-related mechanisms. It should also be noted, that for a few years NATO has been showing a dedicated interest in developing a formal approach to space capabilities, although it does not own or operate space systems and relies for these on member states.[160]

Economy and Trade

According to World Bank data, the combined nominal GDP of the United States and European Union represented 45,4% of global GDP in 2017[161] making the United States and the EU the two largest economic blocks in the world. Economic aspects of transatlantic relations date further back to the international trade of European states with the new Union formed on American soil in 1776 As a result of emerging and later continuing processes of globalization, economic ties in the transatlantic region have further deepened and widened. Trade statistics between the EU and the United States suggest historically close ties supported by the status quo, which showcase that from an EU perspective, the United States constitutes the largest export and second largest (after China) import partner for the EU28.[162] From the opposite perspective the overall picture is similar. The EU is the largest exporter of goods and services to the U.S. market and is the second largest import partner (also after China) of U.S. goods and services.[163]

4.1.2 Transatlantic Cooperation in Space

Europe and the United States also have a long history of cooperation in space, which has taken place at various levels, in different frameworks and – thematically – in a plethora of fields. According to the type of participating actor, cooperative frameworks can be divided into government, agency, and industry levels of cooperation. Concerning specific activities, the deepest ties of transatlantic space cooperation are traditionally to be found in activities such as space science and exploration (followed later by cooperation patterns in earth observation data sharing and the GNSS agenda). Cooperative agency-level undertakings in space science and space exploration have been present since the very beginning of the space era, and have been continuously reinforced over the last two decades as well, as evidenced by various formalised means of cooperation between ESA and NASA (Agreement on Future Cooperation from 2007,[164] Memorandum of Understanding on Space Transportation from 2009,[165] Sentinel Data Sharing Agreement from 2016)[166] or through specific programmatic cooperation on selected joint bi- or multilateral projects. Probably the clearest example (supported also by an intergovernmental agreement) is the International Space Station programme. The productive nature of transatlantic space cooperation is further documented by the collaborative nature of programs such as Rosetta, Cassini-Huygens, the Hubble Space Telescope, the Infrared Space Observatory (ISO), the Solar and Heliospheric Observatory (SOHO) and the International

160 For More information concerning NATO's approach to space see https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/624137/doctrine_nato_air_space_ops_ajp_3_3.pdf

161 For detailed data see https://data.worldbank.org/indicator/NY.GDP.MKTP.CD.

162 USA-EU - international trade in goods statistics, Eurostat, 2018. Retrieved from http://ec.europa.eu/eurostat/statistics-explained/index.php?title=USA-EU_-_international_trade_in_goods_statistics

163 European Union, Office of the United States Trade Representative, 2018. Retrieved from https://ustr.gov/countries-regions/europe-middle-east/europe/european-union

164 NASA and ESA Sign Agreements for Future Cooperation, NASA, (June 2007). Retrieved from https://www.nasa.gov/home/hqnews/2007/jun/HQ_07139_Paris_MOUs.html

165 ESA and NASA Sign Memorandum of Understanding on Cooperation in Space Transportation, European Space Agency, (September 14, 2009). Retrieved from http://www.esa.int/Our_Activities/Space_Transportation/ESA_and_NASA_sign_Memorandum_of_Understanding_on_cooperation_in_space_transportation

166 Sentinel Data Wanted, European Space Agency, (March 15, 2016), Retrieved from http://www.esa.int/Our_Activities/Observing_the_Earth/Sentinel_data_wanted

Gamma-Ray Astrophysics Laboratory (INTEGRAL). Future projected endeavours include among others the James Webb Space Telescope and joint Mars Sample Return campaign. Continuation of transatlantic space cooperation is further confirmed by recent budget statistics, which show a growing ratio of U.S. space programmes that include the participation of European subjects.[167]

EU-U.S. cooperation on Earth observation dates back to case-to-case assistance followed by a collaborative back-up framework (1989) between the NOAA and EUMETSAT, to provide coverage of the Atlantic Ocean and respective continents at times when the other party might not have or might temporarily lose such capability through its own systems. The EUMETSAT-NOAA partnership has remained relevant until the present day, through renewed agreements on joint projects and provision of access to data acquired by space systems of the other partner (e.g. Landsat, Copernicus). Following the GMES / Copernicus agenda evolution at the European level, the EU - U.S. agreement on the facilitation of sharing of Copernicus EO data was signed by the two parties in 2015.[168] A more operational agreement on a lower ESA – NASA / NOAA / USGS level was signed in 2016 (as noted above), this time with a particular focus on access to Sentinel data. The GNSS dimension of transatlantic space cooperation has been mainly involved two priority issues – interoperability, and access to service. With the emergence of European efforts to pursue an autonomous GNSS system, a transatlantic GNSS cooperation scheme was developed by the two parties in 2004, through an Agreement on the Promotion, Provision and Use of Galileo and GPS Satellite-based navigation Systems and Related Applications.[169] Galileo's initial services are fully interoperable with GPS and interoperability with GPS will be valid in achieving full operational capability by 2020. Besides creating end-user benefits (increased precision, availability of service), interoperability and access to signals leads to the increased resilience of GNSS capabilities.

Space cooperation between the EU and the United States has also been supported through diplomatic channels in the form of Space Dialogues between the two partners, which have been repeatedly taking place for more than a decade (the most recent – the 9th session – being in January 2018). Despite the prevailingly positive assessment of space relations between the USA and European partners (EU, ESA, individual countries) it should be noted that the cooperative framework is not all-encompassing and has occasionally gone through hardships (development of launchers, initial phases of Galileo development, cooperation with third countries, uncertainties of long-term support for certain programs and missions). These tensions have not significantly affected transatlantic space cooperation overall. As international cooperative efforts are naturally challenging endeavours, it is natural that they should struggle to overcome barriers in their pursuit. Some transatlantic cooperative efforts (both space and non-space related) have not been able to overcome these challenges, some, and arguably more, have concluded successfully. Space cooperation is usually protected from any deterioration in diplomatic relations. This can be seen in the example of the ongoing utilization of Russian RD-180 engines in U.S. Atlas V launch vehicle.

4.2 Security in Outer Space: A Mix of Arrangements

The issue of security in space is already one area of transatlantic space cooperation frameworks but remains limited by comparison to the rising stakes in this domain. Some areas of transatlantic space cooperation are not primarily concerned with security in outer space but inherently include activities that have explicit space security considerations – SSA data sharing contributing to the SSA capabilities across the Atlantic, GNSS interoperability, and access to service improving the resilience of the satellite navigation capabilities owned by either party.

An overview of the strategic positions of Europe and the United States concerning security in outer space highlights differences in vital interests in pursuit of cooperative frameworks relevant to security in outer space. Whereas the United States aims to maintain strategic superiority (dominance), supported by soft leadership and redundancy of capability through collaboration, the European approach largely reflects pursuit of autonomy and freedom of action, followed by expanding interests in maintaining its position as one of the global space powers, yet being unable to operate self-sufficient capabilities in space situational

167 Machay, M. and Hajko, V. (2015). 'Transatlantic space cooperation: An empirical evidence'. Space Policy, Volume 32, 2015, pp. 37-43, ISSN 0265-9646.
168 European Union and United States Sign Cooperation Arrangement on Copernicus Earth Observation Data, Copernicus, (20 October 2015). Retrieved from http://www.copernicus.eu/news/european-union-and-united-states-sign-cooperation-arrangement-copernicus-earth-observation-data
169 Agreement on the Promotion, Provision and Use of Galileo and GPS Satellite-Based Navigation Systems and Related Applications. (2004).

awareness supporting the security dimension of European space interests.

The matrix of actions, used in previous chapters (SSA, SEPP, SIS), also serves comfortably as a methodical benchmark in this chapter. Outlining specific cooperative frameworks should begin with SSA data sharing instruments and exercises between two partners, usually taking form of agreement between USSTRATCOM on one side and a European stakeholder (national – defence ministries, armed forces branches, intergovernmental – ESA, EUMETSAT), on the other. In space environment protection and preservation, the key evidence of transatlantic cooperation dates back to the end of the 1980s when the first bilateral meetings on space debris took place between NASA and ESA and later evolved into multilateral IADC platform. More recently, European countries, the EU in general and the United States have displayed complementary positions on international space governance efforts, such as a mutual interest in adoption of TCBMs and active participation in the long-term sustainability of outer space activities agenda. Concerning the space infrastructure security segment of the matrix, data sharing cooperation in earth observation and interoperability and mutual access to signals of GNSS systems have contributed to the resilience of service in these two critical capabilities. In addition to this, European countries and the United States participated in the adoption of international standards related to space activities under the auspices of the International Organization for Standardization and adopted specific measures concerned with security by design measures related to the ISS programme.

Security in Outer Space subdomain		**(Transatlantic) Diplomacy and cooperation frameworks** *Harmonise and coordinate space security efforts among stakeholders*
	Space Situational Awareness (SSA) *Monitor space environment threats*	Examples: • SSA Data Sharing Agreements of a bilateral nature • Compatible academic environment with favourable schemes for SSA related research
	Space Environment Protection and Preservation (SEPP) *Keep the space environment safe to operate*	Examples: • IADC Space Debris Mitigation Guidelines (guidelines modelled on EU / U.S. best practices) • Interest in TCBMs and space sustainability agenda
	Space Infrastructure Security (SIS) *Protect the space infrastructure from threats*	Examples: • Interoperability of GNSS systems and access to signals • EO data sharing cooperation • NASA – ESA cooperation on security by design concerning ISS programme missions • Participation of transatlantic actors in development of space-related ISO standards

Table 5: Transatlantic space security cooperation areas

4.2.1 Cooperation in SSA Data Sharing

Bilateral SSA data sharing agreements between the United States and its European (also non-European) counterparts constitute the primary instrument of transatlantic cooperation in space situational awareness. Additionally, several recurrent practical exercises at the operational level between transatlantic partners have taken place in recent years. By sharing interests in the need for protection of space infrastructure from threats and hazards of the near-Earth space, the incentive for information and data sharing is a natural logical step to improving capabilities to protect one's own space infrastructure.

The U.S. stance on SSA cooperation has evolved over time. The Commercial and Foreign Entities (CFE) Pilot Program formalised and streamlined the U.S. cooperation approach to SSA sharing in 2004 and was upgraded into a full-fledged SSA Sharing Program managed by the USSSTRATCOM in 2009.[170] The main U.S. objective of entering

170 The Secure World Foundation argues that the key motivation for this formalization in 2009, was the Iridium-Cosmos collision, which occurred in February 2009, see https://swfound.org/media/3584/ssa_sharing_program_issue_brief_nov2011.pdf

into these agreements was indeed to promote international security and safety cooperation among allies, encourage the transparency of outer space activities, and enhance the quality of the U.S. service delivery system. This policy envisioned the combined development of space doctrine with principles, goals, and objectives that opened the possibility of collaborative sharing of space capabilities in case of crisis or conflict. It sought to expand mutually beneficial agreements with key partners to utilise existing and planned capabilities that could improve the security of U.S. national space capabilities. Growth in the number of SSA sharing agreements in recent years is illustrated in Figure 9, below.

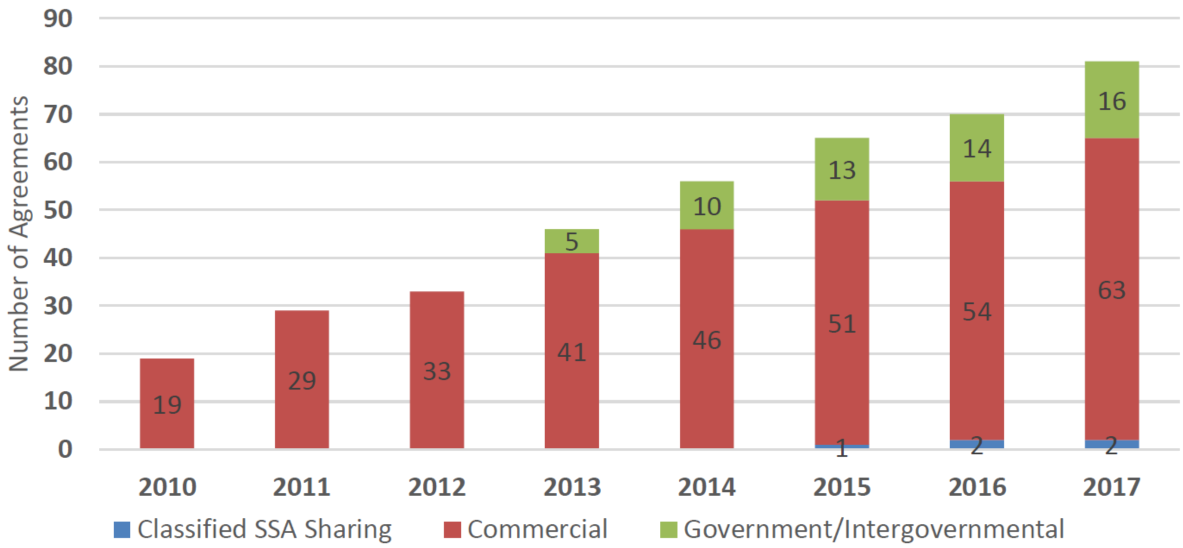

Figure 9: Data sharing agreements signed by USSTRATCOM (IDA)

As of October 2018, the U.S. Strategic Command manages the data sharing programme established through 19 (inter)governmental, 2 classified and more than 70 commercial (e.g. satellite operators or launch providers) SSA data sharing agreements.[171] The majority of agreements pursued at the government level were signed with European countries or international organizations, as seen in Table 6:7, below. Among the commercial actors participating in SSA sharing with USSTRATCOM, private European space companies (such as Eutelsat or SES) can be easily identified.

