# ISSUE

REPORT Nº 29 — July 2016

# Space security for Europe

**RAPPORTEURS**
Massimo Pellegrino
Gerald Stang

## Reports

ISS European Union Institute for Security Studies

# CONTENTS

## Acknowledgements

This Report has been drafted by Massimo Pellegrino and Gerald Stang at the EUISS, and the ultimate responsibility for its content lies exclusively with them. The Report takes into account the exchanges that took place in the framework of an EUISS Task Force on 'Space and Security' that convened from September 2015 until June 2016. The initiative involved distinguished experts from European institutions and bodies, international and intergovernmental organisations, national space agencies, think tanks, industry associations, EU member states as well as prominent personalities in the field of space security. Needless to say, the Report does not necessarily represent all the views of these organisations.

We would first like to thank James Copping (European Commission), Xavier Pasco (Fondation pour la Recherche Stratégique), Andrea Patrono (European Union Satellite Centre), Dumitru-Dorin Prunariu (Member of the United Nations Group of Governmental Experts on TCBMs in Outer Space Activities), Didier Schmitt (European External Action Service), and Kai-Uwe Schrogl (European Space Agency) for their collaboration as members of the Task Force and for their valuable insights throughout the project.

We would also like to convey our gratitude to Jorge Manuel Bento Silva, Jenny Berglund, Gérard Brachet, Pascal Faucher, Christina Giannopapa, Jean-Paul Granier, Veronica La Regina, François Rivasseau, Denis Roger, Heli Tiirmaa-Klaar, and Jean-Jacques Tortora for their presentations during the events organised as part of this project.

Our special thanks go to Luca del Monte, John Fowler, Jason Kedzierski and Mia ter Haar for the material provided on specific topics. The Report also benefited from the valuable inputs of many other distinguished experts in the fields of space and security, interaction with whom constituted a fruitful dimension of our research efforts.

At the EUISS, Marco Funk provided invaluable assistance in fine-tuning the initial versions of the Report, while Gearóid Cronin deserves special thanks for his thoroughness in editing the final text.

The preliminary findings of the Report were presented at the European Interparliamentary Space Conference (EISC) workshop on 'Space and Security' on 18-19 April 2016 in Sinaia, Romania. The Report in its final form has greatly benefited from feedback during the workshop and in discussions afterwards.

*Massimo Pellegrino and Gerald Stang*

*Paris, July 2016*

# FOREWORD

For a long time, our use of space was limited and incremental: first it was for national security, then for telecommunications. Now our societies are almost entirely reliant on space systems for all kinds of technologies – from GPS to the ATM, from phone calls to gas pipelines. Almost every cutting-edge technology being adopted in highly-developed economies increases their dependency on space-based (and mostly unprotected) systems. In military terms, such dependency is even stronger: take precision weaponry, drone surveillance and real-time field communications. With the number of countries and players interested in space capabilities growing, outer space risks being exposed to additional strategic competition and even conflict – with threats ranging from anti-satellite weapons to 'hybrid' operations and cyber attacks. China and Russia have already engaged and invested in this domain, with a view to challenging US dominance, while countries like India and Brazil are striving for access to what is a 'global common' in its own right – and one whose rules are evolving very rapidly.

Europe – including the EU proper and its individual member states – is an important player in and on outer space. It has significant assets and capabilities, albeit spread among various agencies and stakeholders, and it has an overriding shared interest in promoting the autonomy and security of space-based services, in preventing the 'geopoliticisation' and even 'weaponisation' of satellite systems, and in pushing for the adoption of a viable international regime in an area that still lies at the frontier of global affairs and multilateral governance.

The EUISS Task Force convened and coordinated by Massimo Pellegrino and Gerald Stang set out to map this policy space (literally!) at both European and international level, exploring current trends, and also identifying potential avenues for the future. At a time when situational awareness, resilience and preparedness have become crucial factors for virtually all our public policies (and personal lives too), addressing space security represents a much-needed complement to shaping a more incisive common space policy proper as well as a joined-up approach to security at large. Our expectation and hope is that the resulting Report contributes to both the wider strategic reflection promoted by HR/VP Mogherini – which already includes the EU Strategic Review from June 2015 and, now, also the EU Global Strategy (EUGS) – and the dedicated EU 'space strategy' that is to be released later this year.

*Antonio Missiroli*

*Paris, July 2016*

# EXECUTIVE SUMMARY

Nearly 1,300 satellites orbit the earth, operated by 80 different countries and organisations, providing a wealth of services for billions of people. Both civilian and military actors use space systems for an expanding range of activities, including earth observation and environmental monitoring, early warning and reconnaissance, navigation and communications.

However, the strategic value of outer space is threatened as space systems are subject to numerous threats and hazards, including collision with debris and other space objects, the impacts of space weather phenomena, signal jamming, cyber attacks, and even the potential for attack by anti-satellite weapons (ASAT). Irresponsible conduct in space operations also contributes to putting the long-term sustainability of the space environment at risk.

Responding to these threats requires a wide range of tools. As these threats, and the available responses, are often similar for all space actors – whether civil, commercial or military – common threat perceptions may serve as a basis for developing common responses. However, dependency, ownership and sovereignty issues complicate this work, as the leading space actors do not always share common strategic and policy principles. The European space community could thus benefit from common strategic thinking that could facilitate improved resilience of space systems, reduced dependence on external actors, and help ensure a secure and sustainable environment for outer space activities.

## Improving resilience and non-dependence

Increasing the resilience of space systems can begin with the hardening of both the space and ground segments against physical and cyber attacks, building redundancy into satellite constellations, or sharing capabilities with third parties to ensure back-up service provision.

But effective protection of space assets requires embedding security considerations into strategic, policy, technology and funding decisions throughout all of the phases of space programmes, from conception to operation. Extra care is required to future-proof big programmes with long lead times.

In order to develop a common understanding of space risks, and thus facilitate cooperation and integrated responses, the creation of a common risk and resilience assessment methodology for European space infrastructures may be worth exploring. In addition, rather than a separate framework for managing space risks, infrastructure protection measures can be integrated, making use of existing critical infrastructure protection (CIP) efforts and strategies at national and European levels. The existence of legislative and administrative frameworks for CIP at the EU level, with links to national frameworks, can help make the development and implementation of space security measures significantly easier.

In managing major space programmes, the security of the entire data life cycle has to be assured so that both programme partners and service users can be confident in the integrity, reliability, and security of the data. An effort can be made at the European level to develop common principles for managing space data policies.

As the threat landscape evolves, closer engagement between the space and cyber communities will need to become permanent. In the EU, this connection can be enhanced by bringing space actors into the EU cyber dialogue to identify common risks and define appropriate solutions, even though the exchange and disclosure of vulnerabilities is highly sensitive. Stress tests to assess and improve resilience to potential cyber attacks can also become a regular practice, along with the development of formal processes to identify and compensate for when space systems or services have been compromised. Space personnel will need to be continuously re-trained on protecting and recovering the systems, software, data, and devices they use.

As the responsibilities and competencies of European space actors have increased, their need for independent supporting capacities has expanded. Reliance on commercial providers raises questions about how to balance the needs for system control, reliability, bandwidth availability, security, flexibility and affordability. Reliance on other actors comes with additional risks for both member states and European institutional users. One tool for managing these risks could be a permanent cooperative process to research the costs and benefits of relying on commercial partners or a single non-European provider for information and capacity in particular programmes.

Having autonomous and cutting-edge capabilities for space access, earth observation, communications, and navigation and positioning can help strengthen European autonomy of action. This work will need to go hand-in-hand with investments in training and skills enhancement.

## Cooperation among European space actors

The complex governance of European space activities will not easily be rationalised into a common framework any time soon. But with a common vision and good com-

munication, major governance changes are not necessarily required in order to pursue effective action on space security. Building trust among all space institutional actors can be facilitated through the creation of shared and common European policies and strategies, rather than just EU ones.

A common European strategic approach to space security can provide a pillar around which institutions, member states, and industries can articulate their own policies and activities. Such a common approach could help ensure the inclusion of space security priorities, such as resilience, space sustainability, and effective data policy, within broader space strategies and security strategies. This would also facilitate the joint development of both technical and diplomatic proposals to tackle and address space security challenges.

One key element to monitor space risks is the development of Space Situational Awareness (SSA) capabilities for which Europe still depends on the US for detailed information. The EU has recently set up a Space Surveillance and Tracking (SST) support framework involving an open consortium of member states to network existing SST assets and provide anti-collision alert services at the European level. Further development of SSA capabilities would allow Europe to better respond to the full range of threats originating in the space environment.

Closer cooperation on space security can also be envisaged between the civil and military domains, taking advantage of what each group has to offer without necessarily reorganising the governance arrangements for European space systems. Integrating the potential for dual use by both civil and military actors into future space programme development can help concretise this cooperation.

As the number of private space actors and the services they provide continues to expand, a framework for enabling private sector exploitation of space could prove useful, including a review of the regulatory bottlenecks and gaps facing new space entrants in Europe. Incentivising security-conscious behaviour by private companies and other new space actors, as well as reducing the significant uncertainties and costs regarding insurance, financing and liabilities can facilitate commercial activity in space.

## International cooperation

No single body or law governs the use of space, and efforts to improve space governance are complicated by the clashing priorities of major space powers. International cooperation can play a systematic role in reducing tensions, altering threat perceptions and creating a community of stakeholders that share common goals with regard to the long-term sustainability of outer space. The UN remains the primary multilateral forum to discuss space security issues. While the potential for a new international legal regime for space seems slim, some success has been reached with voluntary in-

struments for preserving the safety and sustainability of the space environment and enhancing trust among space actors. Voluntary measures can include both technical guidelines on how to safely conduct space activities as well as transparency and confidence-building measures (TCBMs) on how to communicate about space activities.

Europe attaches great importance to international cooperation for space security and can play a central role in helping set the global agenda. International engagement on space security can proceed in tandem with efforts to strengthen European roles in global space discussions. The EU's major diplomatic initiative in this field, the International Code of Conduct, addresses both military and civil uses of outer space, emphasising principles for responsible behaviour. The Code is not intended to regulate the placement of weapons in outer space, but calls for space powers to prioritise safety and security in their conduct of operations, and to pursue TCBMs related to their space policies and activities. While there is widespread support for both the Code and the ideas it contains, some resistance has been expressed, especially by Russia and China.

It will be important to ensure the Code and its ideas continue to move forwards, and that it is kept on the agenda at bilateral space dialogues and security dialogues, as well as on the table and under discussion at the the United Nations General Assembly (UNGA) with the support of member states. In the long term, the ideas in the Code could even evolve towards a more comprehensive space traffic management regime and the EU could start looking into the matter – discussions at intergovernmental level have already started at the UN Committee on the Peaceful Uses of Outer Space (COPUOS).

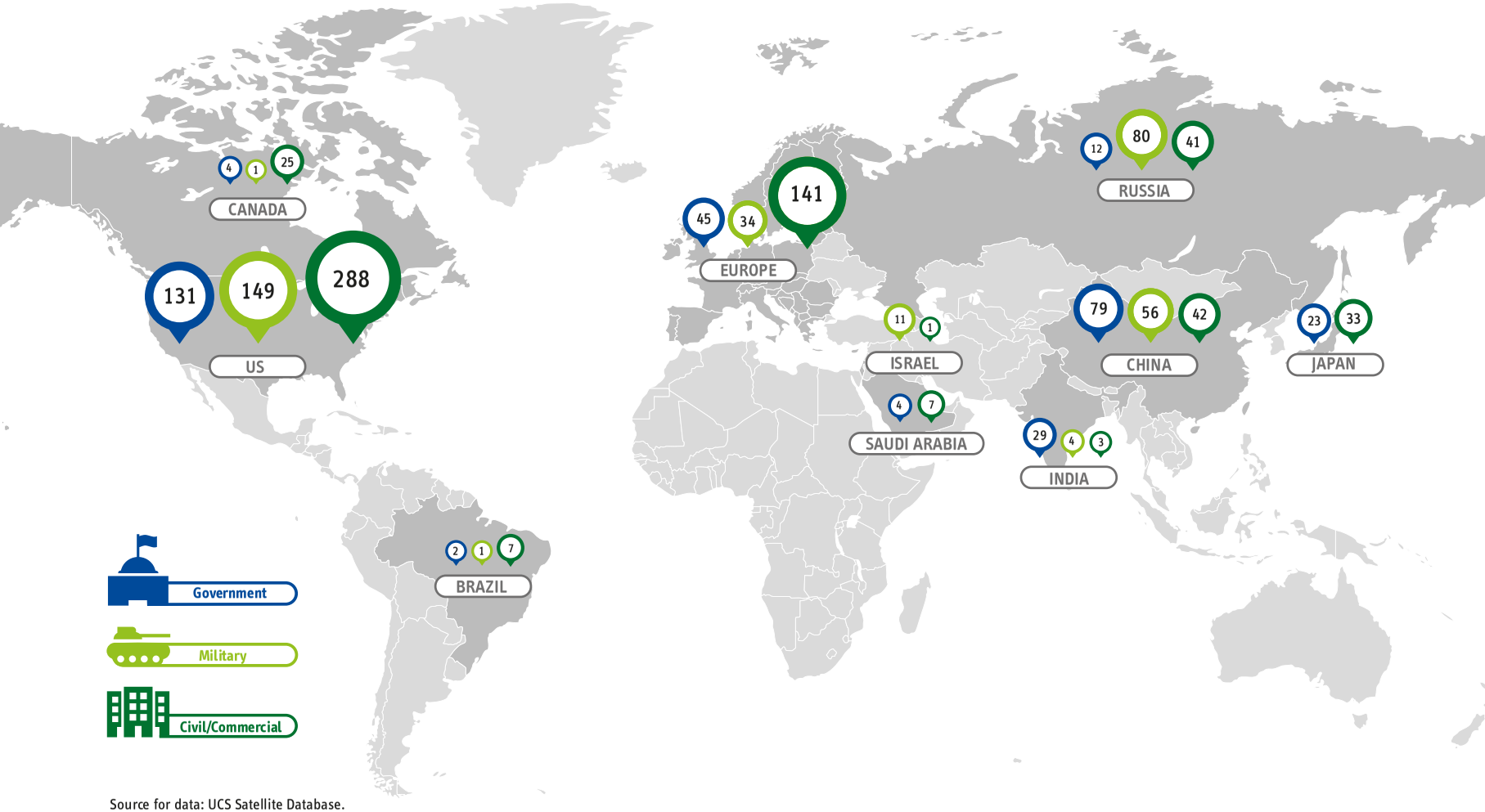
To systematically improve cooperation among European actors on space security matters, mechanisms for regular exchanges can be established, both within Europe and in its external relations. For example, a European Space Diplomacy Network composed of individuals from the EU, the ESA, and member states (perhaps modelled on the existing Green Diplomacy Network) could help pursue shared priorities and coordinate action plans for space diplomacy.

European effectiveness in pushing forward a space sustainability agenda can also be enhanced when European space actors unilaterally implement space sustainability measures. Such action may include, for example, a public and independent review of how the EU, ESA and member states are applying agreed voluntary measures.

It will also be important to bring some space security issues into bilateral dialogues, complementing multilateral cooperation efforts at the UN. In particular, this can involve deeper connections with the United States, who due to their increasing awareness of their vulnerability in space have been led to focus more on diplomatic approaches to enhancing space security. Dialogue cannot be limited to like-minded partners, however. Russia and China can be difficult dialogue partners, but they are still essential for shaping the space environment.

Looking ahead, 2016 is a critical year for space security in Europe. Galileo's initial services will be launched. Copernicus, together with its contributing missions, will further contribute to providing data exploitable by security and defence actors. The SST consortium is expected to deliver its first services. The new EU Global Strategy on Foreign and Security Policy has been released, and the EU will draft a European Defence Action Plan with a view to exploiting and strengthening synergies between security and defence, including in the field of space. Finally, the European Commission will draw up a new space strategy for Europe, the Commission and the ESA are drawing up a joint statement on shared goals for the future of Europe in space, and the ESA is preparing its space security policy. Advancing strategic common thinking on space security will clearly be an important complement to these initiatives and pave the way for other future endeavours.

**Figure 1: Operational satellites for top 10 global space actors**




Source for data: UCS Satellite Database.

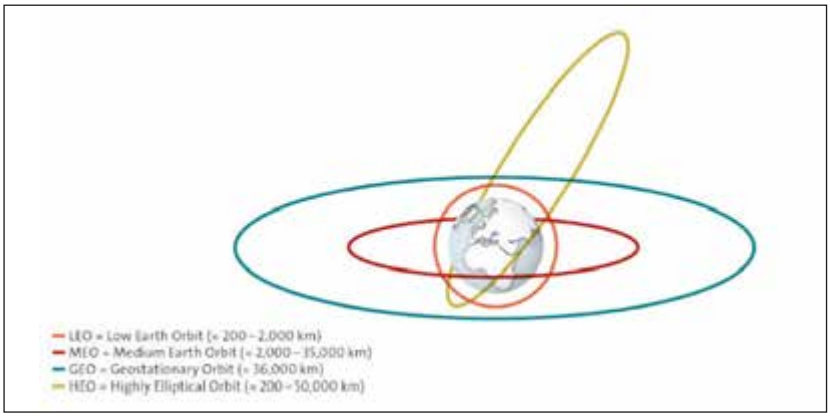
# I. INTRODUCTION – SPACE AND SECURITY IN EUROPE

In the beginning of the Space Age, marked by the launch of *Sputnik 1* in 1957, outer space was an arena for strategic competition between the United States and the Soviet Union. During much of the Cold War, space programmes were demonstrations of technological superiority and a means to gain international prestige. As the two superpowers came to understand both the utility and the risks of using outer space for military purposes, they sought to regulate some aspects of space activities to avoid the danger of an arms race in space. While continuing to expand their space activities, they began a period of *détente* in the 1960s and 1970s with the goal of securing the continued use of space for military purposes, while simultaneously refraining from the actual deployment or use of space weapons. This led to arms control discussions both bilaterally and through the United Nations (UN) and to decades of inertia and stagnation in international discussions on space security.

The dynamics of space activities have undergone a radical transformation since the end of the Cold War as space has become increasingly 'congested, competitive and contested'.[1] This has led to new conceptions of space security that not only focus on military matters, but also on how to reduce risks to all space assets and ensure that space operations can be safe, secure and sustainable in the long term.

Today, nearly 60 countries and 20 organisations own more than 1,300 operational satellites orbiting the Earth, although most are still controlled by a few leading space powers (see Figure 1 opposite).

**Figure 2: Earth orbits**




Source: NASA Global Change Master Directory.

1. Statement of Lieutenant General John W. Raymond before US House Armed Services Subcommittee on Strategic Forces, 25 March 2015.

The military is no longer the primary user of space applications. Commercial satellite operators offer vital services (including to military users) while civilian and research projects abound, using new platforms and technologies. New entrepreneurs are developing low-cost technologies to access space, thereby changing the geostrategic space landscape and shaping international policy options. These ever-increasing capabilities engender new dependencies which, in turn, increase vulnerabilities and security concerns.

## The evolution of space and security in Europe

The growing complexity and interdependence of the global economy has been matched only by the growing complexity and interconnectedness of the global security environment. While the geopolitical and security challenges of the Cold War period are often overly simplified in retrospect, rapid shifts in the economy, technology, geopolitics, and relations between citizens and governments have indeed contributed to a less clear set of challenges facing today's governments. Threats to our security interests can often be internal and external, regional and global, civilian and military, natural and man-made; developing EU action requires navigation of an increasingly connected, contested and complex world.[2] The evolution of the EU's main security-related strategy documents reflects these changes. In 2003, terrorism, proliferation of weapons of mass destruction (WMDs), regional conflicts, state failure, and organised crime were identified as the five key threats. In 2008, cybersecurity, energy security, and climate change were added. By 2010, cross-border crime, violence itself, and natural and man-made disasters were also identified as key threats. In 2015, terrorism, organised crime and cybercrime were again prioritised. As the threat landscape has evolved once again, the new EU Global Strategy on Foreign and Security Policy has added to this list the challenges of hybrid threats and external border management.[3]

Confronting this range of global challenges requires a diverse set of instruments and capabilities. The EU has long prioritised comprehensive responses to security threats, recognising that complex and interdependent challenges require action at multiple levels and over extended timeframes – both to manage crises as they unfold and to address root causes. Space-based assets and services, notably those for early warning, observation, navigation and communication, have become essential tools in this effort, helping security actors address a wide range of challenges. Nevertheless, in contrast to the national security strategies of some countries, such as the United States, connections between space and security have not been central to most EU security documents.[4]

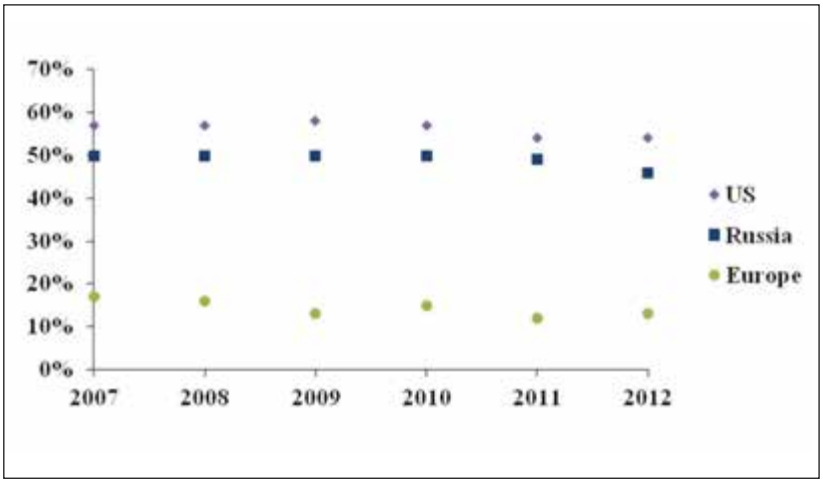
2. HR/VP Federica Mogherini, 'The European Union in a changing global environment - A more connected, contested and complex world', EEAS, Brussels, June 2015.

3. 'A secure Europe in a better world - European security strategy', European Council, 2003; 'Report on the implementation of the European Security Strategy - Providing Security in a Changing World', European Council, 2008; 'Internal security strategy for the European Union - Towards a European security model', European Council, 2010; 'The European Agenda on Security', European Commission, 2015, COM(2015) 185 final, Strasbourg,. 28 April 2015; HR/VP Federica Mogherini, 'Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign and Security Policy', EEAS, Brussels, June 2016.

4. One important exception is the Commission Communication 'Towards a more competitive and efficient defence and security sector', COM (2013) 542, Brussels, July 2013, where an explicit link between space and security was highlighted.

This can be explained by a set of two interrelated factors. First, the EU and most of its member states have only become gradually more engaged in space security matters over the past decade. In fact, the link between space and security in Europe has been quite different from that of other space powers such as Russia and the United States. The strategic, political, and military relevance of space has traditionally been taken into account less across Europe, which has focused more on scientific programmes and civilian space applications. While several EU member states have military space programmes, and Europe has been able to ensure autonomous access to space through its launcher programmes, European space activities have been less focused on security and defence than has been the case in other space powers, despite their dual-use potential. Figure 3 shows that European investment in space activities for defence remains very limited relative to other leading space powers. Among the member states, only France, Germany, Italy, Spain and the UK prioritise the development and ownership of defence space programmes.

**Figure 3: Ratio between government expenditures for defence-related space programmes and government expenditures for space programmes overall (2007-2012)**




Source for data: Christina Giannopapa, 'The Space Sector Economy and Space Programmes World Wide' in Kai-Uwe Schrogl et al. (eds.), *Handbook of Space Security* (New York: Springer-Verlag, 2015).

Second, space security concepts in Europe have developed along multiple tracks. In their national policies, EU member states have drawn a variety of different connections between space and security, with each different formulation reflecting their unique national defence, security and space priorities. Meanwhile, the EU has limited itself mostly to broad, general declarations on the links between space and security, even though it has acquired more competences in both security and space matters, culminating with the Lisbon Treaty which conferred on the EU a competence in space (Article 4(3) of TFEU).

