Cappelletti, Francesco; Papakonstantinou, Vangelis

Conference Paper

A Question of Strategic Legislation: Can the EU deal with cybersecurity issues in space?

32nd European Conference of the International Telecommunications Society (ITS): "Realising the digital decade in the European Union – Easier said than done?", Madrid, Spain, 19th - 20th June 2023

Provided in Cooperation with:

International Telecommunications Society (ITS)

A Question of Strategic Legislation:
Can the EU deal with cybersecurity issues in space?

Francesco Cappelletti, PhD Candidate in Cybersecurity Law, Cyber and Data Security Lab (CDSL), Vrije Universiteit Brussel.
Dr Prof. Vangelis Papakonstantinou, Faculty of Law and Criminology, Vrije Universiteit Brussel, Coordinator, Cyber & Data Security Lab (CDSL).

Figure 1 – Abstract illustration of cybersecurity of Space Systems generated by an AI.

Abstract:
This paper explores the impact of novel and forthcoming regulations on the European Union's (EU) strategic projection, focusing on space systems and their wide-ranging effects on services for European citizens and related industries. By examining space legislation and cybersecurity, this research provides an analytical perspective on whether the EU has strategically implemented regulations in shared competency fields like space and international security. While European Member States face challenges in implementing national space strategies, the EU's relevance extends beyond internal market and industry considerations, showcasing the Union's capabilities in implementing what this study defines as 'strategic regulations' in shared competencies, including international security.

Table of Content

Introduction

The profound influence of rapidly advancing technologies on the network society has manifested technological determinism as an undeniable reality and technology as a vector of global 'power' (McLuhan, 1962; Castells, Cardoso 2005). This dynamic is especially evident in regional economic blocs such as the European Union (EU), where technology regulation and implementation are integral to societal success (European Commission, 2011). The EU has achieved regulatory triumphs, exemplified by recent policies like the NIS 2.0, the Digital Services Act (DSA)/Digital Markets Act (DMA), and the Cybersecurity Act, providing harmonised rules for critical industrial sectors.

The EU is expanding its space capabilities, using it as a strategic tool for autonomy. Leveraging space systems enhances connectivity across sectors and stimulates innovation. The EU has developed a comprehensive legal framework for space actions and is working to strengthen the cybersecurity and resilience of space operations. It is thus emerging as a key actor in space, focusing on collective strength and self-reliance. However, addressing the strategic implications of space technologies represents a frontier challenge. The increasing reliance on space systems for communication and the Internet of Things (IoT) has underscored the necessity for comprehensive security measures to protect critical infrastructures. The focus has shifted from traditional safety engineering to addressing cybersecurity threats due to the complexity of space systems and the rise of cyberattacks. Hence, space security has entered the realm of strategic political dialogues, suggesting that the EU's complex regulatory procedures may be instrumental in devising a robust shared security framework.

While maintaining its reputation as a bastion of data and privacy regulation, the EU faces the challenge of developing a coherent cybersecurity infrastructure for its space systems. The surge in the significance and ubiquitous use of Space Systems necessitates constant updates to the regulatory framework. Specific Treaty implementation and shared competencies with member states contribute to regulatory hurdles, particularly in security matters. Given technology's role in driving *'strategic regulation'*, the advancement of space technologies demands reconsidering security implementation in this sector (European Council, 2021). The recent establishment of an updated space regulation and the European Union Agency for the Space Programme (EUSPA) marks a pivotal moment for addressing the EU's future security and strategic challenges (European Commission, 2021).

This paper explores the relation between novel and forthcoming regulations and the EU strategic projection, focusing on space systems and their wide-ranging effects on services for European citizens and industries. By examining space legislation and cybersecurity, this research provides an analytical perspective on whether the EU has strategically implemented regulations in shared competency fields like space and international security. While European Member States face challenges in implementing national space strategies, the EU's relevance extends beyond internal market and industry considerations, showcasing the Union's capabilities in implementing what this study defines as 'strategic regulations' in shared competencies, including international security.

The first part of this paper will define what *strategic legislation* is in the context of the European Union's regulatory framework, analysing key regulations that contributed to strengthening the EU's strategic projection. The surge of technology has redefined global power dynamics, driving national competitiveness, societal changes, and policy strategies. Incorporating theories about power dynamics, the network society, and the redistribution of power, this part examines how technology intertwines with these concepts. The focus will be on the European Union's strategic use of technology to maintain global influence. Concepts such as 'smart' policies and the EU's pursuit of Digital Strategic Autonomy are essential in the rapidly changing landscape of international relations and technological advancements. This analysis aims to highlight the pivotal role of technology in global power dynamics and the necessity of strategic adaptation.