European Countries and Organisations (11)	Other Countries (8)
Belgium, Denmark, France, Germany, Italy, Netherlands, Norway, Spain, United Kingdom, ESA, EUMETSAT	Australia, Brazil, Canada, Israel, Japan, South Korea, Thailand, United Arab Emirates

Table 6: National SSA DATA Sharing Agreements of the U.S.

These SSA sharing agreements are essential for a number of European institutions and operators for the management of in-orbit operations. Given the limited SSA capabilities of European countries, the European approach to SSA has evolved into an international European effort. The dedicated SSA programme is run by the European Space Agency (which is more focussed on Space Weather and NEOs as member states have been rather hesitant in dealing with the national security considerations of SST through ESA)[172], under the EU umbrella. The SST consortium with so far 5 participating countries (France, Germany, Italy, Spain, UK) was established after the European Union launched the EU SST Support Framework in 2014. The history of cooperative space efforts in Europe created a good foundation for European countries to be eager to cooperate with their neighbours, on SSA. This

171 USSTRATCOM, Brazil sign agreement to share space services, data, USSTRATCOM, August 2018. Retrieved from http://www.stratcom.mil/Media/News/News-Article-View/Article/1607213/usstratcom-brazil-sign-agreement-to-share-space-services-data/

172 McCormick, C. (2015). Space Situational Awareness in Europe: The Fractures and the Federative Aspects of European Space Efforts, Astropolitics: The International Journal of Space Politics & Policy, Volume 13, 2015, Issue 1, ISSN 1477-7622

was further underlined by the critical importance of space in national and European policies. The latest European development, a proposal for a new Regulation of the European Parliament and of the Council establishing the space programme of the Union and the European Union Agency for the Space Programme,[173] presented by the Commission in June 2018, tackles also SSA, which has been now developed into a component of the space programme. Its multilateral nature – among European countries, but also through international cooperation with other countries, mainly the United States - has been clearly articulated in the text.

In recent years there has been an increased frequency of new SSA data sharing agreements between the United States and its European partners, which suggests deepening of SSA cooperation across the Atlantic. In general, lopsided capabilities between the U.S. and European space surveillance network give way to a rather unbalanced exchange of information and the approach to these agreements of the different partners follows different objectives. This exchange of information enables European countries to operate with more credible data and services to secure their space systems, while giving the United States some form of redundancy and duplicity of capability as a safety measure in case of disruption of this capability or where domestic coverage is considered inadequate. So, whereas European stakeholders approach SSA sharing agreements with a strategic interest in mind, fearing that their SSA capabilities would be seriously weakened should SSA sharing become unavailable, U.S. SSA capabilities do not rely that critically on data acquired through SSA sharing instruments.

As such, the USA does not need to approach international SSA sharing agreements with the same strategic concerns as European countries. From U.S. standpoint, the purpose of data sharing is to increase the transparency and visibility of space operations, promote cooperation in security, and improve the quality of American SSA information by gaining access to other databases.[174] Witnessing the 2009 Iridium-Cosmos collision served as a wakeup call, having realised that although global and relatively well developed, U.S. SSA capabilities were not able to predict this destructive event – there was no warning issued of a potential collision between the Iridium 33 and Cosmos 2251 before the collision.[175] Consequently, SSA sharing instruments have been recognised as having the potential to provide U.S. capabilities with an additional layer of threat detection, in case U.S. sensors fall short in detecting potentially dangerous in-orbit situations. A list of transatlantic SSA sharing agreements has been made publicly available by USSTRATCOM, and is provided in Table 7: 8, below.

173 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the space programme of the Union and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013, (EU) No 377/2014 and Decision 541/2014/EU, European Commission, 2018. Retrieved from https://eur-lex.europa.eu/resource.html?uri=cellar:33f7d93e-6af6-11e8-9483-01aa75ed71a1.0003.03/DOC_1&format=PDF

174 Helms, S. 2010. Space Situational Awareness. Power Point presentation for the United Nations Committee on Peaceful Uses of Outer Space (COPUOS). Retrieved from http://www.unoosa.org/pdf/pres/copuos2010/tech-01E.pdf.
175 Weeden, B. (2010). 2009 Iridium-Cosmos Collision Fact Sheet, Secure World Foundation. Retrieved from https://swfound.org/media/6575/swf_iridium_cosmos_collision_fact_sheet_updated_2012.pdf

European partners	Direct interlocutor	Identified benefits for USSTRATCOM	Nature of cooperation
Netherlands (2018)[176]	Royal Netherlands Air Force	Deepening of partnership with Dutch military, step *toward establishing international norms in the space domain*	Data sharing
Norway (2018)[177]	Norwegian Ministry of Defence	*Reinforcement and Protection of EO capabilities in the Artic*	Data sharing, Technical cooperation procedures
Denmark (2018)[178]	Defence Ministry of Denmark / Defence Command	Supporting Danish responsibilities in mapping in the Artic	Data sharing, Cooperation in sensors and platform development
Germany – MoU (2017)[179]	German Air Force	Liaison Officer (LNO) participating in general planning and mutual training opportunities, Member of the EU SST Consortium	Data sharing, promotion of mutual understandings
Spain – MoU (2016)[180]	Spanish Air Force	*Member of EU SST Consortium, host country of SatCen*	Data sharing
Belgium (2014)[181]	Belgium Federal Office for Science Policy	Supporting Belgium's space regulations	Data sharing
United Kingdom (2014)[182]	UK Royal Air Force	Exchange officer based at JSpOC,[183] Five Eye partner, Member of the EU SST Consortium	Data sharing
France (2014)[184]	French Ministry of Defence	*Interoperability with Graves systems, CAESAR*	Data sharing
ESA (2014)[185]		*Better insight over ESA's space operations*	Data sharing
EUMETSAT (2014)[186] **– in partnership with NOAA**		*Protection of EUMETSAT assets working in collaboration with NOAA on the Initial Joint Polar System*	Data sharing, scientific cooperation
Italy	Italian Ministry of Defence	*Member of EU SST Consortium*	Data sharing

Table 7: SSA Data sharing agreements between the USA and European countries

176 U.S. Strategic Command and Royal Netherlands Air Force sign agreement to share space services data, USSTRATCOM Public Affairs, (September 2018). Retrieved from http://www.stratcom.mil/Media/News/News-Article-View/Article/1647946/us-strategic-command-and-royal-netherlands-air-force-sign-agreement-to-share-sp/
177 U.S. Strategic Command and Norway sign agreement to share space services, USSTRATCOM Public Affairs, (April 2017),
178 USSTRATCOM, Denmark sign agreement to share space services, data, USSTRATCOM Public Affairs, (April 2018).
179 USSTRATCOM, German air force sign liaison officer agreement, USSTRATCOM Public Affairs, (June 2017).
180 USSTRATCOM, Spain sign memorandum to share space services, data, USSTRATCOM Public Affairs, (February 2017).
181 U.S. Strategic Command, Belgium sign agreement to share space services, data, USSTRATCOM Public Affairs, (February 2017).
182 DOD Signs Space Data Sharing Agreement with UK, USSTRATCOM Public Affairs, (September 2014).
183 U.S. Strategic Command Fact Sheet Joint Space Operations Center / 614th Air Operations Center, USSTRACTOM, (April 2018),
184 U.S. Strategic Command, France Enhance Space Data Sharing Agreement, USSTRATCOM Public Affairs, (April 2015).
185 USSTRATCOM signs Space-Data Sharing Agreement with ESA, USSTRATCOM Public Affairs, (October 2014).
186 USSTRATCOM enters into Space-Data Sharing Agreement with EUMETSAT, USSTRATCOM Public Affairs, (August 2014).

Based on this list and related sources, some observations about the nature of SSA sharing agreements in the transatlantic context can be made:

- The United States has pursued SSA Sharing agreements with countries that apparently have the most developed SSA capabilities in the European environment, all of the 5 participating countries in the EU SST consortium have signed bilateral SSA sharing agreements with the United States
- With the exception of Belgium, all other national SSA sharing agreements (excluding ESA and EUMETSAT) showcase either the defence ministry or armed forces office as a responsible counterpart for SSA sharing at the "European side" of each SSA sharing agreement. This underscores that although SSA-related R&D is often conducted at agency level (DLR, CNES…), operation of SST assets continues to be left mostly to military actors.
- Media releases by USSTRATCOM following signing of SSA sharing agreements traditionally highlight the importance of SSA sharing with the following quote: "The information is crucial for launch support, satellite manoeuvre planning, support for on-orbit anomalies, electromagnetic interference reporting and investigation, satellite decommissioning activities and on-orbit conjunction assessments."[187]
- Statements by USSTRATCOM also highlight that formalized agreements streamline the process of requesting information gathered by JSpOC.[188]This confirms the aforementioned assessment that the amount of data shared is somewhat imbalanced in favour of the provision of U.S. data / service to its international partners.
- SSA sharing agreements explicitly establish channels for direct information exchange. Additionally, they also open doors for future activities under the agreement framework, such as practical capacity-building oriented experiments, or cooperation in development of future (joint or individual but complimentary) SSA sensors or facilities.

USSTRATCOM's outreach and openness strategy is also beneficial in promoting mutual understanding in transatlantic relations. Senior officials from various countries have been visiting USSTRATCOM over recent years; a few examples include: French Commander Bernard Schuler in 2014, UK Royal Air Force Marshal Phil Osborn and German Army Brigadier General Dirk H. Backen, Roberto Vittori, ESA Astronaut, and the Air Force Brigadier General and ASI Head at the Italian Embassy in the United States In addition to bilateral forms of cooperation on SSA data sharing, USSTRATCOM has initiated the recurrent organization of SSA experiments and exercises with its international partners. Four such experiments have taken place so far, with the latest taking place in 2017 at the Lockheed Martin Facility in Virginia. European partners have participated regularly at these events. During the fourth SSA experiment in 2017, each participating nation maintained a space operations centre (SpOC) to command and control (C2) their respective SSA assets and experimented with fully integrated, notional Federation SpOC (FedSpOC) to demonstrate the value of a combined and integrated C2 capability.189 Scenarios in this exercise, as well as in previous exercises, included conjunctions, manoeuvres, breakups, and launches, as well as specific unusual events (all based on unclassified SSA data).190 Assessments of foreign military officials participating in these exercises and adjacent discussions and forums have highlighted the synergistic nature of such activities and best practices sharing opportunities including both tactical coordination and operational level activities (techniques, procedures, manoeuvres).[191]

Several challenges remain present when considering the future of transatlantic cooperation in space situational awareness. To start with, one can highlight that there is no standardization of international data formatting concerning SSA data.192 The reliance of European

187 E.g. http://www.stratcom.mil/Media/News/News-Article-View/Article/1497343/usstratcom-denmark-sign-agreement-to-share-space-services-data/ or http://www.stratcom.mil/Media/News/News-Article-View/Article/1607213/usstratcom-brazil-sign-agreement-to-share-space-services-data/

188188 DoD Agrees to Share Space Data with South Korea, U.S. Department of Defense, (September 2014), http://archive.defense.gov/news/newsarticle.aspx?id=123097

189 USSTRATCOM Hosts Fourth SSA Experiment with International Partners, USSTRATCOM Public Affairs, (October 2017). Retrieved from http://www.stratcom.mil/Media/News/News-Article-View/Article/1340856/usstratcom-hosts-fourth-ssa-experiment-with-international-partners/.

190 Schiff, B. (2017). Attaining Situational Understanding in the Space Domain, Amos Conference. Retrieved from https://amostech.com/TechnicalPapers/2017/SSA/Schiff.pdf

191 USSTRATCOM hosts space exercise with international partners, USSTRATCOM Public Affairs, (October 2016). Retrieved from http://www.stratcom.mil/Media/News/News-Article-View/Article/984307/usstratcom-hosts-space-exercise-with-international-partners/

192 As such, different stakeholders are using different formats for data used in SSA sharing, which makes effective SSA data sharing more complicated.

partners on U.S. SSA assets opens up the question of the completeness and resilience of U.S. data. The reliance of European stakeholders could also be easily assessed as dependence. Efforts to tackle this state of affairs have been continuously ongoing in Europe, most notably through the development of a dedicated EU SST support framework in a form of SST consortium. European stakeholders constantly present statements highlighting the importance of and need for SSA data sharing, with a prominent position in these endeavours being put on cooperation with the United States.

The new draft regulation, presented in June 2018 by the European Commission also reaffirms this notion, while at the same time fostering further development of European SSA capabilities, which should eventually lead to the development of an autonomous European catalogue of space objects. So far, no operational provisions regarding potential transatlantic cooperation in SSA sharing through the EU SST consortium have been introduced in Europe, though the new draft regulation clearly highlights the importance of international cooperative endeavours. For the time being, the state of European dependence on the United States in SSA remains valid. The sensitive issue of national SSA assets, such as common military ownership of SST sensors, brings another layer of insecurity into maintaining stable international SSA sharing efforts. The declared increased role of a civil actor – the U.S. Department of Commerce, is expected to enable the establishment of closer ties with commercial actors; its impact on SSA sharing with other countries cannot currently be evaluated since it is still in a process of reorganization.

The potential for further and deeper cooperation in the SSA domain is supported by generally favourable R&D environments for transatlantic cooperation in both the United States and Europe. Within the SSA, some cooperative endeavours that have included the participation of European and U.S. institutions have already displayed good results, such as the SOHO program for the Space Weather part of the SSA, or the planetary protection campaign PPOSS, ESA SSA's NEO Segment and the proposed AIDA mission in the NEOs domain. Late 2016 also witnessed a Space Weather and Critical Infrastructures workshop, an initiative funded by the European Commission's Joint Research Centre with the participation of U.S. and European experts to investigate the impact of extreme space weather on critical infrastructures. Within the NEOs segment of the SSA issue, national space agencies in Europe, together with ESA and NASA, have played a pivotal role in the work of the UN-mandated Space Mission Planning Advisory Group, a multilateral forum to discuss international responses to NEO threats.

