Version 1.0
2 November 2021

EURODEFENSE
Space Observatory

Initial Paper

Introduction

Space systems have become critical enablers for a wide variety of applications which are of paramount importance to the functioning of national and regionally/globally integrated economies, as well as the operations of Armed Forces. As a result, not only has investment in their development become a priority, but also their security from natural or accidental threats (space weather, space debris), and from deliberate threats as part of military action or general counterspace efforts of a hybrid nature (information manipulation etc.). This non-paper presents a series of arguments to inform and support a deliberative process regarding the formulation of recommendation on the part of Eurodefense to the European and National authorities on this subject. It aims to a be a descriptive, not prescriptive document.

What does space mean to Europe?

The growing capabilities of space in fields such as remote sensing, navigation, positioning and timing and communications have spawned a vast array of applications and services that have permeated European society and have become embedded in economy, security and administration. This has happened because of their role in command, control, coordination and data gathering for complex systems, whether we are talking about global logistics, integrated power grids or military operations.
Space systems have become critical assets and components of wider critical infrastructure systems in every field identified by the European Union and its Member States. They serve an important coordinating role and, in time, they may serve as the upper layer of command and control for all infrastructure systems, despite the global inequality when it comes to access to space. We can even say that, in accordance with the latest European documents of reference, space systems themselves are critical infrastructures providing essential services and, maybe one day, also goods[1]. Figure 1 illustrates what just one space system, a Global Navigation Satellite System like the European Galileo, the American Navstar, the Russian Glonass and the Chinese Beidou, mean to an advanced society.

[1] Georgescu, A., Gheorghe, A., Piso, M.-I., Katina, P.F. (2019), "Critical Space Infrastructures: Risk, Resilience and Complexity", Topics in Safety, Risk, Reliability and Quality, Seria 36, eBook ISBN 978-3-030-12604-9, DOI 10.1007/978-3-030-12604-9, Hardcover ISBN 978-3-030-12603-2, Series ISSN 1566-0443, Springer International Publishing

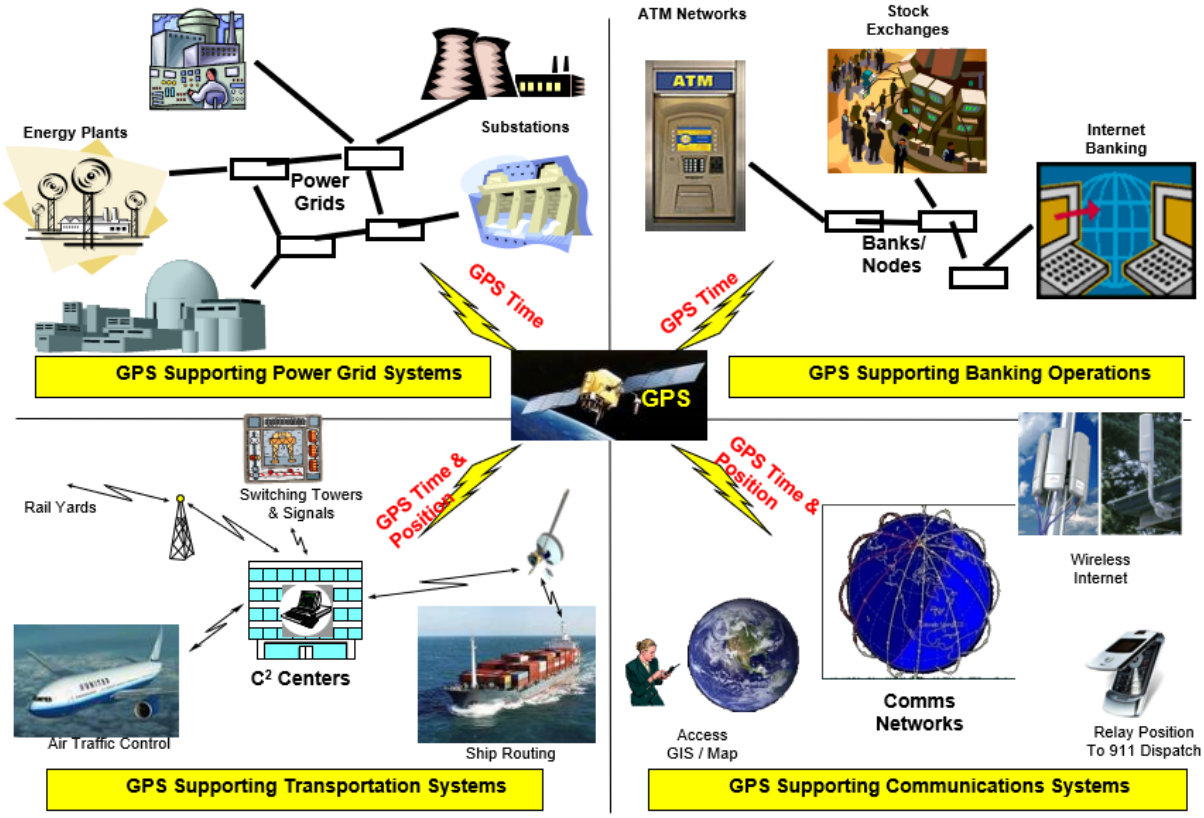

Figure 1. GNSS applications in four fields[2]

The Organisation for Economic Co-operation and Development noted that the world is entering a fifth stage of space development, one in which we are witnesses to "growing uses of satellite infrastructure outputs (signals, data) in mass-market products and possibly for global monitoring of treaties (land, ocean, climate), third generation of space stations, extensive mapping of solar system and beyond thanks to new telescopes and robotic missions, new space activities coming of age (e.g. new human-rated space launchers, in-orbit servicing)"[3]. At the same time, "space inputs permeate many of the products (tangible and intangible) that we consume, which are the result of extensive global supply and production chains or of the processing of information and the combining of symbols within globalized networks"[4].
Figure 2 also serves to illustrate the variety of applications developed through space capabilities.

[2] R. James Caverly, "GPS Critical Infrastructure Usage/Loss Impacts/Backups/Mitigation", 27.04.2011
[3] OECD (2016) Space and innovation. OECD Publishing, Paris. https://doi.org/10.1787/9789264264014-en
[4] Georgescu, A. (2020). "Critical Space Infrastructures - new perspectives on space policy". In Kai-Uwe Schrogl (ed.) (2020), "Handbook of Space Security: Policies, Applications and Programs", pg. 227-244, Springer International Publishing, ISBN 978-3-030-23209-2