The second part of the paper examines the EU's position in developing 'strategic legislation' concerning space systems' cybersecurity. This section compares conventional cybersecurity practices and their applicability to space systems. These challenges, along with others, will highlight the necessity for more efficient implementation of cybersecurity measures explicitly tailored to the unique nature of space systems. The distinct challenges posed by cyber risks in the space sector require the EU to evaluate and update its strategic legislation procedures continuously.

Technology as a vector of power

Investing in research and development is critical for countries aiming for global competitiveness, providing a competitive edge in various sectors. Advancements in technology not only fuel innovation but reshape the geopolitical landscape, enhancing global influence (Criekemans, 2022, pp. 61-96). Technological progress influences societal structures, instigating innovation cycles and impacting democratic organisations. The role of information technology in defining a network society initiates shifts from traditional power dynamics (Castells, 2005). Further, advancements in information technology led to a 'redistribution of power', democratising information, and global economic transformations (Palmer, 1986).

Pursuing technological advancement and redistributive effects is vital in the context of the European Union to ensure long-term success and enhance its power projection. The EU can secure its position as a significant global player by prioritising technological innovation and regulating emerging technologies like space systems. This commitment strengthens the EU's influence, enabling it to shape the dynamics of the international arena actively. The increasing significance of technological advancement, knowledge, and its ownership is driving significant transformations in the concept of 'power'. Robert A. Dahl's traditional understanding of power (Dahl, 1957), which emphasises relational dynamics and various methods of exerting power, remains relevant in this context. However, in this enhanced interpretation of the concept of power, an actor's ability to influence and dictate the behaviour of others can be attributed to several technical advantages. Thus, building on Dahl's postulation, power can be further nuanced within technological advancements, potentially heralding a new paradigm in understanding power in the digital era. Concerning technological advancements, power can be defined as:

'The ability of one actor or entity to influence and control the behaviour of others through technical advantages such as market dominance, superior technological capabilities, access to vast data resources, and advanced infrastructure and logistical systems'.[1]

Technical advantages, spanning advanced hardware, software, and expertise, enable superiority. The ability to manage large data volumes and own advanced infrastructures, including physical assets like manufacturing plants and virtual elements like cloud networks and algorithms, further contribute to these advantages. Consequently, technology serves as an enabler of this concept of power. All this creates an interplay between power, authority, and technology, influencing decisions and market dynamics. Technology-driven power can be legitimised by legal frameworks, regulatory bodies, or industry standards, influencing the EU's strategic positioning. Benefiting from this interlink requires timely, impactful, yet adaptable legislation and decision-making procedures, often termed 'smart' policies. Such policies foster economic development and sustainable growth.[2]

In order to benefit from the interlink between technology and power, legislation and decision procedures (i.e., the revised concept of 'authority' above) is critical. These processes must be timely, impactful, yet flexible and adaptive. Such procedures can also be defined as 'smart' policies. Smart

[1] In the context of this research, this definition of power aims to identify the level to which power dynamics occur. In the context of the EU, it can be considered a single entity (i.e., a company), an agency, one of the Member States, or any of the EU institutions concurring to create regulations to enhance the strategic projection of the internal market.

[2] The concept of authority or legitimate power in the context of the EU can have a positive or negative impact on technologies and their advancement as it directly affects the internal market dimension and industry.

policies can create an enabling framework for economic development, fostering inclusive growth and contributing to sustainable development.[3].

In the EU, policy formulation involves citizens' and stakeholders' feedback and political strategising, particularly regarding new technologies with global impact. This interplay between tech advancement, authority responsiveness, and power dynamics reshapes technology as a power vector (see Figure 2).[4]

This pursuit of technological knowledge is particularly vital for the European Union to ensure long-term success and enhance its power projection. The EU can secure its position as a significant global player by prioritising technological innovation and regulating emerging technologies like space systems, AI and cybersecurity. This commitment strengthens the EU's influence and consolidates its power, enabling it to actively shape the dynamics of the international arena.