For example, the Commission White Paper 'Space: a new European frontier for an expanding Union' of November 2003 acknowledged that 'space has a security dimension and security has a space dimension', and called for a reinforcement of space technologies in support of security and defence policy requirements. A common European framework for space activities gained momentum in 2007 with the development of the first European Space Policy (ESP), a joint document prepared by the European Commission and the European Space Agency (ESA) and approved by the Space Council, a joint formation of the EU Competitiveness Council and the ESA Council at ministerial level. While the security dimension of the ESP was limited relative to its focus on the scientific domain, one of its strategic objectives was to meet Europe's security and defence needs. In that respect, a structured European dialogue on space and security was called for in order to guarantee coordination and optimise synergies. However, follow-up has been rather weak. Despite declared support from the European Parliament and the Space Council, EU action on space security has not always matched the rhetoric, primarily due to the sensitivity of the issue.[5]

Today, the protection of space assets, the reduction of risks in the space environment, and secure and sustainable access to, and use of, space are growing security concerns for Europe. The increasing economic dependence of European citizens on space services in particular has highlighted the need to protect critical and potentially vulnerable space systems, whether private or public, national or European. The fact that these assets are also important tools for security and defence purposes makes this reliance on space more critical than ever. Indeed, the 2011 EU Space Strategy clearly recognises the benefits of space applications and acknowledges that space infrastructure acts as both a security instrument as well as a critical asset to be protected.[6] Security services provided by observation, navigation and communications satellites require the continued security of space systems themselves and the sustainability of outer space activities. It has thus become necessary to introduce appropriate measures to address threats to these assets and the environment in which they operate.

## The emergence of space security in Europe

Since 2007, the EU, ESA and their member states have become more engaged in political and diplomatic initiatives to tackle space security and sustainability challenges, including via the EU proposal for an International Code of Conduct (ICoC) for Outer Space Activities. The aim is to move towards enhanced safety, security, and sustainability of activities in outer space, build confidence among space actors, and limit the creation of space debris (see Chapter 4 for more details). Europe has also played an important role

5. A July 2008 European Parliament resolution on space and security underscored the importance of space assets to the security of the EU and that the ESP should not contribute to the militarisation and weaponisation of space. In September 2008, a Space Council Resolution further defined space and security as one of four new priorities, highlighting the important contribution of space to the CFSP/ESDP and the security of European citizens.

6. This concept was also acknowledged by the 7th Space Council in November 2010, the 2013 Commission Communication 'Towards a more competitive and efficient defence and security sector', the Final Report by the High Representative/Head of the EDA on the Common Security and Defence Policy (CSDP): 'Preparing the December 2013 European Council on Security and Defence', and the Council Conclusion on CSDP of November 2013.

in two UN initiatives on space security and sustainability: the working group on the Long-Term Sustainability of Outer Space Activities (LTSOSA), promoted by the UN Committee on the Peaceful Uses of Outer Space (COPUOS), and the Group of Governmental Experts (GGE) on Transparency and Confidence-Building Measures (TCBMs) in Outer Space Activities.

These international initiatives have been complemented by technical activities, in particular the development of technologies to monitor space objects and understand what is actually happening in outer space. Although ESA and some EU member states have assets that can be used for space surveillance, Europeans largely depend on the US for detailed information about objects populating space orbits and collision avoidance. Europe is therefore pursuing cooperative efforts to improve Space Situational Awareness (SSA) capabilities, with ESA focusing on space weather and near-earth objects (NEO) and the EU setting up a support framework for Space Surveillance and Tracking (SST), based on an open consortium of EU member states and the EU Satellite Centre.

The increasing focus on space security and sustainability issues in Europe is not only a result of the growing reliance on space systems and the evolving nature of space risks, but is also due to the expanding role of the EU as an owner and operator of space assets. This expansion has come about directly as a result of strategic concerns about European technology dependence and an acceptable level of non-dependence in space assets and services.

The EU's Global Navigation Satellite System (GNSS), Galileo, was developed primarily due to concerns about reliance on the American GPS. Galileo will ensure an adequate level of European autonomy and reinforce the resilience of Europe's critical infrastructure. Similarly, Copernicus, the European earth observation programme, has been developed to provide a sufficient level of autonomy in support of European policies. The Commission and ESA have also worked together to identify areas of critical dependence on foreign technology suppliers for which European alternatives would be welcome. ESA has also been central to the development of Europe's launcher projects, Ariane and Vega, which provide autonomous access to space.

At the same time, space infrastructure includes more than simply satellites and rockets. Ground stations and data links are an important part of this interconnected network. They are used to command and control satellites, and can be (and have been) targeted by both physical and cyber attacks. In 2008, for instance, an internet connection was used to hack into a ground station that controlled Terra EOS AM-1, a NASA scientific research satellite. The system was compromised and the responsible party achieved all of the steps required to control the satellite but did not issue any commands.[7] This incident serves as a reminder that security considerations must be addressed throughout the entire development and operations cycle, as satellite components could be infected with malware in the early development phase.

7. Luca del Monte, 'Towards a cybersecurity policy for a sustainable, secure and safe space environment', Proceedings of the 64th International Astronautical Congress (IAC), 2013.

## The European context for space security activities

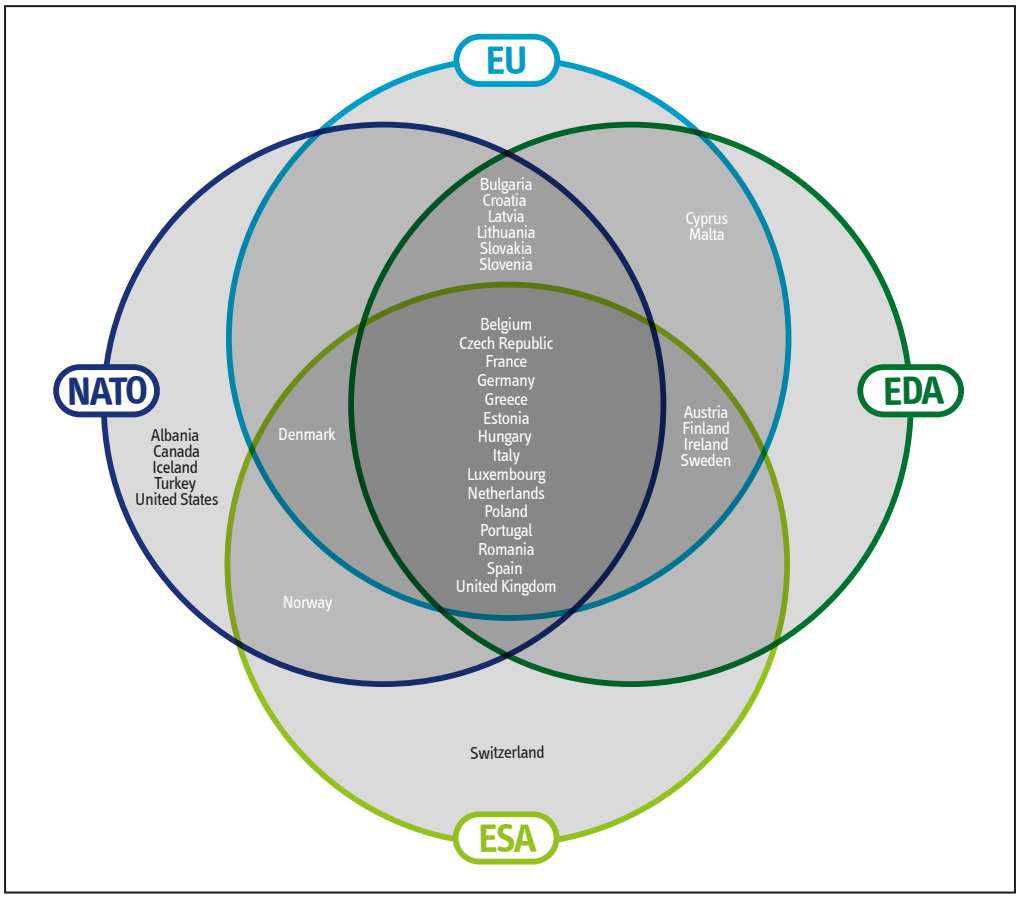
The entry into force of the Treaty of Lisbon granted the EU a stronger role in both space and security matters. It is the third institutional actor in European space governance, together with ESA and EU member states. Within the EU, the European Commission, the European Parliament (EP), the European External Action Service (EEAS), the European Defence Agency (EDA), and the EU Satellite Centre (EU SATCEN) have acquired new and increased responsibilities in space and security matters. Other stakeholders, such as Eurocontrol, the European Aviation Safety Agency (EASA), the European Maritime Safety Agency (EMSA), and Frontex might become increasingly involved, depending on future developments of space security activities. For member states, which are still the main policymakers for both space and security matters, governmental actors include national parliaments, ministries and space agencies. ESA, for its part, is an intergovernmental organisation with 22 member states, whose membership largely, but not completely, overlaps with that of the EU. Following the establishment of a structured dialogue on space and security, as called for during the 4th Space Council, ESA has increased its involvement in security and defence matters through a series of bilateral and multilateral cooperation agreements.[8] This evolution opens the possibility that ESA could be involved in a broader spectrum of space security tasks. At both national and European levels, commercial and industrial actors are essential partners of these three major institutional players. The diverse natures, interests, priorities, capabilities, and responsibilities of all of these actors create significant complexity within European space governance, particularly given their different constituencies, financial rules, legal statuses, and membership (see Figure 4 for more details).

## Report overview

Against this background, the objective of this Report is three-fold. First, it analyses the critical nature of European space infrastructure, both space and ground segments, assesses threats to this infrastructure (particularly cyber attacks) and evaluates possible responses. Second, it analyses the main security considerations related to the EU's current and future space activities – as a satellite owner, as a facilitator for European cooperation, and as a diplomatic actor. Third, it offers a number of ideas for improving European strategic thinking with respect to space security. The Report acknowledges that despite the emergence of the EU as a security and space actor, member states must continue to play essential roles in steering common policies, furthering European space activities and leading technological development.

8. The 2009 EC/EDA/ESA European Framework Cooperation for defence, civilian security and space-related research; and the 2011 ESA/EDA Administrative Arrangement.

**Figure 4: NATO, EU, EDA and ESA memberships**




The next chapter of the Report further examines the links between space and security, explaining why space systems need to be considered when addressing critical infrastructure protection policies, and provides an assessment of, and responses to, the main risks to space assets. The third and fourth chapters analyse security considerations related to EU space programmes, the main challenges to international cooperation on space security and the role of diplomacy in securing outer space. Particular attention is given to Space Situational Awareness in Europe and the EU's major diplomatic initiative, the proposal for an International Code of Conduct for Outer Space Activities. The final chapters analyse the space policies and doctrines of the EU and some of its member states, and assess options for moving forward.

In order to realise the full potential of its significant space-related investments, Europe would benefit from a detailed and coherent reflection on space security leading

to a joined-up approach. This may involve making security a pillar of European space policies and strategies, integrating space into European security strategies, or crafting a more ambitious strategic approach to space security. The objective of any of these approaches would be to frame the existing, scattered European initiatives in a way that promotes the safe, secure and sustainable operation of space activities and services, encourages the development of new space capabilities, and improves European space cooperation. More specifically, the space security component of any of these strategic approaches could address the following issues:

- Resilience of space infrastructure and services
- Space security risks and system protection
- Space sustainability
- Space diplomacy as a means to ensure transparent, sustainable and secure use of outer space
- Space Situational Awareness
- European space cooperation and governance
- Dual-use (civilian-military) approaches for space programmes
- Data policy
- Industrial policies for technological non-dependence
- Research into future challenges and responses, including preliminary assessments of Space Traffic Management (STM)

These issues can have sensitive political and security implications for the governments involved; transforming them into implementable policies would require time and effort to ensure the buy-in of all parties concerned.

Space deserves the highest consideration in European security agendas, and its inclusion into wider security frameworks can help strengthen European autonomy and power in other domains. This may include the development of more institutionalised connections between space and the Common Foreign and Security Policy (CFSP). Europe faces growing, interlinked and asymmetrical threats in multiple fields. Confronting them will require improved cooperation, clear strategy frameworks and the effective use of all available tools.

# II. SPACE SYSTEMS AND CRITICAL INFRASTRUCTURE

Modern societies are highly dependent on the continuous operation of critical infrastructure to ensure the provision of basic goods and services. They consist of assets, systems or parts thereof which are so vital, that their disruption would significantly impact the economy, national security, public health, safety, or social well-being. Examples of critical infrastructure include energy, water, food supply, communication, transportation, and waste processing systems.

Space assets are so deeply embedded in developed economies that a day without fully functioning space capabilities would severely restrict or even endanger our lives. Space systems are critical for running energy grids and telecommunication networks, border and maritime surveillance, crisis management and humanitarian operations, environmental and climate monitoring, verification of international treaties and arms control agreements, and the fight against organised crime and terrorism. Space assets also provide the technological backbone for other critical infrastructures. The synchronisation of power grids and telecommunication networks, for example, is heavily dependent on GNSS timing signals and any disruption would create a domino effect on other critical infrastructures (see Figure 5).

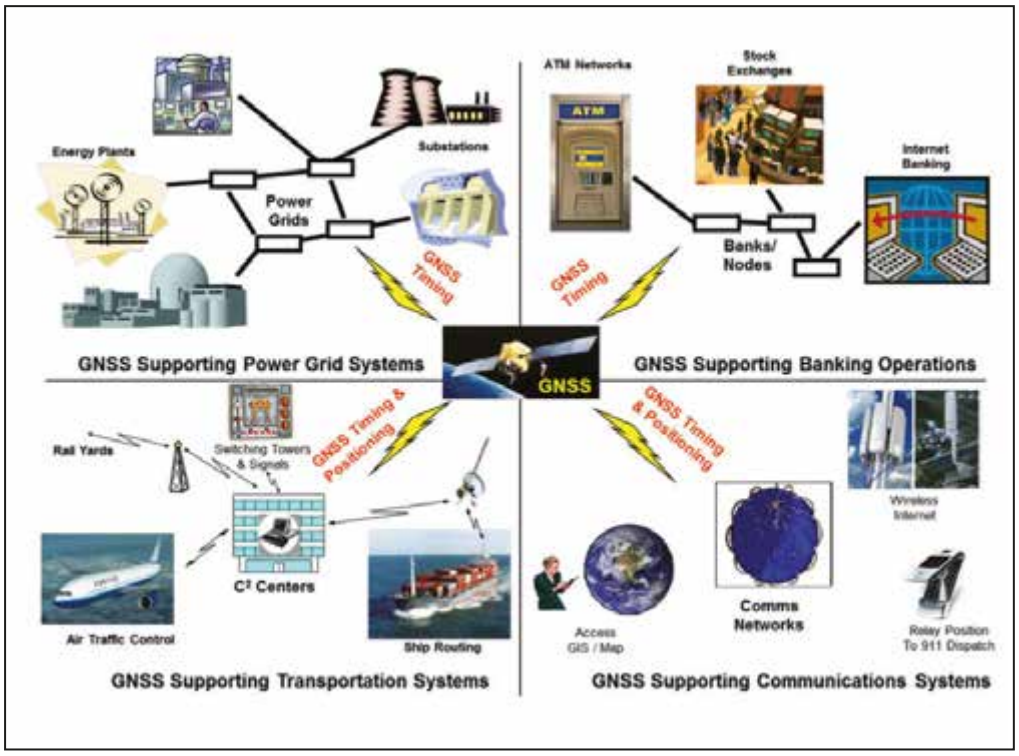
Satellites also play a central role in supporting defence systems and military operations. They are force multipliers that provide intelligence, surveillance, and reconnaissance (ISR) capabilities, as well as communication, navigation, positioning and timing signals. Armed forces do not only use their own space systems, but are also significant consumers of space services provided by private operators. In fact, about 90% of US military communications traffic passes through civilian satellites, many of which privately owned, rather than through dedicated systems designed to withstand attempted interruptions.[1] The reliance of both civilian and military users on space systems therefore places them firmly in the area of critical infrastructure.

Some critical space systems, such as the American GPS, are under foreign control, and the governments controlling those systems retain the authority to disrupt services, even for allies, in case of a national emergency. While the United States announced that it has no intention of ever intentionally degrading public GPS signals (also known as 'Selective Availability') and that the next generation of GPS satellites will not include this feature, other governments might still do so.[2] These dependences engender new and growing vulnerabilities.

1. Liviu Muresan and Alexandru Georgescu, 'The Road to Resilience in 2050: Critical Space Infrastructure and Space Security', *RUSI Journal*, vol. 160, no. 6, 1 December 2015.

2. US Office of the Press Secretary, Statement by the Press Secretary, 18 September 2007. Available at: http://georgewbush-whitehouse.archives.gov/news/releases/2007/09/20070918-2.html

**Figure 5: Today's reliance on GNSS positioning and timing signals**




Source: Modified from R. James Caverly, 'GPS Critical Infrastructure - Usage/Loss Impacts/Backups/Mitigation,' 27 April 2011.

Reliance on space is likely to increase further as space capabilities and services improve in diversity, quality and affordability. Close to 1,500 satellites with a launch mass of over 50 kg are expected to be launched over the next decade; an increase of 50% compared to 2005-2014. This estimate excludes both the expected proliferation of smaller satellites (such as CubeSats), but also the planned OneWeb and Steam mega-constellations for global internet broadband service. Advances in small satellite capabilities and in launch technology (e.g. SpaceX's Falcon rocket family) have already lowered the cost of access to space. About 45% more CubeSats were launched in 2014 than in 2013 (130 vs. 91), accounting for 63% of all satellites launched[3]. However, just as the reliance on space increases, so too do threats and vulnerabilities. Therefore, in order to realise the full potential of investments in space, critical space systems need to be adequately protected and the space environment properly managed.

3. Satellite Industry Association, *2015 State of the Satellite Industry Report,* September 2015.

## Threats to space assets and services

Satellite systems operate in the most hostile environment known to man. They are subject to numerous threats and hazards, both man-made and natural, such as space weather, anti-satellite weapons (ASAT), or collision with space debris and other space objects. Space assets and services are regularly confronted with signal jamming (often unintentional) and cyber attacks. These attacks can often be launched at little cost and require limited technical expertise, making them available to non-state actors such as terrorist groups and criminals, which are not receptive to the logic of classical deterrence. Even in the absence of a particular threat, the stressors of the space environment and the intricacy of space systems mean that unexpected malfunctions may always occur. Another potential threat to space systems relates to hybrid warfare techniques, particularly deception propaganda and other threats associated with information dominance.

A general taxonomy of threats and hazards is summarised in Tables 1 and 2 below. A first level classification consists of intentional and unintentional threats, while a second level classification labels threats by platform, and lists the vulnerable components. An expanded table in Annex 1 lists potential impacts, likelihoods, and mitigation strategies.

**TABLE 1:** INTENTIONAL THREATS TO SPACE SYSTEMS AND SERVICES

| Intentional threats to space systems and services | Vulnerable component |
|---|---|
| ***Space-based*** | |
| Kinetic energy weapons (e.g. in-orbit ASAT) | Satellites |
| High-altitude nuclear weapons (e.g. electromagnetic pulses) | Satellites; ground segments; data links |
| Directed energy weapons (e.g. laser, microwaves) | Satellites; ground segments; data links |
| ***Ground-based*** | |
| Kinetic energy weapons (e.g. ground-based ASAT) | Satellites |
| Physical attack | Ground segments; data links |
| Sabotage | Data links |
| ***Interference and content-based*** | |
| Cyber attacks (e.g. bugs, backdoors, malicious software, data interception, denial of service, spoofing) | Satellites; ground segments; data links |
| Jamming | Satellites; ground segments; data links |

Source: modified from Michael Sheehan, 'Defining Space Security' in Kai-Uwe Schrogl et al. (eds.), *Handbook of Space Security* (New York: Springer-Verlag, 2015).

**TABLE 2:** UNINTENTIONAL THREATS (I.E. HAZARDS) TO SPACE SYSTEMS

| Unintentional threats to space systems and services | Vulnerable component |
|---|---|
| ***Space-based*** | |
| Space weather (e.g. solar flares, geomagnetic storms, cosmic radiation) | Satellites; data links; ground segments |
| Space debris | Satellites |
| ***Ground-based*** | |
| Natural disasters (e.g. floods, fires, earthquakes) | Ground segments; data links |
| Loss of utility supplies (e.g. black-outs, water outages) | Ground segments; data links |
| ***Interference and content-based*** | |
| Human interference (e.g. terrestrial and other space-based wireless systems) | Satellites; ground segments; data links |
| Solar and atmospheric disturbances | Satellites; ground segments; data links |

Source: modified from Michael Sheehan, 'Defining Space Security' in Kai-Uwe Schrogl et al. (eds.), *Handbook of Space Security* (New York: Springer-Verlag, 2015).

## Intentional threats

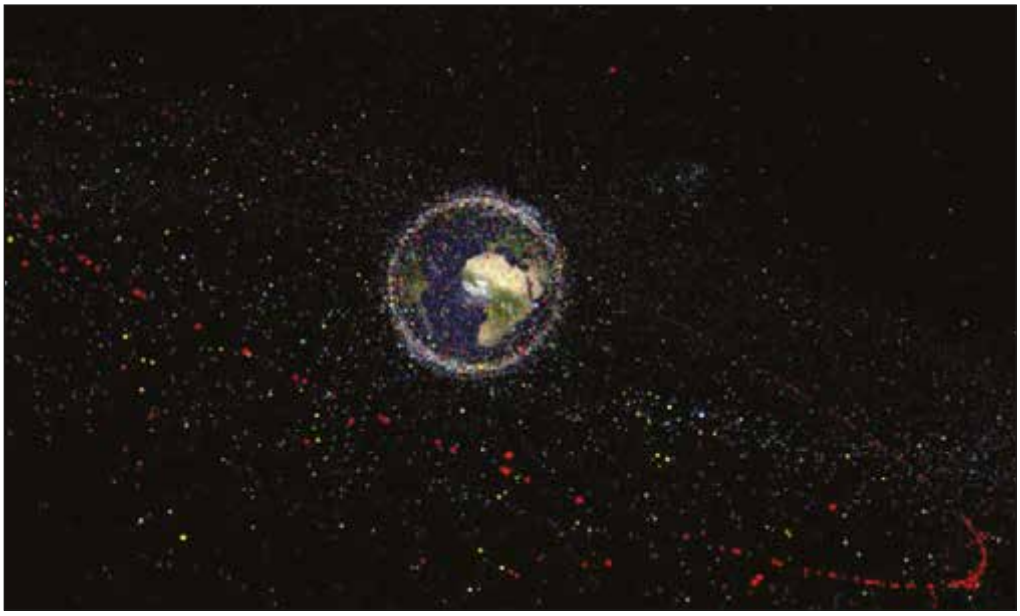
The development of weapons to shoot down or disrupt satellites dates back to the Cold War, when American and Soviet space programmes were military-driven and had a dual-use philosophy regarding new technologies. Today, many other actors can develop anti-satellite weapons, multiplying the risk of outer space weaponisation and missile proliferation. In 2007, China destroyed one of its own satellites with a ground-based ASAT attack, and demonstrated its capability to manoeuvre near satellites in geosynchronous orbit. Within the last year, Russia has also tested missiles capable of taking down satellites, and practised manoeuvres that have brought its satellites close to others, which is seen by many as another type of weapons test[4]. The US also is testing manoeuvrable space vehicles (e.g. the X-37B). Increasingly, non-kinetic weapons such as lasers or electromagnetic pulses have been seen as less damaging to the space environment, potentially less traceable, and having different deterrence objectives, particularly if they are used to interrupt or disable rather than to destroy other satellites. The value and threat of counter-space actions continues to inform the space security strategies and defence planning of the major space powers.

4. "Un satellite militaire français de télécommunications espionné par un engin 'non identifié' ", Opex360, 31 May 2016.