4.2.2 Space Environment Protection and Preservation

The strategic concerns of the United States and Europe in this domain display more complementarity than in the previous section – predominantly a mutual interest in space debris mitigation. Still, it could be argued, that whereas the U.S. approach reflects strong national security considerations related to the need to protect its space systems, the European approach highlights the synergistic potential of space as an enabler in more economy-driven policies (agriculture, meteorology banking, transportation…). Both the US and Europe in this domain are concerned with soft leadership, reflecting the interests of both partners in promoting the importance of space sustainability, which effectively serves soft power-related aspects of regional policy objectives (pursuit of TCBMs, LTS agenda). A slight discrepancy can be observed in active debris removal technology development, on which Europe is placing a comparatively higher priority.[193]

Transatlantic cooperation on the coordination of the space debris problem established a foundation for the future creation of the Inter-Agency Space Debris Coordination Committee (IADC). NASA – ESA bilateral meetings on space debris starting from 1987 later evolved into a multilateral platform, first by including Japan and later through creating a dedicated platform in the form of the IADC. Although some other cooperative arrangements related to space debris were pursued at that time both by NASA and ESA, e.g. with Russia, the IADC has been a child of initially bilateral NASA – ESA coordination meetings on space debris mitigation. It was at the 8th of such meetings, in 1992 (which at that time already included the participation of Japan) that the need for a formalised multilateral platform was recognized, circulated for review and eventually approved.[194]

The IADC functions today as the most prominent international forum of governmental bodies for the coordination of activities related to

193 Weeden, B. (2017). US space policy, organizational incentives, and orbital debris removal, The Space Review. Retrieved from http://www.thespacereview.com/article/3361/1

194 Johnson, N. (2015). Origin of the Inter-Agency Space Debris Coordination Committee. Retrieved from https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20150003818.pdf.

the issues of man-made and natural debris in space,[195] with its main achievement being presented in the form of IADC Space Debris Mitigation Guidelines in 2002, which later served as a basis for the adoption of UN Space Debris Mitigation Guidelines in 2007. It can be argued that transatlantic models of Space Debris Mitigation served as a model for developing the IADC guidelines. In essence, partnership and coordination of efforts between the USA and its European partners led to the creation of mechanisms that transcended the transatlantic perspective and provided a useful tool on a universal level. The IADC continues its work on an annual basis.

The relevance of space debris mitigation efforts was strongly embedded in the recent pursuit of the Guidelines on the Long-term Sustainability of Space Activities (LTS) at the UNCOPUOS, resulting in the recently produced compendium of LTS guidelines.[196] The rationale of the LTS agenda brought together not just transatlantic partners – there was widespread approval of its necessity. Its relevance was strongly supported by the fact that the United States and several European countries took deep interest in its work plan and actively participated in developing the set of guidelines, thus providing a credible diplomatic foundation. More generally speaking, shared interests in pursuing space TCBMs over the last decade provide another example of space-security related cooperation in a transatlantic perspective. Similarly, even though most of these initiatives in addition to the LTS agenda, such as the Group of Governmental Experts on TCBMs in space, or support provided by the United States to the International Code of Conduct for Outer Space Activities, were pursued on a broader multilateral level, they deserve to be mentioned, as they all included noticeable transatlantic support.

4.2.3 Space Infrastructure Security

In terms of space infrastructure security two primary transatlantic cooperative patterns for advancing the concept of resilience of space systems are to be acknowledged (GNSS interoperability followed by access to signals, and EO data sharing). Additionally, some cooperative patterns between NASA and ESA on the International Space Station Programme (concerning programme security architecture of ISS utilization) and participation of transatlantic space actors in development of space-related standards under the auspices of the International Organisation for Standardization could also be highlighted.

The technical details of these cooperative frameworks in GNSS and EO suggest that the concept of resilience applies rather to the resilience of service than to the actual hardening of systems in a way that they have more capacity to withstand destructive effects. Through a cooperation agreement on Galileo and GPS, followed by more operational work on the basis of this cooperation, the EU and the United States were able to achieve a level of resilience, in which the negative consequences of service dropout of one's own system could be mitigated by reliance on continuous service provision from the other partner. Resilience is further supported through the different operational characteristics of each system, such as signal formats of frequencies, which make it impossible for a potential attacker to jam both with one single disruptive effort.[197] In such a case however, further work needs to be done on the end-user side to foster development of receivers able to process signals from both GPS and Galileo. Some of the technical and operative details of all possible scenarios, including access to restricted signals, have been areas with a limited level of formalised cooperation. The concept of service resilience applies to the EO satellites infrastructure. The most prominent in this regard is a long lasting partnership between NOAA and EUMETSAT, through joint projects and the provision of coverage when requested.

The inability of transatlantic partners to achieve consensus on U.S. access to Galileo's PRS signal over the last years, leaves the topic open for multiple possible future developments. At the same time, it casts a negative light on shared responsibility for this so far unresolved issue. On the other hand, both GNSS and EO cooperative frameworks do have the potential to affect global perspectives in their respective domains, such as through the initiative of the Global Earth Observation System of Systems[198] or collective efforts in achieving the benefits stemming from the Global Navigation System of Systems capabilities. The

195 IADC Space Debris Mitigation Guidelines, United Nations Office for Outer Space Affairs, (September 2017). Retrieved from http://www.unoosa.org/documents/pdf/spacelaw/sd/IADC-2002-01-IADC-Space_Debris-Guidelines-Revision1.pdf.

196 For the time being, LTS guidelines require further elaboration at the national level, since the 2018 session of the UNCOPUOS did not result in consensus with respect to the form in which the guidelines will be presented to the UN General Assembly.

197 Hein, G. (2006). GNSS Interoperability: Achieving a Global System of Systems or "Does Everything Have to Be the Same?", Working Paper, Inside GNSS. Retrieved from http://insidegnss.com/auto/0106_Working_Papers_IGM.pdf.

198 About GEOSS', Group on Earth Observations, (July 2018). Retrieved from https://www.earthobservations.org/geoss.php.

prominent position of European and U.S. actors in discussions conducted on these issues, together with the declared interest to pursue future GNSS compatibility and interoperability as well as EO data sharing on a global level, creates a credible force in efforts to find universal common grounds in GNSS compatibility and interoperability and Earth observation data sharing.

Concerning the International Space Station programme, this multilateral cooperation established in 1998 among five primary partners (NASA, JAXA, Roscosmos, CSA and ESA for 11 European participating governments) brought another form of transatlantic cooperation on issues related to security in outer space, this time within a broader multilateral effort. The model of work for ISS utilization is based on the Intergovernmental Agreement (IGA) from 1998. In addition to some safety obligations regarding the utilization of the station being anchored already in the IGA, in 2002 a charter was signed establishing a closer relationship between NASA and ESA payload safety panels concerning the ISS missions,[199] to foster closer collaboration and reduction of duplicities in payload safety review processes. Space infrastructure security stood also at the beginning of the ATV utilization, which emerged initially as a result of the Materials and Processes Reciprocal Agreement defining the process for selection and certification of materials used in the Space Shuttle and the International Space Station, signed between ESA and NASA in 2000.[200]

Both national as well as international standards are applicable to U.S. and European space stakeholders, who need to comply with them to be eligible to take part in space programmes in the United States or Europe. In the United States, NASA and DoD set different security procedures and standards applicable to space missions; in Europe, the European Cooperation for Space Standardization has been at the forefront of European space standards development. In addition to different national standards, the International Organisation for Standardization maintains a compendium of international standards applicable to security in outer space. Both the United States and European countries took part in the international working groups leading to the publication of these ISO standards.

199 Closer ties between NASA and ESA Safety Organisations, European Space Agency, (July 23, 2002). Retrieved from https://www.esa.int/Our_Activities/Human_Spaceflight/International_Space_Station/Closer_ties_between_NASA_and_ESA_safety_organisations.

200 Orlandi, M. et al. (2013). 'The role of ESA TEC-QTE in the ISS Safety Process', 6th IAASS Conference. Retrieved from http://iaassconference2013.space-safety.org/wp-content/uploads/sites/28/2013/06/0900_Orlandi.pdf.

5. Way Forward: Parallel Routes Towards Common Objectives

5.1 Comparative analysis of U.S. and European approaches

5.1.1 Different Policy Drivers

When comparing the U.S. and European approaches to security in outer space, a series of parameters should be considered:

- Strategy & Policy / Institutional organisation
- Operational implementation / Activities and Capabilities
- Commercial policy / Role of private industry; and
- Legal & Regulatory framework / International cooperation.

The following table presents a brief synthesis of the overall assessment resulting from the description made above of the respective space & security policy and operational frameworks on each side of the Atlantic. This comparative analysis is necessarily based on a simplified assessment of different concepts to capture key areas of convergence and divergence.

Parameter	United States	Europe
Strategy & Policy / Institutional organisation		
Strategy and ambitions	National security; Military superiority; Global leadership; Promotion of commercial market	Protection of economy and society; Meeting security requirements for services; Achieve autonomy
Organisational culture	Responsibility sharing among institutional actors (intricate decision-making process as a consequence of a a higher number of national actors); top down approach to military/civil domains	Loosely coordinated multiple levels of actors and decision-makers (national, intergovernmental, supranational)
Ongoing policy-making milestones	New national space security strategy; Initiation of a national STM policy, Initiation of establishment of the Space Force/Command within the DoD; Review of private space regulations	New regulation proposal by the EC (SSA component of the Space Programme; EU Agency for the Space Programme…); new Defence Space Strategies (UK & France); Greater coordination in security and defence policies under consideration
Operational implementation / Activities and Capabilities		
Capabilities	Self-sufficient (unmatched SSA capabilities, coverage to be complemented)	Reliance on non-European SSA data sources; Improvement of SSA capabilities expected as a result of a greater effort
Major undertakings	Improvement of SSA capabilities (various programmes, Space Fence); Expansion of SSA sharing agreements; Further integration of commercial capabilities	EU SST Consortium; Proposed SSA component of the Union Space Programme; EU Agency for the Space Programme (security accreditation across the Union Space Programme); National assets development; EU co-owned SST sensors
Key actors	Sharing of responsibilities between DoD and DoC (SSA/STM); Other national institutions (NASA, NOAA, FCC, FAA)	European countries (mainly MoDs with support from national agencies); EU and its agencies (evolving role under consideration: EC, EEAS, GSA, SatCen); ESA (capability-building)

Commercial policy / Role of private industry		
Private capabilities	Developing commercial activity in SSA data and related services	Mostly contractors (R&D projects, development and manufacturing)
Involvement of private actors	Congressional support for commercial endeavours;Mature technologies catering for operational defence needs; USSTRATCOM relationships with industry; Expansion of Office of Space Commerce within DoC	Repeated calls for more industry-led initiatives; Weak market dynamics for space security
Legal & Regulatory framework / International cooperation		
International initiatives	Active in international fora; Reluctance to enter legally binding international regulations; Agreement on pursuit of TCBMs	Active in international fora; Preference for pursuit of TCBMs; Ill-fated ICoC (possible upcoming renewed initiative); Supportive of binding international regulations
Domestic regulatory aspects	Existing regulatory framework in process of updating and reorganizing; Security protocols developed at operational level	National space legislations; Security accreditation in EU programmes; ECSS standards applicable at operational level
Views of transatlantic cooperation	Predominantly SSA data sharing: potential to complement and enhance domestic capabilities	Predominantly SSA data sharing: increasing political will to secure own infrastructure with domestic critical capabilities.

Table 8: Summary Table of U.S. and European approaches to Space Security

Key Takeaways

Based on the comparative analysis above, the overview of strategic considerations of security in outer space in the United States and Europe can be summarised as follows:

European approach: Synthesis	U.S. approach: Synthesis
The European approach to security in outer space builds upon a multi-layered institutional structure of European space activities, which creates a European governance model that can come across as difficult to fathom by external actors. Security considerations with relation to space were first initiated at national level, integrated within space programs of European countries. From the inception of their governmental space systems, Member States have set up national policies. Security in space gained significant attention at the international institutional level through the work of ESA and EUMETSAT, as well as at the top political level of the EU, following the recognition of strategic European interests in maintaining and operating space systems. Strategic concerns and the importance of space security are well acknowledged in key political documents adopted at EU level. Even though the nature of these space security related concerns still remains mostly civilian, the pivotal role of space as an enabler for other key policies such as agriculture, digital, or defence, is well understood. Further European integration calls for harmonisation and setting-up of a new governance model, which is complex since it implies sharing sensitive information and some transfer of sovereignty.	The U.S. approach to security in outer space is relatively more straightforward since supranational governance issues are not an area of concern. There is a stronger military dimension in space security issues, which is highlighted by the critical importance of space systems in foreign and national security policies. Security aspects of space activities have been leveraged in the United States for a longer period of time (in comparison with Europe) and have historically reflected the relevant position that space has had across various administrations. U.S. capabilities related to security in outer space largely outweigh those of other spacefaring nations including Europe as a single actor in space security. One recent trend suggests that the U.S. administration is more inclined to pursue a more commercially focused space policy and, notably in national security areas. Greater focus is also visible in rather assertive statements on the importance of space control, dominance and leadership in space, with variations in the wording depending on the incumbent administration. On the other hand, the importance of partnerships has also been stressed and appears to be a focal point in current U.S. Space Policy. A more prominent role of civil space actors in SSA data gathering and sharing is also expected.

Table 9: Overview of European and U.S. approach to security in outer space

It is clear that the mechanisms and drivers at work on both sides of the Atlantic for the definition and the implementation of respective space security policies greatly differ.