In recent years, the European Union underwent a mindset shift to prevent itself from being overshadowed by the dominance of technological champions, such as the United States and China, by providing a level playing field to industries in the internal market. The EU aims to assert independence and maintain global influence, embracing the 'Digital Strategic Autonomy' (Cappelletti et al., 2022). This ensures relevance amid evolving international relations and technological advancements, avoiding a mere mediating role between technological competitors.

EU's Strategic Legislation

The prior discussion underscored technology's significant role in exerting power and the importance of 'smart policies' in European legislative strategies. However, the space legislation domain requires a unique evaluative lens. The critical role of space sectors in shaping Europe's future necessitates robust policies that transcend conventional policymaking. The assessment of these policies should focus on strategic legislation designed to maximise the technological potential from market and industry perspectives. The possession and access to advanced technology alone do not guarantee power in traditional international relations terms; it must be supported by comprehensive policies, regulations, and standards to foster a vibrant market economy.

Given the European Union's extensive and diverse market and the intricate global network of interdependent nations and markets, a re-evaluation of the power-technology relationship must include additional variables. Political culture, policy direction, internal market structure, leadership, management, and the capacity to innovate and adapt to emerging technologies are key indicators of technological success and power. These elements, in conjunction with technology, form the constituents of power. Balancing technological advancement with these other constituents is pivotal to gaining a competitive edge globally (Lewis, 2022). In the context of the European Union, *strategic legislation* can be defined as

"*A set of laws and regulations aligned with the EU's overall strategy and aimed at achieving planned goals. Strategic legislation benefits stakeholders and promotes cooperation within the internal market*".

Strategic legislation must be implemented promptly and timely, allowing it to contribute effectively to the EU's strategic projection. The term encompasses a set of proposals, laws and regulations developed and implemented in alignment with the EU's overall strategy and political

[3] A 'smart policy' is a forward-looking plan that balances immediate needs with long-term sustainability and growth. Examples include policies incentivising renewable energy use, smart city initiatives integrating technology for efficient city management, schooling policies improving digital literacy and adapting curriculum for the digital age, health policies promoting preventative measures for long-term public health improvement, and environmental policies to reduce pollution and preserve natural resources. While these guidelines may require short-term investment and adaptation, they are designed with a vision for lasting benefits and improvements.

[4] This process entails two main components. Firstly, it involves receiving feedback from citizens and stakeholders, which can be positive or negative, shaping policy outcomes and development either independently or through stakeholder involvement. Secondly, the political dimension and strategic projection play a crucial role.

direction. These laws aim to achieve strategic priorities and goals identified by the Commission every five years at the beginning of a new term. The legislation benefits EU citizens, businesses, and other stakeholders while ensuring compliance with the EU framework and promoting international cooperation. The European Commission ensures that such legislation is evidence-based, adheres to best practices, and continuously evaluates effectiveness, efficiency, relevance, and coherence (European Union, 2021). However, defining what legislation can be defined as 'strategic' implies dwelling in the realm of policies, political choices, and preferences that compete in shaping the regulatory procedures.

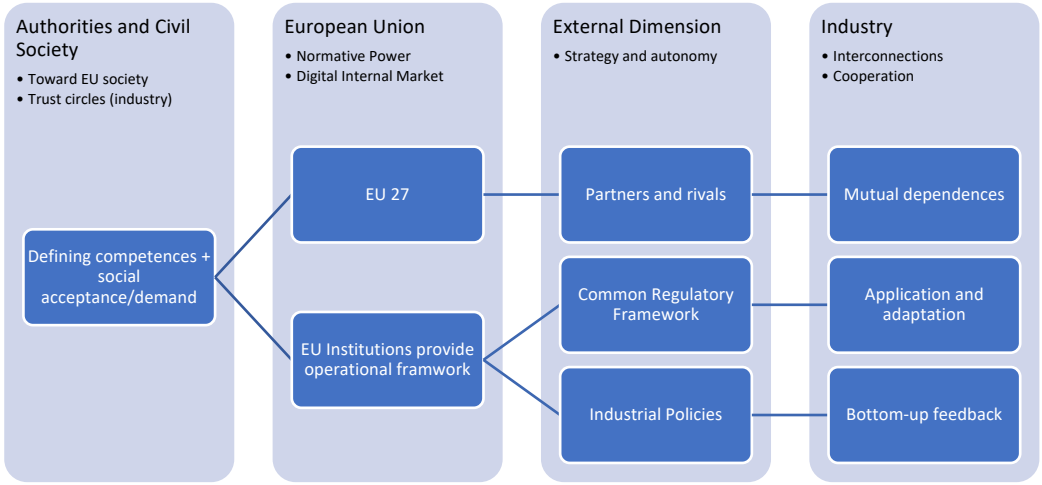


Figure 2 - Dimensions of "Strategic Autonomy Europe" and sources of power (elaboration of the author on F. Cappelletti, G. Pogorel. A. Nestoras, 2022.