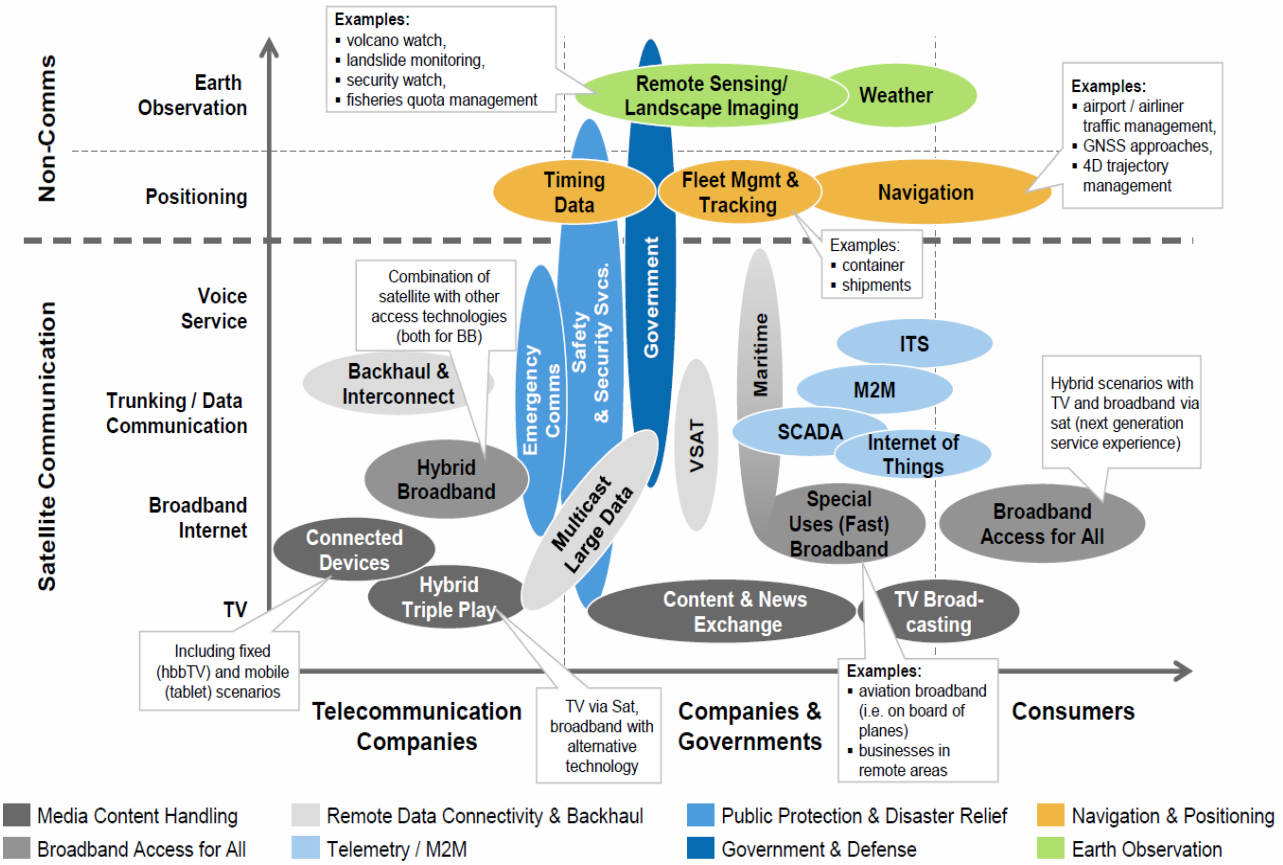

Figure 2. Applications of satellite systems[5]

The global space economy is an increasingly important source of asymmetric advantage for wealthy and innovative countries, but also a means for catch-up growth for developing countries. The Organisation for Economic Co-operation and Development defined it as "the full range of activities and the use of resources that create and provide value and benefits to human beings in the course of exploring, understanding, managing and utilizing space. Hence, it includes all public and private actors involved in developing, providing and using space-related products and services, ranging from research and development, the manufacture and use of space infrastructure (ground stations, launch vehicles and satellites) to space enabled applications (navigation equipment, satellite phones, meteorological services, etc.) and the scientific knowledge generated by such activities. It follows that the space economy goes well beyond the space sector itself, since it also comprises the increasingly pervasive and continually changing impacts (both quantitative and qualitative) of space-derived products, services and knowledge on economy and society"[6].
Bryce Aerospace and Technology, an American consultancy, calculated that the global space economy was worth 366 billion euros in 2019, including research, basic science, manufacturing,

[5] Acker, O., Pötscher, F., Lefort, T. (2013) Why satellites matter. The relevance of commercial satellites in the 21st century – a perspective 2012-2020. Booz & Company, Italy, https://www.esoa.net/Resources/Why-Satellites-Matter-Full-Report.pdf
[6] OECD (2019). The Space economy in figures: how Space contributes to the global economy. OECD Publishing, Paris, available at https://doi.org/10.1787/c5996201-en

launch services and the commercialization of services produced through space system operations[7], as seen in figure 3. The rate of development of the global space economy exceeds the rate of growth for the world itself, attesting to the growing demand for space services. This is also illustrated by a London School of Economics study regarding the multiplier effect of investment into space, which is between 5 and 12 depending on sub-domain, meaning that every euro invested produce 5-12 euro in additional economic activity[8].

The OECD report also cites various estimates by investment firms: "A 2018 report by the investment firm Goldman Sachs predicted that the space economy would reach USD 1 trillion in the 2040s, while a different study by Morgan Stanley projected a USD 1.1 trillion space economy in the 2040s. A third study by Bank of America Merrill Lynch has the most optimistic outlook, seeing the market growing to USD 2.7 trillion within the same timeframe"[9].