Nevertheless, both the United States and Europe are concerned by the emergence of new threats that might compromise their interests in space and on the ground. As a consequence, outer space security is gaining priority in respective civil and defence space agendas.

In this respect, despite the discrepancies highlighted above in the respective approaches to outer space security, many factors contribute to the expectation of a higher degree of convergence in these matters in the near and medium terms.

5.1.2 Shared Perception of a Growing Vulnerability

The United States and Europe share a largely common assessment of space security challenges ahead. However, given cultural differences ranging from strategic vision to operational considerations, they prioritize these challenges differently in their respective space policy frameworks, in particular in the civil and military segments of space activities.

As a consequence, this initial joint assessment leads to quite different concrete results in terms of a vision of the way forward. The need to recognize that potential misunderstanding will occur has to be understood and resolved.

5.1.3 Strong Reinforcement of the U.S. Space Security Policy

The U.S. National Space Policy prioritizes space security as a prerequisite for the protection of its national security. In this context, the U.S. approach to outer space security is driven, first and foremost, by the perception of a growing vulnerability of key national space assets. This assessment drives the need to protect space infrastructures against a number of risks, in particular military threats (e.g. ASAT, cyberattacks, and intentional interferences), and to prepare a tactical response. The proposal of President Trump to create a Space Force - a military organisation separate from the Air Force for the conduct of in-space military operations - is a symbol of this vision. However, although this proposal seems quite in line with the overall U.S. approach to space and security issues, it is raising a number of concerns and there is a vivid public debate at the moment around such option, which will ultimately be arbitrated by the Congress.

In parallel, the announcement of the national Space traffic Management initiative under the authority of the Department of Commerce is the civilian complement.

In fact, if at first glance the U.S. governance model displays a seemingly fully integrated structure, several interviewees stressed that U.S. bureaucratic processes can be intricate as a consequence of the multiplicity of engaged stakeholders. At this point in time, it is clear that there will be a strong military side in the United States concerning the on-going development of the various outer space security challenges. The balance that will be found with civilian options and the potential diplomatic implications are still to be determined.

5.1.4 Rising Sensitivity to Space Security Issues in Europe

In comparison, in Europe, public debates on outer space security issues are just starting and no consensus has emerged among policy makers to tackle them as short-term, pressing operational priorities.

European stakeholders are fully aware of the multiple challenges ahead but the European space security ecosystem remains complex and multi-layered, structured along a general principle of national leadership and sovereignty. The prominent place of security concerns in the EU strategy for space, the inclusion of the SST/SSA programme under the umbrella of the European Union, the achievements of the EU SST Consortium to pool resources and the multiple initiatives of ESA, are clear indications that these issues are now an integral part of the European space policy. However, priorities continue to differ between the various stakeholders, resulting in delays in actually translating the perception of vulnerability into concrete operational cooperative decisions addressing the full range of potential threats.

In this context, the announcement of the first UK and French Space Defence Strategies, as well as the latest statements of the German government, are strong signals. These moves highlight a change of attitude towards space security.

- The German Defence Minister Ursula von der Leyen has supported the forging of 'a common strategic culture for Europe'[201] and the German government has stated that the development of an 'independent

[201] German Governement. (2018). *Speech by Federal Minister of Defence Dr Ursula von der Leyen on the occasion of the opening of the 54th Munich Security Conference in Munich*. Retrived from: https://www.bmvg.de/resource/blob/22180/a4b7d92394e5ff6b7689c79cc71fa9d9/20180216-download-eroeffnungsrede-englisch-data.pdf. (16 February 2018).

space surveillance capacity of the EU' is key,[202] giving momentum to a bolder approach to European autonomy in this matter.

- The French Minister for Armed Forces, Mrs. Florence Parly, made the case for a space defence policy building on European cooperation in September 2018 when denouncing the behaviour of the Russian spy satellite Louch-Olymp orbiting around the French-Italian military telecom satellite Athena-Fidus.[203]
- In a similar vein, French President Emmanuel Macron has stated that 'European defence cannot be solely structured around relationships with the U.S' and that 'equilibriums, automatisms on which alliances were built [since the Cold War] must be revisited' - notably in the field of cybersecurity, chemical weapons, classical warfare, territorial conflicts, space security, and artic areas.[204] He has announced the establishment of a Defence Space Strategy to be ready by 2019.[205]
- UK Foreign Minister Gavin Williamson has announced the launch of a UK Defence Space Strategy.[206]

The rising political significance of space security could very well trigger a reassessment of European ambitions and accelerate the consolidation of the European approach to the issue across the different stakeholders (governance, objectives, architecture, and more).

5.2 A Fertile Ground for a Reinforced Partnership

5.2.1 State of Play: A Complex Mix of Arrangements

Current transatlantic relations in space security encompass a complex mix of dialogues and cooperation frameworks involving different U.S. and European stakeholders. They are organised through multiple channels, including:

- **Bilateral government-to-government channels:** these revolve predominantly around 11 data sharing agreements of USSTRATCOM with European countries and international governmental organisations (ESA, EUMETSAT). This model of cooperation is augmented by regular practical exercises for partner nations and liaison officers posted to the United States to work in close cooperation with their counterparts. Bilateral cooperation on other space projects (e.g. in space exploration or space science) beyond security in outer space can further foster transatlantic relations in outer space activities.
- **Europe-wide to U.S. channel**, which includes:
    - Permanent EU – U.S. Space Dialogue at diplomatic level (most recently held in January 2018 with the participation of various U.S. and European officials. (Space security was put forward as a major agenda item).
    - Case-by-case cooperation between U.S. and European organisations (e.g. NOAA/EUMETSAT, NASA/ESA) on specific programmatic topics: space exploration, remote sensing, meteorology and the ISS programme.
    - GNSS issues, concerning mainly EU – U.S. relations on the compatibility and complementarity of the GPS and Galileo systems. After initial U.S. concerns following the EU decision to proceed with Galileo development, both parties reached an agreement on GPS / Galileo interoperability in 2004, and continue to cooperate in satellite positioning, navigation and timing at bilateral as well as multilateral level. At the same time however, talks on U.S. access to Galileo's PRS have not yet been finalised given the sensitive nature of this issue.
- **Multilateral** channels**:** U.S. and European stakeholders have been displaying

[202] Deutscher Bundestag. (2018). *Deutschland gut in der Raumfahrtforschung.* Retrieved from: https://www.bundestag.de/presse/hib/-/566972.

[203] Le Monde. (2018). *La France accuse la Russie de tentative d'espionnage par satellite*. Retrieved from: https://www.lemonde.fr/international/article/2018/09/07/paris-revele-une-tentative-d-espionnage-russe-sur-un-satellite-franco-italien-en-2017_5351908_3210.html. (7 Septembre 2018).

[204] Le Monde. (2018). *Les orientations diplomatiques d'Emmanuel Macron : «sécurité» en Europe et «crise humanitaire» en Syrie*. Retrieved from: https://www.lemonde.fr/international/article/2018/08/27/europe-syrie-libye-macron-devoile-sa-feuille-de-route-diplomatique_5346644_3210.html. (27 July 2018).

[205] French Government. (2018). *Discours du Président de la République Emmanuel Macron à l'Hôtel de Brienne.* Retrieved from: http://www.elysee.fr/declarations/article/discours-du-president-de-la-republique-emmanuel-macron-a-l-hotel-de-brienne/ (13 July 2018).

[206] The Guardian. (2018*). Defence secretary unveils strategy to protect UK satellites*. Retrieved from: https://www.theguardian.com/politics/2018/may/21/defence-secretary-unveils-strategy-to-protect-uk-satellites (21 May 2018).

converging views and positions on space security at space-related international fora, such as UN COPUOS, Conference on Disarmament, IADC, ITU, Cospas-Sarsat, ICG, and others Mutual interest in pursuit of international space TCBMs was visible e.g. in the recent "long-term sustainability of outer space activities" agenda within the UNCOPUOS. The example of ESA – NASA cooperation on debris mitigation, which evolved from bilateral coordination meetings into a full-fledged multilateral platform in the form of the IADC, is particularly relevant here. Recently, NATO has expressed interest in further elaborating a proper space policy. At the moment, it fully relies on its member states when it comes to space capabilities and neither owns nor operates its own space assets.

- **Government-to-Industry and Industry-to-Industry cooperation**: This channel is becoming increasingly relevant in the wake of the expansion of private capabilities, in particular in the field of SSA. A number of USSTRATCOM SSA data sharing agreements with commercial operators (including European) illustrates this trend, as well as the case of the Space Data Association, a commercial operators' non-profit cooperation relying on governmental and private services to foster exchange of information and best practices concerning responsible space behaviour. Involvement of private industry in space security is bound to increase.

Despite these various successful collaborative frameworks, or maybe because of their multiplicity, no formal and inclusive framework has yet been established at political level between the United States and Europe. As a consequence, so far, transatlantic cooperation has been confined to a case-by-case-basis, and as far as outer space security is concerned, to bilateral, government-to-government agreements.

Several factors can explain the somewhat fragmented transatlantic cooperation framework. Among them, the dual and multi-layered organisational structure of both U.S. and European governance may very likely be a major obstacle to a more integrated approach. Indeed, while Europe still faces difficulties in translating stakeholders' positions into Europe-wide policies and programmes, interviewed U.S. officials also stressed that, although the integration of the U.S. line of command suggest a capacity to federate and coordinate on the U.S. side, decision-making still faces hurdles to align positions and interests of the different organisations and departments involved.

Overall, interviewed U.S. and European stakeholders and experts highlighted the following strengths and weaknesses of current transatlantic relations:

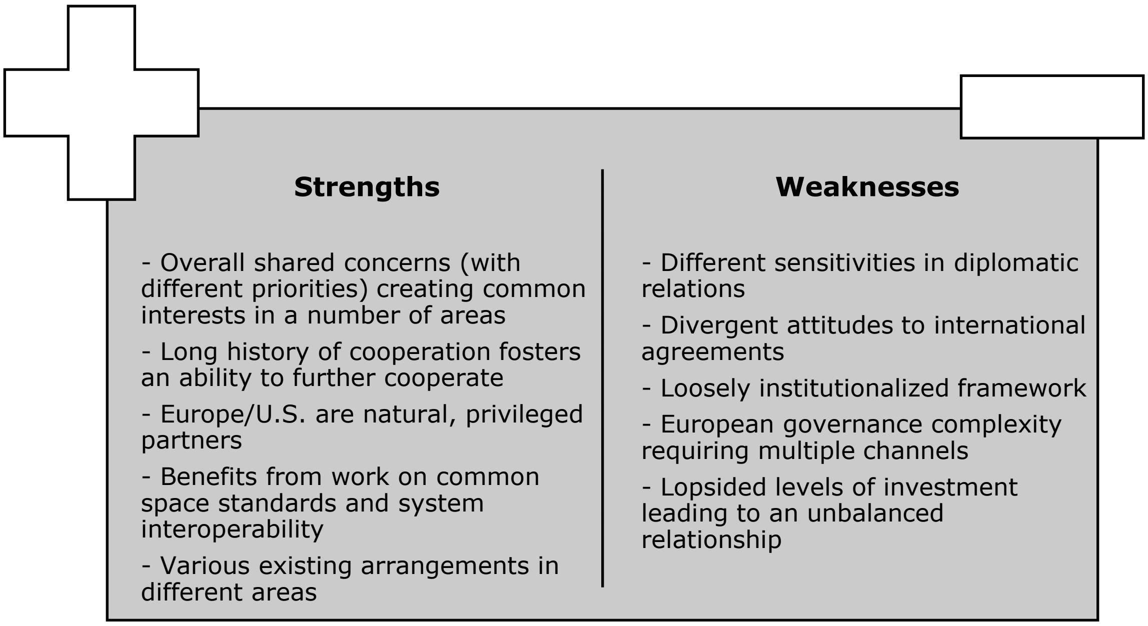

Figure 10: Interviewees' views on strengths and weaknesses of transatlantic cooperation

5.2.2 Towards Reinforced Cooperation Seeking Mutual Benefit

Interviewees uniformly underlined that establishing a more comprehensive and inclusive relationship, based on reinforced cooperation seeking mutual benefits, will require several preliminary steps:

- A joint assessment of the situation,
- Mutual understanding of each partner's priorities,
- Shared interest in cooperation based on mutual benefits,
- The capacity to converge on common objectives,
- A balanced contribution from the actors.

Notwithstanding these prerequisites, recent and planned developments in the field of space security policy on both sides seem to provide a fertile ground for the United States and Europe to broaden the scope of their current space-related relations and to consider what could be the drivers for a reinforced cooperation in space security:

- In the United States, the Space Strategy 2018 and Space Policy Directive-3 will profoundly alter the way space security is envisioned and organized across military and civil/commercial branches. Upcoming developments will have consequences for international partners. Beyond changes in arrangements, these developments also open up opportunities for new areas of cooperation such as Space Traffic Management.
- In Europe, the declared ambition to strengthen European autonomy in space security will result in an increase in resources for capacity-building and in the consolidation of the European approach. At the same time, expected further space policy and programmatic developments might encourage a fresh look at cooperation with third countries, in particular with the United States.

Opportunities offered by this changing environment for reinforced cooperation are discussed in more detail in chapter 5.3 below.

The future of transatlantic relations in space security will also be influenced by the development of general political and diplomatic relations between the United States and Europe. From this perspective, and although cooperation in space is usually unaffected by political ups and downs, transatlantic relations are currently experiencing a serious deterioration in a number of fields including security and defence. The implications of this deterioration in the domain of space security remain unclear at this stage.