## Hazards

The majority of space systems are concentrated in a limited number of orbital bands, valuable because they pass directly above important markets or areas of scientific and military interest. Decades of launches, accidents and collisions have produced nearly 30,000 objects (17,000 of which are tracked and catalogued) larger than 10 centimetres and 750,000 objects larger than a centimetre. Even millimetre-sized objects (more than 170 million are estimated) are extremely dangerous. While most eventually re-enter the Earth's atmosphere, this usually requires a low orbit or an inordinate amount of time. This means that accidental collisions with debris or even satellites are quite possible. Indeed, in 2009, the Iridium 33 and Kosmos-2251 satellites collided, producing over 2000 long-term fragments of debris. The US Strategic Command (STRATCOM) recorded more than 8,000 collision-warning notifications in 2014 alone, 121 of which translated into collision avoidance manoeuvres, including by the International Space Station (ISS). Orbital space is one of the least regenerative environments known to man, and there have been fears that if the density of space objects becomes too high, one final collision may produce a self-sustaining chain of collisions, rendering low earth orbit (LEO) a dangerous minefield (a phenomenon referred to as the 'Kessler syndrome').

**Figure 6: Satellites and space debris (larger than 10cm) orbiting Earth**



Source: ESA.

Space weather is another threat. Cosmic radiation, solar flares and coronal mass ejections can damage satellite payloads and sensitive electronics through exposure to highly energetic particles. Space weather also disturbs the ionosphere, degrading communications and GNSS signals. In 2003, increases in solar activity forced astronauts in the International Space Station (ISS) to take refuge in specially shielded areas, and multiple satellites were lost.[5] Space weather can also lead to significant damage on earth. The 1859 Carrington event, the largest solar storm ever recorded, disrupted measurement devices, and severely damaged the telegraph network, while smaller geomagnetic storms in March 1989 cut electricity supplies to six million people in Quebec and forced the grounding of many airplanes. [6] A 2008 report by the US National Research Council[7] estimated that another Carrington-level event could cause damages of $2 trillion in the first year for the US alone, with a recovery time of four to ten years, without counting damages caused globally or lost economic opportunities.

**Box 1 – Cyber attacks: an emerging threat to satellites**

Space systems present a triple opportunity for hackers: the hardware and software embedded in a satellite, the information that the satellite transmits, and the network of ground stations it relies upon. Not only do satellite data and services make attractive targets for cyber attacks, but there is also the risk that hackers could take physical control of satellites via remotely configurable computers or network intrusion of ground stations. Cyber attacks could even lead to the destruction of a satellite, for instance by adjusting solar panels to overcharge the energy system or by moving it into the path of other satellites.

Because space systems contain a variety of components, often manufactured by foreign suppliers, there is a potential for compromised hardware to harbour latent backdoors, bugs, or malwares that can be activated once in space. In one case, ESA purchased microcircuits that only an in-depth microscopic analysis could prove had been degraded at a fundamental level. Had the attack not been detected in time, it would have helped hackers access the satellite.[8] Long lead times in the space industry also contribute to satellite vulnerability. It is not unusual for a satellite to require a 10-year 'time-to-market', which can make some of the security preparations outdated unless project management includes design re-schedule plans to adapt to advances in cyber technology. The intense competition to launch new satellite networks may also push commercial actors to develop cheaper solutions that might be less secure. This may also affect the military domain, which increasingly relies on commercial satellite communications; this makes it a priority for military users to account for potential security gaps resulting from their reliance on civilian systems.

5. Muresan and Georgescu, op. cit. in note 1.

6. Ibid.

7. National Research Council, Severe Space Weather Events – Understanding Societal and Economic Impacts: A Workshop Report (Space Studies Board, Division on Engineering and Physical Sciences, National Research Council, Washington, DC, 2008).

8. Ari Rabinovitch, 'Space age perils: hackers find a new battleground on the final frontier', Reuters, 22 October 2015.

Cybersecurity requires a holistic approach. The resilience of cyber systems will be built upon effective encryption, robust system architectures, continual software updating and effective monitoring and response. For space systems, this can be complemented by a specific focus on hardening ground segments. Ground station terminals are often off-the-shelf computers and network equipment which are widely known and replicated. They are vulnerable to standard cyber attacks with potentially serious impacts and need protection using the most advanced techniques, and buttressed by systematic connections to Computer Emergency Response Teams (CERTs) and immediate responses to any potential software security hole as soon as detected. Should breaches occur, protocols must be in place to limit the damage, trace the sources, and adjust security for other systems that may be similarly threatened in the future.

One of the main challenges for both space and cyber personnel is to understand how the cyber landscape will evolve in the next 15 years, so as to design new generations of satellites accordingly. In the meantime, cybersecurity awareness needs to be raised within the entire space community, from regulators to end-users. Space projects are often conducted with a scientific culture of openness and transparency which make them vulnerable to cyber threats. While military satellites still rely heavily on encryption and security through obscurity, many civilian systems are not properly protected. More cooperation and information sharing is needed to identify common risks and define appropriate solutions, even though the exchange and disclosure of vulnerabilities is highly sensitive. The space industry, including public and private operators, is well-placed to start this information-sharing process, which could lead to the creation of a common repository of cyber-based occurrences and serve as a basis for further benchmarks, sharing of best practices, and implementation of counter-measures.

European space actors have an opportunity to cooperate more closely on their cybersecurity efforts to facilitate protection of their data, missions, and the satellites they develop, including by supporting the security needs of satellite telecommunications operators through technology development. For example, the EDA and ESA have been expanding their cooperation on cyber issues. The ESA conducted two classified studies with support from industry players to establish technical recommendations and an ESA-wide cybersecurity policy.[9] This led to the establishment of a cyber range at the ESA facility in Redu with the aim of providing a training, simulation and testing environment to respond to and recover from cyber attacks. The ESA and EDA have recently concluded a letter of intent to include this facility within the set of cybersecurity ranges to be pooled by EDA member states in the framework of its wider cyber defence agenda. Striving for coherence among the various technical guidelines and cybersecurity policies across the continent can further help facilitate these efforts.

9. Luca del Monte and Stefano Zatti, 'Preliminary reflections about the establishment of a cybersecurity policy for a sustainable, secure and safe space environment', *Proceedings of the 64th International Astronautical Congress (IAC)*, 2015.

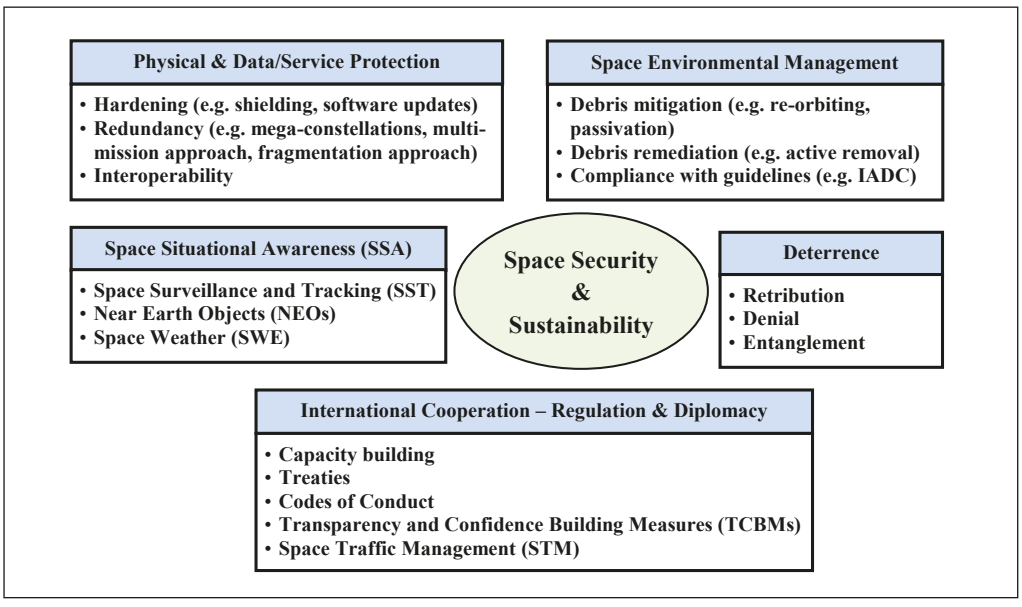
## Responses

There are several options to increase the security of space systems, ensure a space environment free from threats, and enhance the sustainability of outer space activities. They include the physical protection (i.e. hardening) of ground- and space-based assets, space environment management, Space Situational Awareness, deterrence, as well as political and diplomatic instruments (see Figure 7). European space actors have made significant investments to respond to these challenges, but not all threats can be anticipated, and efforts to eliminate all sources of risk are neither feasible nor cost effective. In this context, the international space community's attention has shifted towards resilience to ensure service delivery in case of disruptive events.

The difficulty of protecting critical space systems is heightened by the challenge of pursuing effective cooperation internationally, with each state prioritising different goals and means of managing their infrastructure dependence and sovereignty choices. Countries with no space programme depend on space systems controlled by other countries or that are the property of foreign companies operating under foreign laws.

Many of these threats, and the kinds of responses available, are identical across all space actors, whether commercial, institutional or military and whether European, American, Russian or Asian. Increasing awareness of shared concerns about space weather, debris, accidental collisions, non-state cyber attacks and accidental jamming may influence how space actors choose to cooperate with each other to face these and other threats. This will have implications for designing and managing protection and information systems, and for the pursuit of diplomatic endeavours, both within Europe and across the globe.

**Figure 7: Responses to threats and hazards to space systems and services**



## Physical and data/service protection

Physical protection can involve the hardening of space systems (e.g. adding advanced radiation shielding or more robust electronic components able to withstand space weather phenomena), changing designs to place sensitive devices away from probable impact trajectories, or changing how constellations are designed and used. The deployment of new and numerous satellite constellations adds redundancy, contributing to service robustness. The multi-mission approach used by Copernicus, for example, with contributing missions in tandem with dedicated Sentinel satellites, augments the availability, redundancy and integrity of data. These changes have costs, of course, as reliance on multiple data sources requires extensive data protection measures to handle transmissions from the many different systems, and hardening efforts may entail additional costs or be limited by satellite payloads.

The weight limitations of space launch systems imply that every system must be tailor-made to suit its unique mission requirements. This limits the ability of other satellites outside of the mission-specific units to serve as substitutes or extra capacity to increase the resilience of the system-of-systems. Another limiting factor is the current lack of refuelling capabilities, which reduces the lifetime of satellites even when the components themselves are still operational. A solution to minimise these limitations and associated effects would be to divide space architecture among several spacecraft, so that losing one of them does not jeopardise the whole system (the 'fragmentation approach').

The development of cyber protection measures is required throughout the design, deployment and operation of space assets. The rapid pace of change in the cyber world means that satellites can no longer be launched and left to themselves, but instead often require on-board software updates to maintain protection levels (see Box 1 on cyber threats for more details). Owners of space assets must also carefully manage their supply chains, verifying that their suppliers are trustworthy and effective in their own security protocols, in order to ensure that defective or compromised components are not introduced.

Developing ground-based resilience to the threats emanating from space is an option available even to non-space-faring nations. This may include using thermal control systems to protect terrestrial energy systems against 'space weather' or creating signal-boosting ground stations for GNSS constellations. Importantly, an appropriate equilibrium should be maintained between space services and ground-based systems for collecting data and transmitting information.

In sum, redundancy is difficult to achieve, hardening is expensive, replacement is time consuming and threats are omnipresent, which makes dependence on critical space infrastructure even more worrying.

## Space environment management

Keeping space clean helps ensure the long-term sustainability of outer space activities. Europe has an excellent track record in this area. It has produced only about 6% of orbital space debris and has been active in establishing and implementing requirements to reduce debris. Measures for effective space environmental management are multiple and diverse. They involve space debris mitigation and remediation activities, as well as compliance with international guidelines, such as those issued by the Inter-Agency Space Debris Coordination Committee (IADC) and the UN COPUOS.

One way to reduce space debris creation is to remove satellites from densely populated regions at the end of their missions, either by moving them into very low orbits to facilitate re-entry and burn-up, or by moving them into graveyard orbits and 'passivating' them by consuming any stored energy. The IADC recommends the following procedure:

- In Low Earth Orbit (< 2,000 km): re-entry in less than 25 years;
- In Geostationary Orbit (36,000 km): manoeuvre to graveyard orbit of +/- 200 km from GEO.

Even when responsible re-orbit is accomplished, spacecraft break-ups are likely to happen due to leftover fuel, material fatigue or pressure increase in batteries. Passivation of propulsion and power systems would ensure that the remaining propellant and batteries are correctly discharged. Furthermore, 'design-for-demise' technologies can ensure that spacecraft burn up completely upon re-entering the Earth's atmosphere.

Active debris removal technology is also being studied, including by private industry, but technical and legal challenges have been raised relating to the capture of space objects, as well as the dual-use potential of these technologies. The future development and deployment of such technologies may become more urgent should the debris problem continue to worsen, but an internationally agreed legal regime would be needed since the owner of the debris is the sole party responsible for it.

ESA Clean Space, for example, looks into the necessary technology required to lower both the terrestrial and space environmental impacts of space operations. While it builds on existing research for active debris removal, such as the ROGER and DEOS projects, it also aims to develop new methods for de-orbiting or re-orbiting to ensure effective post-mission management for satellites and launchers.

## Space Situational Awareness (SSA)

Space Situational Awareness is the capability to assess activities in space and, in particular, monitor hazards to space infrastructure. SSA information is useful for reducing the

risks of collision between space assets, for tracking debris, or for planning future manoeuvres. SSA is also useful for governments to understand the strategic evolution of the space environment, characterising possible hostile behaviours or violation of space treaties. Governments that do not possess such capabilities risk becoming victims of false information.

Although ESA and some member states have SSA assets, Europe still depends on the US Space Surveillance Network for detailed information on space objects, as it lacks autonomous sources of information. To improve its capabilities in this regard, the EU has recently set up a support framework involving an open consortium of member states to network existing SST assets and provide anti-collision alert services at the European level. Further plans include the development of fully-integrated SSA capabilities, with a view to respond to the full range of threats originating in the space environment (see Chapter 3 for details).

## Deterrence

Intentional threats to space assets may be deterred if any prospective aggressor can be persuaded that the risk, cost and potential for failure of such an attack would outweigh the benefits. In fact, both Cold War superpowers were aware of their common vulnerability, and this type of mutually assured destruction (MAD) is one reason why ASAT development was relatively limited during the Cold War.

Deterrence mechanisms can be based on threats of retribution, denial, or entanglement. Deterrence by retribution would involve threatening punishment against the adversary's satellites or other targets that would dramatically increase the opponent's costs and place their assets at risk. In wartime, should the aggressor realise that such an attack would exponentially increase its chances of success, threatening to shoot back its satellites would have very little deterrent effect. Deterring attacks on those satellites that are not of essential strategic value (such as in the nuclear chain of command) will thus require well-crafted strategies more similar to those used for terrestrial deterrence (e.g. denial).

Deterrence by denial would entail persuading the aggressor that it is not worth performing an attack against a satellite, as the chances of success are low and potential benefits limited. Building satellite system resilience is thus a way to deter a well-informed adversary.

Deterrence by entanglement, on the other hand, is based on the concept of interdependencies that would prevent an actor from attacking foreign satellite constellations which also serve the attacker's interests. However, for countries that are less dependent on space infrastructure, the level of interdependency is not balanced, and the mutual destruction of space infrastructure in times of conflict could potentially be worth the cost.

Deterrence can be greatly reinforced through multinational engagement. Sharing capabilities with third parties, and thus infusing redundancy into a country's own systems, spreads and dilutes some of the risks. However, hostile non-state actors or rogue states may have no such compunctions and may have options for attack that bypass any deterrence strategy. If managed poorly, increased capability-sharing and interconnection among systems might actually increase the risk of cyber attacks, as attackers would have a larger number of individual nodes and potential weak points to access.

### International cooperation

International cooperation can play a major role in reducing tensions, altering threat perceptions and facilitating shared activities to protect space systems and prevent space from becoming a new battlefield. Good communication and effective diplomacy can help create a community of stakeholders sharing common goals and values with regard to the long-term sustainability of the outer space environment. The full spectrum of international cooperation mechanisms includes capacity building, legally binding treaties, customary law, arms control agreements, test bans, voluntary codes of conduct, international guidelines for space debris mitigation, transparency and confidence-building measures, and other multilateral or bilateral diplomatic actions.

While the idea of a new formal international legal regime may meet with some resistance, TCBMs are expected to play a major role in encouraging states to maintain the security of space. Europe has been at the forefront of this issue and plays a pivotal role in addressing the issue of space sustainability through a proposal for an International Code of Conduct for Outer Space Activities. Future frameworks could possibly include space traffic management concepts similar to current air and sea traffic management regimes.

Europe also pursues space security through its bilateral relationships, including dialogues that the EU and ESA have held with Brazil, China, Japan, Russia, South Africa and the US, on topics that include satellite navigation, earth observation and joint space research (see Chapter 4 for details).

## The EU and Critical Infrastructure Protection

Critical Infrastructure Protection (CIP) is a framework that recognises the critical nature of infrastructures and their extensive interdependencies. Initially developed in the EU as a response to terrorist threats, today's EU CIP policy has shifted to the 'all-hazards approach' and fits into the broader framework of homeland security and civil protection policies.

Space security has been present in CIP discussions since the conception of the first common EU framework for CIP, the 2006 European Programme for Critical Infrastructure

Protection (EPCIP), and was discussed in early documents as one of eleven critical infrastructure sectors.[10] Although a Commission communication setting out its approach towards this sector was long planned, a formal inclusion of space systems within critical infrastructure frameworks gained little traction.

The subsequent Council Directive 2008/114/EC focused on the energy and transport sectors, indicating ICT as an area for possible future CIP expansion. While this directive set the conditions for identifying and designating European Critical Infrastructures (ECIs), and established the minimum requirements for their protection, it also required member states to share information and be open about their vulnerabilities. Although the implementation of the directive has been patchy, with few new ECIs identified and Operator Security Plans produced, it has contributed to improving the level of awareness and cooperation, especially on a bilateral basis. Member states thus questioned whether the same results might have been obtained through other, less resource-intensive means than a directive, as recognised by the 2012 Commission Working Document that reviewed the EPCIP.[11]

The findings of this 2012 review were further reflected in a new approach to the European Programme for Critical Infrastructure Protection, laid out in a Commission Staff Working Document from August 2013.[12] This approach sets out a revised and more practical implementation of the EPCIP, focusing on interdependencies between sectors and across national boundaries, since threats to any specific critical infrastructure can have significant wider impacts. This document identifies Critical Infrastructure (CI) sectors that did not receive significant attention in previous documents, with a view to developing tools for improving CI resilience. For example, it outlines an approach to CIP in which Galileo was identified as one of the four critical infrastructures of a European dimension, though this has not led to its formal designation as a 'European Critical Infrastructure', as defined in the 2008 directive. The reshaped EU CIP approach also recognises that space and cyber infrastructures are intimately linked, reaffirming concepts mentioned in EU documents on preparedness for cyber attacks.[13]

The EPCIP remains a work in progress. Various EU policies contain ambitious plans for prevention, preparedness and response, but leave it up to member states to protect criti-

10. European Commission Press Release, MEMO/06/477. The 2005 Green Paper on a European Programme for Critical Infrastructure Protection, COM(2005) 576 final, also listed 'space and research' as a sector of critical infrastructure. The Commission later restated that space infrastructure is critical infrastructure: see European Commission, Communication to the Council, the European Parliament, the European Economic and Social Committee of the Regions, 'Towards a Space Strategy for the European Union that benefits its citizens', COM(2011) 152 final, Brussels, April 2011.

11. European Commission, 'Commission Staff Working Document On The Review Of The European Programme For Critical Infrastructure Protection (EPCIP)', SWD(2012) 190 final, Brussels 22 June 2012.

12. European Commission, 'Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection - Making European Critical Infrastructures more secure', SWD (2013) 318 final, Brussels, 28 August 2013.

13. European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection – 'Protecting Europe from large-scale cyber attacks and disruptions: enhancing preparedness, security and resilience', COM(2009) 149. Brussels, March 2009; and Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, 'Achievements and next steps: towards global cybersecurity', COM(2011) 163, Brussels, March 2011.

cal infrastructure located in their own territory, as is the case with Galileo and EGNOS ground stations. While the existence of a legal instrument (i.e. the 2008 directive) has encouraged the development of CIP policies and has allowed for the creation of specific national CI bodies, the future evolution of the EU's role in protecting critical space infrastructure is unclear. The arguments in favour of a stronger EU role seem nevertheless comprehensible; the EU will own space assets for years to come and failures in space infrastructure could have transnational effects, as interdependencies are not limited to single countries. Nevertheless, the ultimate responsibility for CIP remains with member states and infrastructure operators.

Despite this situation, the EU will still have an important role to play. While currently limited to a supporting and facilitating role, the EU will continue to shape CIP policy developments, foster cooperation among members of the CIP community, and allocate funding to support key policy objectives. Concrete actions are already visible. Over €11 million in Horizon 2020 funds have been allocated to space research projects in the field of 'security in space', in addition to €23.6 million distributed through the Seventh Framework Programme for Research and Technological Development (FP7). Furthermore, the European Commission has encouraged the adoption of risk assessment and risk management methodologies based on a 'system approach', where critical infrastructure is treated as an interconnected network. In doing so, the Commission has recognised that sectoral measures would reach their limits as soon as cross-sectoral issues arise, as is the case with complex space systems that include the interaction of both cyber and physical layers. This is an area where the EU can support member states, as they have repeatedly expressed an interest in this. The Commission's efforts to develop new risk assessment methodologies for critical infrastructure protection have been an important step in this regard.[14]

One of the main future challenges for the EU in the field of CIP policy would be the coordination of the many potential separate space CIP approaches. The EU may continue to facilitate closer cooperation between member states and the private sector, including through private-public structured dialogues. This could pave the way to addressing the role of space systems within critical infrastructure frameworks and motivate Europe to take the initiative on future CIP policy.

## An agenda for the EU

Critical infrastructure protection has so far been applied at national and EU levels for terrestrial infrastructure with less focus on space assets. However, the critical importance of space systems is no longer in doubt. Effective guidelines for the protection of space infrastructure would help systematise and improve efforts to identify threats, mitigate vulnerabilities and minimise disruptions to space systems.

14. European Commission, Joint Research Centre, *Risk assessment methodologies for critical infrastructure protection. Part II: A new approach,* 2015.

National efforts alone, including those of the premier space powers, might have limited success without being embedded into wider international efforts. Improved international cooperation, including the potential creation of stronger institutional, legislative and administrative frameworks to govern space activity can help achieve effective critical space infrastructure protection. Some progress has already been registered in building the legislative and institutional framework for critical space systems protection and development at the international level. The UN COPUOS conducts varied research and regularly issues policy recommendations to member states regarding threats, opportunities and the implementation of new standards for achieving economic and security synergies. The International Telecommunications Union (ITU) and the Inter-Agency Debris Committee (IADC) regulate certain aspects of space governance and risks. There has even been an attempt at codifying aspects of commercial law in order to reduce uncertainties and costs for private/commercial actor involvement in space, through the Space Asset Protocol of the International Institute for the Unification of Private Law (UNIDROIT).

Ultimately, due to the fragmented nature of EU security systems and national jurisdictions, there is a need and opportunity for EU-level research on critical infrastructure dependencies and inter-dependencies with regard to space systems, such as that performed by the United States.

## Looking ahead

The incentives to use space services are increasing and it is thus up to the responsible stakeholders (governments, service providers, consumers, technical authorities and international organisations) to create appropriate instruments for identifying and addressing the associated risks. Managing the threats to space systems combines technical issues with legal and diplomatic ones, and also requires trade-offs relating to the allocation of scarce budgetary resources at national and European levels. There are a few strategic considerations to keep in mind in this regard.

Firstly, economic efficiency is, in a sense, inimical to security. Doing more with less, especially in the field of space services, leads to greater critical dependencies and risk of disruption, which is why the growth of private interests in space should not only be assessed as a positive development.