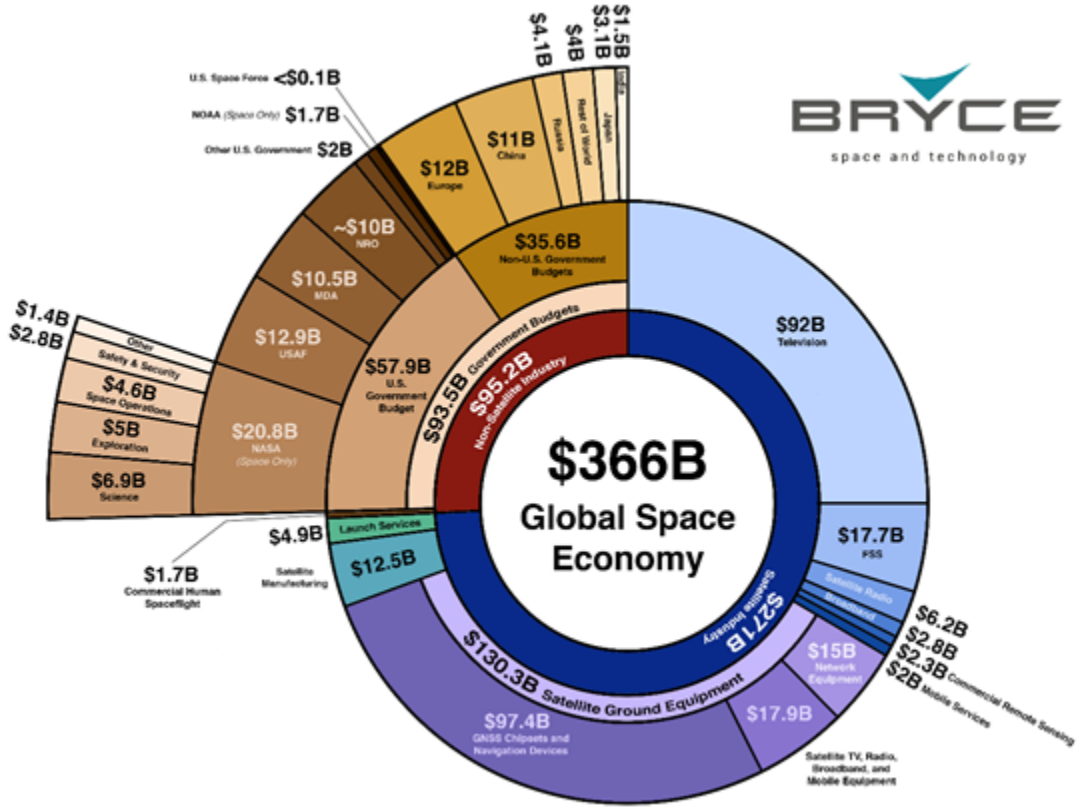

Figure 3. The 2019 Global Space Economy at a Glance[10] (original adjusted for readability)

[7] Bryce Space and Technology (2019) The 2019 Global Space Economy at a Glance. https://brycetech.com/reports/report-documents/Bryce_2019_Global_Space_Economy.png

[8] Sadlier, G., Flytkjær, R., Halterbeck, M., Varma, N., Pearce, W. (2018). Return from Public Space Investments. An initial analysis of evidence on the returns from public space investments. London School of Economics, 2015, https://londoneconomics.co.uk/wp-content/uploads/2015/11/LE-UKSA-Return-from-Public-Space-Investments-FINAL-PUBLIC.pdf

[9] Idem 6

[10] Idem 7

Contemporary changes

Recent evolutions have motivated this initiative by emphasizing the extreme importance placed on space as a new frontier for various forms of competition. Firstly, the European Union created the European Union Agency for the Space Programme to manage its space efforts, whereas, until now, separate agencies were responsible for managing individual space assets (the Galileo Global Navigation Satellite System, the GMES/Copernicus Earth Observation constellation and the future GOVSATCOM government communications constellation) developed in partnership with the European Space Agency, a separate intergovernmental organization. The European Union also created a Directorate General for Defence Industry and Space (DG-DEFIS). In addition, recent proposed evolutions of the European Programme for Critical Infrastructure Protection[11] and of the Directive on Security of Network and Information Systems[12] acknowledged space as a critical sector by listing it in the expanded line-up of sectors for which critical European entities offering essential services will have to be identified, designated and managed. For critical infrastructures, which had previously been restricted at European level to the energy and transport sectors, this is part of a major revision in approach which acknowledges the interdependencies across sectors of activity, not just geographic regions, which the pandemic impact has underlined. The proposal includes ten sectors, namely energy, transport, banking, financial market infrastructure, health, drinking water, waste water, digital infrastructure, public administration, and space.

In 2019, NATO declared space to be a new operational domain, alongside land, sea, air and cyber (previously introduced in 2016), which means that it must now consider what it means to fight in a "contested, congested and competitive space environment"[13]. NATO has had an evolving approach to space. 2012 brought its first mandate, 2016 the second one, an action plan in 2017 with a Space Working Group, and, in 2018, a first policy on reporting space operations. The promise of the 2018 Brussels Summit declaration was fulfilled in June 2019, with the declaration of space as an operational domain alongside land, sea, air and cyber. The current Action Plan features a High-Level Space Policy Framework, with a policy approved in May 2018 on space support for operations, education and training, cooperation and engagement. The 2018 Trident Juncture Exercise became the first to include space-based elements.

These evolutions also take place in the context of a heating up of competition in space in parallel with an evolving panoply of threats to space systems, which are now accessible also to non-state actors. The 2010s saw an anti-satellite weapons test from China in 2014 and from India in 2019. While China had previously conducted a successful test in 2007, which was widely criticized for the amount of space debris it created, it was the Indian test that highlighted the proliferation of ASAT capabilities and the subsequent impact on the space security environment. The Donald Trump Administration created a new branch of the US Armed Forces, the Space Force, a move which was then implemented by other countries around the world, despite decades of global discussions around preventing the militarization of space.

---

[11] COM(2020) 829 final - Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities

[12] COM(2020) 823 final - Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

[13] Department of Defense, Office of the Director of National Intelligence (2011) National Security Space Strategy Unclassified Summary. Washington DC, https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2011/item/620-national-security-space-strategy

It is in this context that Europe must define collective positions, approaches and toolboxes to protect its interests in space, both as a continuing factor in growth, prosperity and innovation, but also to secure it in a complex, dynamic and worsening security environment. Last, but not least, partnerships for space are also emerging as an important dimension for partnerships with third countries. China and Russia have reportedly initiated significant partnerships for space with other countries, which have been termed as "strategic space sector capture", by providing services, equipment, training and funding as part of a comprehensive dependency-inducing partnership[14], as illustrated in figure 4.