Overall, interviewed U.S. and European stakeholders and experts highlighted the following opportunities and challenges for reinforced transatlantic cooperation in security in outer space:

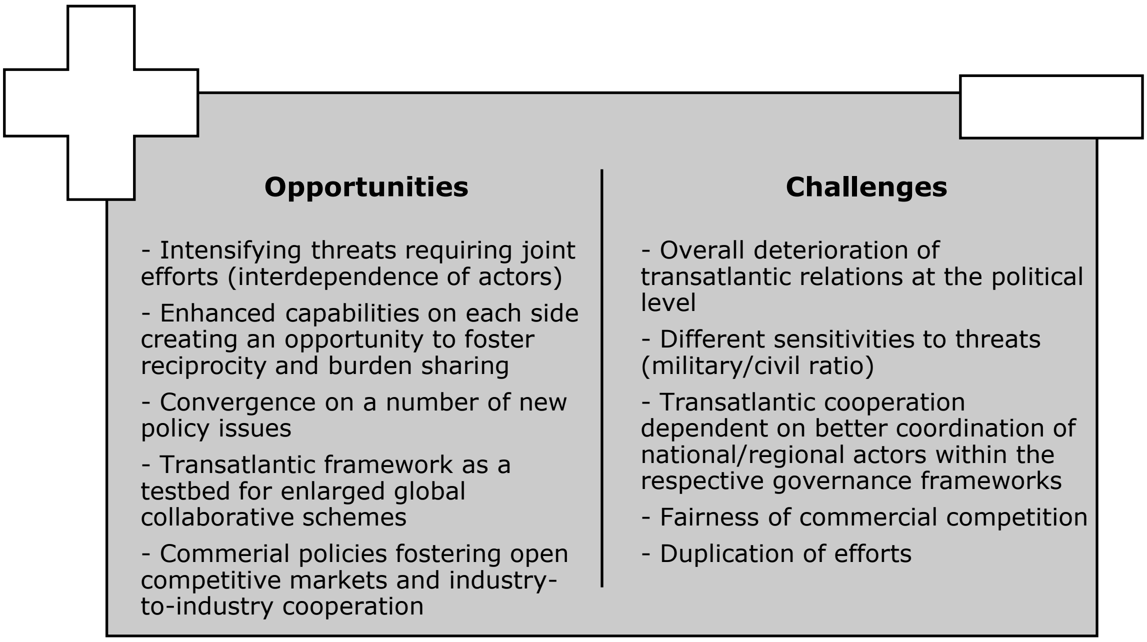

Figure 11: Interviewees' views on opportunities and threats for reinforcement of transatlantic cooperation

Operational implementation / Activities and Capabilities

The United States and Europe conduct activities in similar domains (SSA, SEPP, and SIS) but the current state of affairs including policy, resources, and capabilities, is strongly lopsided. As a consequence, the resulting imbalanced relationship impacts Europe's bargaining power in future potential negotiations, as well as its attractiveness for a reinforced partnership. While U.S. capabilities relevant to security in outer space (in particular SSA capabilities) are technically mature and designed for self-sufficiency (although coverage can always be complemented), European capabilities are still under development, both at national and European levels. Therefore, Europe still relies on U.S. SSA data and services for several of applications.

On the European side, SSA-related activities are mostly handled through dual use publicly owned and operated facilities, although no responsibility sharing scheme similar to that currently taking shape in the United States between DoD and DoC has been announced so far. At the same time, recent developments suggest an increasing role of the European Union in ownership and management of SST assets along the lines of the draft resolution submitted in October 2018 by the European Commission to its member states for the next Multi-Annual Financial Framework. Another illustration of this trend is the positioning of SatCen as the front desk for the distribution of information and services exploiting the SST data currently delivered by the Consortium.

In a nutshell, there are obvious discrepancies between the U.S. and European approaches to outer space security, as well as a strong imbalance in the level of resources allocated to such activities. However, recent trends from both shores of the Atlantic suggest a convergence on the assessment that outer space security requires additional efforts and resources, as well as a redefined institutional framework (Space Fence, Space Force, SSA component of the EU Space Programme). The conjunction of these factors might open a window of opportunity to consider the potential mutual benefits of closer transatlantic coordination / cooperation / collaboration in these matters.

Commercial policy / Role of private industry

Over the last few years, the U.S. private sector has been particularly active in developing the basis for a commercial offer for SSA services. Given the nature of activities to be performed, such as visualization, advanced computing, big-data analytics and Artificial Intelligence, the expertise of industry is envisioned to help leverage technical know-how in senior technologies to more effectively address quickly emerging space threats.

In addition, U.S. policy makers frequently stress the merits of making commercial options available as a means of globally improving the security of operations in orbit. Indeed, the present analysis confirms that U.S. industry has gained a high degree of maturity in the field of SSA data gathering and advanced exploitation through a growing number of SMEs and other legacy companies. In Europe, the number of private initiatives targeting this line of business is much more limited, partially owing to weaker domestic market dynamics and/or unclear perspectives regarding critical data policy.

In fact, SSA services are at the convergence of two key priorities of the long-established U.S. space strategy: space commerce and national security. As a consequence, the U.S. Congress has displayed great political support for these private initiatives, stressing the potential benefits from the expected higher efficiency of private management, as well as the will to support the competitiveness of the domestic industry. This materialised in particular in the creation of the Office of Space Commerce at DOC, which has no equivalent in Europe.

Legal & Regulatory framework / International cooperation

The United States and Europe share the vision that outer space security issues will be better addressed through pooling of resources, in particular with each other. A prerequisite for this is to be able to converge on some legal and regulatory provisions.

For the time being, the difference in the appreciation of the stakes related to space security, as well as the need to comply with the current overarching diplomatic framework, complicates the process of finding common grounds for balanced cooperation. Additionally, the international legal implications of such endeavour must be assessed against the provisions of the various national space legislations and strategies in Europe.

5.3 What Scope for a Reinforced Transatlantic Partnership?

5.3.1 Shifting U.S. Posture Towards National Leadership

The growing importance placed on security in outer space by the United States and Europe in their respective strategy and policy frameworks is based on the shared assessment that space infrastructures are exposed to increasingly serious security challenges. In an ever more congested and contested space environment, space security challenges are:

- ***Multiple and diverse*** in nature and origin and as a consequence require a coherent set of diverse preventive, operative and curative measures (i.e. holistic approach).
- ***Interrelated and interdependent,*** creating a situation of mutual dependence and responsibility between the different actors involved in space activities (countries, civil / military, public / commercial, agencies / industry…).
- ***Ubiquitous and inclusive,*** although the degree of exposure and vulnerability of space systems to specific threats (e.g. collision, cyberattacks, spoofing, jamming) may vary.
- ***Intensifying,*** driven by endogenous and exogenous trends including:
  - Increasing space activity in terms of the number of launches and objects in orbit but also the number of governmental and commercial actors operating space systems;
  - New concepts, technologies and capabilities (e.g. mega-constellations, miniaturized systems, in-orbit servicing);
  - An ever more connected space infrastructure to 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.

This situation, which is expected to further deteriorate in the future, ultimately creates risks for the economy, society and security at large.

With the recent adoption of Space Policy Directive 3 (i.e. National Space Traffic Management Policy), the United States made an important step forward in recognising the severity of issues at stake and the urgency of setting up a framework to prevent and mitigate space security threats. More specifically, the policy recognises that "the future space operating environment will be shaped by a significant increase in the volume and diversity of commercial activity in space" and that "as the number of space objects increases, [the current] limited traffic management activity and architecture will become inadequate."[207] In this context, the U.S. policy aims to "develop a new approach to space traffic management that addresses current and future operational risks."[208]

The new policy directive marks a shift in the U.S. posture and underlines a clear political willingness to accelerate activities through national-led engagements.

The policy does not necessarily challenge the relevance of multilateral efforts in space security. In fact, the policy recalls that "it is a shared interest and responsibility of all space-faring nations to create the conditions for a safe, stable, and operationally sustainable space environment",[209] recalling that a fully effective approach can only be envisioned as the outcome of a coherent and inclusive global effort. Notwithstanding, such a national-led approach can be understood as a reaction to the limited progress achieved at the international level on space security and sustainability topics. Indeed, the multilateral efforts in which both the United States and Europe actively participate (e.g. IADC space debris mitigation guidelines, Long-Term Sustainability guidelines, International Code of Conduct, Prevention of an Arms Race in Outer Space – PAROS…) are significantly slowed down by the recurring difficulty of making actors with diverging views and interests converge on necessarily constraining international measures.

5.3.2 Potential for Transatlantic Cooperation

No transatlantic collaboration at pan-European level can be envisioned in the field of the military activities that are currently being considered by the U.S. Administration in the field of Space Security. None of the partners would probably consider this as an option at this point in time.

[207] U.S. Government. (2018). Space Policy Directive-3, National Space Traffic Management Policy, (June 18, 2018).

[208] Ibid.

[209] Ibid.

On the civilian side, the establishment of a national Space Traffic Management framework is the next step implied in U.S. space security policy. If this example is followed by other countries, the development of multiple, possibly divergent, national and regional STM frameworks in parallel to international negotiations may occur.

The implementation of this U.S. policy, which will have consequences across the entire spectrum of preventive, operative and curative space security measures, has major implications for Europe and transatlantic relations, and is clearly the main driver for revisiting transatlantic cooperation in line with developments on the European scene.

5.3.3 Space Traffic Management: Stakes and Implications for Europe

The U.S. Space Traffic Management policy aims to tackle a number of security challenges related to the expected boom in space traffic, especially related to the deployment of mega-constellations and of non-manoeuvrable spacecraft (e.g. cubesats). With the aim of providing a structure for the control and management of in-orbit operations, STM is characterised by the development of a normative approach through "best practices, technical guidelines, safety standards, behavioural norms, pre-launch risk assessments, and on-orbit collision avoidance services".[210]

The development and implementation of a full-fledged Space Traffic Management architecture is a difficult task. Beyond intricate policy and governance aspects, STM involves the supervision of a complex chain of information/data to support operational decision making.

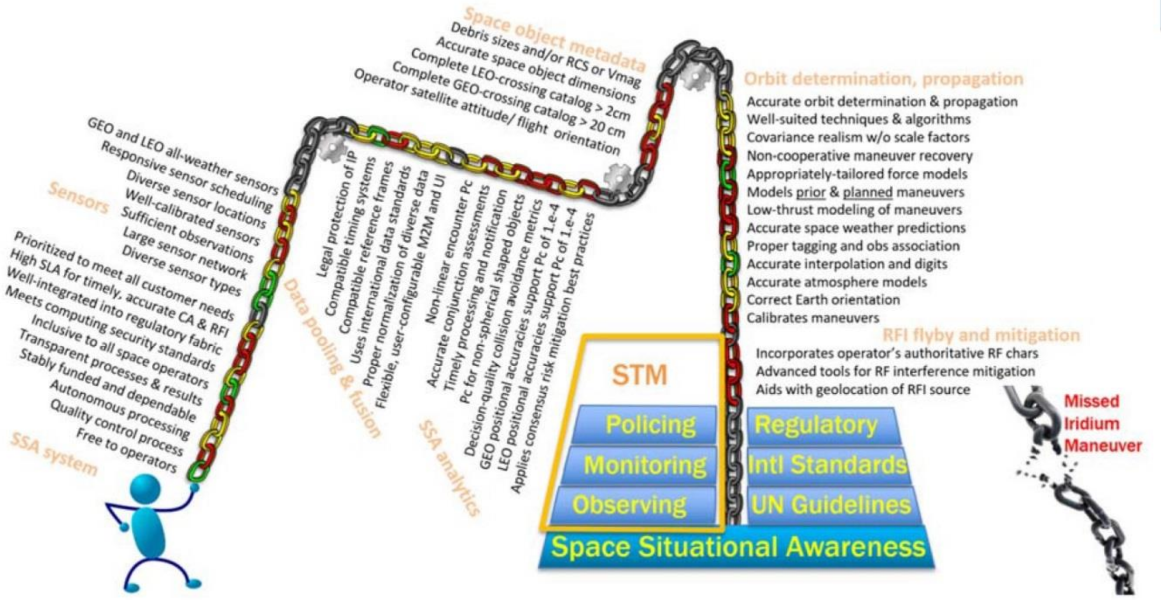

Figure 12: Portrayal of SSA data value chain for STM (Analytical Graphics)

More specifically, the development of an STM architecture raises the following major stakes:

- ***SSA data enhancement*** to reach the appropriate accuracy required to safely plan, coordinate, and synchronize in-orbit activities and mitigate collision risks;
- ***SSA data policy*** to set up appropriate information management structures (collection, fusion, distribution) safeguarding data integrity, reliance and confidentiality;
- ***Specification of STM best practicies and norms*** to enhance the safety, stability, and sustainability of operations in the space environment across different stakeholders (military, civil, commercial);

This study argues that transatlantic relations should be revisited and potentially reinforced along these lines taking into account the complementarity between political and operational cooperation frameworks.

[210] U.S. Government. (2018). Space Policy Directive-3, National Space Traffic Management Policy, (June 18, 2018).

SSA data enhancement and data policy

"Timely, accurate, and actionable data are essential for effective SSA and STM."[211] For this reason, the United States seeks to enhance SSA capabilities through the development of new sensors, the improvement of SSA data sharing (i.e. interoperability and greater data sharing) and the purchase of SSA data and services.

Enhancing SSA data precision and accuracy necessarily implies relying on multiple data sources including:

- National SSA data (based on domestic systems);
- SSA data from third parties (based on foreign/commercial SSA systems)
- Satellite operators' data (incl. satellite orbital parameters and manoeuvres).

Improving currently available SSA data through multiple data sources, or "crowdsourcing", will also bring new challenges related to data availability, reliability and integrity. Effective management of these issues will involve 1) a revisit of data sharing agreements with international and private partners and, 2) a clear policy for the integration of commercial SSA data and services.