Secondly, the extremely hazardous environment of space is actually useful for stress-testing systems without the threat of systemic disruptions. The strengthening effect of permanent or recurring stressors has been termed ‘anti-fragility’. For instance, the losses resulting from small-scale solar flares have highlighted the importance of shielding and redundancies, and have arguably made the system more resilient in the long run. Had the space environment not been so harsh, there would have been a risk of only realising the full devastating effects of space weather when a Carrington-level event would have wiped out most space systems.

Thirdly, the greatest protection for space systems is to have built-in redundancies and substitutive capacity, both within the particular constellation or system, but also throughout the entire system. Greater inter-operability and standardisation of equipment can help achieve this, in addition to economic gains from economies of scale.

Furthermore, circumstances are a key factor in assessing the importance of a space system. For example, while the loss of a weather satellite may not be a major blow to security under normal circumstances, it is if it happens during a hurricane. Likewise, the loss of the Japanese ALOS remote sensing satellite just as the Fukushima nuclear reactor disaster unfolded was detrimental to crisis response efforts.

Lastly, space and terrestrial infrastructures can be best protected if countries, companies and international organisations integrate them into overarching CIP efforts and strategies. Space infrastructures operate globally, thus rendering their critical role even more apparent, as there is no hope of regional containment in case of disruptions. In the end, we are only as secure and as prosperous as the entirety of our critical infrastructures will allow.

# III. SECURITY DIMENSIONS OF EUROPEAN SPACE ACTIVITIES

This chapter outlines the 'what' and the 'why' of some key EU space activities, including connections with broader European security issues. It addresses the evolution and governance of these activities, and investigates the security challenges and responses related to the initiation, design and operation of particular space-related programmes. These include strategic non-dependence, the integration of resilience/protection into the design and operation of space programmes, and the challenges of data policy – its collection, management, protection and related sovereignty issues.

European space activities can be categorised as national, EU, ESA or multilateral cooperative programmes. Europe has independently developed programmes in all the key categories of space capabilities, with the exception of human access to space.

Space activities in Europe have been driven primarily by civilian rather than defence considerations, with military purchases accounting for only a tenth of the European space manufacturing market in recent years, mainly conducted at the national level exclusively. This is markedly different from the situation for other space powers, and means that Europe's civilian systems – both commercial and institutional – are essential for enhancing continental research and industrial capacities. Europe's space programmes also provide strategic services that are critical for maintaining its economic and political strength (see Chapter 2 for details). Table 3 divides European space activities into six main categories:

- The intergovernmental launcher programme run by ESA provides Europe with an acceptable level of autonomous access to space. The successful completion of the Ariane-6 and Vega-C programmes, currently under development, will sustain European autonomy beyond the next decade.

- Originally used primarily by national militaries, earth observation satellites are increasingly being developed, launched and used by commercial, institutional and environmental actors, including the EU's Copernicus programme.

- Satellite telecommunication is a mature market. At national level, satellite communications (SatCom) programmes are the most common and advanced type of programmes, generally developed for military purposes (MilSatCom). Following a 2013 European Council mandate, the European Commission and EDA are cooperating with member states and ESA on preparations for a governmental SatCom system (GovSatCom) that should offer improved security and control compared to commercial systems, without the associated costs and security controls of MilSatCom.

- Global Navigation Satellite Systems (GNSS) have historically been beyond the reach of all but two states, Russia and the US, although programmes with regional coverage are being developed by China (currently expanding into a global effort), India and Japan. The EU's Galileo programme will provide global coverage by 2020.
- A limited range of Space Situational Awareness **(**SSA) programmes and Space Surveillance and Tracking (SST) sensors and processing facilities are operated by ESA and some EU member states. A framework for cooperation between these states and the EU is being developed to deliver EU-wide services.
- For satellites tasked with security-sensitive electronic intelligence (ELINT) and early warning, collaboration between member states is limited.

**TABLE 3:** EXAMPLES OF PUBLIC SATELLITE PROGRAMMES IN EUROPE*

| | Launchers | Earth Observation | SATCOM | Navigation & Positioning | SSA/SST | ELINT-Early warning |
|---|---|---|---|---|---|---|
| **National Programmes** | | Present: SPOT (FR), Helios 2 (FR), Pléiades (FR), COSMO-SkyMed (IT), SAR-Lupe (DE), TerraSAR-X (DE), TanDEM-X (DE)<br>2016:2018: CSO (FR), CSG (IT), SARah (DE), PAZ (ES), Ingenio (ES) | Present: Skynet 5 (UK), SatcomBw (DE), SECOMSAT (ES), Syracuse (FR), Sicral (IT)<br>2017-2019: Heinrich Hertz (DE), Comsat NG (FR), SigMa (IT) | | GRAVES (FR), TAROT (FR), TIRA (DE), Starbrook (UK), Fylingdales (UK), Chimbolton (UK) | Present:<br>ELISA (FR)<br>2020+: Ceres Future Early Warning Space Based System (FR) |
| **Cooperative Multilateral Programmes** | | Helios 2 – COSMO-SkyMed (FR-IT), Helios 2 – SAR-Lupe (DE-FR), ORFEO (IT-FR) | Sicral 2 (IT-FR), Athena-FIDUS (IT-FR), ESCPC (EDA), ETISC (EDA), SECTELSAT (EDA), NSP2K (NATO) | | | 2020+: Ceres (FR) |
| **ESA Programmes** | Present: Ariane-5, Vega<br>2016-2021: Ariane 6 | Earth Explorers, Proba-V | EDRS | | ESA SSA Programme | |
| **EU Programmes** | | Copernicus | Exploratory work on GovSatCom | Egnos, Galileo | SST support framework (EU, FR, UK, DE, IT, ES) | |

**This list is not exhaustive, highlighting major programmes and missions. It does not include weather satellites, science missions or extra-European international partnerships.*

Sources: Modified from Veclani *et al*, 2014, with additional information from the ESA.

The four EU activities listed in Table 3 above (Galileo/EGNOS; Copernicus; SST support framework; and GovSatCom) are discussed in more detail below.

## Galileo and EGNOS

Galileo is the EU's Global Navigation Satellite System (GNSS). It has had a long and challenging development period, with its goals, governance, funding, and security considerations undergoing multiple changes over more than two decades. The primary driver for creating a European navigation and positioning system was to guarantee uninterrupted GNSS services as a strategic asset for Europe, since the GPS is controlled by the US military and the US government originally retained the right to degrade GPS signals at its discretion. although the US announced that it would discontinue this Selective Availability capability in 2000, other world powers, including Europe, chose to develop their own systems anyway. While the GPS, BeiDou (China) and GLONASS (Russia) are military programmes, Galileo is the world's only civilian-controlled system. Although its Open Service, Commercial Service and Search and Rescue signals will be available for use by all users, a Public Regulated Service (PRS) is available to all PRS participants for government use.

Galileo was originally envisaged as a partnership with the private sector and other governments. The involvement of external partners proved controversial, both in terms of how it might affect the key goal of ensuring European autonomy in satellite navigation, as well as due to security concerns, as China simultaneously began developing its own system under military control. Therefore, by 2008, the EU decided to take full control of the project. Galileo is now recognised as an essential project in terms of European autonomy, infrastructure resilience and technological/industrial development. It is currently in its deployment phase, with 14 satellites in orbit and initial services expected by the end of 2016. Full operation is planned for 2020, providing global coverage with up to 30 satellites.

The European Geostationary Navigation Overlay Service (EGNOS), has been the first EU venture into satellite navigation. It is a satellite-based augmentation system that increases the accuracy of GNSS positioning (GPS today and Galileo in the future) to provide information on its reliability in Europe. EGNOS provides three services: Open Service, Safety of Life and EGNOS Data Access Service.

Galileo and EGNOS were both designed and developed by ESA, with initial funding from the EU and ESA member states. Today, they are fully owned and funded by the European Union and managed by the European Commission: this marks the first time that the EU will develop and operate such high tech and large-scale infrastructure. Galileo will provide several services worldwide:

- A freely accessible Open Service providing position and timing services;

- A Commercial Service that allows for a higher data throughput rate and enables users to improve accuracy;

- A contribution to the Search and Rescue (SAR) support service of the international COSPAS-SARSAT system, detecting distress signals and relaying messages to ground stations;

- A Public Regulated Service (PRS) with encrypted position and timing signals, high service continuity and controlled access. The PRS provides two signals that are protected against jamming and spoofing by advanced interference mitigation technologies. Each EU member state decides who may become an authorised PRS user on its territory, with expected use by emergency response, national security and military institutions. EU bodies, including the Council of the EU, the Commission, and the EEAS may also use the PRS, along with non-EU states and international organisations, subject to bilateral agreements.

Galileo is protected by a series of location-based, technical and operational measures. Location-based measures involve the duplication of critical parts of the system, including the Galileo Control Centres and the Galileo Security Monitoring Centre. The security architecture for Galileo and EGNOS is well established, with three main bodies providing oversight.[1] The Commission has overall responsibility for the management and the security of the programme. The European GNSS Agency (GSA) handles the security tasks via:

- the independent Security Accreditation Board, which is responsible for a range of tasks, including approving satellite launches, providing Authorization to Operate (ATO) systems in different configurations, providing ATOs for the ground stations, and taking decisions on PRS technology manufacturers;

- the Galileo Security Monitoring Centre, which manages PRS access, and monitors and takes action regarding security threats and operational issues.

The Council of the EU (and the High Representative in case of emergency) exercises responsibilities to avert threats arising from the deployment, operation or use of Galileo or EGNOS or in the event of a threat to the operation of the system or its services.

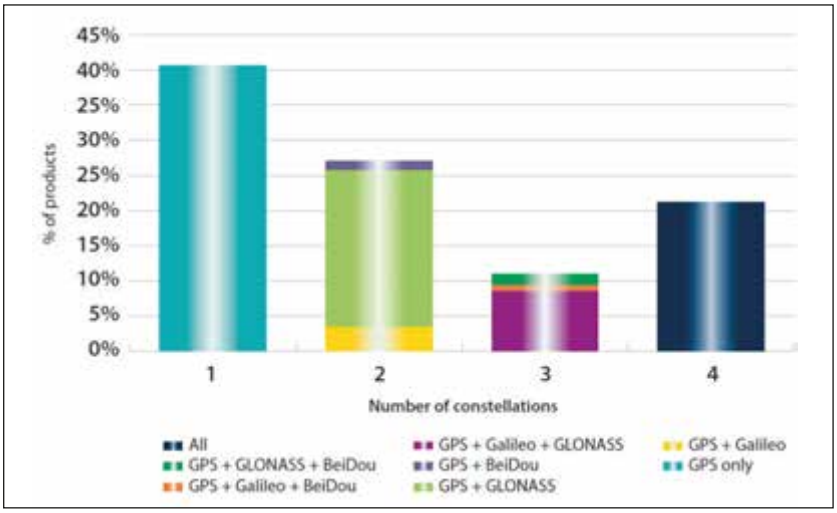
GNSS services are public infrastructure that facilitates economic activity, although estimates of the economic benefits vary widely. While only GPS and GLONASS are fully operational, China plans for its BeiDou system to have global coverage by 2020, India's regional IRNSS system is expected to be operational by the end of 2016, and Japan's QZSS system may be running by 2018. By 2020 there will be more than 100 GNSS sat-

1. See Council Decision 2014/496/CFSP of 22 July 2014 on aspects of the deployment, operation and use of the European Global Navigation Satellite System affecting the security of the European Union; Regulation (EU) No 1285/2013 of the European Parliament and of the Council of 11 December 2013 on the implementation and exploitation of European satellite navigation systems; Regulation (EU) No. 912/2010 of the European Parliament and of the Council setting up the European GNSS Agency; and Decision No 1104/2011/EU of the European Parliament and of the Council of 25 October 2011 on rules for access to the public regulated service of Galileo.

ellites in orbit, creating a competitive service market. Galileo will cover the Asia-Pacific region, for example, along with three other systems.

GNSS owners, including the EU, encourage the use of their own systems; the GSA is responsible for liaising with user communities about Galileo services and increasing the EU's share of the global GNSS market. Indeed, the GSA is providing €100 million to promote chipset and receiver development until 2020. Galileo's market share of GNSS equipment is estimated to be about one third of the global market, and the Commission has worked to identify policy options to secure the market uptake of Galileo, for which EU action within the scope of application of the TFEU would be welcome.

**Figure 8: Capability of available receivers to track multiple GNSS signals**




Source: GNSS Market Report, Issue no. 4, March 2015, © European GNSS Agency, 2015.

## Security considerations, lessons and priorities

*Autonomous capacity*: The primary reason for creating Galileo, avoiding dependence on external actors, remains a key factor when considering the protection of the Galileo system, the rollout of services, and the potential design of future Galileo generations. Europeans still rely on the GPS for many sensitive and high security issues, and would have to manage the repercussions if it became unavailable. In addition, dependence on applications and receivers that use non-European GNSS systems has commercial and strategic repercussions for governments wishing to support domestic industries and limit dependence on foreign technologies. Yet after 20 years of GPS reliance, adding Galileo to new and existing systems will not be automatic. Increasing numbers of chips and receivers are able to connect to multiple GNSS systems in a complementary manner, but this is not yet the default option. At the same time, while full EU ownership was determined to be the best

option for Galileo, this does not mean that all major space programmes require monopolistic development and control. As the number and capacity of both public and private space actors grows, new relationships may add value, even while the same challenges relating to strategic control and technological autonomy will need to be addressed.

*System protection*: A key lesson from the development of Galileo protection systems is to understand and address the strategic and security considerations of the system throughout its entire design, development, deployment and operation cycles. The continuous internalisation of security considerations – from the strategic level to the technical level – can be challenging when the rationale, governance model, business plan, and user community are in flux. Damage to individual satellites belonging to large, multi-satellite constellations may not necessarily disrupt GNSS services, but the system must still be protected against radio-frequency interference, jamming, signal falsification (spoofing), space weather impacts, or cyber attacks (see Chapter 2 for a full list of systemic threats).

*Security and defence connections*: The challenge of internalising security issues into system design is linked to the question of choosing partners for space projects. Galileo was designed as a civilian system under civilian control, but its signals will be used by other actors, including defence institutions, according to member state preferences. Despite limited defence interest and involvement in Galileo's early development, largely due to heavy reliance on the GPS, it is increasingly seen by both European and American militaries as enhancing their space resilience. In fact, the US has started dialogues with the EU concerning potential uses of the European GNSS, as Galileo is a potential second capability and deterrence contributor to the GPS. Today's militaries no longer question Galileo's usefulness, but are focused on how to access the service instead.

There is now also more acknowledgement that the potential threats faced by all space actors are similar, and that shaping cooperative responses makes sense. Early work on the next generation of Galileo has already started, thereby necessitating strategic thinking about user communities, contributing partners and security designs. As Galileo use becomes more common in the military sphere, civilian owners/designers can benefit from military resources and skillsets for designing security measures, even while retaining governance and operational autonomy. While many security ideas, mechanisms and systems begin with a military focus, they can find modified applications in the civilian domain. Increasing military use of Galileo should thus not be seen as a threat, but rather as an opportunity to strengthen system protection.

## Copernicus

Copernicus is the EU's earth observation (EO) programme, built on a partnership between the EU, ESA and member states. It uses data from multiple sources to facilitate work on the environment, transportation, energy, civil protection, internal market development, international cooperation, and foreign and security policy. As the system

develops, it will provide added value in crisis situations, as European member states and institutions seek near real-time data to facilitate critical decision-making.

Satellite EO programmes were first developed as national programmes, often run by member state militaries (see Table 3). Four EU member states have or will have national capacities. These four, along with other EU member states, Norway and Switzerland, also participate in EO programmes through ESA, or contribute funding to various partnership programmes in exchange for access. The idea of a common European EO programme was first presented in 1998, as the Global Monitoring for Environmental Security (GMES) programme. By 2001, the European Council called for the development of a European programme for Global Monitoring for Environment *and* Security. The system was formally kicked off in 2008 via a cooperative plan between the Commission and ESA (providers of the space component). In December 2014, the name was changed to Copernicus.

Copernicus builds on existing European and national capabilities, gathering information from the EU's new Sentinel earth observation satellites and data obtained through 'contributing missions': satellites operated by ESA, EUMETSAT, commercial companies, EU member states or third countries. This satellite data is complemented by networks of measurement equipment on the ground, such as ocean buoys and air quality monitoring sensors.

Copernicus provides six services:

- Land observation services provided at pan-European and local levels by the European Environment Agency, and at the global level by the Joint Research Centre (JRC) – operational since 2012;

- Atmosphere monitoring services provided by the European Centre for Medium-Range Weather Forecasts (ECMWF) – operational since 2015;

- Climate change services also provided by ECMWF – operational since 2015;

- Marine environment monitoring services provided by Mercator Ocean – operational since 2015;

- Emergency management services provided by the JRC – operational since 2012;

- Security services – scheduled to start in 2016:

    - Border surveillance provided by the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (Frontex), with the support of the EU Satellite Centre;

    - Maritime surveillance provided by the European Maritime Safety Agency (EMSA);

- Support to external action provided by the EU Satellite Centre.

The first Copernicus-dedicated Sentinel satellite was launched in April 2014, with up to 12 satellites expected to be in orbit by 2020. The budget for Copernicus within the Multiannual Financial Framework for 2014-2020 provides €4.3 billion, including €3.15 billion for ESA to cover the satellite network's operation and the construction of the Sentinel satellites.

## Security considerations, lessons and priorities

*Autonomous capacity*: As the EU has been entrusted with responsibilities and competencies in multiple fields, its need for autonomous supporting capacities has expanded. The history of the Copernicus programme reflects this evolution, progressing from an important but relatively narrowly-focused environmental monitoring programme into a strategically and tactically important tool that helps the EU make informed decisions and act using its own means. Minimising reliance on external actors for situational awareness on the ground has become an essential requirement. Protecting this autonomy involves more than simply launching and protecting space assets. It also involves fostering skillsets and human capacities to manage the programmes, coordinate with contributing missions, protect data and conduct the analysis to support decision-makers.

*Security and defence connections*: The Copernicus programme has three main areas of security support, regarding border surveillance, maritime surveillance and support to external action. The EU's comprehensive approach to crisis management allows it to draw on both civilian and military assets to support CSDP missions, as well as conflict prevention activities. As EU involvement in security issues expands, and as the threats to European security continue to change, the tools being used will need to be designed, managed and protected in a manner that reflects their evolving role. While even environmentally-focused programmes require robust protection in their own right, the use of Copernicus for security purposes probably increases the potential threats to the system, making it even more important to ensure the prioritisation of security considerations for the system's assets and procedures. This includes cooperation with security and defence actors involved in CSDP and border protection, who are thus users of Copernicus services.

*Data policy*: The free and open data policy of the Copernicus programme makes services openly available to global users, though with certain restrictions. Because Copernicus is a cooperative programme that relies on input from contributing missions, retaining the confidence of both data providers and service users requires that the security of the entire life cycle of the data be assured, guarding both how publicly owned data is shared and how data from contributing missions is managed. The capacity to manage huge amounts of data from heterogeneous sources is essential, balancing the need to keep the service open and useable, while still retaining sufficient control of data access to protect sensitive information. Strong cooperation in access to and sharing of national assets, data and services requires close cooperation between relevant EU entities and member states, and consis-

tent data policies that maximise the secure exploitation of data and its derived services. This will be especially challenging with the evolving relationships between government systems and commercial systems in terms of assets and data sharing. Importantly, the 2015 review of the Copernicus Security Framework confirmed that security of data and information within the Copernicus programme is adequately handled. It concluded that, in general, the current concept of entrusting the delegates to handle the security of data within their standard policies and processes is sufficient. Recommendations resulting from this analysis are currently tackled in the framework of the Copernicus Committee.

## Space Situational Awareness

Space Situational Awareness (SSA) is the capacity to view and understand the space environment and its evolution. In Europe, SSA covers three main areas:

- Space Surveillance and Tracking (SST) – identifying, characterizing, and tracking manmade objects in orbit;
- Near-Earth Objects (NEOs) – monitoring comets and asteroids that may affect earth;
- Space weather – monitoring and predicting the potential effects of space weather.

However, as stated in the 'Joint Framework on countering hybrid threats – a European Union response', the Commission proposes to expand these areas of activity to monitor hybrid threats to space infrastructures.

Maintaining situational awareness facilitates access to space and allows safer operation of space-borne systems. It allows the anticipation of emerging concerns such as space debris, the threat of in-orbit collisions, off-orbit failure or electromagnetic interference so that protective action may be taken. Being able to autonomously generate and use this information is not only an issue of credibility for a responsible space actor contributing to the sustainability and security of outer space, but also a strategic asset for technological non-dependence.

Private satellite operators track their own satellites using laser ranging, GPS telemetry, or satellite radio frequency signals. Although they are often able to provide exact data about their own satellites, disclosure and sharing of this data is not always a common practice, except where SST data is exchanged for SST services, as with the US system. The Space Data Association (SDA), for example, tracks objects in GEO orbit in order to prevent collisions, avoid interference and geolocate the sources of harmful interference. Members of the SDA are satellite operators – both public and private – including EUMETSAT, NASA and NOAA.

EU member states control a range of assets that can be used for SST, including surveillance and tracking radars, optical telescopes and data processing facilities as well as expertise (see Table 3 for details). Within Europe, states with SST assets have traditionally been hesitant to share their SST data, although France and Germany have cooperated on some projects. Many national SST assets were developed for ballistic missile tracking and are controlled by national militaries; the information that they generate is treated as very sensitive.

However, due to the substantial resources required, SST cannot easily be pursued at the national level. Most of the nations which own and operate military satellites, such as Japan and South Korea, are developing SSA capabilities and pursuing special military relations with the US on that matter. Only the United States has a fully developed global SST system, inherited from the Strategic Defence Initiative which developed a dedicated capability. Europe remains dependent on American information sharing. Cooperative activities in Europe formally started in 2007-2008 at ESA with a preparatory SSA programme. However, although ESA has the assets and expertise necessary to contribute to all areas of SSA, it is currently focusing its efforts on tracking NEO and understanding space weather phenomena. Meanwhile, member states remain hesitant about intergovernmental cooperation via the ESA framework involving potentially sensitive SST activities.

## EU SST support framework

In 2010, the Space Council recognised the need for effective European SSA capability and called upon the European Commission, in collaboration with the HR/VP, ESA and the member states to develop proposals that build on existing national assets. At the same time, the EDA was working on defining the needs for European military users and the potential for developing a Recognised Space Picture. In 2013, the Commission proposed a common SST framework underpinned by active member state participation. This was developed using an incremental approach, initially bringing together France, Germany, Italy, Spain and the UK to sign a consortium agreement and an implementing arrangement with the EU Satellite Centre in 2015. These states each own and operate SST components, and could potentially facilitate cooperation with assets, staff and processing capacities. Member state space agencies are the official counterparties to the agreement, although most of the main SST assets are under military control. The consortium will then expand to other interested member states with available resources. Poland and Portugal are expected to join in the near future. In line with the SST Decision, the EU will not contribute SST sensors, so its role will be different than for Copernicus and Galileo where it acts as programme owner and operator. This arrangement between the EU and a group of member states is a unique cooperation model among space or defence programmes.

Funding for the project will initially be drawn from Galileo, Copernicus and H2020 budgets, with €70 million earmarked over 6 years until 2020 to exploit assets and set up processing

capabilities. The Commission has earmarked an additional €120 million to upgrade the SST sensors of the Consortium as part of the H2020 Research Framework Programme.

The SST decision foresees the delivery of three services through the EU SatCen and generated by the Consortium:

- Supporting spacecraft operators by providing a service for collision avoidance (alerts);
- Creating surveys for fragment detection;
- Monitoring uncontrolled re-entry of space objects into the atmosphere.

## Security considerations, lessons and priorities

In addition to the space security benefits of generating or having access to SSA information, three key security issues need to be taken into consideration: dependence, data sensitivity, and diplomacy.