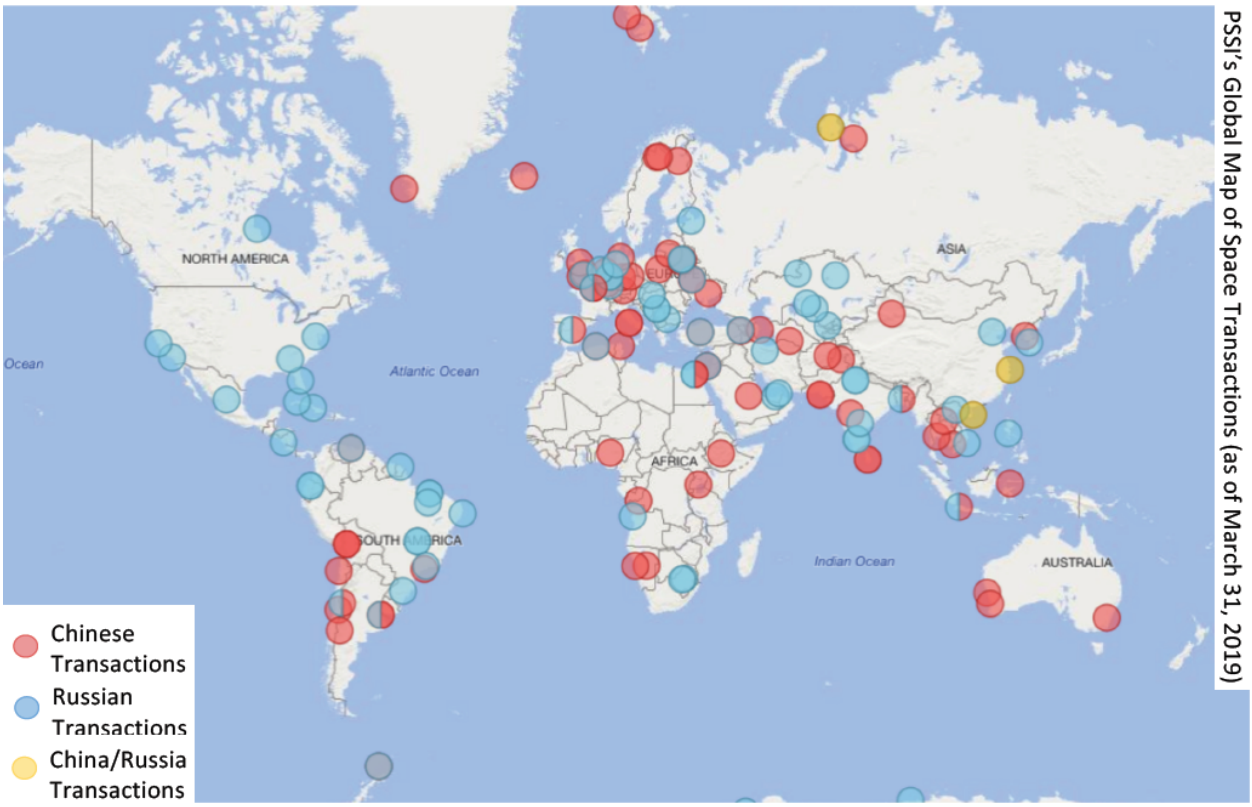

Figure 4. The database of Russian and Chinese space transactions of all types, as identified by the Prague Security Studies Institute[15]

At the same time, China has recently announced a space component to the Belt and Road Initiative, to complement the Arctic Silk Road, the Digital Silk Road and the Health Silk Road, the latter having been initiated during the Covid-19 pandemic. It is titled the Belt and Road Initiative Space Information Corridor and features comprehensive partnerships for the creation and use of space systems and the planning of common space missions. Its future projects include[16]:

[14] Robinson J, Robinson R, Davenport A, Kupkova T, Martinek P, Emmerling S, Marzorati A (2019) State Actor Strategies in Attracting Space Sector Partnerships: Chinese and Russian Economic and Financial Footprints, Prague Security Studies Institute, Prague, available online at: http://www.pssi.cz/download/docs/686_executive-summary.pdf

[15] Idem

[16] Jiang, H. (2018). The Spatial Information Corridor Contributes to UNISPACE+50. Presentation to UN Committee on the Peaceful Uses of Outer Space, 2018, https://www.unoosa.org/documents/pdf/copuos/stsc/2018/tech-08E.pdf

- A BRICS remote sensing constellation;
- Earth observation, communications and broadcasting, navigation and positioning, and other types of satellite-related development;
- Application product development;
- The Moon, Mars and other deep space exploration programs and technical cooperation;
- Construction of ground infrastructures such as data receiving stations and communications gateway stations;
- Launch and carrying services;
- Space debris monitoring, early warning, mitigation, and protection;
- Space weather cooperation;
- Import and export of and technical cooperation in the field of whole satellites, sub-systems, spare parts, and electronic components of satellites and launch vehicles, ground facilities and equipment, and related items;
- Research on space law, policy and standards;
- Personnel exchanges and training in the space field.

Beijing also inaugurated in 2008 the Asia-Pacific Space Cooperation Organization (APSCO) which counts among its members Bangladesh, Iran, Mongolia, Pakistan, Peru, Thailand, Turkey, Indonesia, and Mexico as an observer. It also features the following shared capabilities: Data Sharing Network, Space Segment Network and Interconnection of Ground Systems, Ground-Based Space Object Observation (APOSOS) Network, Disaster Monitoring Network, Space Application Network, and an Education and Training Center Network. The main regional competitor to APSCO is the Asia-Pacific Regional Space Agency Forum (APSRAF) coordinated by Japan, with projects such as Sentinel Asia for disaster management, SAFE (Space Applications for Environment) for environmental issues, Climate R³ (Regional Readiness Review for Key Climate Missions) and Kibo-ABC (Asian Beneficial Collaboration through "Kibo" Utilization)[17].

Recent evolutions in space

There has been an effervescence of space activities, as exemplified by two main trends:

- The rapid advancement of China's manned space flight programme, its robotic exploration programme and, particularly, its creation of a full spectrum of space capabilities, from global positioning to Earth Observation, something that, until now, only the United States, the Soviet Union/Russia and the European Union and its Member States have managed;
- The trailblazing efforts of SpaceX in developing reusable rockets and private transport services for cargo and humans to and from space at a lower cost.

We may discern the following overall trends in the evolution of space activities:

- The rise in the number of applications made possible by space systems;
- The rise in the number of beneficiaries of space services;

[17] Caba-Maria, F., Georgescu, A., Mureșan, L., Mușetescu, R. C. (coord.) (2020). Promoting the Belt and Road Initiative and 17 + 1 Cooperation in Central and Eastern Europe, from the Perspective of Central and Eastern European Countries. Eikon, 2020, ISBN: 978-606-49-0389-1, https://mepei.com/report-policy-analysis-promoting-the-belt-and-road-initiative-and-17-1-cooperation-in-central-and-eastern-europe-from-the-perspective-of-central-and-eastern-european-countries/

- The penetration of space into more and more sectors, which can be summed up through its integration in critical infrastructure systems, from energy, transport and communications, to finance, public administration and many others;
- From the latter elements, we deduce an increase of our dependence on space, both qualitatively and quantitatively, which becomes a liability which must be managed in the context of a deteriorating security environment.

Within the space sector itself, the following evolutions are partly responsible for the trends listed above:

- The democratization of access to space through lower barriers, leading to new entrants such as previously non-spacefaring nations, start-ups and SMEs, as well as universities;
- The rapid increase in the number of space systems, as exemplified by the Starlink Constellation of SpaceX, with over 1,600 satellites launched since 2018;
- Their clustering in Low Earth Orbit, which is not only the most economically valuable overall, for this reason, but also the most crowded, the most dangerous in terms of debris density and the most exposed to ASAT weaponry of all types;
- The lowering of cost and technology barriers for access to space, through:
  - The lowering of launch costs;
  - The spread of smallsat and cubesat standardized platforms for satellite systems (as exemplified by the Starlink mass produced smallsats);