The strategic projection of the European Union is primarily shaped by a series of acts and regulations encompassing sectors such as finance, foreign policy, food production, defence, and technology. As illustrated in the following table, these policies and actions reflect the EU's ambition to drive political, economic, and societal progress while enhancing its normative and strategic power in a global context.

Table 1 - Sources that Contribute to Strengthening European Strategic Projection

EU's Political and Institutional Progress	**Description**
European Monetary Union (1992)	Establishing the single currency system.
European External Action Service (2010).	EU's diplomatic service for foreign policy.
European Banking Union (2012).	Strengthening the financial system and supervision.
Common Agricultural Policy / Common Fisheries Policy (2014)	Sustainable food production and management.
Common Security and Defence Policy / PESCO (2017)	Enhancing EU's defence capabilities.
Strengthening the role of the euro	a. Digital euro (legislative, incl. impact assessment, Article 133 TFEU, Q2 2023) b. Scope and effects of the legal tender of euro banknotes and coins (legislative, Article 133 TFEU, Q2 2023)
Transnational Electoral Lists in 2024 Elections	Encouraging pan-European democracy.

EU's Soft Power Instruments – Normative Power Europe	**Description**
GDPR (2018)	Comprehensive data protection and privacy.
Green Deal (2019)	Ambitious climate and environmental goals.
AI Regulation (2021).	Ensuring ethical and legal AI development.

DSA + DMA package (2022)	Digital market competition and online safety.

EU's Technological and Industrial Strategic Projection	**Description**
NIS Directive (2016)	Network and information system security.
Roaming Regulation (2017)	Eliminating mobile roaming charges.
European Electronic Communications Code (2018).	Modernising telecommunication rules.
A New Industrial Strategy for Europe (2020)	Strengthening industrial competitiveness.
Fit 4/55 (2021)	Reducing emissions for climate goals.
European Industrial Alliances	Collaborative industry networks.
5G Action Plan (2016) / Horizon Europe (2020)	Boosting research and innovation.
Proposal for Batteries and Waste batteries regulation (2020)	Sustainable battery production and recycling.
Cybersecurity Act (2019)	Strengthening cybersecurity certification and resilience.
NIS2 directive (2022)	Enhancing network and information system security.
Proposal for European Chips Act (2022)	Boosting semiconductor production and competitiveness.
Proposal for EU Cyber Resilience (2022)	Protecting critical infrastructure from cyber threats.
Single Market Emergency Instruments (2022)	Ensuring market stability during crises.
Proposal for Critical Raw Materials	European critical raw materials act (legislative and non-legislative, incl. impact assessment, Article 114 TFEU, Q1 2023)
Spectrum management for Digital Decade	New radio spectrum policy programme (RSPP 2.0) (legislative, incl. impact assessment, Article 114 TFEU, Q3 2023)

Core values in the EU, such as cohesion and solidarity, privacy, non-discrimination, equality and social justice, define and further shape the ‘normative power’ dimension. In this context, cybersecurity is increasingly acknowledged among these fundamental rights in scholarly discourse. Despite its complexity, introducing a cybersecurity right in EU law is feasible with existing foundations. Defining its content and implementation is critical for digital self-protection and policy compliance. The established data protection model can guide this undertaking, addressing EU competence and national security issues. It is of utmost importance to appropriately incorporate cybersecurity within conventional security frameworks (Papakonstantinou, 2022).

Specific EU regulations can be identified as ‘strategic’ due to their all-encompassing and forward-looking approach to crucial issues. These include initiatives like the Common Security and Defence Policy/PESCO, which encourages defence cooperation among EU states; GDPR, setting stringent data protection standards; DSA/DMA package, regulating online platforms; Cybersecurity Act, which establishes a robust cybersecurity framework; and the AI Act, ensuring ethical AI use. Together, these laws embody the EU's strategic policy direction for fostering security, privacy, and innovation in the digital era. Although the proposed list of EU strategic legislation is only part of the legislative effort under which the EU went within the path towards European integration, the primary objective of this paper’s first section is to establish a foundational understanding upon which to concentrate concerning the EU space strategy.