*Autonomous capacity*: SST efforts in Europe have historically suffered from a mismatch between high ambitions and limited cooperation. SSA spending in Europe is fragmented and far below that of the US, where military demand drives spending. In fact, SSA/SST in the US is a by-product of missile defence programmes, and has only recently been considered to be a key dual-use capability. Like China and Russia, Europe has limited capacity to track objects that are not located over its own territory and has therefore been largely dependent on American provision of SSA information. SSA has become a major area of focus for the US in recent years; it is developing an S-band space fence, wide field telescopes, and new partnerships to share data and site sensors. While American systems are the most developed, research is already being conducted on how to advance from existing passive systems to a real-time system that would make it possible to pre-empt potential threats. However, this would require capacity-heavy, high fidelity systems which would reduce bandwidth available to other applications.

Capabilities matter in international SSA discussions: only after France started tracking US military satellites did the US step up cooperation on SSA. France, Germany, Italy, Spain, the UK and ESA have information-sharing agreements with the US, primarily to receive American data, but also to contribute information from their own assets. The EU SST support framework is designed to help overcome this situation. Most of the members of the SST consortium have specific military relationships with the US, and the SST decision allows members to undertake necessary contacts and negotiations with Third States to improve the quality and autonomy of EU SST services.

*Data Policy*: SSA can involve more than mapping space objects – it is used to understand how satellites move, how they are used, and what they may do in the future. Security and

transparency issues will thus remain important in designing and managing SSA systems and in sharing the information that they generate. For example, strategic spy and military satellites could become visible to a wider audience, allowing interpretation of their capabilities, vulnerabilities and threat potential. European SST cooperation thus requires robust and sophisticated work on data policies and access rights, balancing openness with data protection, and managing the interests of multiple data providers and user communities. The security of the whole life cycle of the data has to be assured so that the availability, redundancy, integrity and validity of the data are assured, and that approved users can be sure that data delivery is secure and continuous.

The data challenge will only become more difficult as continuing improvements in sensors, software and processing power change what is trackable and by whom – effective SST assets are not all controlled by militaries any more. Private companies can provide SSA information to companies and states that used to be available only to the US government. The US Department of Defense has even contracted a private company, Analytical Graphics Inc. (AGI), to provide data management for space and defence purposes. AGI operates a commercial system (COMSPOC) which aggregates information from multiple unclassified sources, updating space maps without tasking assets to individual objects in the same way as military assets that were developed to track Soviet ICBMs. While this method cannot guarantee the reliability of its open-source data, and objects may have incomplete information for some periods, it is a harbinger of more, perhaps unwelcome, transparency in space operations.

***SSA as a diplomatic tool***: States wishing to keep their space assets hidden may see SSA capability development as a threat to their assets. SSA systems have in fact been developed mainly by national armed forces and can be also used for offensive purposes. SSA can also be a deterrent factor, since knowledge of what assets are visible and exposed may discourage aggressive actions. Effective SST capabilities could therefore help improve European positioning in international discussions on the development of SSA assets and the use of SSA data, providing European negotiators with a competitive information advantage.

As SSA capabilities become more widely available, they may also come to be seen as a tool for improving transparency and confidence building (see Chapter 4). SSA cooperation, even on a limited basis, could potentially lead to the development of a shared space objects catalogue for use by all space actors, facilitating collision avoidance and leading in the future to space traffic management. Various models have been proposed, ranging from better data sharing to creating an international SSA organisation that can catalogue and share data. Issues of frequency and orbit assignment are already dealt with in the dedicated international (ITU), European (CEPT) and national frameworks.

## Satellite communications

Satellite communications (SatCom) are space-based technologies that provide communications (point-to-point) and broadcasting (point-to-multi-points) services. SatCom have proven to be critical tools to facilitate government action, from transmitting diplomatic communications and planning emergency responses to maintaining command and control of security and defence activities. They are essential for enabling both civilian and military missions in areas with limited infrastructure. SatCom systems were first developed and controlled by national militaries, becoming a backbone for intelligence, surveillance and reconnaissance (ISR) activities, for the control of UAVs and for improving the network-enabled capabilities of combat units. Military satellite communications (MilSatCom) will remain in national hands for the foreseeable future, though there has been some SatCom cooperation on bilateral and trilateral bases (see Table 3 for details).

The recent launch of ESA's first European Data Relay System (EDRS) satellite marks an important step towards broader European SatCom cooperation, in this case as part of a pan-European civilian effort. EDRS will use laser communications to transmit large quantities of data from Copernicus Sentinel satellites down to Europe in near-real time. A second important example of European SatCom cooperation is the EU SatCom Market (formerly EU SatCom Procurement Cell – ESCPC), a service provided by the EDA as a one-stop shop to commercially source SatCom services. The EDA acts as the central purchasing body to obtain satellite bandwidth/airtime in all commercial bands, as well as terminal leasing. However this system may not provide the guarantee of availability required for a governmental service.

In 2014, the European Commission launched a study to define civilian user needs while the European Defence Agency (EDA) simultaneously pursued work to define military needs. Both governmental user communities, civil and military, share similar needs for SatCom. However, the current fragmentation of governmental demand can represent an obstacle to the deployment of proper security solutions and hamper cost-effectiveness. As a result, action has been underway in multiple areas. The EDA has been tasked with the development of proposals by the end of 2016 for a new collaborative SatCom programme, while ESA is proposing a three year preparatory programme to develop GovSatCom-related technologies and launch architectural design studies. At the same time, the Commission is considering the launch of an impact assessment, which is the prerequisite for a legislative proposal.

A potential GovSatCom system could be more robust and secure than commercial satellite services, but more readily available and accessible to regular government users than expensive dedicated MilSatCom systems. There are many open questions about how such a system would be designed, funded and governed, as well as about which mix of civilian and military institutions would use it. The status of existing systems and the impact on European industry would also need to be taken into account.

## Security considerations, lessons and priorities

*Commercial reliance*: SatCom are now used for a wide range of strategic, tactical and commercial applications. There has been rapid expansion of commercial capacities in recent years; SatCom have historically been the most (perhaps the *only*) profitable field of satellite usage. Bandwidth demands have been surging among government users as well, and government partnerships with private SatCom providers have become a normal business. They provide bandwidth as needed to complement government systems during crises and international expeditionary action – even if they are not all designed with the same security considerations as MilSatCom services. Most (or all) member states use commercial systems; even EU member states with their own SatCom services, as well as the US, use commercial support on an as-needed basis, often partnering with domestic satellite operators. France works closely with Airbus Defence and Space, for example, while the UK works with Paradigm (using former government Skynet satellites).

Discussions of potential partnerships with commercial providers involve questions about balancing the needs for system control, resilience, bandwidth availability, security, flexibility and affordability. Reliance on commercial systems comes with additional risks for both member state and European institutional users. When working with commercial actors, even those who often work closely with governments, industrial partners may not always have the security measures, protocol and capacities that government partners often require.

EU satellite operators depend more and more on the purchase of satellite bandwith by the Pentagon's DISA. However the US Department of Defense procurement procedure is likely to change. Structuring a demand for GovSatCom at the EU level would be one way to offer a guaranteed market to the satellite operators, encouraging further investment.

*Dual users, dual governance?* During the current process of reviewing user needs and possible models of cooperation, it will be important to remember the lessons learnt from the Copernicus and Galileo programmes, where ownership and governance models evolved over the years as the objectives of the systems changed. It would therefore be preferable to develop any potential system with comprehensive consultations in a federative multi-stakeholder process. Governance challenges will be difficult to resolve, considering the civil/security/military and intergovernmental/national mix of actors with differing interests in the system. While some space capabilities remain under national and/or military control, several areas exist where increased cooperation between civilian and defence activities can reduce costs and improve efficiency.[2]

2. Communication from the Commission to the European Parliament, 'Towards a more competitive and efficient defence and security sector', {SWD(2013) 279 final}, Brussels, July 2013.

## Looking ahead

Several common themes emerge across Europe's various different space activities. Firstly, there is clear value in ensuring an adequate level of European autonomy by developing independent technical competences and operational capabilities. A full understanding of the costs and benefits of relying on the US or commercial partners for information and capacity requires careful analysis.

Furthermore, there is a common challenge of integrating effective system protection measures throughout the conception, scoping, design, development, deployment and operation phases of space programmes. A more protection-oriented approach would help the EU be considered a more reliable partner in international cooperation efforts and increase market and user uptake of its two flagship programmes. With major trends (big data, computer speeds, cyber threats, new space actors etc.) developing quickly, extra care is required to future-proof big programmes with long lead times. Understanding changes in purpose and governance during the long-term development of Copernicus and Galileo, which resulted in differences between original intentions and current use or intentions, can help us understand how to develop other programmes.

Another recurrent theme is the apparent need for a new approach to data policy in order to provide effective security control. There is also a range of considerations connecting EU space activities with defence and security issues. While civil-military connections have long been the centre of debate, such as where and when dual-use projects are appropriate, what the security requirements should be, and with what implications for the nature and security of civilian governance, several factors are making this debate less divisive or problematic.

The nature of threats to space assets, and the types of responses that are possible, are very (although not entirely) similar for all actors in space – whether civilian, commercial or military, regardless of nationality. These common threat perceptions may readily serve as a basis for developing common responses. The nature of these activities often makes them dual-use by nature. The raw data produced by satellites is neither civilian nor military, but the way in which data is shaped and used makes it civilian or military. Galileo and Copernicus are potentially dual-use systems, with defence communities willing to make use of civilian capabilities under civilian control. SST capacities will be useful for protecting both civilian and military systems, while SatCom systems developed for commercial use are regularly used by defence departments.

As the Lisbon Treaty has increasingly been applied more fully, EU involvement in security issues has intensified, bringing the EU into closer cooperation with a range of European and international partners on defence and security issues. The EU is now well positioned to take on a key role in effectively responding to the shared threats facing its member states. The links between civilian and military programmes could therefore be increasingly seen as an opportunity for cooperation, as civilian systems can remain under civilian control while cooperating with defence partners that share the same concerns and objectives.

However, such cooperation is neither automatic nor obvious, otherwise it would have been pursued already. There remain different perspectives among member states about threat perception, options for addressing these threats, and what resources to devote in response. For example, there is the question of how to spend funds on any particular space activity if the costs and immediate operational benefits lie primarily with a few countries which own and operate space assets. It is thus vital to proceed with EU space activity development incrementally, gradually building balances of matching interests among member states and increasing collective confidence. However, this slow, pragmatic development of common interests has led to convoluted processes and changing priorities for space activities in the past. If systems have not been conceptualised and implemented with clear strategic direction or adequate protection from the start, this *ad hoc* development may therefore lead to *ad hoc* (and very expensive) security measures.

# IV. INTERNATIONAL COOPERATION FOR SPACE SECURITY

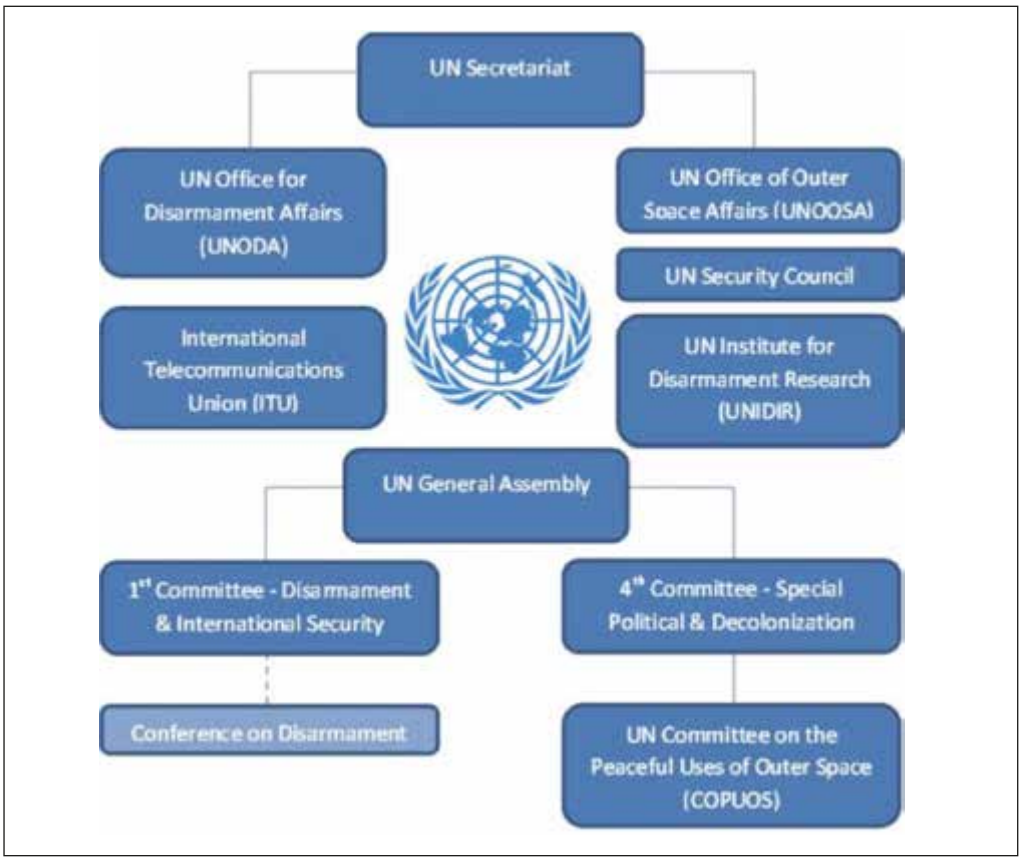
After almost 60 years of human activity, outer space is relatively lightly regulated. The UN Outer Space Treaty was signed in 1967, one year before the nuclear Non-Proliferation Treaty (NPT), and forms the primary foundation for outer space law. It addresses both arms control issues, the primary focus at the time of its creation, as well as conduct issues – how states operate in outer space. In particular, it bans the placement of nuclear weapons in space, requires states to avoid contamination of space, and makes states responsible for their space activities and liable for damages. All major space powers are parties to the treaty. Subsequent agreements on rescue, liability, space object registration, and the moon and other celestial bodies were added during the 1960s and 1970s. While no new treaties have been signed since that time, multilateral efforts have successfully led to some voluntary and non-legally binding agreement initiatives in the last decade.

The UN remains the primary multilateral forum to discuss space security issues, organised in several fora (Figure 9). The First Committee of the United Nations General Assembly (UNGA) is responsible for international security and disarmament matters, and is where the Conference on Disarmament (CD) reports on its work, including on space security issues. Unfortunately, the Conference on Disarmament has been highly politicised and progress on many issues has been stalled for decades, with few exceptions.

The Fourth Committee of the UNGA deals with special political and decolonisation issues, including outer space, and is where the UN Committee on the Peaceful Uses of Outer Space (COPUOS) reports on its work. The UN COPUOS is the primary international forum for the development of rules governing activities in outer space. It has a purely civilian focus and does not work on military or weaponisation issues. While many EU member states are COPUOS members, and the European Space Agency (ESA) has a permanent observer status, the EU does not. Its work is supported by the UN Office for Outer Space Affairs (UNOOSA), which serves as its secretariat.

The International Telecommunications Union (ITU) is the UN's technical agency responsible for allocating global radio spectrum and satellite orbital slots. Active since 1865, it has been regulating frequency and interference issues since 1963. All EU member states are also members of the ITU. While the EU is a non-voting sector member, the European Commission has played a coordinating role for member states.

**Figure 9: Main UN bodies relevant for space activities**




Outside the UN, several bodies play a role in facilitating discussion and research on space security, notably the International Academy of Astronautics and the International Institute of Space Law and the European Centre for Space Law.

International discussions on space security issues take place in all of these venues. While progress has been made on some issues, such as debris mitigation, others remain stalled due both to differences in what states wish to prioritise and the mechanisms by which they see space cooperation moving forward. Today's discussions on space security can be classified into two main categories: legally binding proposals and voluntary (or soft law) measures for responsible behaviour. The potential for a new formal international legal regime beyond the existing space treaties may seem slim, partly due to the long entrenchment of opposing positions among the leading space powers as well as to the rapid multiplication of governments that operate space assets. But progress on voluntary initiatives continues to move forward, as the self-interest of states is generally served by efforts to preserve the space environment and protect space.

## Legally-binding proposals

The Outer Space Treaty bans the placement of weapons of mass destruction in space, but is silent on other types of weapons, notably earth-based weapons that targeting space objects. In the decades since the signing of the treaty, there have been multiple attempts to address this gap. Initiatives on the Prevention of an Arms Race in Outer Space (PAROS) have been discussed at the UN and the Conference on Disarmament since at least the early 1980s, with rhetorical support from all sides, but limited progress. From those first discussions until today, there has been a long-running rift between Soviet/Russian/Chinese efforts towards a legally-binding treaty that prevents the placement of weapons in outer space and the attitude of Western states, which point to the emptiness of such a treaty without mechanisms for verification and compliance. PAROS discussions have thus become bogged down over incompatible national interests. While the US, for example, has an interest in defending its own freedom of action in space, where its technological superiority grants it important strategic advantages, China and Russia, playing technological catch-up, would prefer to hobble American efforts.

Discussions on legally-binding proposals have been primarily centred on arms control rather than on seeking to regulate space activities *tout court*. In discussing efforts to get countries on board for legally-binding approaches, lessons may be learned from past efforts, notably from the Non-Proliferation Treaty (NPT). The NPT requires that signatory states accept an explicit bargain – in exchange for not going nuclear, they could receive multilateral technical assistance on peaceful nuclear research and applications. The nuclear weapons states, in addition to providing this assistance, agreed to work toward nuclear disarmament. In later years, the nuclear-weapon states have been criticised for not sharing their technology and for the limited progress towards disarmament. This perception is important for how it may influence efforts to reach agreements in other fields of endeavour, including space, where a small group of powers have advanced capacities, and other states may mistrust their intentions and willingness to follow through with promises.

### Treaty on the Prevention of the Placement of Weapons in Outer Space (PPWT)

In 2008, after six years of discussions, China partnered with Russia in proposing to the UN Conference on Disarmament a draft 'Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects' (PPWT). Although it does not specifically deal with disarmament, it argues that adhering states should not place any type of weapons in space. Critics of the PPWT, however, note that the proposal lacks clear definitions of space weapons or threats, and that it allows the development, testing and storage of weapons, although not their deployment in space. It is also missing any credible monitoring or verification measures. Importantly, it ignores both ground-based weapons that could be used against satellites and issues related to dual-use technologies. The PPWT may thus be near useless as an

arms control treaty, as it allows for space weaponisation without really limiting an arms race in space. Nonetheless, efforts to push the treaty have met with some success in the UN and buttressed anti-Western sentiment. In particular, Belarus, Iran, Kazakhstan, Republic of Korea and Turkey stated that the proposal represents a good model for a future universal space treaty.[1] These diplomatic differences are potentially problematic for efforts to push forward other space security initiatives, including the EU proposal for an International Code of Conduct.

### No first placement initiative

In 2015, the UNGA approved a non-binding Russian resolution, forwarded from the Conference on Disarmament, restricting states from being the first to deploy weapons in outer space. The initiative passed the General Assembly with only four nations in opposition, including the US, while the member states of the European Union abstained.[2] Although the initiative suffers from the same flaws as the more ambitious PPWT, the voting split in the UNGA is worth noting when considering how the European Union and its member states approach space security both within and outside formal UN settings. The continuing appeal of such arms control rhetoric remains a factor in shaping international discourse on space security, potentially impacting efforts to win support for other space security initiatives.

## Voluntary measures

With limited progress on any new treaties, there has been increased emphasis on voluntary instruments aimed at preserving the safety of the space environment and enhancing trust among space actors. This includes proposals that focus less on what tasks individual satellites undertake (including potential military activities) than on what impact their operations have on the surrounding environment and on the activities of other space actors. Voluntary measures have the advantage of being flexible, testable, and useful for facilitating harmonisation among actors with different perspectives, without the need for intrusive verifications. More importantly, provisions contained therein constitute 'soft law' and are expected to be more easily negotiated and adhered to than legally-binding treaties. Once undertaken with sufficient consistency by enough of the right actors, voluntary measures can also develop into customary law, paving the way towards legally binding measures. While this transition can be seen as positive step by the supporters of voluntary approaches, it can also raise alarm bells among others who may see such efforts as an attempt to detract attention from stronger and alleg-

1. Gunjan Singh, 'PPWT: An Overview' in Ajey Lele (ed.), *Decoding the International Code of Conduct for Outer Space Activities*, Institute for Defence Studies and Analyses (New Delhi: Pentagon Security International, 2012).

2. United Nations,'General Assembly Adopts 63 Drafts on First Committee's Recommendation with Nuclear Disarmament at Core of Several Recorded Votes', Sixty-ninth session of UN General Assembly, 62nd Meeting (AM), GA/11593, 2 December 2014. Available at: http://www.un.org/press/en/2014/ga11593.doc.htm

edly more promising instruments. States may also be hesitant to sign up to voluntary pacts, only to find that the rules, expectations and pressures have changed, changing the 'voluntary' nature of the agreement. More worrisome, however, may be the opposite challenge: rather than deepening and progressing, voluntary measures may end up being honoured only with rhetoric or even ignored altogether.

Voluntary measures can include both technical guidelines for how to safely conduct space activities as well as transparency and confidence-building measures (TCBMs) for how to communicate about space activities. Commonly proposed conduct guidelines include procedures to prevent and minimise any form of damage and harmful interference (see Table 4 on page 60). TCBMs may include information sharing about policies, capabilities, intentions, spending, programmes, and SSA data about debris and the status of space assets. Other TCBMs include notifications (of launches, re-entries, tests and manoeuvres), the granting of access to space facilities, and consultative mechanisms to keep open channels of communication. If adhered to, TCBMs can keep doors open, leading to a culture of cooperation and openness to collective security ideals. The leading global initiatives including voluntary measures each involve a different balance of technical guidelines and TCBMs.

## IADC Space Debris Mitigation Guidelines

Technical guidelines on how to conduct space activities while limiting the proliferation of space debris were developed by the Inter-Agency Space Debris Coordinating Committee (IADC), an inter-governmental forum composed of 13 national space agencies, including those of France, Germany, Italy, and the UK, plus ESA. In 2007, under the auspices of the COPUOS, the IADC issued a series of voluntary guidelines for limiting debris during normal operations, for managing post-mission disposal, and for minimising the potential for on-orbit break-ups or collisions. The guidelines were adopted by the Scientific and Technical Sub-Committee of COPUOS (Feb 2007), COPUOS (June 2007) and the UNGA (December 2007). Notably, after years of negotiations, the guidelines were first approved mere weeks after China's January 2007 ASAT test increased the total amount of traceable long-lasting debris by 25%.

## Working Group on the Long-Term Sustainability of Outer Space Activities

In June 2007, the UN COPUOS began discussions on the issue of long-term sustainability of outer space activities. An *ad hoc* group of experts worked through 2008 and 2009 to develop the Brachet Code of Conduct, addressing a wide range of technical issues such as space debris mitigation and remediation, the safety of space operations, the radio-electric spectrum, and space weather; the group also reviewed existing international mechanisms to improve the safety and sustainability of space activities. This

work, while conducted informally, led to the creation of a formal Working Group on the Long-Term Sustainability of Outer Space Activities in 2010. The Working Group is developing a report on long-term sustainability – reviewing today's best practices, operating procedures, technical standards, and safety policies – upon which they will develop voluntary guidelines for the conduct of activities in outer space.

The 59th COPUOS session (June 2016) saw important progress as the first set of long-term sustainability guidelines were agreed. These guidelines are now ready for states and international organisations to consider implementing on a voluntary basis; the EU role in negotiations is gaining strength, as a common position was maintained throughout the meeting.