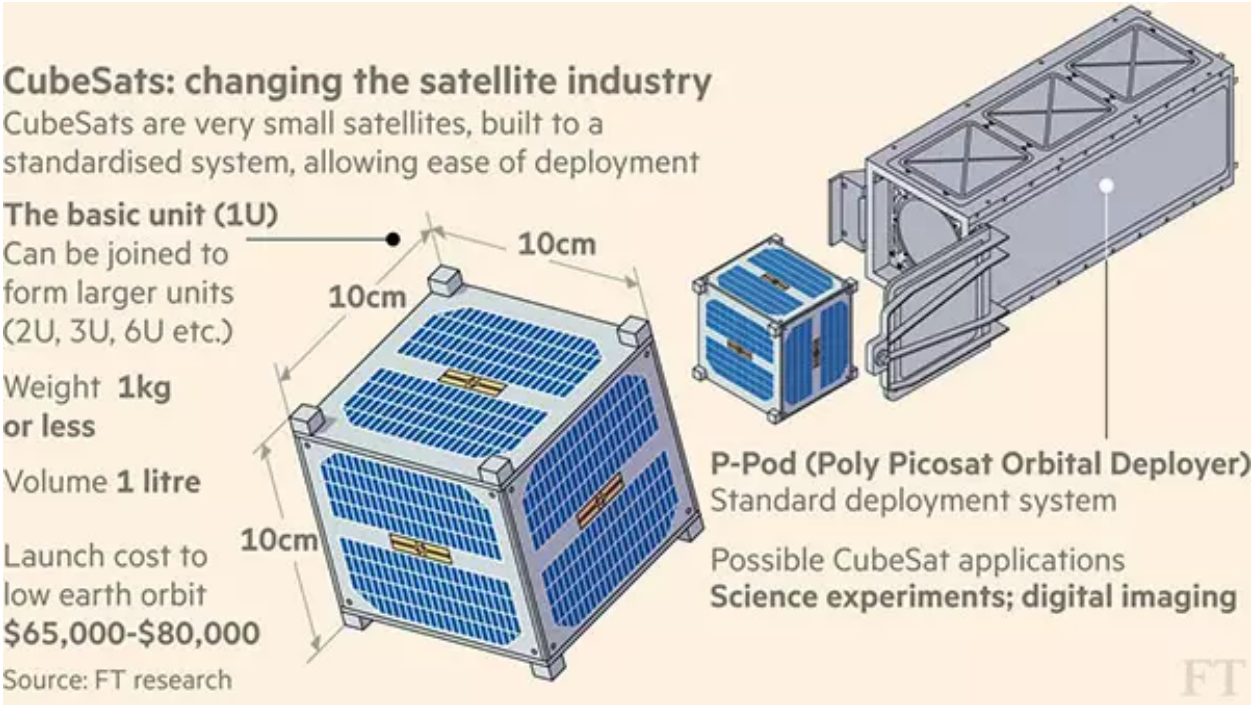

Figure 5. Cubesat architecture (source: Financial Times)[18]

  - The use of commercial off-the-shelf hardware and software for these platforms, enabling a further lowering of costs;

[18] Cookson, C. (2016). Nano-satellites dominate space and spread spies in the skies. FT Research, 11 July 2016, https://www.ft.com/content/33ca3cba-3c50-11e6-8716-a4a71e8140b0

- The miniaturization of equipment, which makes relevant activities possible on smaller, more compact systems.
- The rapid rise in space economic activities (manufacturing, launch, commercial services, scientific exploration), outstripping global economic growth.

The extraordinary recent growth in the number of satellites has almost been due entirely, in the past decade, to actors such as SpaceX and the widespread use of standardized platforms. Table 1 illustrates the current number of satellites, collated from open sources. The yearly rate of growth is almost 50%.

Table 1. Union of Concerned Scientists Open Source Satellite Database[19]

Satellite Quick Facts *(includes launches through 31.12.2020)*			
Total number of operating satellites: 3,372			
United States: 1,897	Russia: 176	China: 412	Other: 887
LEO: 2,612	MEO: 139	Elliptical: 59	GEO: 562
Total number of US satellites: 1,897			
Civil: 34	Commercial: 1,486	Government: 165	Military: 212

The space security environment

Space is one of the harshest environments known to man, where a combination of extreme temperatures, radiation and other spaceborne phenomena frequently leads to spontaneous malfunctions on the part of space systems.
There are two main non-deliberate threats that are specific to the space environment, though they may also directly impact Earth-based infrastructure systems:

1. Space debris are the accumulated stock of inert objects in various Earth orbits, resulting from human activity (and, less often, natural processes, like asteroid fragmentation) which pose a navigation hazard for space systems through the high velocities of orbital travel. This means that even debris as small as a grain of sand can damage or destroy a system. Numerous entities, including the EU, have invested in Space Situational Awareness initiatives in order to monitor the situation to the limited extent possible (as seen from the table below) and to provide early warning of collisions so that satellites may maneuver out of the way of incoming large objects (thereby shortening also their mission duration through the expenditure of limited fuel). Despite the great size of the volume of the sphere of human activity around Earth, collisions are not only possible,

[19] Union of Concerned Scientists Open Source Satellite Database, accessed 05.05.2021, https://www.ucsusa.org/resources/satellite-database

but also a frequent threat, with alerts for maneuvers sent out weekly. This is especially a problem in Low Earth Orbit, where human activity is most concentrated in a lower volume of space and in valuable orbits that service certain markets. Efforts are underway to devise methods for ensuring the cleanup of space debris (in addition to the cleaning effect of natural orbital decay in LEO), but also to incentivize responsible behaviour in space with regards to the launch, operation and decommissioning of space systems in order to minimize the number and mass of debris created.

Table 2 – European Space Agency publicly available data on space debris (May 2020)[20]

Space Debris by the Numbers (ESA, 2020)	
Number of rocket launches since the start of the space age in 1957	About 6060 (excluding failures)
Number of satellites these rocket launches have placed into Earth orbit	About 11670
Number of these still in space	About 7200
Number of these still functioning	About 4300
Number of debris objects regularly tracked by Space Surveillance Networks and maintained in their catalogue	**About 28600**
Estimated number of break-ups, explosions, collisions, or anomalous events resulting in fragmentation	More than 560
Total mass of all space objects in Earth orbit	More than 9400 tonnes
Number of debris objects estimated by statistical models to be in orbit	➢ **34000 objects greater than 10 cm** ➢ **900000 objects from greater than 1 cm to 10 cm** ➢ **128 million objects from greater than 1 mm to 1 cm**

In addition, a number of ASAT weapon systems and coercive strategies rely on the threat of debris generation in order to create a minefield that degrades the space systems of the target over time. The incentive for states to refrain from casual use of these means is that every state is now dependent on space systems and the debris threat is a collective one that must be managed, not aggravated to the cost of all parties. This does not mean that displays of power through actions that create debris (ASAT tests such as those of the US, China and India) as well as threats of "mutually assured destruction" in space are not possible. An important concern is also the action of rogue states and of non-state actors, which may decide that a kinetic approach (the production of debris through the destruction of a system or simply the spread of a payload of ball bearings in space) serves their objectives, while they themselves are insulated from the consequences.

2. Space Weather is an umbrella term for a wide variety of phenomena emanating from deep space or from the Sun which consist of radiation and charged particles which may impact electronic systems both in orbit and on Earth. Ever since the second Industrial Revolution, but especially since the world has digitized and become more global, our exposure to these threats has grown by

[20] European Space Agency, http://www.esa.int/Safety_Security/Space_Debris/Space_debris_by_the_numbers

leaps and bounds. Solar weather phenomena, especially, are also harmful to ground-based communications and energy systems. There have been numerous examples in the past of satellites being rendered inoperable (sometimes temporarily) because of solar weather, but also of power outages due to electricity grid malfunctioning during periods of intense solar activity.