The distribution of information to diverse stakeholders will also require establishing a robust data policy to ensure confidentiality across military and civil branches and between partners.

An essential aspect of this issue will be to delineate military and civil domains in terms of data access. Developments observed in the United States suggest that a top-down approach is currently the preferred option with the military branch in charge of domestic SSA capabilities and responsible for the establishment of a public catalogue corresponding to a subset of information and data available to them. In Europe, such a top-down approach enabling a delineation of military/civil domains has not been implemented, as so far, SST cooperation efforts have been mainly dedicated to networking national capabilities that are based on integrated dual frameworks.

Implications for Europe and transatlantic cooperation

- Data sharing agreements will remain the backbone of transatlantic cooperation. A revisit of these agreements towards more balanced cooperation for mutual benefit should be based on:
  - An enhancement of European SSA capabilities to close the capability gap and increase Europe's bargaining power;
  - A suitable balance between the desire for European autonomy and transatlantic complementarity in the prioritisation of European SSA capabilities development;
  - The progressive emergence of European leadership through the attribution of specific mandates to the European Union to lead SSA international cooperation;
- Enhanced data sharing will imply revisiting arrangements regarding data policy. This implies:
  - A compatible data policy;
  - Provisions to ensure the integrity of the data and address cyber threats;
  - Provisions to ensure the confidentiality of the data along a shared delineation of military/civil domains.
- Europe needs a clear policy to frame the role of the private sector as a key stakeholder in an integrated approach to SSA/STM. Beyond the involvement of private operators as providers and users of SSA data and STM services, such a policy should also address:
  - The integration of commercial SSA data in European capabilities and the necessary provisions to ensure effective data fusion;
  - The conditions to be met to enable the emergence of an open transatlantic market for SSA/STM-related data and services.

Specification of STM best practicies and norms

Switching from an informative to a normative approach to STM implies the specification of norms of behaviour through non-binding best practices, as a preparatory first step, and eventually through standards to be integrated in the regulatory regime governing space activities. From this standpoint, standards and best practices will have to be considered in a consistent manner encompassing preventive, operative, and curative measures across the full life cycle of space systems:

- Spacecraft and launcher design and manufacturing,
- Launch operations and separation,
- In-orbit operations,
- End of life and deorbiting.

[211] Ibid.

In this respect, the U.S. Administration intends to "support the development of operational standards and best practices to promote safe and responsible behaviour in space. A critical first step in carrying out that goal is to develop U.S.-led minimum safety standards and best practices to coordinate space traffic [...] and to use them to inform and help shape international consensus, practices, and standards." 212

Even though the United States will work on the development of a national approach, in coordination with its own industry, such an approach ultimately needs to be coordinated at international level to be fully effective given the strong interdependence between global actors.

In particular, it remains to be seen whether the ultimate goal of Space Traffic Management is the setting up of a centralised authority defining the details of avoidance manoeuvres to be implemented and directing the operators to execute them, or if it will be left up to the operators to define and implement the most appropriate actions.

Implications for Europe and transatlantic cooperation
• Europe must play a role in the development of best practices and standards that will shape a future international approach to STM to remain a key actor in the global space scene and to mitigate the competitive bias that such norms might create for industry. • To participate in the elaboration of STM norms, Europe must, at least, converge on its own approach to STM. This requires, as a first essential step, to set up a dedicated forum gathering all relevant European key stakeholders: EEAS, EU, ESA, member states, manufacturers, operators as well as military organisations. • The development of a set of common (or at least compatible) norms of behavior in space could form a second backbone for transatlantic cooperation.

5.3.4 General Conclusion

A global effort is necessary to achieve security in outer space. To be positioned as a key player in the international space scene, Europe must contribute its share to this endeavour. Much needs to be done on the European side to ensure balanced cooperation with other key players including, in particular, the United States.

An important near-term step for Europe is to define the desired degree of autonomy to be achieved and subsequently, to assess the means necessary to meet these requirements. This will also highlight the need to establish a European space security policy and to optimise the current intricate framework to foster coherence, cost-effectiveness and leadership. This is a matter of driving the emerging political will across European countries towards common views, joint objectives and rational responsibility sharing.

The rise of space security as a priority of U.S: and European space policies, respectively, and the changing political and operational environments on each side of the Atlantic create new opportunities to revisit the currently loosely organised transatlantic relations. On the European side, fostering reinforced transatlantic cooperation in space security, as intended by the Space Strategy for Europe, would require:

- Taking full advantage of the new opportunities offered by a more ambitious European effort in SSA. Also a desirable reinforcement of regional cooperation in this field is essential to improve Europe's bargaining power though:
  - Consideration of the added-value of European SSA capabilities for the United States (complementarity, resilience, interoperability) in European SSA capability-building roadmaps and data policies;
  - Fostering the emergence of European commercial actors able to compete/cooperate in an open transatlantic SSA market;
- Preparing a European approach to Space Traffic Managament. This implies, first of all, setting up a dedicated forum to coordinate the views, needs and possible contributions of different stakeholders such as the EU, ESA, member states, manufacturers and operators.

212 U.S. Government. (2018). Space Policy Directive-3, National Space Traffic Management Policy, (June 18, 2018).

Annex

A.1 European national strategies addressing space security in Europe

	France	Germany	Italy	United Kingdom	Spain
National space agency	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)

Table 10: European national strategies addressing space security in Europe

A.2 List of national space legislation enacted by European countries

Country Name	Document
Austria	Austrian Outer Space Act, in force since 2011
Belgium	Law on the Activities of Launching, Flight Operations or Guidance of Space Objects, 2015 (amended)
Denmark	Danish Outer Space Act of 2016
France	French Space Operations Act, No. 2008-518 of 2008
Germany	Satellite Data Security Act, 2007
Luxembourg	Law on the exploration and use of Space resources, 2017
Netherlands	Space Activities Act, 2007
Norway	Act on launching objects from Norwegian territory into outer space, No. 38, 13/06/1969
Sweden	Act on Space Activities (1982:963) Decree on Space Activities (1982:1069)
United Kingdom	Space Industry Act 2018 Draft Spaceflight Bill (in progress) Outer Space Act (OSA) of 1986

Table 11: List of national space legislation enacted by European countries

France

Although experimental, France operates the most advanced SSA system in Europe. The GRAVES radar (Grand Réseau Adapté à la Veille Spatiale) is under the responsibility of 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 2,200 orbiting objects. 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. Additional optical capabilities complement this list with, among others, the French systems SPOC (Système Probatoire d'Observation du Ciel), ROSETTE and TAROT (Télescope à Action Rapide pour les Objets Transitoires). The French SSA System draws on a number of sources including DoD data, the national catalogue Almanac, and inputs from satellite owners and operators. GRAVE is able to detect the presence of a satellite, a satellite manoeuvre, the launch of a new satellite, or the disappearance of one. For the last, the system is able to assess the ephemeris of space debris to determine their origin.

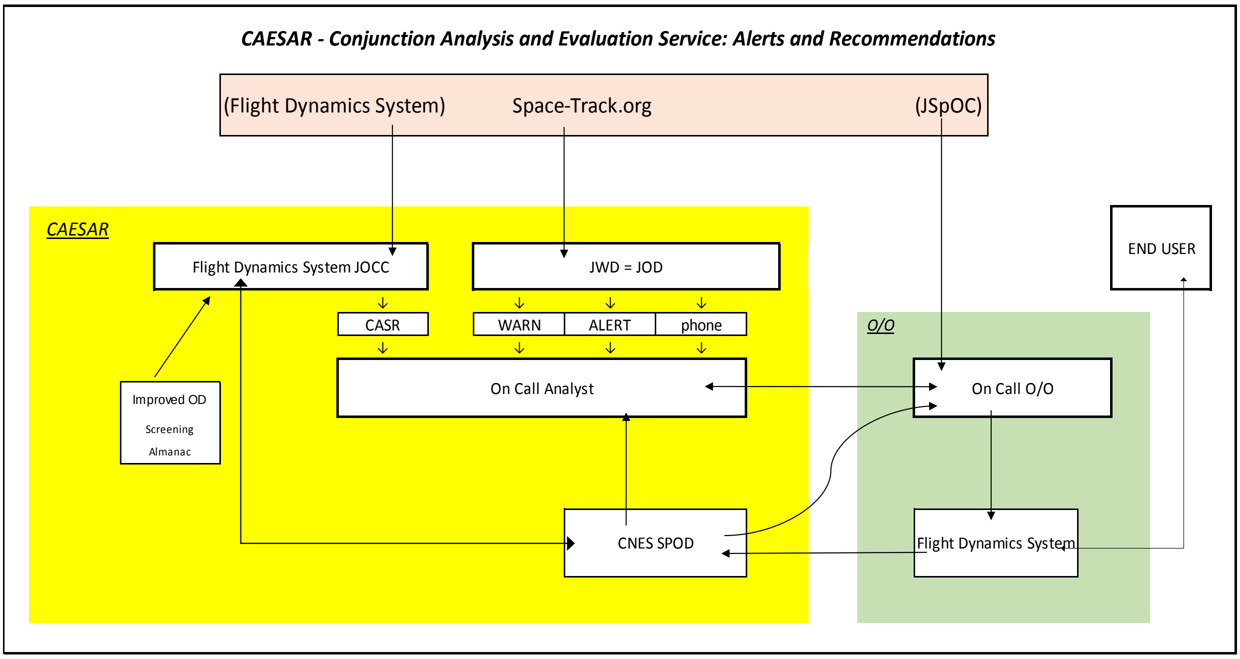

Figure 13: French CESAR process

At operational level, the Conjunction Analysis and Evaluation Service, Alerts, and Recommendations (CAESAR), processes flows of information and can autonomously generate the manoeuvres of the satellite for which they produce Conjunction Analysis (CA).[213] The software Java for Assessment of Conjunctions (JAC) contributes to the work of operational teams in charge of in-orbit collision risks. JAC is tasked to analyse close approach alerts and provide a synthetic vision of each close approach described by CDMs. The overall procedure is to evaluate the level of risk using own criteria. France also offers JAC Basic (support for CA) and JAC Expert (relying for CA). JAC Expert is used by Canada, the United States, Malaysia, and the UK. JAC Basic includes Canada, Japan, France, the US, Malaysia, South Korea, Indonesia, Germany. Spain, Luxemburg, Taiwan, Brazil, Qatar, the UK, Monaco, and Israel. The CS Communication and Systems in France offers software solutions on a variety of applications such as command and control, flight dynamics – now used by the French government - and on-board satellite software. The GRAVES system enables the French military to track satellites in LEO – of roughly the size of a micro satellite. Interestingly, the system can spot spy satellites, it is estimated that about 30 of them have been

213 IDA Report SSA Global Trends 2018: https://www.ida.org/idamedia/Corporate/Files/Publications/STPIPubs/2018/D-9074.pdf

identified – both Chinese and American. [214] Since 2016 the GRAVES system has been going through a modernisation phase for about € 20-30 million to address the weaknesses of the system.[215]

Germany

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 gives room for synergies with the French GRAVES system, as it contributes to the identification of spotted objects. Germany aggregates data from open sources, cooperation (through a USSTRATCOM data sharing agreement), civil organizations (e.g. ESOC), domestic sensors, military intelligence, and space weather reports, as shown in the following figure.

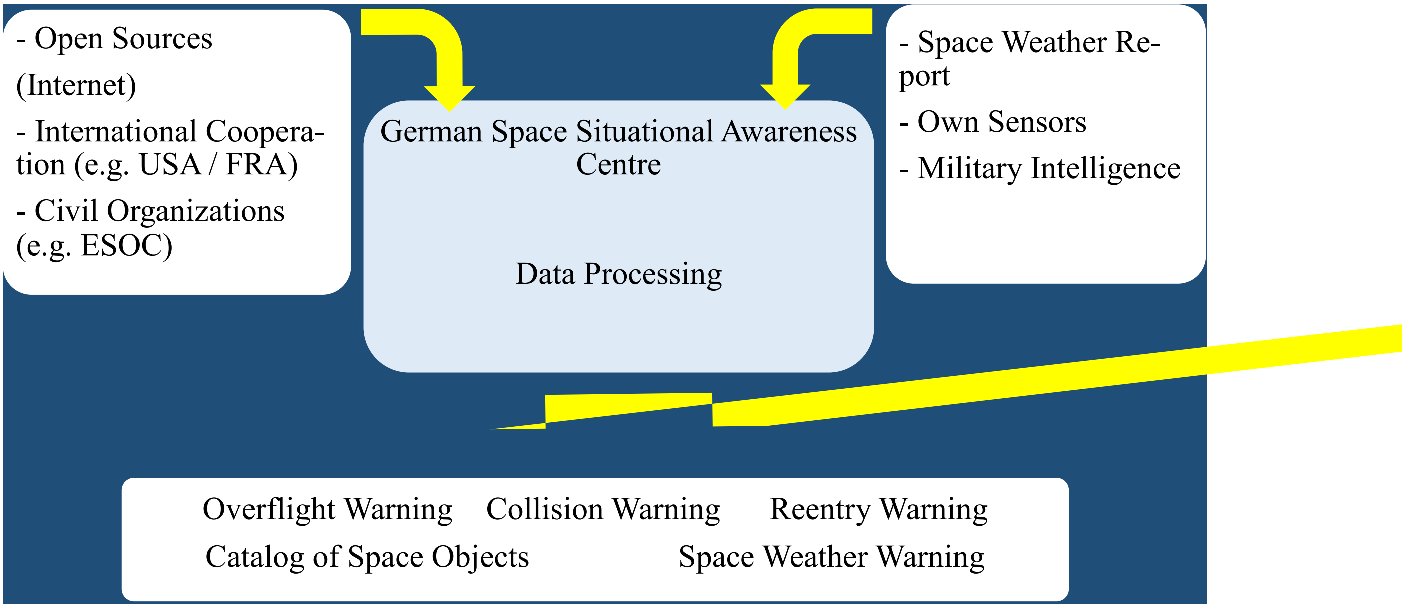

Figure 14: German SSA data processing

As far as software is concerned, the DLR's Institute for Simulation and Software Technology is developing a software framework for distributed computing for the Backbone Catalogue of Relational Debris Information (BACARDI) project using high performance computer technology. It is an informational system used to process sensor-derived data. In 2015, the German Space Situational Awareness Center (GSSAC) was set up to take the lead on SSA activities. Among other tasks, GSSAC will operate the new GESTRA system. GESTRA (German Experimental Space Surveillance and Tracking Radar) is the wide-range space surveillance project conducted by the Frauenhofer Institute for High Frequency Physics and Radar Techniques for the Space Administration of DLR.[216] The project consists of a new radar equipped with an electronically steerable antenna that is able to scan large areas of sky within milliseconds thanks to advanced semiconductor technology. GESTRA is also a mobile and portable system. The system is expected to become operational by 2019 and to be operated by GSSAC. GESTRA will create a catalogue of space debris present in near-Earth space (orbital heights up to 3,000 km). In 2011, the German Space Agency funded a small satellite project for € 15 Million to better monitor asteroids.[217]