## International Code of Conduct for Outer Space Activities

The diplomatic deadlock over arms control discussions has encouraged the international community to pursue new venues for moving forward on space security. Stimulus for new initiatives was provided by the UNGA resolution 61/75 of December 2006 inviting member states to submit concrete proposals for TCBMs to promote international cooperation and help prevent an arms race in outer space. This instigated multiple efforts, including an Italian suggestion in March 2007 on the possibility of a comprehensive code of conduct. After further consultation within Europe, and in the tense climate resulting from the 2007 Chinese ASAT test, the EU published an initial draft of a voluntary code for outer space activities in late 2008. Today's version (March 2014) is the result of revisions (September 2010, June 2012, and September 2013) following bilateral and multilateral consultations with international partners.

While addressing both military and civilian uses of outer space, the Code is not intended to regulate the placement of weapons in outer space, but focuses on principles for responsible behaviour. It calls for space powers to prioritise safety and security in their conduct of operations, and to pursue TCBMs related to their space policies and activities (see Table 4 on page 60 for details). The Code also proposes the potential sharing of SSA-related information, organising visits to space facilities and supporting developing countries in space. The Code, while voluntary, would be a formal document that states would sign up to, and includes mechanisms for holding regular meetings and reviews. Notably, the Code includes a consultation mechanism through which subscribing states could request consultations to find mutually acceptable solutions should they potentially be affected by activities of other subscribing states.

The Code was not formally presented for negotiation at the Conference on Disarmament or COPUOS primarily due to its overarching nature: its focus on debris mitigation made it unsuited for the CD, while its security content prevented it from being formally introduced to COPUOS. Nonetheless, EU member states have ensured that the Code was discussed in these and other venues. The Code was presented on the margins of a COPUOS meeting in Vienna in June 2012 as the starting point for its discussion in

international fora. In order to secure international support, the EU organised meetings in Kiev and Bangkok in 2013, Luxembourg in 2014 and most recently at the UN in July 2015 in New York, taking into account feedback from these discussions. While there is widespread support for both the Code and the ideas it contains, some resistance has been expressed, especially from Russia and China. The process of developing the Code has been criticised for being EU-driven and insufficiently inclusive, with some states arguing that such initiatives should be developed only under the UN umbrella.

Other obstacles have slowed international acceptance of the Code. For example, a procedural motion at the start of the July 2015 meeting in New York downgraded the event from a negotiation to a consultation because the EU does not have member state standing at the UN. China has claimed that efforts to sell the Code have detracted attention from their own efforts on the moribund PPWT, and that weaponisation issues are absent. Some states also expressed concerns that the Code could limit their freedom of action in outer space. This includes newer space powers, which are worried about entry barriers that even a voluntary code could impose. The explicit reference to the right of 'self-defence' in the Code has also become an issue for disagreement.

Following the 2015 New York meeting, the EU and its member states reassessed their approach, concluding that the EU should continue to support negotiations within the UN on a non-legally binding agreement for both military and civilian activity. It was agreed that the United Kingdom, Germany and Italy should help lead the process forward, supported by the other member states and the EEAS.[3]

## Group of Governmental Experts' report on TCBMs in Outer Space Activities

Discussions in the Conference on Disarmament, tabled in the UN's First Committee, led to a UNGA mandate for a Group of Governmental Experts (GGE) to investigate TCBMs to improve security in space. The GGE, with representatives from 15 countries, including all major space powers, presented its report in July 2013 with recommendations for states to take voluntary action on two main types of TCBMs – information sharing (on goals, policies, programmes and even military spending in space) and notifications (of launches, manoeuvres, re-entries, break-ups and emergencies). It also recommended that states open their facilities to visits, create consultative mechanisms to ensure continued dialogue, and pursue cooperation and outreach activities, including with new and non-space powers. The Group also recognised the importance of existing commitments related to disarmament and non-proliferation, and that voluntary political measures can pave the way to legally binding obligations. The Report and its recommendations were universally welcomed by the international space community, but implementation has been slow; no space actors have yet systematically applied its recommendations.

3. Remarks by Bruno Hanses (EEAS) before 2016 UNIDIR Space Security Conference , 'Sustaining the Momentum: the Current Status of Space Security' (UNIDIR, Secure World Foundation, The Simons Foundation), Geneva, 28–29 April 2016.

**TABLE 4:** COMPARISON OF MAJOR INTERNATIONAL COOPERATION EFFORTS ON SPACE SECURITY

| | PPWT | International Code of Conduct | GGE Report on TCBMs | LTS Working Group (Draft Guidelines) |
|---|---|---|---|---|
| **Proposing Entity** | **Russia & China** | **EU** | **UNGA** | **UN COPUOS** |
| **Legal status** | Legally-binding treaty | Voluntary agreement | Voluntary guidelines | Voluntary guidelines |
| **Conduct Guidelines** | · No weapons in outer space;<br>· No threat or use of force against space objects;<br>· Will not engage in activities inconsistent with the treaty, or incite others to do so. | · Do not damage or destroy space objects;<br>· Minimise risk of collisions;<br>· Minimise debris creation;<br>· Implement IADC debris mitigation guidelines. | Implement other guidelines, including those developed through COPUOS. | · Conduct only activities of a peaceful nature;<br>· No cyber disruption;<br>· No deliberate alterations of space environment;<br>· Have structures, procedures and competencies for planning and conducting space activities sustainably;<br>· Respect ITU regulations on spectrum protection & ensure equitable access to geostationary orbit. |
| **TCBMs** | · The Executive Organisation of the Treaty shall collect and distribute any information provided by parties (the information to be provided is not specified). | · Notification of launches, manoeuvres, re-entries, malfunctions and collision risks;<br>· Information sharing on policy, strategy, research programmes and SSA info;<br>· Site visits & demonstrations. | · Information sharing on policy, goals, space military expenditures, registrations and orbital parameters of space objects;<br>· Notification of launches, manoeuvres, re-entries, malfunctions and emergencies;<br>· Site visits & demonstrations. | · Information sharing: develop a mechanism or procedures for information exchange on space activities, debris, space weather<br>· Enhance space object registration;<br>· Notification of launches is encouraged;<br>· Investigate shared rules for active removal and/or intentional destruction of space objects. |
| **Resolving grievances** | States concerned over possible violations may request clarifications, then consultations. The Executive Organisation may convene review meetings, and refer matter to UNGA or UNSC if not mutually resoluble. | States affected by activities contrary to Code may request consultations to find mutually acceptable solutions. | | |
| **Outreach and support** | | Is supported, especially toward developing countries. | Is recommended, notably within UN system. | · Raise public awareness of the importance of space sustainability;<br>· Support scientific, technical and legal capacity-building &improved data accessibility |
| **Verification** | None | None | None | None |
| **Coordination** | The Executive Organisation shall hold meetings on amendments, develop procedures for collective data sharing and conduct consultations into alleged violations. | · Regular meetings and Code reviews by subscribing states;<br>· Coordination points of contact established;<br>· Electronic database for sharing data. | · Coordination focal points established;<br>· Consultations are encouraged, notably using existing mechanisms. | · Provide contact details for information exchange bodies;<br>· Develop appropriate mechanism or procedures for information exchange on space activities. |

## Approaches to space security and diplomacy of major space powers

### United States – from dominance to resilience

The United States is the world's only space superpower, with advanced capabilities in all areas and space budgets far outstripping the other space-faring nations' (Table 5). During the Cold War, the US was focused on its primary adversary, both in terms of military supremacy and national prestige, with defence and intelligence requirements driving capability development, domestic space policy and its approach to international space diplomacy. Military counter-space actions were seen as the biggest space security threat, with the sustainability of the space environment becoming a bigger issue since the 1990s. In the last 25 years, U.S. space systems have been increasingly used for both expeditionary action and for enhancing the national security of the US – it relies more on space for military, intelligence, scientific and commercial activities than any other country.

**TABLE 5:** LARGEST SPACE BUDGETS (2013)

| Country | Budget (billion Euros) | GDP (billion Euros) |
|---|---|---|
| **USA** | 29.6 | 12,648 |
| **China** | 4.6 | 6,903 |
| **Russia** | 4.0 | 1,579 |
| **Japan** | 2.7 | 3,690 |
| **France** | 2.0 | 2,059 |
| **Germany** | 1.3 | 2,736 |
| **Italy** | 0.9 | 1,559 |
| **India** | 0.9 | 1,407 |
| **Canada** | 0.4 | 1,374 |
| **UK** | 0.3 | 1,899 |
| **ESA** | 4.3 | |

Source for data: OECD and ESA. Budgets include ESA contributions

There is no comprehensive governance system for American space activities but American space activities are still shaped by centrally directed strategic thinking. In recent years, the US has issued three key space documents, reaffirming that space is a national vital interest.[4] Each of these documents addresses space security issues, calls for the promotion of responsible, peaceful, and safe use of space, prioritises deeper coopera-

4. The National Space Policy of the United States of America (June 2010), the US National Security Space Strategy (January 2011), and the Space Policy of the Department of Defence (October 2012).

tion with key international partners, and emphasises the importance of TCBMs and international norms of behaviour for space security and sustainability. The documents also each call for improved US capabilities, increased system resilience, and for the US to be prepared to deter aggression, defeat attacks and operate in a degraded space environment.

Because of its reliance on space systems, US space assets are increasingly viewed as possible sources of vulnerability, reinforcing US interest in protecting them. While the US still remains committed to retaining global leadership in all space fields, its strategic thinking has been shifting from a focus primarily on maintaining dominance in space to a wider approach that also ensures continued resilience in the face of growing threats.[5]

This interest has translated into three main axes of activities. First, the US has undertaken a major modernisation of its space surveillance network - the world's only global SSA system – devoting additional domestic resources and partnering with more than 60 governments and organisations that have space surveillance capabilities. Second, it has developed programmes focused on operationally 'responsive space' (using quick launches, small disaggregated satellites, etc.), as well as new approaches towards the international partners and commercial operators that are seen as essential components of their security architecture. This is the case for telecommunications (through the use of commercially-hosted payloads and commercial bandwidth by the military), earth observation, and for SSA, with a growing role for private actors. Third, the US has also fostered R&D programmes for 'defensive' and 'offensive counter-space' to protect against possible hostile actions and to deter adversaries. Some of these efforts are controversial for other countries, as some American capabilities, notably in missile defence, SSA-dedicated satellites, and rendezvous-capable satellites, have been flagged as dual-use capabilities that can become or facilitate offensive threats.[6]

Multilaterally, the US contributes to all of the initiatives on voluntary technical guidelines and TCBMs discussed above. It debated internally about the potential impact on its space operations before offering support for the International Code of Conduct. Ensuring that its use of space for strategic purposes will not be unduly constrained has been an important factor in shaping American responses to the arms control initiatives presented at the UN.

With its advanced capabilities, the US has perhaps approached international bilateral cooperation as a one-way provision of assistance and data by the US, as part of a larger political relationship. Increasing capacity development by other states, along with a diminished confidence in its space dominance, has led to a renewed interest in what assets, data and resilience contributions different partners can bring.

5. See, for example, remarks by US Deputy Assistant Secretary of State Mallory Stewart, 'Formulation, Coordination, and Implementation of Promoting Space Security and Sustainability,' at 2015 Space Resiliency Summit, Alexandria, VA, 9 December 2015.

6. Sheng-Chih Wang, *Transatlantic Space Politics: Competition and Cooperation Above the Clouds* (London: Routledge, 2013).

The EU-US space dialogue, initiated at the EU-US summit in 2005, has achieved progress in the fields of earth observation, space research, navigation and GPS-Galileo interoperability (kicked off via the 2004 EU-US GNSS agreement). The mutual interest in increased transatlantic space cooperation also covers issues related to security and defence, which are dealt within a specific framework and under the joint supervision of the European Commission and the EEAS. Discussions regarding US access to the EU's positioning, navigation, and timing (PNT) services have recently been initiated, with the US planning to employ dual-use receivers (Galileo/GPS enabled) for its systems. Although negotiations on the utilisation of Galileo by the US are expected to start soon, interoperability and signal/system protection issues can become obstacles for which appropriate responses must be found. The last EU-US dialogue meeting took place in Washington DC on 10 December 2015. These dialogue meetings with the US, as well as with the other countries, are carried out at a technical level and are non-binding.

## Russia – a former superpower

Although far from matching US capabilities, Russia continues to be a global space power, maintaining capacities in all key asset classes and developing new space systems with increased manoeuvring capabilities. It is currently the only country providing human access to the international space station and operates the only functional global GNSS system (GLONASS) other than GPS. While funding has increased during the Putin years, a series of commercial, technical and launch failures have led to a massive reorganisation of the entire sector under Kremlin control.[7] Different strategic plans for the space sector have been developed, but in the current period of upheaval and reorganisation, it is unclear of their value in understanding Russian space priorities. Declared priorities for Russia's civilian programmes include human spaceflight, scientific research activities and support for the International Space Station, while the military has the completion of a functioning comprehensive early warning system as major goal, which is necessary for Russia's nuclear deterrent.

On the international stage, Russia plays the role of a proud but weakened anti-American power. With its short-lived satellites and large numbers of launches, and subsequent accumulation of space debris, Russia's action on space sustainability has been honoured primarily with rhetoric. Its technical troubles have also limited its attractiveness as a commercial partner on space projects. The importance that it places on its strategic nuclear deterrent, and its worries over American missile defence systems, colours its approach to space and security diplomacy. Russia's recent missile tests have been labelled as being related to ASAT development and its satellite rendezvous and proximity operations have been seen as intelligence-gathering activities; this has not contributed to enhancing confidence and preventing mistrust.

7. Christophe Venet, 'Space security in Russia,' in Kai-Uwe Schrogl et al. (eds.), *Handbook of Space Security* (New York: Springer-Verlag, 2015).

But Russia has contributed to all of the initiatives on voluntary technical guidelines and TCBMs discussed above (GGE, LTS, and IADC). It has also cosponsored the PPWT and been highly critical of the EU proposal for an International Code of Conduct. It has also criticised the US for its lack of positive initiatives and its resistance to any new space treaty ideas. Russia's positions on these issues within the UN, notably the PPWT, have won considerable support in parts of the world and there are now fears that, together with China, they could set the tone in international space security discourse. Russia has also pursued space diplomacy outside the UN, building relations through its support of the International Scientific Optical Network (ISON) across several countries in the global south, via technical space observation cooperation.

The EU established a dialogue on space cooperation with Russia in 2006 and the last meeting took place in June 2013. While full resumption of cooperation with Russia is not envisaged before the full implementation of the Minsk agreements, the EU remains open for constructive contacts. Cooperation in science, research and innovation is one example where relations with Russia continue, applying the EU's science diplomacy approach. Russia has participated in a large number of FP7 research projects on space. Separately, an ongoing EU-ESA-Roscosmos Space Dialogue developed two working groups: one on information satellite systems (including GNSS systems and EO satellites), and one on space sciences and technologies. Efforts to cooperate further on space debris modelling and information exchange, and on systems for providing space warnings and coordinating SSA interactions were discussed. Technical discussions with Russia are currently limited and take place mostly in a multilateral context (e.g. different UN fora).

## China

Reflecting its reticence about transparency in governance, China has not yet released any national space strategy or policy. But a review of its space activities and diplomatic posture allows us to interpret its key goals.

Despite decades of arms embargos, China has quickly become a major space power, with independent launch capabilities, an expansive human spaceflight programme, and a range of communications, surveillance, earth observation and navigation satellites. Following its January 2007 ASAT test, China has further developed its anti-satellite capabilities, including through non-destructive tests in 2013 and 2014. In particular, its 2014 firing of a missile into geosynchronous orbit raised questions about the extent of China's space capabilities and ambitions.[8] This unease has been compounded by evidence of successful rendezvous and proximity operations with other satellites in LEO.

China's goals, actions and diplomatic priorities in the space realm reflect its broader approach to international affairs and national security. It seeks to rapidly build up its national capacities to ensure full independence of action. It is hesitant to commit to any

8. Jeffrey Lewis, 'They Shoot Satellites, Don't They?' *Foreign Policy*, 9 August 2014.

international agreements that may limit its freedom of manoeuvre or may slow its build-up of national power. Decision-making is driven by national security goals, with military thinking and defence actors playing central roles and no substantive separation between civilian and military space activities. Like the US and Russia, China has directed great efforts at advancing its capacity to use space for military and defence purposes.

In international multilateral fora, China has been an active participant in space security and sustainability discussions, supporting the GGE, LTS and IADC initiatives. However, as these initiatives have all been developed following China's 2007 ASAT test, Beijing has clearly lost the moral high ground in space security-related discussions. China does not always share European priorities. It is not a signatory to the Hague Code of Conduct against Ballistic Missile Proliferation and has not been supportive of the EU initiative on an International Code of Conduct; it has instead worked closely with Russia to develop and push the PPWT.

At the bilateral level, the fact that efforts at cooperation with China on the Galileo programme eventually met with failure did not bode well for continued space partnership with Beijing, which has been rather limited. But diplomatic progress has been made in recent years. The EU-ESA-China Dialogue on Space Technology and Cooperation has met three times since 2012, discussing technical cooperation possibilities across all asset types. The third meeting of the EU-ESA-China Space Dialogue took place in June 2015. The meeting was an opportunity to take stock of the current space collaboration (in the earth observations, satellite navigation and space research field) between the three parties. The next meeting will take place in China in October 2016. Work on space security issues has been more limited, primarily due to the sensitivity of the topic.

## Main challenges to international cooperation

While some progress has been made on international cooperation regarding space security, a few key areas can be flagged as potential obstacles:

- Incompatible perceptions of the international security environment, and subsequent divergent national security goals and priorities.
- Historic geopolitical differences, such as between developing and developed states or between the West and the former Soviet states. This may lead to the nurturing of biases and suspicions that inhibit trust-building in space security discussions.
- Diverging preferences for the mechanisms, methodologies and settings to address and tackle key challenges – i.e. whether to pursue legally binding treaties or instruments of soft law (e.g. technical guidelines or voluntary codes), whether to do so with any particular forum or mandate, and what participants to include in the full discussions.

- Differing visions for the use of space. Military and defence demands have historically driven spending and policy among the largest space powers. Commercially driven space investments play a relatively larger role in Europe and for most new space powers. This difference can impact on how the two groups of space actors will approach issues of deterrence, counter-space capabilities, and the pursuit of collective security.

- Differing capacities that impact on how countries view the potential costs and constraints of international cooperation initiatives. Less advanced space actors may see the development of certain initiatives or cooperation tools as obstacles to their future presence in space. The leading space powers, for their part, may welcome some mechanisms to regulate space activities, but resist other measures that they see as restricting their freedom of action or expanding their presence in space.

- Ensuring compliance, even where states agree or express diplomatic support. For example, no space power has systematically implemented the recommendations of the Group of Governmental Experts and respected voluntary guidelines on debris mitigation.[9]

- Lack of coordination and communication efforts outside of formal UN settings.

## Looking ahead: space traffic management

The International Code of Conduct is not intended to replace other initiatives, but rather to complement them in accordance with the existing legal framework for outer space activities. On closer view, it contains elements for a potential comprehensive regulation of space activities in the future: Space Traffic Management (STM). The creation of an STM regime is a long term goal that incorporates aspects of both TCBMs and conduct guidelines. Rather than today's piecemeal engineering of space law, STM is a holistic concept that looks at the regulation of space activities comprehensively, aiming at the provision of a complete set of 'rules of the road' for the safe, secure and sustainable use of the space environment. Moving toward STM would in all likelihood involve the integration of current legal provisions and technical standards into one comprehensive text, the creation of new interacting levels and forms of regulation (including a legal delimitation of airspace and outer space), and new ways of organising and supervising space activity. Fully developed STM would probably involve active use of shared SSA data, a notification system for launches and orbital manoeuvres, concrete traffic rules (e.g. right of way, prioritisation of manoeuvres), and improved information sharing in multiple areas. More importantly, it

9. While 95% of satellites launched between 1957 and 2013 were registered, registration often happens months or years later, after being detected, characterised, and tracked by others, and not always with correct data. This has been a problem involving multiple space powers, although at last count Russia was up to date with its registration information (2014) See Jonathan McDowell, 'Adherence to the 1976 Convention on Registration of Objects Launched into Outer Space', Jonathan's Space Page, available at: http://planet4589.org/space/un/un_paper1.html.

would establish mechanisms for implementation and control, potentially including arbitration and enforcement measures. Much of this would be new and would require effective operational oversight from some current or future international body.

However, it is unclear how such a regime, replete with transparency requirements, could develop from the existing international legal framework and whether it would limit freedom of action in outer space.

The 2016 session of the Legal Subcommittee of the UN COPUOS marked the first formal discussion (at the intergovernmental level) of the contribution of STM to the safety of space operations and security in space.

## Europe in the mix

The space sector is going through important changes, with growing competition, commercialisation, congestion and the globalisation of value chains impacting state priorities. This, in turn, is affecting international relations in space, shaping which ideas and projects bring space actors to work together. While established space actors may look to a variety of partners when they plan their future programmes, newcomers to space generally prioritise cooperation with partners from which they can benefit via potential transfers of technology and expertise. In this context, Europe has a long tradition of openness towards international cooperation in space, including through the EU space flagship programmes Galileo and Copernicus, through space policy dialogues, and via Horizon 2020.

International engagement on space security can therefore proceed in tandem with efforts to strengthen European roles in global space discussions. This can include reinforcing the use of space assets for addressing global challenges (such as environment protection, climate change, sustainable development, and disaster response) while at the same time building space economic diplomacy to promote the European industrial base. International space cooperation can thus become a diplomatic tool that serves both as a market opener for the promotion of European solutions abroad and as a door opener to deeper cooperation on space security issues. And just as it is important to integrate space security priorities into broader space discussions, it is also important that space is integrated into EU external policy, embedded within the wider political and diplomatic framework.

Increased engagement and closer cooperation among the different European space actors – with roles, responsibilities and exposure depending on the particular issue and milieu – will be essential. Europe has unique strengths that make it well suited to shape global space discussions and promote sustainable norms of behaviour for space security. It is composed of different countries, often with contrasting interests, and when it speaks with one voice, Europe already represents a tried and tested mul-

tilateral view. Member states have played active roles within the GGE on TCBMs and the development of LTS guidelines, and helped promote and shape the EU proposal for an ICoC. The ESA has been involved in regulatory efforts to control space debris, primarily within the IADC (along with some European national space agencies) and UN COPUOS. And while not always present or able to participate in the same way as other entities within UN bodies, the EU has been able to use the ICoC to get involved in multilateral space security and sustainability discussions.

However, additional aspects need to be taken into account, including the role of the EU within the system of international space law. For example, while the ESA is a signatory to two of the five space treaties (i.e. the Registration Convention and Liability Convention), the EU is not, as it is not an intergovernmental organisation. Thus, although the EU is an owner and operator of satellites, EU-owned satellites are registered by the ESA in agreement with the Registration Convention. Further debate and action on the potential for the EU register, including by reviewing its position with respect to international space law as a whole, would be positive steps. In this respect, the positioning of the EU with respect to the main space fora and conventions will need to continue to evolve.

# V. ENHANCING EUROPEAN STRATEGIC THINKING IN SPACE SECURITY

Efforts to improve the security of space assets and the sustainability of space activities can be best facilitated where clear policies and a supportive strategic framework are in place. Strategic thinking about space security should take into account the different roles that space plays for European economy, security, autonomy and unity. A clear and shared European strategic approach to space security can provide a pillar around which institutions, member states, and industries may articulate and calibrate their own policies, activities and priorities, connecting these ideas to the capabilities and resources available. It can help drive cooperation among different European space actors, including non-space powers, and encourage them to think broadly about the world and how to shape the future. Good strategy should be forward-looking, modular, and adaptive to handle the fast-paced changes in technology, economics and geopolitics.