An incomplete list of such events includes:

- 1-2 September 1859 – the Carrington Event – the first and strongest solar storm ever recorded, setting telegraph poles on fire and allowing them to run without electricity through geomagnetically induced currents. A repeat of this event would have devastating consequences today;
- 4 August 1972 – at the dawn of the space race, but when mankind was still resilient to space weather;
- 13-14 March 1989 – the strongest storm of the modern age, leading to blackouts in Quebec and the United Kingdom and to the loss of contact with over 1.000 space assets;
- 20 October 1989 – the Hydro-Quebec power failure left millions of people without electricity for 9 hours;
- 14 July 2000 – the Bastille Day Storm was only 37% of the intensity of the one in 1972;
- 15-16 July 2000 – 70% of the intensity of the 1972 storm;
- 30-31 October 2003 – the Halloween Storm provided key information on the vulnerability of satellite systems and led to blackouts in Sweden;
- 4 November 2003 – the largest X-ray emissions since studies began; comparable to the Carrington Event, however it took place while the Pacific Ocean was in the daylight zone.

The figure below, from Bell Labs via the Royal Academy of Engineering, illustrates the main effects of space weather on technological systems.

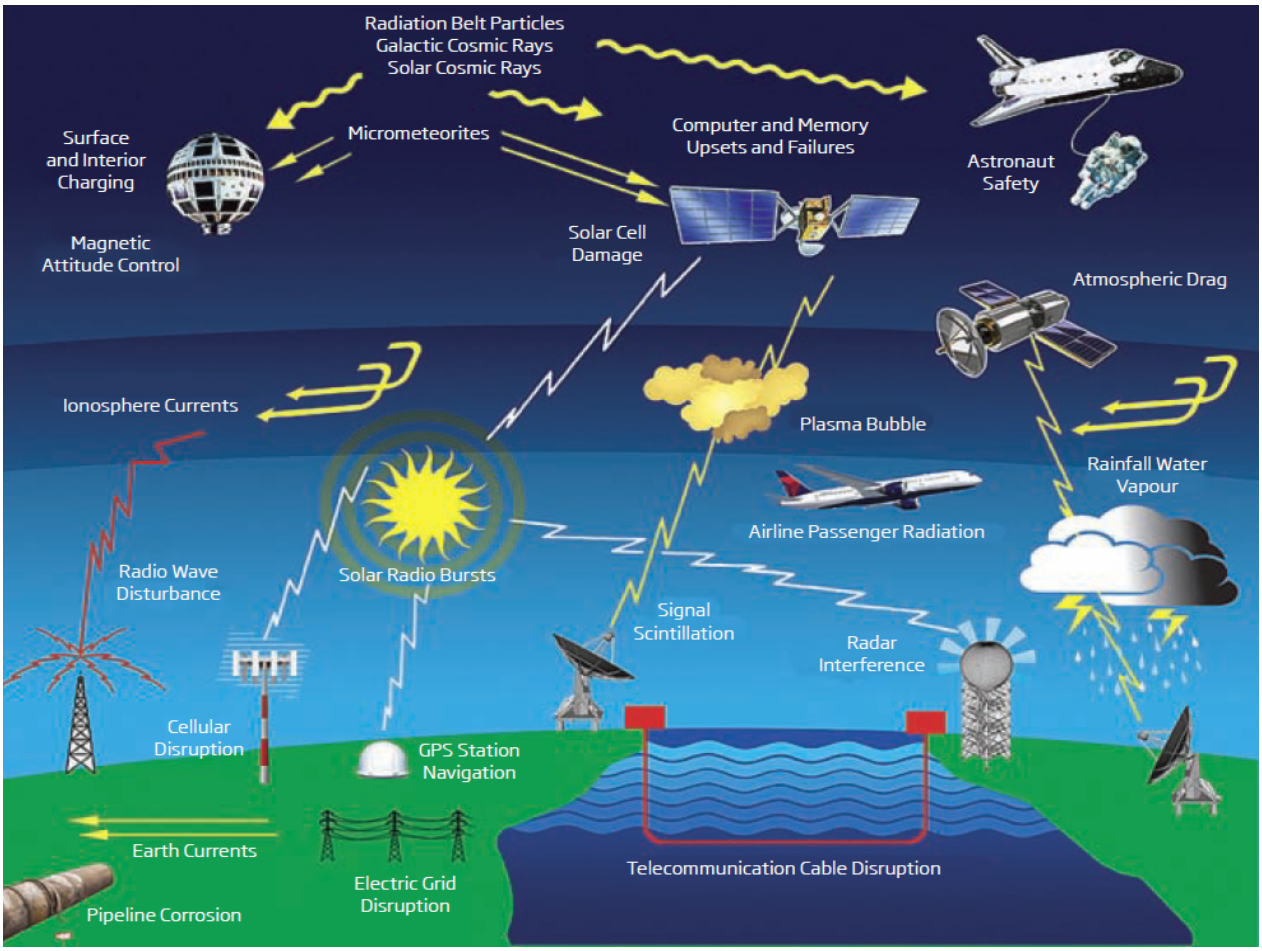

Figure 6. Space weather impact on built systems[21]

Deliberate threats

A vast array of deliberate threats has coalesced in recent years, available both to state actors, including rogue states, and to non-state or state-sponsored actors. These run the gamut from highly destructive to subversive, from destroying a satellite to stealing or manipulating its data output. Space systems are uniquely vulnerable to deliberate threats due to several factors:

- Their transparent and predictable positioning;
- Their high cost and difficulty of replacement;
- Their mission specific profile, which makes it less likely that additional capacity is present to compensate for the loss of one system, due to limited substitutability and interoperability. Constellations get around this problem, but they also depend on the redundancy their planners have built into them at great cost;
- The weight and size constraints, which often limit the presence of shielding or redundancies that would make a system more resilient;
- Their technical limitations, in terms of in-orbit repairs or refueling, which have not yet been surmounted and which gives them limited recovery ability;

[21] Royal Academy of Engineering (2013) Extreme space weather: impacts on engineered systems and infrastructure, ISBN 1-903496-95-0, Online at http://www.raeng.org.uk/publications/reports/space-weather-full-report

- Their complexity – a space system is not just the satellite itself, but also the ground control center, the ground amplification station, the communication links and so on. They are an infrastructure and are vulnerable from multiple angles because of this. For instance, one may not need to jam the satellite if one can jam the control center;
- The dependence of a high number of beneficiaries on a low stock of space assets, especially for specialized tasks such as Global Navigation, Positioning and Timing;
- The orbital dynamics of space systems, which regularly brings them into visual range of rogue and failed states;
- The proliferation of ASAT capabilities, especially of the low cost and accessible variety, such as jamming, hacking, laser blinding, which can be done with modified off-the-shelf products and commonly available technical knowledge. This means that also non-state actors or rogue states may find it easy to disrupt the functioning of space systems, if not outright destroy them;
- The lack of an institutionalized security governance architecture in space to prevent and punish transgressions, as well as of basic frameworks that, on Earth, govern liability, pollution, resource abuse and other important issues. For instance, standards for limiting the number of debris created during operations are adopted voluntarily, with no possibility of sanction for transgressors.