214 ONERA. (2017).Retrived from: https://www.onera.fr/sites/default/files/.../pdf/.../20161212-CP-Graves-ONERA.pdf
215 Michel Cabirol. (2016) Surveillance spatiale. Retrieved from: http://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/surveillance-spatiale-la-france-modernise-le-systeme-graves-a-minima-602219.html
216 Andreas Brenner. (2018) GESTRA New space surveillance capabilities in Germany. Fraunhofer FHR. Retrieved from: https://www.fhr.fraunhofer.de/en/press-media/press-releases/gestra-new-space-surveillance-capabilities-in-germany.html
217 Frankfurter Rundschau. (2008) DLR will "kosmische Geschosse" besser aufspüren. Retrieved from: http://www.fr.de/wissen/astronomieraumfahrt/asteroiden-dlr-will-kosmische-geschosse-besser-aufspueren-a-1181242

Italy

In Italy, the Croce del Norte system, ASI's multistatic radar system, was built to detect debris and Near Earth Objects (NEO). The Italian Space Agency and the Ministry of Defence also developed the COSMO-SkyMed (Constellation of Small Satellites for Mediterranean basin Observation) radar satellite constellation orbiting at 620 km, which is made of four satellites.[218] From 2018 onwards, the next generation of satellites will be launched.[219] Although that system is designed for Earth Observation, the bistatic radar sensitivity is evaluated for both catalogued and uncatalogued objects in the surroundings of the COSMO-Skymed constellation. Other valuable SSA assets can be found in Italy, as summarized in the following figure:

SPADE (optical telescope)
(Matera – MT)

- Owner: ASI under installation at ASI/CGS, operated by e-GEOS.
- Performed Tests: GEO and LEO space debris campaign to support IADC research, made by "Univ. La Sapienza

(Matera – MT; Medicina - BO; Noto – SR)

- Owner: INAF/IRA (Medicina and Noto).
- Owner: ASI, Operated by e-GEOS (Matera).
- Medicina: space debris monitoring and NEO detection in bistatic configuration (As RX).
- Noto: Space Debris activities.

MLRO (Matera Laser Ranging Observatory)
(Matera – MT)

- Owner: ASI, operated by e-GEOS.
- Very precise Laser ranging for Satellites and Moon.
  Suitable for Precise Tracking applications. Not yet tested on uncooperative objects (Space Debris).

Figure 15: Italian SSA assets

Particularly noteworthy is the creation of SpaceDyS, a spin-off company of the Celestial Mechanics Group of the University of Pisa that develops SSA data-related software.[220] Among various services and products, SpaceDys offers orbital determination services for natural and artificial objects orbiting the Earth. The NEODyS website (Near Earth Objects Dynamics Site) provides daily data on the probability of impact monitoring.

Spain

In Spain, SSA's greatest assets are its telescope Fabra-ROA in Montsec and the La Sagra Sky Survey Telescope, both able to survey and track debris. Their telescopes feed the EU SST Consortium with SSA data. Spain recently invested € 20 Million in the development of a national Space Security system.[221] On the private sector side, it is noteworthy that the Spanish company Elecnor Deimos is also actively involved in SSA development across the three domains.[222] In the field of Space Weather, the company offers geomagnetic and solar indices archive and forecast, and atmospheric effect estimations.[223] In the field of SST, the company has built a complete product chain covering system simulations, sensor systems, image processing systems, space object operators, re-entry notifications, and identification of space objects. The system in charge of performing such missions is called Deimos Sky Survey, based in Puertollano. As far as asteroids are concerned, also referred to as Near Earth Objects (NEO), Elecnor Deimos is developing orbit determination and cataloguing capabilities. Prior to that, the company developed ESA's SSA CO-I NEO system requirements, contributed to the establishment of a NEO coordination centre, and performed analysis for ESA's P2 SWE X Project.

United Kingdom

In the UK, the British Chilbolton Facility for Atmospheric and Radio Research, operated by the Rutherford Appleton Laboratory, also supports the characterization of orbital objects thanks to a 25-metre steerable parabolic dish

218 e-Geos. (2018). *COSMO-SkyMed. Retrived from:* http://www.e-geos.it/cosmo-skymed.html
219 Corriere Comunicazioni. (2017). Cosmo-SkyMed pronto alla sfida "second generation." Retrived from: https://www.corrierecomunicazioni.it/cyber-security/cosmo-skymed-pronto-alla-sfida-secondo-generation/
220 http://www.spacedys.com/about-us/
221 La Moncloa. (2014) Spain invests 344.5 million euros in space programmes. Retrieved from: http://www.lamoncloa.gob.es/lang/en/gobierno/news/Paginas/2014/20141202-eu-space-agency.aspx
222 Elecnor Deimos Group. (2018). *What we do*. Retrieved from: http://www.elecnor-deimos.com/activities/space/
223 Elecnor Deimos Group. (2018). Space *Situational Awareness*. Retrieved from: http://www.elecnor-deimos.com/activities/space/space-situational-awareness/

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. The British PIMS (Passive Imaging Metric Sensor) uses a telescope at Herstmonceux in the United Kingdom, another in Gibraltar and a third in Cyprus, which have the potential to contribute to space tracking activities. Another valuable asset of the country –owned, however, by the United States - is the Ballistic Missile Early Warning System (BMEWS) operated by the Royal Air Force Base in Fylingdales. Questions have been raised about the possibility of getting data from that system for an independent European catalogue. CAMRa (advanced Meteorological Radar) and Starbrook are radar and optical sensors owned by UK civil and private entities but that may contribute to SST. In the field of space weather, the CIRCE project is studying the effects of space weather, notably ionospheric disturbances, on telecommunications.[224]

Summary

The following table summarizes European capabilities in the field of SSA:

Country	Data Collection	Data Processing	Data Products	OCM
UK				
France				
Germany				
Italy				
Spain			?	
Poland				
ESA SSA				
ESA SST				

Data Collection
- No data collection
- One or more sensors, not used for SSA
- Building/using or planning one or more sensor(s)
- Domestic sensor capability or sharing
- Actively involved in sharing with one or more countries

Data Processing
- No data processing
- Doing or planning to do some data processing
- Processing in-house data with outside capabilities
- Has full in-house processing capabilities

Data Products
- No data products
- Deliver products based on 18th SPCS data
- Can deliver value-added products, but still reliant on outside data
- Can independently deliver products

- No recent revisions
- Recently Revised
- Establishing
- Under Revision
- n/A

Table 12: European capabilities in the field of SSA

The overview of European SSA capabilities shows a true disparity, also among the Members of the EU SST Consortium. This is to be explained by different national strategies and political motives, and different levels of investment. The EU SST Consortium pools national capabilities under the same umbrella, however it appears clear that European SSA capabilities are far from sufficient for meeting European countries' operational needs. SSA development strategies are different depending on each country, with some countries, such as France, pushing for independence and other countries that are leveraging their optical and radar capabilities to play a role in Space Security. This heterogeneity of interests is challenging at governance level as it brings up the question of how to harmonize them and put synergies in place between different strategies. Ultimately, the level of autonomy the European Union wants to achieve, which still needs to be defined, will depend on the level of investments it is willing to commit. Cooperation will, however, still play a vital role for European stakeholders, especially taking into consideration the evolving nature of the space environment.

224 Berenice Baker (2018) A journey through space and time: the UK's space programme. Retrieved from: https://www.airforce-technology.com/features/journey-space-time-uks-space-programme/

A.4 Overview of European and U.S. activities in security in outer space

The following tables, based on the ESPI security in outer space matrix, provide a list of European and U.S. activities and measures related to 'Security in Outer Space' organised by domain and field of action. These lists are 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*	• 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 States SST systems development and upgrade	• Compliance with space objects registration obligations and procedures	• SSA data sharing agreements
	Space Environment Protection and Preservation (SEPP) *Keep the space environment safe to operate in*	• 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)	• National space legislations in European Member States (e.g. end-of-life obligations)	• Contribution of ESA and national space agencies to IADC and vote on space debris mitigation guidelines • European Union proposal for an International Code of Conduct for Outer Space Activities • Contribution to COPUOS 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*	• EU FP7 and H2020 grants (research into reducing the vulnerability of space assets, security of space assets from in-orbit collisions) • Development of technologies, standard and procedures by a variety of stakeholders (ESA, national space agencies, commercial operators, industry and non-space governmental actors)	• 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)	• Collision avoidance procedures and coordination with foreign agencies and operators

Table 13: European actions and measures related to 'Security in Outer Space' (ESPI)

Security in Outer Space subdomain	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*
Space Situational Awareness (SSA) *Monitor space environment threats*	• Space Surveillance Network (SSN) • Space Fence • Hallmark • OrbitOutlook • NOAA's Space Weather Prediction Center • NASA's Solar and Heliospheric Observatory • NASA Center for Near Earth Object Studies	• Space objects registration obligations and procedures • STM framework development • Space Policy Directive-3 • Policy for Space Weather Events • National NEO Preparedness Strategy and Action Plan	• SSA data sharing agreements • Space-Track.org • NASA Space Weather missions partnerships • NOAA-EUMETSAT data exchange • Emergency notification service • DoC front office
Space Environment Protection and Preservation (SEPP) *Keep the space environment safe to operate*	• Linked technologies development (e.g. Restore-L) • NASA's Restore-L, RRM3 and Raven • NanoRacks and Orbital ATK	• Space law (e.g. end-of-life obligations) • Standards for space environment-friendly satellite design (e.g. passivation devices) • Government Orbital Debris Mitigation Standard Practices • SPD-2 and 3 licensing process	• IADC Space Debris Mitigation Guidelines
Space Infrastructure Security (SIS) *Protect the space infrastructure from threats*	• Security enhancing technologies development (e.g. secure links) • Security-by-design know-how • Advanced security and technology development in the frame of military programmes • Development of optical beam technology	• Space programme security rules and procedures • Security standards • Supply chain control processes (e.g. export/import rules, testing procedures) • Supply-chain management guidelines • DoD Information Assurance requirements	• Strategic partnerships with commercial firms • Develop international processes

Table 14: U.S. actions and measures related to 'Security in Outer Space' (ESPI)

A.5 Organizational chart of U.S. security in space in the Executive branch

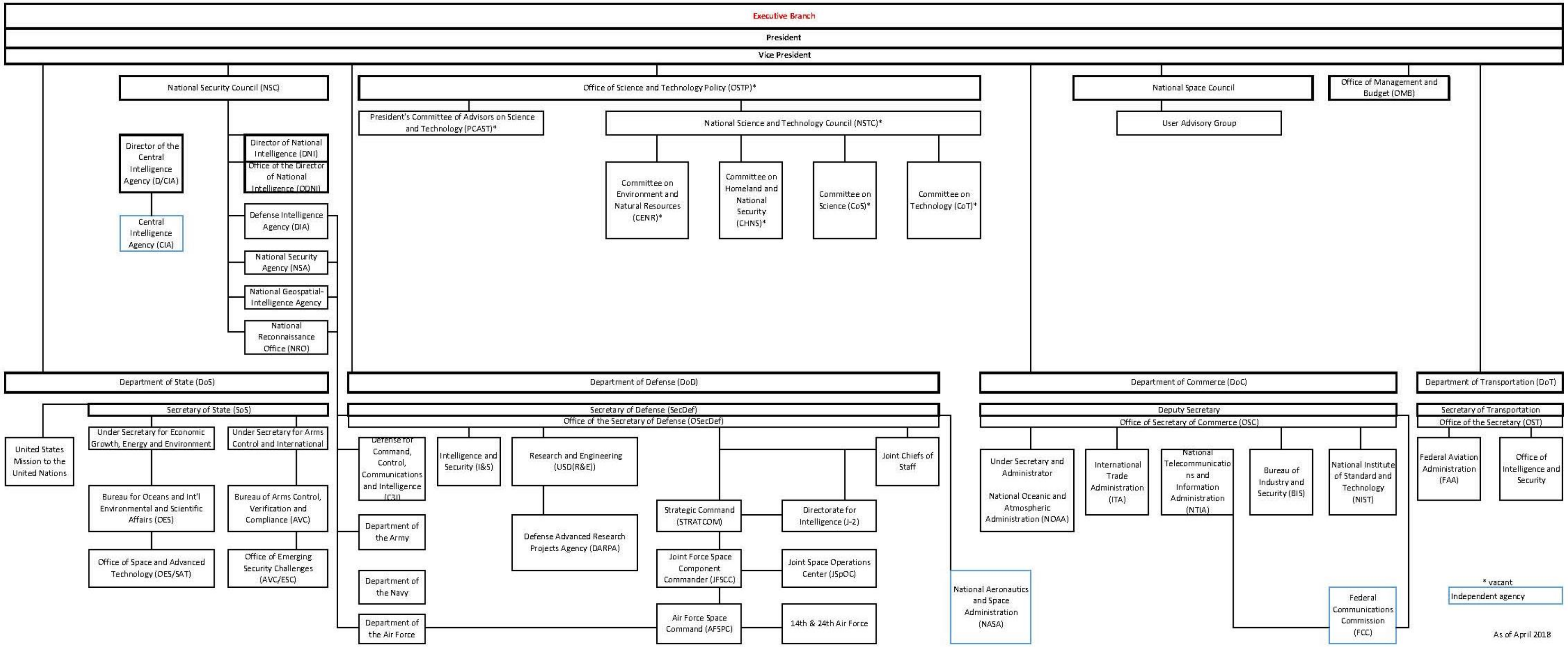

Figure 16: Organizational chart of U.S. security in space in the Executive branch (ESPI)