A well-crafted strategic framework can create the basis for common action, facilitating responses to the challenging security aspects of space activities that have been investigated in the first four chapters of this report. Among the global space powers, only the United States and the United Kingdom have issued explicit space security strategies (using very different approaches). Other space-faring nations, including several member states of the EU, have issued space strategies (although not always using that term), that describe the goals and fields of actions for their space activities (see Table 6 on page 71). Overarching strategic documents for 'Europe' were issued in 2000 and 2007 by the Space Council (with ministers in charge of space issues from the member states of ESA and the EU), and for the 'European Union' in 2011 by the European Commission. Sectoral documents have been issued by the Commission on space industrial policy (2013), and by the ESA on space exploration (2015), while a series of supporting resolutions have been adopted by the European Council and the European Parliament on multiple issues.[1]

Both at the member state level and at the European level, space security issues have not been central to these strategic documents, which has inhibited the development of space security policies. Although the Lisbon Treaty provides the EU with competences in both space and security, there still remains a lack of strategic thinking in space security, partly because of the difficulty of shaping a common approach involving the various stakeholders for European space governance.

1. See, for example, Council Decision (CFSP) 2015/203 of 9 February 2015 in support of the international Code of Conduct; and European Parliament resolution of 8 June 2016 on space capabilities for European security and defence (2015/2276(INI)).

## European space governance

The major space-faring nations have very different approaches to managing space programmes, as well as different priorities for their space activities. Crafting and following clear space strategies in which space security and sustainability are prioritised remains a work in progress for all of them. In the case of some states, notably the US, France and Russia, space security issues are addressed in their national security strategies. But even the biggest powers have activities spread over multiple civilian, military or commercial institutions, and are not always efficient at enunciating and following their policies effectively.

Major space powers like the US, Russia and China, while coming around to a common awareness of space sustainability, continue to emphasise the use of space for military/defence purposes as the dominant space security issue. While this emphasis has been slow to translate into good policy and constructive work on space sustainability, it has ensured that protection and resilience thinking have been central to much of their space activity. The situation is different in Europe. Some member states engage in significant military activities in space, but the defence sector in Europe is only a minor portion of overall space spending (around 10%, compared to more than 50% in the US). With a historic focus on science, technology and industry, prioritisation of security, system protection and resilience has been less integral to European space strategies and has therefore not played a major role in the evolution of European space programmes.

This is compounded by the complicated space governance situation in Europe. The full range of space capabilities, from launchers to GNSS to ELINT technologies, are used in Europe, but controlled by a complex mix of sovereign entities that do not always subscribe to a common space strategy or to the same space security policies. As some aspects relate to national security, member states' interests in this respect must be assured, as they will continue to be the main drivers of space activity.

Since the creation of the ESA (1975) and the burgeoning of EU space programmes in the late 1990s, the nature and threats to space activities have evolved significantly, and will continue to change at an increasing pace. The governance of European space activities has evolved more slowly, however. Due to pre-existing interests and capacities in space, centres of governance are dispersed.

At the national level, member states with significant space programmes have developed civilian, military and often dual assets around national space agencies that can manage a broad range of activities (see Table 3 in Chapter 3). The space strategies of the leading member states vary in their priorities, in the roles played by civilian and military domestic institutions, and in terms of how they seek to shape the future of space activities at the continental level, via the EU, ESA, or bilateral or multilateral cooperation efforts. The ESA has played a central role in the development and management of many civil European space programmes in the last 40 years, and manages a large chunk of national space budgets (generally a third or more of total space budgets). ESA projects have thus been a major component of planning for national space priorities.

**TABLE 6:** SELECTED EU MEMBER STATE SPACE STRATEGIES

| | France | Germany | Italy | UK | Spain |
|---|---|---|---|---|---|
| **Agency** | Centre national d'études spatiales (CNES) | Deutschen Zentrums für Luft- und Raumfahrt (DLR) | Agenzia Spaziale Italiana (ASI) | UK Space Agency (UKSA) | Centro para el Desarrollo Tecnológico Industrial (CDTI) |
| **Ministry of report** | Higher Education & Research | Economics and Technology | Education, Universities and Research | Business Innovation and Skills | Economy and Competitiveness |
| **Primary space strategy/ policy** | French Space Strategy (2012) | The space strategy of the German Federal Government (2010) | Strategic Vision 2010-2020 (2010) | UK Space Policy (2015) | Strategic Plan for the Space Sector 2007-2011 (2006) |
| **Space security strategy/ policy** | - | - | - | UK National Space Security Policy 2014 | - |

At the European level, the ESA is the largest space actor, with a budget that exceeds that of all other counterparts, with the European Commission as its largest funder. Those European countries with limited space capacity rely significantly on the ESA to pursue civil space activities and develop their space industry. The ESA is a unique intergovernmental agency that manages a large portfolio of activities, including space science (astronomy and astrophysics), earth observation, telecommunication, navigation, human spaceflight and robotic exploration, launchers, meteorology, and R&D in all these areas. While the ESA has not historically been involved in security and defence matters, this situation has evolved in recent years.[2] The ESA has set up a regulatory framework to cope with security-related requirements, is progressively engaged in cyber resilience, cooperates with the EDA and the European Commission on a list of actions for strategic non-dependence for critical space technologies, and is now working on a space security policy.

The European Union has competencies over a variety of security and defence policy areas, and is becoming a major space actor, with over €12 billion devoted to space activities in the period 2014-2020. It acts through a large number of institutions and agencies, including the European Commission, the European Parliament (EP), the EU Council General Secretariat, the EEAS, the EU Satellite Centre, the EDA, and the GNSS Agency

2. See EC/EDA/ESA European Framework Cooperation for Defence, Civilian Security and Space-related Research of November 2009; ESA/EDA Administrative Arrangement of June 2011. The ESA's founding convention states that the purpose of the Agency shall be for exclusively peaceful purposes, which allows it to cooperate on non-aggressive security-related activities.

(GSA). In the last decade the steady build-up of the Copernicus and Galileo programmes, owned by the European Union, has added strength to European space capabilities. These programmes have been put in place as EU-owned assets, as civil programmes under civil control. While defence aspects were not initially part of the remit, the use of the EU space assets for security purposes has long been considered. The ownership of space assets and infrastructure has also led the EU to more closely consider system protection, particularly as not all existing systems were conceived to meet modern safety criteria, e.g. when it comes to evolving threats like cyber attacks.

Cooperation between the EU and ESA has been the focus of much analysis in recent years.[3] There has only been one meeting of the Space Council since the coming into force of the Lisbon Treaty in late 2009 – cooperation has continued on many issues, with the ESA/EU Framework Agreement renewed in 2016, but progress could be further facilitated by the development of a shared strategic policy framework to shape this cooperation.

## The road towards a 'European space posture'

The development of a common vision can help bring clarity to the complex European puzzle of space activities, especially when it comes to security. Recognition of shared priorities is the first step in any process of developing common goals, cooperative projects or even shared programmes. A common vision can also help define a role in international affairs and clarify this role for international partners.

Where a common vision has been lacking, Europe has been forced to react to events. For example, US support for commercial launch vehicles has led to the development of the SpaceX and its Falcon 9 launcher. This pushed the European space industry to rapidly propose a more efficient alternative for Ariane 6 than originally planned by ESA and CNES, rushing into a five year development process. Though the EU has become a very important launch customer, there is no doctrine or strategy that encompasses all aspects of European launchers, from guarantied independence, to sustainability of launch sites, or public procurement of launches. Similarly, the lack of an integrated strategic view led to the abandonment of the Automated Transfer Vehicle (ATV) after 5 flights to the ISS. Today, commercial US spacecraft (like the SpaceX's Dragon) service the ISS.

The complex nature of European space governance is unlikely to be simplified soon. But with a common vision and good communication, major governance changes are not necessarily required in order to pursue effective action. Governance diversity can be a source of resilience and creativity, as different governments/institutions work with different strengths in different milieus in a complementary manner. While the EU and ESA have divergent financial rules, membership, and political accountability mechanisms,

3. European Commission, 'Establishing appropriate relations between the EU and the European Space Agency', COM(2012) 671 final, Brussels, 14 November 2012; European Commission, 'Progress report on establishing appropriate relations between the European Union andthe European Space Agency (ESA)', COM(2014) 56, Brussels, 6 February 2014

their partnership provides unique strengths. The EU, as the central player in most of the continent's integration action, brings important political accountability and regulatory competences and a guiding role in shaping industrial/market policies. The ESA has technical and managerial skills, experience in managing complex R&D projects, and its working arrangements provide optionality that member states appreciate.

The nascent cooperation between the Commission and EU member states on SST, the increasing engagement of the EDA in space issues, and the recent openness of the ESA to engagement in security issues all show that the evolution of European space cooperation is gradually overcoming historic institutional separations. While a common shared strategy document may not be possible in the short term, cooperative thinking on strategic approaches is increasingly possible. And strategic thinking at the continental level can draw from, tie into and feed into the strategy processes for the member states.

## Towards a security focus?

Nowhere is the importance of continental cooperation more clear than in addressing security issues. Today, Europe suffers from the absence of a common vision for security and defence, and this is reflected in the various space strategies at both the EU and national levels. There has been a lack of clarity, from political decisions on programmes to technological development, service provision, and diplomatic action that has made it more difficult to integrate security and resilience thinking into European space activities. The fact that the Galileo PRS signal is only depicted as a civilian asset is one example of this.

Decisions on the Galileo second generation, next earth observation programs, new R&D programmes and other post-2020 space activities need to be prepared, starting now, while new programmes like GovSatCom are already being looked into, and EU SST services are becoming operational. And at the international level, recent progress on space sustainability discussions may not continue without European engagement.

Table 7 below shows which issues have been highlighted as priorities in various space strategies. While most of the space strategies analysed here have touched on some of the key space security issues in this report, not everything can truly be a priority. The table shows that space sustainability, resilience and protection are not strongly prioritised within the space strategies of the leading member states. Only the UK has developed an explicit space security policy in Europe, while the other leading states address space and security to varying degrees within their national space policies and security policies.

**TABLE 7:** MENTIONS OF HEADLINE GOALS/PRIORITIES IN CURRENT SPACE STRATEGIES

| | European Space Strategies (2000, 2007, 2011) | Member State Strategies (FR, DE, IT, UK, ES) | Space Security Strategies (UK, US) |
|---|---|---|---|
| **Industrial Policy/Space sector support** | 3 | 4 | 1 |
| **Security and Defence (& dual use)** | 3 | 3 | 1 |
| **Science and technology** | 3 | 3 | 0 |
| **Applications (EO, GNSS, SatCom)** | 3 | 2 | 0 |
| **International cooperation** | 3 | 4 | 2 |
| **ISS and Exploration** | 2 | 3 | 0 |
| **Access to Space/Non-dependence** | 2 | 2 | 0 |
| **Vision - Citizen focus** | 2 | 2 | 0 |
| **Governance & regulation within EU** | 2 | 0 | 0 |
| **Markets for space services** | 1 | 2 | 0 |
| **SSA** | 1 | 0 | 0 |
| **Shape (contribute to) Europe in space** | 0 | 4 | 0 |
| **Space sustainability/stability** | 0 | 2 | 2 |
| **Public private partnerships** | 0 | 1 | 0 |
| **Establish unified legal framework** | 0 | 1 | 0 |
| **Resilience/protection** | 0 | 0 | 1 |
| **Space security risks** | 0 | 0 | 1 |
| **Deter aggression** | 0 | 0 | 1 |
| **Operate in degraded environment** | 0 | 0 | 1 |

## Looking at strategy content

The first European space strategy was issued jointly by the EU and ESA in 2000. This was replaced with a common policy in 2007 issued by the Space Council. These early strategies/policies developed a common vision for all of Europe, calling for the ESA, the EU, and their respective member states to increase coordination of their activities and programmes in pursuit of shared goals.

The third key space document was not issued jointly by the EU and ESA, but by the Commission in 2011, with four key objectives for the European Union:[4] promote techno-

4. European Commission, 'Towards a space strategy for the European Union that benefits its citizens' , COM(2011) 152 final, Brussels, 4 April 2011.

logical and scientific progress; foster innovation and industrial competitiveness; ensure that European citizens fully benefit from European space applications; and strengthen Europe's role in space at an international level. While subsequent sectoral documents have been issued, this 2011 strategy serves as the most important and comprehensive strategy for the EU in the post-Lisbon era.

Table 7 shows that several issues have been central to strategic thinking about space for Europe and its member states, and will likely continue to be in any future space strategy. For each of these issues, it will be important to understand and integrate any potential security components as well as developing new ones:

- **Space for citizens –** As highlighted in the 2011 Commission paper, European space activities must be developed in a way that benefits European citizens. The growing reliance of European society on space services magnifies the impact of any disruption, so there is increased need to ensure resilience of space assets and services, and to reduce threats and hazards in the space environment;

- **Nurturing markets for space services –** As Russian commercial space struggles show, maintaining resilience in the delivery of space services is a necessary factor for facilitating development, trade, market uptake and investment in space assets, services and applications, both domestically and internationally;

- **Industrial policy -** European public institutions are customers, regulators, and funders for the European space industry. Future engagement may involve not just commercial and technological synergies, but also work towards a common culture of security, so that the private sector can plan for and respond to security challenges;

- **Science, technology and space exploration –** Pushing forward the frontiers of science and technology is an essential task of space actors, both private and public. As space debris, cyber attacks, spectrum interference and other risks grow, not only will European technological capabilities be essential to address these threats, but the technologies and programmes themselves will require new levels of protection;

- **Applications (EO, GNSS, SatCom) –** The Copernicus and Galileo programmes are central to European space activities; the resilience of these assets and the services they provide must be secured.

- **Non-dependence of critical technologies and services -** Strategic non-dependence in fields such as space access (launchers), navigation, telecommunications and earth observation remains a key factor when considering the protection of space assets, the rollout of services, and the potential design of future generations of projects;

- **International cooperation –** Europe is a global economic power, an important developer of space technology, and has the resources to develop into a diplomatic leader on space issues. Europe can use its economic and technological strengths to its advantage, with EU institutions, member states, and the ESA working in partnership to pursue European priorities on the international stage, including with respect to space sustainability;

- **Space for security and defence –** The development of a cohesive EU space policy may represent another asset for CSDP (which serves both civilian and military objectives), ensuring better synergy between civilian and military efforts. A convergence in thinking about the nature of space risks can lead to increased security partnerships between civilian and military space actors, without necessarily requiring changes in governance arrangements for either types of programme;

- **Governance & regulation within the EU –** While continuing dialogue on the long-term evolution of European space governance, addressing space security concerns can already be pursued today by focusing on shared issues of interest.

In addition to these issues, which have already been addressed to some extent in different European policy and strategy documents, space security issues deserve even more attention. Strategic thinking should include not merely descriptions and justifications of existing programmes and budgetary plans, but also address the difficult management and protection of systems. The following space security issues have not been prominently addressed in existing European space strategies:

- **Resilience –** Prioritising resilience as a unique area of focus within strategy documents can help ensure that it receives the attention and resources necessary. A resilience framework can facilitate work on identifying and addressing risks to space infrastructure, assist the development of common responses for space system protection, and encourage frameworks for regular exchange on national, European and international needs on space security;

- **Space sustainability –** While existing strategies may touch on space sustainability in the context of international cooperation, improving the sustainability of the space environment is an objective that can be pursued at multiple political and technical levels, both unilaterally and in cooperation with other space actors;

- **Space Situational Awareness (SSA) –** Understanding the situation in space is of strategic value, as it facilitates international dialogues and enables strategic decision-making in the area of space and security. It also helps facilitate space operations, the protection of space assets, and additional strategic analysis for the long term, regardless of the current status of European cooperation. Furthermore, the viability of any future international instrument to regulate space activities may require SSA information to detect and attribute irresponsible behaviour;

- **Data policy –** As the space industry becomes ever more data intensive, the capacity to securely share and manage data can benefit from common rules and frameworks that facilitate cooperation and data sharing among European space actors, ensuring that security restrictions on data do not negatively affect European competitiveness and innovation.

It is now an opportune moment to have a new look at European space policy; not just at the EU level, but for Europe as a whole. This report is published at a time when security concerns have risen to the forefront of European agendas; furthermore, 2016 will bring:

- an EU Global Strategy on Foreign and Security Policy;
- a European Defence Action Plan;
- a Commission Communication on a Space Strategy for Europe;
- a Joint Commission/EEAS communication on the EU's response to hybrid threats;
- an ESA space security policy.

However, not all European space actors will necessarily have the capacity or interest to engage with creating an overall strategic framework. This is especially the case in the field of space security, for which the outcomes will not have equal impacts on all member states, as some have much higher stakes due to their national space and defence programmes and domestic space industry.

# VI. OPTIONS FOR MOVING FORWARD

Within Europe, there are multiple areas where the impact achieved by individual member states acting alone is likely to be insufficient, and where improved integration on a European level makes sense. There is a particular window of opportunity now for more integrated European efforts since the security and sustainability threats facing space actors are increasingly seen as common challenges for which common responses are appropriate. There has also been a move towards greater comfort with dual-use approaches and increased partnerships between civilian and military space actors, without undermining the core, sometimes separate, interests of either group. Action at the European level has the advantage of facilitating resource optimisation with greater economies of scale, and of building cohesive political support for actions that benefit all of Europe. Common action can be useful in addressing even divergent security priorities of member states, as can be seen with the recent work on space sustainability issues at the UN, despite the even more widely divergent priorities of the states involved. This chapter offers a number of options for addressing space security challenges.

## Increasing resilience of space systems

### Holistic protection

Protecting critical space systems requires that a focus on systemic resilience be embedded into policy and technology development, funding decisions and management frameworks. With the continued acceleration of several key trends (big data, computer speeds, cyber threats, new space actors etc.), while development and operational phases retain their long timeframes, extra care is required to future-proof big programmes. This is particularly important as assets and derived services may have a potential dual use in the course of their lifetime; dual use must be foreseen during the inception so that proper requirements are embedded upfront. Security elements, therefore, can be designed not just for civil services from a civil provider, but with the expectation of potential security and military use.

During the process of reviewing user needs and possible models of cooperation, it will be important to bear in mind the lessons from past experiences where ownership and governance models evolved as system objectives changed. As much as possible, it would be preferable to develop any new European systems with multi-stakeholder consultations that effectively match governance arrangements to the programme needs.

## Cyber protection

No industry or institution is immune to cyber threats, and each has the responsibility to develop appropriate defences. For the space community, closer and permanent cooperation with the cyber community will be imperative. In the EU, this connection can be enhanced by bringing space actors into the EU cyber dialogue. Because cyber is ubiquitous, government cyber strategies cannot be created for every domain, from space to energy to social services. Each specific service domain will need to address cyber issues themselves, while also bringing in support from the expert cyber community. As part of this, space personnel will need to be regularly retrained on protection of the systems, software, data, and devices they use.

The space and cyber communities can also work together at the international level. There have already been discussions on cyber within COPUOS, instigated by Russia, which could be built upon. As there have been Groups of Governmental Experts on both cyber and space, it may even make sense to develop a similar project focused on the connections between cyberspace and outer space.

One important community that has expertise and experience in addressing cyber challenges is the defence community. Many aspects of terrestrial critical infrastructure protection and cybersecurity originally developed with a military focus, and forging closer connections on cyber issues may allow European space actors to benefit from military resources and skillsets.

For existing space systems, the conduct of regular stress-tests to assess resilience against potential cyber attacks should become a regular practice. These tests can help organisations prepare for how to reliably deliver the necessary services when a threat materialises.

The changing nature and intensity of cyber threats means that space service providers need to continually reassess their connections with outside providers or partners that may be ineffective or lax in their own cybersecurity efforts. Ensuring supply chain security is an ongoing process, requiring tests for validation and verification for all companies, particularly when non-EU suppliers are involved.

An option that may help mitigate such a risk would be for governments to look at regulating the hardening of commercial satellites. This may lead to higher costs in some instances, but also enhance the wider recognition of European-made satellites as having high quality and protection standards; this aspect may end up being a key factor, as cybersecurity issues are expected only to increase during the lifetime of a satellite.

Finally, despite all best efforts, there will be breaches and failures in cyber protection. While these failures are rarely publicised (to protect public confidence, private reputations and to avoid being set up for new attacks), the whole space community in Europe would benefit from a formal process to recognise, understand, and compensate for when particular space systems, services, or products have been compromised by a

cybersecurity issue. The sharing of this information can help lead to the development of best practices within the European space community, but will require advanced efforts to ensure that the information is available and used at appropriate security clearance levels.

## Critical infrastructure protection

Rather than a separate framework for governing space risks, the protection of infrastructures in space and on earth can be integrated, making appropriate use of CIP efforts and strategies at the national and European levels. While space activities can involve unique challenges, existing risk assessment methodologies will still be applicable, including those that are built into European CIP systems. The existence of legislative and administrative frameworks for CIP, with interconnections with national frameworks, can make the research, adoption and implementation of space security measures significantly easier.

Seeking convergence on the understanding of space risks can facilitate cooperation and integrated responses, where appropriate. The creation of common risk assessment methodologies for European space infrastructures may provide added value. A common methodology can provide a joint understanding of risks, which can then be translated into actionable conclusions by and for different stakeholders and institutions. Developing and benefiting from such a shared assessment methodology may work best if it is used as part of a regularised process or working group involving European space actors.

## Data policy

The security of the entire data life cycle has to be assured so that the availability, redundancy, integrity and validity of the data are protected, and its delivery is secure and continuous. An effort can be made at the European level to develop common agreed principles for space data policies; such a set of principles could then be applied to different programmes and contexts. Strong cooperation in the sharing of national assets, data and services will require close collaboration between relevant EU entities and member states, as well as consistent prioritisation of data policies that maximise the secure exploitation of data and its derived services. It will be a challenge to balance openness with data protection, and manage the interests of multiple data providers and user communities. This work may address questions such as how much will member states be willing to share their data and how much will military sensors be made available for use, so that any data policies developed will set parameters for both how publicly owned data is shared and how privately provided data is managed. The goal of such a process would be to facilitate cooperation in the sharing of, and access to, national assets, data and services among European actors, who could be confident that the specific data management system developed for any particular space project or programme would have been developed using a common policy framework that prioritised protection.

In developing such a policy that could be applied across multiple platforms and governance models, a thorough review of existing initiatives may prove valuable. The SatCen example could serve as one potential reference, with its data policy, functions (with the EEAS acting as tasking authority at the EU level to coordinate requests to the SatCen), and early integration of security aspects within the technical specification of services (e.g. its download centre for secure distribution of products and services).

## Non-dependence

Reliance on commercial providers raises questions about how to balance the needs for system control, reliability, bandwidth availability, security, flexibility and affordability. Reliance on other actors comes with additional risks for both member states and European institutional users. The potential GovSatCom program could be a smart step toward managing dependence issues in the SatCom field. Together, the ESA, the European Commission and the EDA have agreed on a list of actions for strategic non-dependence for critical space technologies. This list could be used as a starting point for a permanent cooperative process that analyses the costs and benefits of relying on commercial partners or a single non-European provider for information and capacity in particular programmes. This analysis would be useful not only for planning an effective balance of institutional ownership and operation of European space systems and services, but also to shape the rules for cooperation and sharing with external partners.

## Human capital

As the responsibilities and competencies of key European space actors have increased in recent years, their need for supporting capacities has expanded. This also requires the fostering of skillsets to manage programmes and conduct analysis to support decision-makers. An adequate workforce is crucial all along the value chain of space assets, up to information exploitation and the use of services. Human capital is still fundamental to the process of the interpretation and handling of data and its derived services (for example to cross-check alarms generated by automatised systems), in order to avoid potentially dangerous disclosure of sensitive information. This is particularly critical for Earth Observation data whose volume and types are greatly increasing. It may be valuable for European space actors to complete a comprehensive survey of key space skills, complemented with a catalogue of security functions to assess the level of risk of any specific role/post and plan suitable training programmes accordingly.