Space systems have also undergone several transformations that have increased their vulnerability:

- Firstly, a greater proportion of these systems is made up of cubesats and smallsats, for which cost not security was the main concern. They are unlikely to have redundant components, shielded components or very good protection from cyber threats;
- The revolution in accessibility of space through the lowering of barriers has been achieved, in large part, through standardization and the use of commercial off-the-shelf components and software. This, however, reduces *security through obscurity* and increases the knowledge of potential aggressors with regards to the system. There are satellites running on the Android operating system, on open-source operating systems or Arduino motherboards. Many of these components and software are unpatched and unpatchable and provide knowledgeable attackers with opportunities to use exploits from ordinary cyber criminality (commoditized malware, backdoors etc.). The clash between the philosophy of easily replaced systems (phones, tablets) and long duration systems (industrial control systems, satellites, even the house thermostat) in the Internet-of-Things era and in a commercial-off-the-shelf and patch-as-you-go paradigm leads to severe security issues[22];
- Our increasing reliance on them has turned them into increasingly attractive targets for disruption as part of hybrid warfare. Much of this critical dependency is transborder and trans-jurisdictional and therefore difficult for national authorities to manage and mitigate.

The Center for Strategic and International Studies publishes a yearly threat assessment report for space. The tables below highlight the main types of attacks and how they fit with regards to five criteria (attribution, reversibility, awareness, attacker damage assessment and collateral damage)[23].

[22] Falco, G. (2018) Job One for Space Force: Space Asset Cybersecurity. Cyber Security Project, Belfer Center, Harvard University, 12 July 2018, https://www.belfercenter.org/publication/job-one-space-force-space-asset-cybersecurity

[23] Harrison, T., Johnson, K., Moye, J., Young, M. (2021). Space Threat Assessment 2021. Center for Strategic and International Studies, April 2021, https://www.csis.org/analysis/space-threat-assessment-2021

Table 3. Kinetic and non-kinetic physical deliberate threats (source: CSIS Space Threat Assessment 2021)

	Kinetic Physical			Non-Kinetic Physical			
Types of Attack	Ground Station Attack	Direct-Ascent ASAT	Co-orbital ASAT	High Altitude Nuclear Detonation	High Powered Laser	Laser Dazzling or Blinding	High Powered Microwave
Attribution	Variable attribution, depending on mode of attack	Launch site can be attributed	Can be attributed by tracking previously known orbit	Launch site can be attributed	Limited attribution	Clear attribution of the laser's location at the time of attack	Limited attribution
Reversibility	Irreversible	Irreversible	Irreversible or reversible depending on capabilities	Irreversible	Irreversible	Reversible or irreversible; attacker may or may not be able to control	Reversible or irreversible; attacker may or may not be able to control
Awareness	May or may not be publicly known	Publicly known depending on trajectory	May or may not be publicly known	Publicly known	Only satellite operator will be aware	Only satellite operator will be aware	Only satellite operator will be aware
Attacker Damage Assessment	Near real-time confirmation of success	Near real-time confirmation of success	Near real-time confirmation of success	Near real-time confirmation of success	Limited confirmation of success if satellite begins to drift uncontrolled	No confirmation of success	Limited confirmation of success if satellite begins to drift uncontrolled
Collateral Damage	Station may control multiple satellites; potential for loss of life	Orbital debris could affect other satellites in similar orbits	May or may not produce orbital debris	Higher radiation levels in orbit would persist for months or years	Could leave target satellite disabled and uncontrollable	None	Could leave target satellite disabled and uncontrollable

Table 4. Electronic and cyber deliberate threats (source: CSIS Space Threat Assessment 2021)

	Electronic			Cyber		
Types of Attack	Uplink Jamming	Downlink Jamming	Spoofing	Data Intercept or Monitoring	Data Corruption	Seizure of Control

Attribution	Modest attribution depending on mode of attack	Modest attribution depending on mode of attack	Modest attribution depending on mode of attack	Limited or uncertain attribution	Limited or uncertain attribution	Limited or uncertain attribution
Reversibility	Reversible	Reversible	Reversible	Reversible	Reversible	Irreversible or reversible, depending on mode of attack
Awareness	Satellite operator will be aware; may or may not be known to the public	Satellite operator will be aware; may or may not be known to the public	May or may not be known to the public	May or may not be known to the public	Satellite operator will be aware; may or may not be known to the public	Satellite operator will be aware; may or may not be known to the public
Attacker Damage Assessment	No confirmation of success	Limited confirmation of success if monitoring of the local RF environment is possible	Limited confirmation of success if effects are visible	Near real-time confirmation of success	Near real-time confirmation of success	Near real-time confirmation of success
Collateral Damage	Only disrupts the signals targeted and possible adjacent frequencies	Only disrupts the signals targeted and possible adjacent frequencies	Only corrupts the specific RF signals targeted	None	None	Could leave target satellite disabled and uncontrollable

The defence perspective

The Armed Forces were among the first to utilize space capabilities and to explore issues related to security and deliberate threats to these systems. The table below highlights the main dependency of military operations on space systems.

Table 5. Space dependencies on military operations (source: NATO ACT, declassified)[24]

Space dependencies in military operations	
SATCOM	**SSA**
Satellite Communications: • Degrade Command & Control (C2); • Loss of remotely piloted aircraft ops; • Degraded beyond-line-of-sight comms.	Space Situational Awareness: • Loss of overflight prediction; • Loss of space surveillance; • Degraded force protection.
ISR	**SEW**

[24] Presentation by Stephanie Vrac from NATO ACT during a NATO Advanced Research Workshop on Critical Space Infrastructures organized in Norfolk, Virginia, USA by Old Dominion University, 21-22 May 2019

Intelligence, Surveillance, Reconnaissance • Degraded Intel Collection; • Degraded targeting; • Degrade Battle Damage Assessment.	Shared Early Warning • Degraded ballistic missile early warning; • Degraded force protection; • Degraded passive defense.
PNT	**Terrestrial and Space Weather**
Positioning, navigation and timing • Limited precision guided munitions; • Loss of friendly force tracking (IFF); • Network timing.	Terrestrial and Space Weather • Loss of forecast for mission planning; • Loss of interference forecast; • Loss of optimal electronic settings.

The new space environment features adversaries that seek to disrupt space systems in order to severely degrade the capabilities of the Armed Forces to achieve their mission in the context of growing reliance on space capabilities, in particular data gathering, navigation and synchronization. A 2019 US Defense Intelligence Agency reported that "foreign governments are developing capabilities that threaten others' ability to use space […] China and Russia, in particular, have taken steps to challenge the United States […] [China] continues to improve its counterspace weapons capabilities and has enacted military reforms to better integrate cyberspace, space, and EW into joint military operations"[25]. One study stated that "operations are reliant on the adequate provisioning of critical space services, and adversaries seek to disrupt this access in order to limit […] capabilities, hamper the fulfilment of core missions and hinder active operations"[26]. The successful Indian ASAT test begs the question of how many countries and entities also possess these capabilities, but do not find it useful to announce them as such.