The EU Space Program and its evolution

Space encompasses the vast expanse beyond earth's atmosphere, including celestial bodies and the region where satellites and spacecraft operate. It is integral to various sectors and applications. **Satellite** types include communication satellites for global connectivity, earth observation satellites for environmental monitoring, navigation satellites for precise positioning, and weather satellites for forecasting and disaster management. **Launchers** propel satellites into desired orbits. Space services include satellite communications, imagery, navigation, research, supporting telecommunications, agriculture, disaster response, and more. **Space security** protects assets, infrastructure, and data from cyberattacks, space debris, and unauthorised access. This entails developing secure communication systems, safeguarding critical infrastructure, and fostering international cooperation for responsible space activities.

Space systems are one of the main in-development fields of interest in the technological landscape of modern European industry. The reliance on space technologies shifted away from the sole concept of positioning, navigation, and timing (PNT) functions. Communication technologies are increasingly reliant on space systems' support infrastructure and components. The full-scale deployment of new communication networks and the exponential increase in the use of the Internet of Things (IoT) made terrestrial-based infrastructures increasingly dependent on space-based systems. In this context, it is essential to ensure the security of the whole infrastructure.

Space systems are becoming an essential element of the global connectivity infrastructure, such as 5G and future networks (6G)[5], and other applications, including agriculture, natural disaster response, smart cities, renewable energies, and health. In agriculture, it enables precision farming and integrated solutions, empowering farmers to increase yields, save resources, and facilitate safe landings and autonomous machines. During natural disasters, EU Space can help in rescue operations, providing support during floods, fires, earthquakes, and other disasters. In implementing IoT in municipalities and creating smart cities, space systems contribute to urban mapping, planning, and infrastructure monitoring, enhancing urban transport and intelligent waste management. In the renewable energy sector, EU Space assists in siting renewable energy facilities and evaluating potential energy generation and environmental impacts. Additionally, in the health field, EU Space plays a role in forecasting air quality and UV radiation, providing valuable insights into their impact on public health (European Commission, 2022).

Considerable time (in terms of European integration and the advancement of technologies) had elapsed since 2007, when the European Commission and the European Space Agency (ESA) jointly introduced an extensive political framework to establish a robust and sustainable space sector within Europe.[6]. The proposal at that time aimed to coordinate civil space programs, develop European space applications, preserve autonomous access to space, and increase synergy between defence and civil space programs, enhancing cooperation between the Commission and ESA (European Commission, 2007). Since then, space has often been on the European Commission's agenda.

The EU's competencies in space have evolved through treaty changes, progressively expanding into new fields and bringing the EU closer to space and its applications. Despite the lack of explicit legal basis, the EU has creatively utilised its existing competencies to engage in the space sector, establishing flagship programs like Galileo (the European global satellite navigation system) and the Global Monitoring for Environment and Security (GMES) and Copernicus. The Lisbon Treaty introduced space-related articles, providing a legal framework for the EU's actions in previously uncovered areas and officially recognising the EU's competence in the space domain in

[5] The relevance of space for 5G networks is crucial in providing essential attributes such as ubiquitous coverage, seamless connectivity, and network resilience. Integrating satellite and terrestrial networks is crucial for establishing the global connectivity infrastructure of 5G. The European Space Agency (ESA) has launched the 'Space for 5G and 6G' program to support integrating satellite technology into 5G networks and facilitate the development of innovative technologies and services. See ESA, 2023.

[6] For a perspective on different space regulations per country over time, see Appendix - Table 5.

its Art. 189[7] (European Union, 2016) giving a mandate to the EU to draw up a European Space Policy. Space is, therefore, a shared competence of the EU and its Member States. As a result of the growing use of space systems and the advancement of applications in recent years, Europe is striving for a more coordinated approach to space, moving beyond its previous position where it sought to be 'non-dependent' on space technology rather than fully independent (Reillon, 2017, p. 30).