## Advancing European SSA

The unique governance model for cooperative SST services in Europe, based upon an open consortium of member states operating assets under national control, has been welcomed by member states. The model can thus be maintained in the future, and the SST Decision could be updated to facilitate the long-term funding of the programme and manage the possible evolution of SST services. The SST model could evolve in the direction of SSA to respond to a wider spectrum of challenges, such as space weather and information on suspicious behaviours in space. This last item would also be an important element for the viability of any effort towards enforcing norms of responsible behaviour in space activities, as it may help to both deter and attribute hostile acts in space. The EU SST consortium also provides an important mechanism for advancing partnership on situational awareness. For example, with the US, it can develop towards a mutual dependence that offers complementarity and redundancy for the satellite operators. The potential for enhancing SSA cooperation via NATO may also be investigated. Finally, the development of a market for added value SST services at the European level is worth studying, taking into account the need to preserve data security and ensure reliable sources, while seeking to benefit from the increasing capabilities of the commercial sector in SSA both in Europe and in the US.

## Advancing civil-military cooperation in space

As the EU's involvement in security issues continues to expand, and as threats to European security continue to mutate, space security responses will need to be designed, managed and protected to meet this evolving situation. The increasing connective links between the civilian and military domains could be seen as an opportunity for security cooperation in space – sharing information and expertise, without necessarily reorganising the governance arrangements for European space programmes. Civil systems can remain under civilian control, but even though many security ideas, mechanisms and systems have begun with a military focus, they can often be translated into the civilian domain.

Further debate on the challenges and benefits of deeper civilian-military cooperation would be welcomed. For defining future space programmes, in particular, it would seem important to take a holistic view of Europe and of the needs of space actors who will be dependent on those space services, including militaries. New space programmes or initiatives maintain focus on the services provided to their user categories. As long as these services are of a civil nature, the status of the entity owning and/or operating the systems or of the final users should not represent an obstacle to their further development, provided that the governance framework allows for enhanced security and confidence.

Going further, a versatile system design, and clear but flexible governance, can guarantee an optimal use of resources. In that sense, dual-use design strategies may become the norm for future programmes. Examples of such programmes already in place include the Italian CosmoSkyMed and the French Pleaides programmes for earth observation.

## The private sector and new space actors

As more companies become involved in space activities and space markets become more competitive, the development of a framework for enabling private sector exploitation of space could provide great value. International organisations such as UNIDROIT have led the way in trying to make outer space a friendlier business environment, including by taking inspiration from maritime customs, practices and law to put forward proposals regarding similar commercial governance of space. A review of the regulatory bottlenecks and gaps facing new space entrants in Europe could be a helpful first step.

In support of this, a further improvement in space security can be achieved by incentivising security-conscious behaviour by private companies and other new space actors, encouraging them to respect norms and regulations for space activities. Reducing the significant uncertainties and costs regarding insurance, financing and liabilities can facilitate commercial activity in space. Planning for the deorbiting of satellites at the end of their lifecycle would become financially prudent, and this cost would likely be included in the insurance premium. Increasing asset robustness through shielding could become a priority if this would result in lower insurance premiums and more accessible financing.

Support for new space actors in improving their security efforts could also come via regular sharing of information from effective SSA systems. This information could help them achieve better management of orbital planning and satellite manoeuvres, reducing fuel usage for manoeuvrable assets, extending their lifetime or increasing payloads. Systematically delineating the benefits, costs, and data security limitations of such information sharing with the private sector would be a first step in determining the value of such an effort.

Capacity building can also be a tool for maximising benefits from newcomers while limiting potential negative consequences. This may come in the form of dedicated efforts to introduce the principles, laws, norms, and best practices for secure, safe and responsible activities in space for new European space actors, both public and private. Such an effort, potentially embedded in the activities carried out by space business incubator centres, could help smooth the path toward responsible use of space for new entrants to the European space sector.[1]

1. In the United States, the Secure World Foundation (SWF) is in the process of producing a handbook for new actors in space, including states, universities and the private sector, covering many of the same issues.

## Multilateral international cooperation

Building on the work already done on promoting sustainable norms of behaviour in outer space, Europe is well-positioned to help set the global agenda for space security. Active engagement can help ensure that other countries, whose goals may differ from those of the EU and its members states, do not dominate the tone and content of international discussions. Implementing TCBMs and keeping discussions open on codes of conduct can be important, low-cost ways of maintaining forward momentum, broadening appreciation of the idea that cooperation and transparency bring value to all participants. Going it alone is a recipe for reduced security for everyone both in space and on earth.

There is immense value in the International Code of Conduct. The ICoC and its ideas can continue to be pushed forward in several ways. It could be kept on the agenda at bilateral space dialogues and in bilateral security dialogues. Member states can also keep the ICoC on the table and under discussion at the UNGA. At the same time, it will also be important to continue to support other TCBMs and responsible behaviour initiatives, both diplomatically and by serving as model space actors in applying them unilaterally. Lessons learned from the consultation process relating to the ICoC and disagreement over its provisions relating to self-defence can help inform these diplomatic actions.

As the ICoC contains elements of what may become a framework for a space traffic management (STM) regime, it may be useful if EU institutions and member states begin discussing STM as a long-term evolution from the ICoC.

Europe can use its many voices to its advantage, with the EU institutions, EU member states, and the ESA working in partnership on space security and sustainability issues on the international stage. The EU, as mandated by its member states, is continuing to define its role in UN bodies and as an international space actor. It has enhanced observer status at the UNGA (including its committees and working groups), allowing it more speaking rights than standard observers. The EU also has the advantage of having all the member states representing it, as well as close relations with the ESA. The ESA is present in the IADC as a member, and within the COPUOS and the LTS Working Group as a permanent observer.

One method for concretising this pan-European cooperation would be to create a European Space Diplomacy Network composed of individual members of EU, ESA, and member state delegations around the world who have connections with space issues. Such a network could help translate shared priorities into action plans for space diplomacy so that Europe speaks as much as possible with one voice. The Green Diplomacy Network working on environmental issues has already used this model to great effect, as its members engage with existing networks, fora, and conferences to foster international discussions on issues of priority for Europe.

European effectiveness in pushing forward a space sustainability agenda can be enhanced when European space actors unilaterally implement space sustainability measures. Such action may include, for example, a public and independent review of how European space actors are applying, or are planning to apply, the recommendations within the GGE report, the ICoC, the IADC Space Debris Mitigation Guidelines, and the LTS guidelines by the COPUOS. This may be complemented by conducting a review of implementation of past treaties, including UN registration. Pursuing full implementation of these codes and treaties will require domestic policy and operational procedure modifications, but can blaze a trail for others to follow.

Europe could attempt to engage newer and less advanced space actors in space security matters by highlighting European perspectives (emphasising the benefits of cooperation, transparency, collective security), buttressed by technical support. Private space actors have different incentives than public space actors, and these differences should be taken into account. States that are new to space issues may perhaps take similar approaches to common space security challenges as some developing states approach climate change – they are anxious to develop and progress, and so are not always thrilled with rules and demands issued by others, particularly if the problems (climate change or space debris, respectively) were primarily created by others. Helping new space actors prepare and implement integrated plans for managing space security risks can help ensure that new programmes and projects are developed with integrated security thinking. Europe's interests are served by making it attractive for everyone to join and benefit from a sustainable space environment on mutually beneficial terms. Relationship-building with developing space nations is also very useful for earning their support in international diplomatic efforts, including supporting the ICoC.

One possibility with a long-term perspective would be to conduct a review of potential initiatives in the field of arms control to identify obstacles towards renewed arms control progress. While decades of gridlock on the issue do not provide encouragement for rapid progress, it can be important to develop ideas for alternatives that may be applicable at a time when the political conditions have changed. As European efforts in space security left the issue of space weaponisation aside, in the longer term, the EU and its member states could investigate norms entrepreneurship for arms control in space (including potentially by declaring unilaterally their intention not to develop and test space weapons), while still acting as a mediator between contrasting blocs (US and Russia/China).

## Bilateral international cooperation

There is also an important place for bringing some space security issues into bilateral dialogues, complementing multilateral cooperation efforts at the UN. International partners are still adjusting to the EU as a European space actor, and learning how it works together with the member states and ESA. There is thus value in improving the

outreach and communications factor of EU diplomacy, showing EU value added for space security discussions beyond technical considerations. Even the US and China, which harbour distrust over each other's space intentions, have included space debris, the long-term sustainability of outer space, satellite collision avoidance and their overall space policies in their initial bilateral dialogue in 2015.

In shaping these dialogues, it makes sense to build on existing discussions and prioritise partnerships with like-minded partners that have endorsed the principles of the ICoC. In particular, this can involve forging deeper connections with the US. Effectively building this relationship can involve additional efforts to understand the dynamics of how the US approaches space, national security, and space security issues. Understanding American goals and approaches will also be essential as Europe develops strategies and seeks to understand where potential dependency issues are problematic.

Dialogue cannot be limited to like-minded partners, however. Russia and China can be difficult dialogue partners, but they are still essential for shaping the security of the outer space environment. Winning their support for European approaches and priorities for space security will require patient and consistent engagement, keeping them in the loop on European thinking and giving them opportunities to actively engage on these issues on terms that make sense for them.

Finally, the EU is still best known for its huge and attractive internal market. Commerce has long been used as a door-opener for the EU in international cooperation discussions, and can perform this role *vis-à-vis* space security issues as well. This can be done if dialogues on space include discussions both on security issues and on investment issues. It may be a tough balancing act to push for greater commercial cooperation with third countries on space issues, seeking greater market access for European space firms moving abroad, when European industry wants European governments to buy domestically and limit American inroads into our markets. But work in this area is important for our relations with other countries. Commercial space actors in Europe, Asia, and even Latin America are developing rapidly, so the commercial space sector is no longer as US-centric as it had been. Other countries are worried about the commercial activities in the US, mistrusting how the US is managing and partnering with commercial actors who then enter global markets. This creates an opportunity for the EU.

## Enhancing strategic thinking on space security

The complex evolution of European space programmes, with different starting points, drivers, and governance models, will not be easily rationalised into any common framework; but it should be possible to use similar framing questions on security and protection to find common answers that can be applied differently as circumstances and governance arrangements require. Overcoming national sovereignty worries over common EU policy-making, and concerns relating to future relationships between the EU and

ESA, require building trust among all space institutional actors. This can be facilitated through the creation of European policies and strategies, rather than just purely EU ones, helping make European cooperation central to each member state's space strategy.

One option for moving forward on this would be to create a mechanism for regular exchange on national, European and international needs on space security. This may come as part of a reinvigorated and regularised process of institutionalised cooperation at the highest levels between the EU and the ESA, with participation of EDA and other key organisations on an *ad hoc* basis An option for facilitating such a development could be the production of a joint EU-ESA report to map out space security priorities in common, then mapping out potential areas for building effective joint responses.

Concurrent with efforts to improve cooperation on space security in Europe will be efforts to develop space security strategic thinking. In deciding in what type of framework to situate space security ideas, three non-exclusive options stand out:

1. Integrating space security into broader space strategy and policy documents;

2. Integrating space security into broader defence and security strategies;

3. Developing a dedicated space security strategy.

In addition, when investigating which of these option(s) will work best for Europe, the success of the choice should take into account how well that option supports the following goals:

- Raise overall awareness and generate greater political attention and willingness to cooperate;

- Promote harmonisation of space security thinking among member states, European institutions, the ESA and the wider space community;

- Facilitate development of dedicated policies and programmes for resilience and protection;

- Strengthen the development of security mindsets;

- Build trust from international partners as they recognise European progress in space security and sustainability;

- Frame the scattered existing initiatives in the field of space security;

- Recognise space as a tool that is part of the EU foreign policy toolkit.

# Annexes

# THREATS TO SPACE INFRASTRUCTURE

**TABLE 1:** IN-ORBIT INFRASTRUCTURE

| Intentional | | | |
|---|---|---|---|
| **Threat** | **Effect** | **Mitigation** | **Priority** |
| Kinetic Energy Weapons (KEW)<br>- Passive ASAT<br>- Exploding ASAT<br>- Passive ASAT | Satellite partially or totally destroyed | International law, export control, rules of the road, TCBMs, deterrence, SST | Very low |
| High-altitude Nuclear Weapons (EMP) | Satellite destroyed; excitation of Van Allen belts | International law, export control, rules of the road, TCBMs, deterrence, SST | Low |
| Directed Energy Weapons (DEW) | From signal disturbance to mechanical destruction effects | Depends on the specific threat (see below) | Medium |
| Laser-based ASAT | Sensors damaged/destroyed and mechanical damage | Classified | High |
| High-power microwave ASAT | Sensors temporary or permanently blind; receivers and electrical components degraded | Self-protection devices | Medium |
| Electronic Warfare (EW) | Ranges from signal disturbance to loss of satellite control | Depends on the specific threat (see below) | Very high |
| Jammers | Radar satellites and communications transponders temporarily or permanently incapacitated | Specific waveforms, nulling antennas, beamforming, jammer location neutralisation | Very high |
| Cyber attacks | Hijacking of transponders, degradation of a satellite and its components, loss of information, spoofing | Cryptography, secured software, process standardisation | Very high |

| Non-intentional/Natural | | | |
|---|---|---|---|
| **Threat** | **Effect** | **Mitigation** | **Priority** |
| Space debris | Physical damage to a satellite, space debris pollution | TCBMs, SST, shielding | High |
| Space weather (e.g. solar flares radiation) | Bugs, component damage, mission duration decrease | SSA, Space weather monitoring and forecast, specific components, specific software | High |
| Unknown space phenomena | Component failure | Redundancy, hardening, resilience, R&D | Medium |

**TABLE 2:** DATA LINKS

| Intentional | | | |
|---|---|---|---|
| **Threat** | **Effect** | **Mitigation** | **Priority** |
| Jamming | Denial of service of communications and/or radar systems | Radio-frequency coordination at national and international levels, nulling antennas, specific waveforms, jammer neutralisation | High |
| Spoofing | Wrong information provided | Cryptographic authentication procedure, integrity checks | Medium |
| Cyber attacks | Denial of service | Cryptography, secured software | Very High |
| Interception | Information compromised | Cryptography, specific waveforms | High |

| Non-intentional/Natural | | | |
|---|---|---|---|
| **Threat** | **Effect** | **Mitigation** | **Priority** |
| Interference | Denial of service of communications and/or radar systems | Radio-frequency coordination at national and international levels, nulling antennas, specific waveforms | Medium |

**TABLE 3:** GROUND INFRASTRUCTURE

| Intentional | | | |
|---|---|---|---|
| **Threat** | **Effect** | **Mitigation** | **Priority** |
| Physical attacks | Loss of communication with satellites, temporary or permanent disruption of the ground segment | Redundancy, specific hardening measures, increased physical security procedures | Medium |
| Sabotage | Loss of communication with satellites, ground segment breach | Hardening | Medium |
| Cyber attacks | Denial of service, information stolen/ compromised | Cryptography, authentication procedures, secured software, integrity checks | Very high |
| Back doors | Information compromised | Cryptographic authentication procedures, integrity checks | High |

| Non-intentional/Natural | | | |
|---|---|---|---|
| **Threat** | **Effect** | **Mitigation** | **Priority** |
| Natural disaster (e.g. floods, fires, earth-quakes) | Loss of communication with satellites, temporary or permanent disruption of the ground segment | Redundancy, specific hardening measures, increased physical security procedures | Medium |

**TABLE 4:** TECHNOLOGY/INDUSTRY THREATS

| **Threat** | **Effect** | **Mitigation** | **Priority** |
|---|---|---|---|
| Technology transfer | Third-party space programme competition for resources | Coordinated export control regimes, space industrial policy | High |
| Supply shortage | No system deployed | Space industrial policy | High |
| Lack of launch opportunities | Satellite grounded | European launch policy, framework contracts | Medium |
| Loss of industry know-how | No system deployed | Space industrial policy, space R&D programmes | Medium |
| Loss of spectrum and orbital resources | No system deployed | Coordinated EU position at European and ITU levels | High |

# LIST OF BIBLIOGRAPHICAL REFERENCES

Cristina Alcaraz and Sherali Zeadally. 'Critical Infrastructure Protection: Requirements and Challenges for the 21st Century', *International Journal of Critical Infrastructure Protection* (IJCIP), vol. 8, 2015, pp. 53–66.

R. James Caverly, 'GPS Critical Infrastructure - Usage/Loss Impacts/Backups/Mitigation,' 27 April 2011, accessed at http://www.swpc.noaa.gov/sites/default/files/images/u33/GPS-PNTTimingStudy-SpaceWeather4-27.pdf.

Luca del Monte and Stefano Zatti. 'Preliminary reflections about the establishment of a cyber-security policy for a sustainable, secure and safe space environment', *Proceedings of the 64th International Astronautical Congress (IAC)*, 2015.

Tobias Evers. 'The EU, Space Security and a European Global Strategy', *UI Occasional Papers*, no. 18, The Swedish Institute of International Affairs, 2013.

Adrian Gheorghe *et al.* (eds.). *Infranomics: Sustainability, Engineering Design and Governance* (Cham: Springer International Publishing, 2014).

John Johnson and Adrian Gheorghe. 'Antifragility Analysis and Measurement Framework for Systems of Systems', *International Journal of Disaster Risk Science*, vol. 4, no. 4, 2013, pp. 159-168.

Veronica La Regina. *SatCom Policy in Europe*, ESPI Report 32 (Vienna: ESPI, 2011).

Ajey Lele (ed.). *Decoding the International Code of Conduct for Outer Space Activities*, Institute for Defence Studies and Analyses (New Delhi: Pentagon Security International, 2012).

Jeffrey Lewis, 'They Shoot Satellites, Don't They?' *Foreign Policy*, 9 August, 2014.

Lucia Marta. *Code of conduct on space activities: unsolved critiques and the question of its identity*. FRS note no. 26/2015, December 2015.

Lucia Marta. *The European Space Surveillance and Tracking Service at the crossroad*, FRS Defense & Industries no. 5, October 2015.

Patricia McCormick. 'Space Situational Awareness in Europe: The Fractures and the Federative Aspects of European Space Efforts', *Astropolitics: The International Journal of Space Politics & Policy*, vol. 13, no. 1, January 2015, pp. 43-64.

Forrest E. Morgan. *Deterrence and first-strike stability in space: a preliminary assessment* (Santa Monica: RAND Corporation, 2010).

Liviu Muresan and Alexandru Georgescu. 'The Road to Resilience in 2050: Critical Space Infrastructure and Space Security', *RUSI Journal*, vol. 160, no. 6, December 2015, pp. 58-66.

Max M. Mutschler and Christophe Venet. 'The European Union as an emerging actor in space security?', *Space Policy*, vol. 28, no. 2, May 2012, pp. 118-124.

Scott Pace. 'Security in space', *Space Policy*, vol. 33, no. 2, 2015, pp. 51-55.

Wolfgang Rathgeber, Nina-Louisa Remuss and Kai-Uwe Schrogl. 'Space security and the European Code of Conduct for Outer Space Activities', *Disarmament Forum*, no. 4, 2009, pp. 33-41.

Jana Robinson and Michael Romancov. 'The European Union and Space: Opportunities and Risks', *Non-Proliferation Paper*, no. 37, EU Non-Proliferation Consortium, 2014.

Kai-Uwe Schrogl *et al.* (eds.). *Handbook of Space Security* (New York: Springer-Verlag, 2015).

Kai-Uwe Schrogl. *Space Traffic Management - The new comprehensive approach for regulating the use of outer space*, ESPI Flash Report no. 3, October 2007.

Pierre Soille and Pier Giorgio Marchetti (eds.). *Proceedings of the 2016 conference on Big Data from Space* (Brussels: Joint Research Centre, 2016).

UNGA. *Report of the Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities*, A/68/189, 2013.

Anna C. Veclani, Nicolò Sartori, Emiliano Jr. Battisti, Jean Pierre Darnis & Elena Cesca, 'Space, Sovereignty and European Security Building European Capabilities in an Advanced Institutional Framework', European Parliament, Directorate-General for External Policies of the Union, EXPO/B/SEDE/2012/21, January 2014.

Christophe Venet, 'Space security in Russia,' in Kai-Uwe Schrogl *et al.* (eds.), *Handbook of Space Security* (New York: Springer-Verlag, 2015).

Sheng-Chih Wang, *Transatlantic Space Politics: Competition and Cooperation Above the Clouds* (London: Routledge, 2013).

Jan Wouters and Rik Hansen. *The Other Triangle in European Space Governance: The European Union, the European Space Agency and the United Nations*, Working Paper no. 130 (Leuven: the Leuven Centre for Global Governance Studies, 2013).

# ABBREVIATIONS

| | |
|---|---|
| ASAT | Anti-satellite weapons |
| CFSP | Common Foreign and Security Policy |
| CI | Critical Infrastructure |
| CIP | Critical Infrastructure Protection |
| COPUOS | Committee on the Peaceful Uses of Outer Space |
| CSDP | Common Security and Defence Policy |
| EASA | European Aviation Safety Agency |
| ECI | European Critical Infrastructures |
| ECIP | European Programme for Critical Infrastructure Protection |
| ECMWF | European Centre for Medium-Range Weather Forecasts |
| EDA | European Defence Agency |
| EDRS | European Data Relay System |
| EEAS | European External Action Service |
| EGNOS | European Geostationary Navigation Overlay Service |
| EMSA | European Maritime Safety Agency |
| EO | Earth Observation |
| EP | European Parliament |
| ESA | European Space Agency |
| ESDP | European Security and Defence Policy |
| ESP | European Space Policy |
| GEO | Geostationary orbit |
| GGE | Group of Governmental Experts |
| GLONASS | Global Navigation Satellite System |
| GNSS | Global Navigation Satellite System |
| GovSatCom | Governmental satellite communications |
| GPS | Global Positioning System |
| GSA | European GNSS Agency |
| HR/VP | High Representative of the Union for Foreign Affairs and Security Policy/Vice-President of the European Commission |

| | |
|---|---|
| IADC | Inter-Agency Space Debris Coordination Committee |
| ICoC | International Code of Conduct |
| ICT | Information and Communications Technology |
| ISR | Intelligence Surveillance and Reconnaissance |
| ITU | International Telecommunications Union |
| JRC | Joint Research Centre |
| LEO | Low earth orbit |
| LTS | Long-Term Sustainability |
| LTSSA | Long-Term Sustainability of Space Activities |
| MilSatCom | Military satellite communications |
| NASA | National Aeronautics and Space Administration |
| NEO | Near-Earth Object |
| NPT | Non-Proliferation Treaty |
| PAROS | Prevention of an Arms Race in Outer Space |
| PPWT | Treaty on the Prevention of the Placement of Weapons in Outer Space |
| PRS | Public Regulated Service |
| R&D | Research and Development |
| SAR | Search and Rescue |
| SatCen | European Union Satellite Centre |
| SatCom | Satellite communications |
| SSA | Space Situational Awareness |
| SST | Space Surveillance and Tracking |
| STM | Space Traffic Management |
| STRATCOM | Strategic Command |
| TCBMs | Transparency and Confidence-Building Measures |
| TFEU | Treaty on the Functioning of the European Union |
| UAV | Unmanned aerial vehicle |
| UN | United Nations |
| UNGA | United Nations General Assembly |
| UNIDROIT | International Institute for the Unification of Private Law |
| UNOOSA | UN Office for Outer Space Affairs |
| WMDs | Weapons of Mass Destruction |

# NOTES ON THE AUTHORS

**Massimo Pellegrino** joined the EUISS in February 2015. His main research focus is space security, and in particular the dimensions of 'security in space' and 'security from space', including the connections between cyber and outer space. Prior to joining the EUISS, he worked in different capacities at the European Space Agency (ESA), European GNSS Agency (GSA), European Commission, and Italian Ministry for Foreign Affairs. He received a Master's Degree in Space Studies from ISU, as well as a Master's Degree in Accounting and Financial Management, and a Master's and a Bachelor's Degree in Industrial Engineering from the University of Naples Federico II.

**Gerald Stang** is a Senior Associate Analyst at the EUISS. He holds BSc and MSc degrees in chemical engineering from the University of Saskatchewan and an MA in international affairs from the School of International and Public Affairs at Columbia University. He specialises in climate and energy geopolitics, non-traditional security issues, and global governance and security challenges – from the Arctic to outer space.


**European Union Institute for Security Studies**
100, avenue de Suffren | 75015 Paris | France | www.iss.europa.eu