Space systems are, increasingly, an "Achilles' heel" for the Armed Forces of Europe and, therefore, European strategic autonomy and effectiveness can only take place in the context of security of supply for space services, respecting the need for data confidentiality, integrity and availability. The disruption of space systems can take Information Age militaries back into the Industrial Age and eliminate an important asymmetric advantage against adversaries, which is why space systems are priority targets during, but also before conflicts.

One particular American-led exercise, Pacific Vision, also highlighted another unique military vulnerability – the high dependence on civilian space systems for key services, especially telecommunications. 90% of American military telecommunications are routed through civilian assets, which lack the shielding, protection and overall resilience of military satellites[27]. This is a result of the powerful expansion of military consumption of space services and is just one instance of military reliance on civilian critical infrastructures.

Priorities for Europe

As mentioned in the beginning, this is a descriptive paper, which does not advance particular recommendations. However, we can derive key priorities for Europe in terms of space both from

[25] *** (2019). Challenges to security in space. Defense intelligence Agency, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf

[26] Tatar, U., Gheorghe, A.V, Keskin, O., Muylaert, J. (Eds.) (2020), " Space Infrastructures: From Risk to Resilience Governance", IOS Press, NATO SPS Series D, vol. 57, ISBN, 978-1-64368-073-6

[27] Easton, I. (2010), The Great Game in Space - China's Evolving ASAT Weapons Programs and Their Implications for Future U.S. Strategy. Project 2049 Institute, http://project2049.net/documents/china_asat_weapons_the_great_game_in_space.pdf

the European documents of reference which have been published, the recent evolutions in European space governance and the realities of the evolving space environment:

- Accessible, affordable and sustainable access to space services for European citizens and businesses as a precondition of continuity, resilience, growth and innovation;
- Europe must maintain itself as a leader in innovation and production the aerospace field and must reduce the existing gap with regards to new technologies, such as reusability;
- European strategic autonomy in space – Europe must build, maintain and protect a full spectrum of space capabilities so that it will not be reliant on those of other powers. The next project in this regard is the secure government communications satellite system, GOVSATCOM;
- Europe must achieve resilience to risks, vulnerabilities and threats deriving from its increasing reliance on space systems, both at the level of its militaries, and at the level of society and economy;
- Europe must create the toolbox with which to pursue its interests in a free and peaceful access to space, through a combination of multilateral agreements on rules of conduct, sectoral diplomacy and the development of instruments of deterrence against attacks on its space systems;
- The European Armed Forces must have safe and secure access to space services in order to maintain their qualitative edge in an environment beset by cyber and electronic warfare threats;
- Europe must emulate other actors in developing fair and sustainable comprehensive space partnerships with third countries, whose development will rely on space and which might otherwise become unduly beholden to European systemic rivals;
- Overall, Europe must integrate space into its toolbox for internal and external governance in all fields, from environmental and economic, to the security one.

One avenue of potential contribution on the part of Eurodefense on the subject of space is in formulating a space perspective on the Strategic Compass. The example in figure 7, dating from April 2021, presents an EUISS perspective on how the four “baskets” of the Strategic Compass can be intertwined with space. The Strategic Compass process is an important running initiative that may help the EU to advance its present ambition and profile with regard to the space domain. Without improved autonomy in space, not only economic but also political and military risks will grow for the EU and its Member States. The Strategic Compass constitutes a real opportunity for the EU to develop a sustainable, comprehensive EU space and defence strategy that orchestrates the necessary multidomain, interdepartmental and multinational approach and their respective policies. Eurodefense can elaborate new ideas and approaches in this regard.

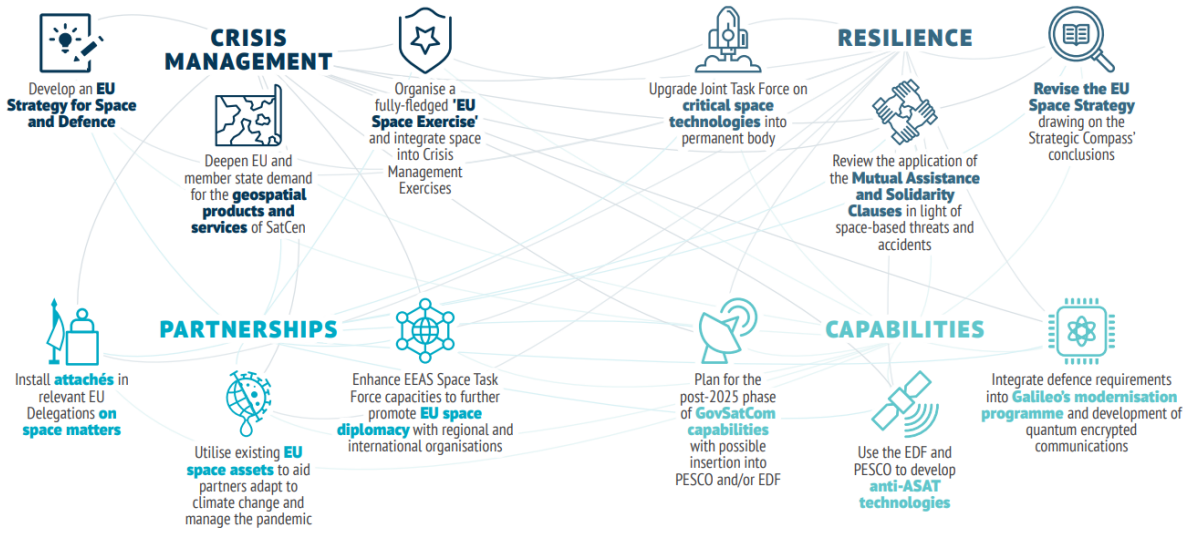

Figure 7. Space and the Strategic Compass (source: EUISS)[28]

Conclusions

As critical enablers for the functioning of modern, prosperous and advanced societies, our reliance on space systems is both extensive, intensive and growing quickly. This also extends to the Armed Forces. Because of this, Europe must become proactive in increasing its resilience to space system disruption and must cultivate strategic autonomy in this regard, while maintaining itself as a leading actor in a lucrative field of high technology and exerting a positive influence on the development of space security governance. The fact that all major players are critically dependent on space is not a guarantee of good behaviour or self-imposed limitations on coercive or disruptive operations, especially with the rise of capable non-state and rogue state actors. What is certain is that the rapid advances in space technology and capabilities are accompanied by rapid advances in the frameworks through which states and alliances seek to maximize the economic, political and strategic potential of space, while minimizing or managing their exposure to this challenging security environment. Europe has, so far, been one of those proactive entities, but there also other steps that it may take to further pursue its interests and secure its future in space.

[28] Fiott, D. (2021). Securing the Heavens: How can space support the EU's Strategic Compass? European Union Institute for Strategic Studies, April 2021, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_9_2021_0.pdf