A.6 Authority and role of departments as defined by the SPD-3

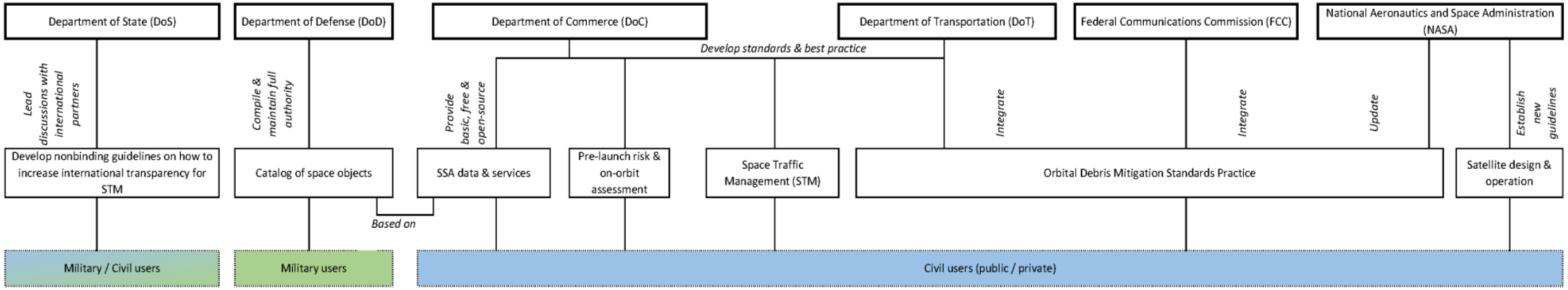

Figure 17: Authority and role of departments as defined by the SPD-3 (ESPI adapted from SPD-3)

A.7 List of Interviewees in the United States

Name	Position	Organisation
Michael Gleason	Senior Policy Analyst	Aerospace Corporation
Daniel Oltrogge	Director, Centre for Space Standards and Innovation	Analytical Graphics
Jeffrey Trauberman	Vice President of Space, Intelligence and Missile Defense (Ret.)	Boeing
Jonathan Margolis	Acting Deputy Assistant for Science, Space and Health	Bureau of Oceans and International Environmental and Scientific Affairs
Frank Rose	Lead Researcher	Brookings Institution
Constanze Stelzenmüller	Cooperation Lead Researcher	Brookings Institution
Richard H. Buenneke	Senior Space Policy Advisor	U.S. Department of State
Kenneth Hodgkins	Director of Space and Advanced Technology	U.S. Department of State
David Koplow	Lecturer	Georgetown University Law
Henry Hertzfeld	Director and Professor	GWU's Space Policy Institute
John Logsdon	Historian and Professor	GWU's Space Policy Institute
Benjamin Corbin	Research Fellow	IDA Science & Technology Policy Institute
Reina Buenconsejo	Research Fellow	IDA Science & Technology Policy Institute
Bhavya Lal	Research Fellow	IDA Science & Technology Policy Institute
Asha Balakrishnan	Research Fellow	IDA Science & Technology Policy Institute
Marina Hague	Research Assistant	Innovative Analytics & Training
Kevin O'Connell	President and CEO	Innovative Analytics & Training
Joe Pelton	Executive Board Member	International Association for the Advancement of Space Safety
Chirag Parikh	Office Director	National Geospatial-Intelligence Agency
Scott Pace	Executive Secretary	National Space Council
John Giles	Senior Policy Advisor	National Space Council
Victoria Samson	Head of Washington Office	Secure World Foundation
Brian Israel	General Counsel	Planetary Resources
Timothy Stryker	Outreach and Collaboration Branch Chief	USGS Land Remote Sensing Program

Table 15: List of Interviewees in the United States

A.8 List of Interviewees in Europe

Name	Position	Organisation
Jens Utzmann	Project Manager in Security in Space	Airbus Defence and Space
Willsch Klaus-Peter	Chairman of the Aviation and Space Group	Deutsches Bundestag
Ruben Wright	Head of SSA	Deimos Space UK
Jean-Luc Bald	First Secretary for space	European External Action Service
Florent Mazurelle	Space and Security Coordination Officer	European Space Agency
Denis Moura	CNES Delegate to SatCen	European Union Satellite Centre
Regina Peldszus	Co-Chair, DLR Delegate	European Union SST Consortium
Jean-Francois Bureau	Head of Institutional Affairs	Eutelsat
Gustav Lindstrom	Director	EU Institute for Security Studies
Jean-Marie Bockel	Chairman of the Interparlamentary Space Group	French Senate
Xavier Pasco	Director	Foundation for Strategic Research
Gerarld Braun	Head of SSA Department	German SSA Center
Nayef Al-Rodhan	Director	Geneva Centre for Security Policy
Jana Robinson	Space Security Program Manager	Prague Security Studies Institute
Jean-Claude Traineau	Director for Space	ONERA
Florent Müller	Programme Manager	ONERA
Norbert Paluch	CNES representative	European representatives
Micheline Tabache	ESA representative	European representatives
Marc Jochemich	DLR representative	European representatives

Table 16: List of Interviewees in Europe

List of Acronyms

Acronym	Explanation
A	
ACCORD	Alignment of Capability and Capacity for the Objective of Reducing Debris
AEOLDOS	Aerodynamic End-of-Life De-Orbit System
ADR	Active Debris Removal
AFFECTS	Advanced Forecast For Ensuring Communications Through Space AFFECTS
AFRL	Air Force Research Laboratory
APT	Advanced Persistent Threat
ARMOR	Advanced Radar for Meteorological and Operational Research
ASI	Agenzia Spaziale Italiana (Italian Space Agency)
ASAT	Anti-Satellite
ATMOP	Advanced Thermosphere Modelling for Orbit Prediction
B	
BMEWS	Ballistic Missile Early Warning Sys-tem
C	
CAMRa	Chilbolton Advanced Meteorological Radar
CAP	Common Agricultural Policy
CARA	Conjunction Assessment Risk Analysis
CESAR	Conjunction Analysis and Evaluation Service, Alerts, and Recom-mendations
C2	Command and Control
CD	Conference on Disarmament
CDAOA	Commandement de la Défense Aérienne et des Opérations Aériennes
CFE	Commercial and Foreign Entities
CFP	Common Fisheries Policy
CFPS	Common Foreign & Security Policy
CNES	Centre Nationale D'Etudes Spatiales (French Space Agency)
CNEOS	Center for Near Earth Object Studies
CONOP	Concept of Operations
COSMO-SkyMed	Constel-lation of Small Satellites for Mediterranean ba-sin Observation
ComSpOC	Commercial Space Operations Center
UN COPUOS	United Nations Committee on Peaceful Uses of Outer Space
COSPAR	Committee on Space Research
CIRCE	Climate Change and Impact Research
CIKR	Critical Infrastructure and Key Resources
CSDP	Common Security and Defence Policy
CSMs	Conjunction Summary Messages

Acronym	Explanation
D	
DEW	Direct Energy Weapons
DAMIEN	Detecting and Mitigating the Impact of Earth-bound Near-Earth Objects
DARPA	Defense Advanced Research Projects Agency
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
U.S. DoT	United States Department of Transportation
DSTL	Defence Science and Tech-nology Laboratory
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
EISCAT	European Incoherent Scatter Scientific Association
ESA	European Space Agency
ESC	Expert Service Centre
ESEC	Space Security and Education Centre
EU	European Union
EUMETSAT	European Organisation for the Exploitation of Meteorological Satellites
EU SST	European Union support framework for Space Surveillance & Tracking
F	
FAA	Federal Aviation Administration
FedSpOC	Federation SpOC
FCC	Federal Communications Commission
G	
GDP	Gross Domestic product
GEO	Geostationary Orbit
GESTRA	German Experimental Space Surveil-lance and Tracking Radar)
GGE	Group of Governmental Experts
GNSS	Global Navigation Satellite System
GRAVES	Grand Réseau Adapté à la Veille Spatiale
GSMC	Galileo Security Monitoring Centre
GTRA	GNSS Threat Response Architecture
GVA	Gross Value Added
GOVSATCOM	Governmental Satellite Communications
GSA	European GNSS Agency

Acronym	Explanation
GSSAC	German Space Situational Aware-ness Center
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
INTEGRAL	International Gamma-Ray Astrophysics Laboratory
ITU	International Telecommunications Union
ISO	Infrared Space Observatory
ISS	International Space Station
J	
JAC	Conjunction Analysis and Evaluation Service, Alerts, and Recom-mendations
JFSCC	Joint Force Space Component
JspOC	Joint Space Operations Center
L	
LEO	Low Earth Orbit
LWS	Living With a Star
M	
MEO	Medium Earth Orbit
MFF	Multi-annual Financial Framework of the European Union
N	
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NEO	Near Earth Objects
NEODyS	Near Earth Ob-jects Dynamics Site
NDS	National Defense Strategy
NFP	No First Placement of Weapons in Outer Space
NOAA	National Oceanic and Atmospheric Administration
NSpC	National Space Council
NSS	National Security Strategy
NSSS	National Security Space Strategy
NSTC	National Science and Technology Council
O	
OSCE	Organization For Security and Co-operation
ODMSP	Orbital Debris Mitigation Standard Practices
O2	OrbitOutlook
O/O	Owner/Operators

Acronym	Explanation
ONERA	Office National d'Etudes et de Recherches Aérospatiales (French Aerospace Lab)
P	
PAROS	Prevention of an Arms Race in Outer Space
PIMS	Passive Imaging Metric Sensor
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
PRS	Public Regulated Service
PSSI	Prague Security Studies Institute
QoS	Quality of Service
R	
RFI	Radio Frequency Interferences
R&D	Research and Development
RFW	Radio Frequency Weapons
RPO	Rendez-vous and Proximity Operations
S	
SAB	Security Accreditation Board
SAFE	Space Situational Awareness and Framework for Entity
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
SpaceDebEMC	Space Debris Evolution, Collision risk and Mitigation
SPD	Space Directive
SPOC	Système Probatoire d’Observation du Ciel
SPR	Strategic Space Portfofio Review
SOHO	Solar and Heliospheric Ob-servatory
SSA	Space Situational Awareness
SSN	U.S. Space Surveillance Network
SST	Space Surveillance and Tracking
S&T	Science and Technology
STM	Space Traffic Management
SWAMI	Space Weather Atmosphere Model and Indices
SWE	Space Weather

Acronym	Explanation
SWIFF	Space Weather Integrated Forecasting Framework
SWPC	Space Weather Prediction Cemter
SWORM	Space Weather Operations Research and Mitigation
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
UNCOPUOS	United Nations Committee on the Peaceful Uses of Outer Space
UN-SMPAG	United Nations Space Missions Planning Ad-visory Group
U.S.	United States
USGS	United States Geological Survey
USSTRATCOM	U.S. Strategic Command
W	
WG-LTS	Working Group on the Long-term Sustainability of Space Activities

Research Advisory Board

An Advisory Board was established to provide guidance for this study and to provide expert perspectives on key findings of the research team. More specifically, the Advisory Board contributed to:

- Validating the study findings at the end of the interview phase;
- Providing expert perspectives throughout the research;
- Discussing elements and conclusions proposed by the research team;

The Advisory Board was composed of the following members:

- Dr. Henry Hertzfeld: Director, Space Policy Institute.
- Dr. Xavier Pasco, Director, Fondation pour la Recherche Stratégique;
- Dr. David Koplow, Director of the Aerospace Security Project, Georgetown University;
- Dr. Brian Israel: General Counsel, Planetary Resources;
- Dr. Jana Robinson, Space Security Program Manager, Prague Security Studies Institute;
- Dr. Gustav Lindstrom, Director, European Union Institute for Security Studies;

The research team would like to express its sincere gratitude to the Advisory Board members for their insightful contributions to the study and useful guidance throughout the writing of the report. Their support was instrumental to shaping the project and brought fresh perspectives both for the report itself and potential follow-up projects.

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 George Washington University Space Policy Institute

The George Washington University Elliott School of International Affairs, a world leader in research, graduate study, and informed discussion related to issues of science, technology, and public policy, established a Space Policy Institute in 1987. The Institute conducts research, offers graduate courses and organizes seminars, symposia, and conferences on topics related to domestic and international space policy.

More information on the GWU SPI is available online: https://spi.elliott.gwu.edu/

About the Authors

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

- Marco Aliberti, Senior Research Fellow
- Martin Sarret, Research Fellow
- Tomas Hrozensky, Research Fellow
- Lisa Perrichon, Research Intern
- John Rowley, Research Intern

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