Different documents addressed the need for the EU to strengthen resilience, security, and cybersecurity in outer space. Creating a Strategic Compass also reinforced space security in 2022, with a plan for strengthening the EU's security and defence policy, focusing on action, investment, partnerships, and security (EEAS, 2022). While the documents refer to "strategic enablers and next-generation capabilities", there is no direct reference to the cybersecurity of space systems. Other documents, however, seem to define the issue more clearly. The significance of bolstering the EU's defence policy in outer space is explored in other communications, highlighting the strategic value of space and the protection of critical space infrastructures. Moreover, the increase in the EU's prominent presence in the sector and initiatives concerning Space Traffic Management (STM) are under discussion, emphasising the need for effective implementation and collaboration (EEAS, 2021).

Regulation (EU) 2021/696 and Decision (CFSP) 2021/698 have established recent developments in EU space regulation. With these regulations, the EU establishes the European Union Agency for the Space Programme (EUSPA), which is responsible for managing various space programs (including Galileo, EGNOS, and Copernicus). Its scope is to foster innovation and economic growth in the European space sector. By overseeing satellite navigation systems, security accreditation for the Copernicus program, and the development of space-based governmental and security applications, EUSPA's creation signifies the EU's commitment to enhancing its role and autonomy in space, promoting a more resilient and competitive European space sector (European Parliament and Council, 2021). Furthermore, the introduction of Regulation 2023/588 and its Secure Connectivity Programme demonstrates the European Union's commitment to further addressing security challenges in space. By enhancing communication capacities for governmental users, businesses, and regions with limited connectivity, this regulation contributes to overall security and resilience in EU's space systems (European Parliament and the Council, 2023).

The Council Decision (CFSP) 2021/698 highlights the importance of ensuring the security of systems and services deployed under the Union Space Programme, explicitly focusing on the European Global Navigation Satellite System (GNSS). Recognising the strategic dimension and potential impact on the security of the Union and its Member States, the Council establishes the necessary measures to avert threats and mitigate harm arising from the deployment, operation, and use of space-related systems and services. This decision emphasises the significance of space technology, data, and services in preserving strategic interests and acknowledges the potential security threats they may face. It also highlights the role of EUSPA in ensuring the operation and security of the Galileo Security Monitoring Centre (GSMC) and the collaboration among Member States, the Council, the Commission, and other stakeholders in managing and addressing security concerns. (European Union, 2021a).

---

[7] *Article 189 – TFUE:*

1. To promote scientific and technical progress, industrial competitiveness and the implementation of its policies, the Union shall draw up a European space policy. To this end, it may promote joint initiatives, support research and technological development and coordinate the efforts needed to explore and exploit space.
2. To contribute to attaining the objectives referred to in paragraph 1, the European Parliament and the Council, acting following the ordinary legislative procedure, shall establish the necessary measures, which may take the form of a European space program, excluding any harmonisation of the laws and regulations of the Member States.
3. The Union shall establish any appropriate relations with the European Space Agency.
4. This Article shall be without prejudice to the other provisions of this Title.

The EU Space Programme (2021-2027) aims to strengthen Europe's position in space, stimulate economic growth, and address climate change and technological innovation. The budget of this program is €14.8 billion and aims to provide continuous, high-quality space-related data and services, enhance safety and security, promote international cooperation, and mitigate space debris. The newly established EUSPA manages the programme, which objectives include:

- delivering uninterrupted, high-quality, and secure space-related data and services.
- maximising socio-economic benefits.
- enhancing safety and security.
- promoting the EU's global space role.
- ensuring the sustainability of outer space activities.

The institutional commitment to secure and resilient global connectivity has been strengthened with the introduction of the Infrastructure for Resilience, Interconnectivity, and Security by Satellite (IRIS²) in the regulation 2023/588, which lays down the objectives of the Space programme, the budget for the period 2023-2027, the forms of Union funding and the rules for providing such funding, as well as the rules for the implementation of the programme. IRIS², which falls under the Secure Connectivity Programme, represents a significant advancement for the satellite constellations of the European Union. The primary aim of IRIS² is to enhance communication capabilities for governmental users, businesses, and regions with limited connectivity. The satellite constellations facilitated by IRIS² support various governmental applications, including border surveillance, crisis management, and secure communications for EU infrastructures. These applications highlight the significance of addressing cyber risks specific to space systems. In addition to governmental applications, IRIS² enables mass-market applications such as broadband satellite access and cloud-based services. These commercial applications also need robust cybersecurity measures to protect the integrity and security of the services provided. Initial services are expected by 2024, with full operational capability by 2027. One of the key objectives of IRIS² is to ensure the long-term availability of reliable, secure, and cost-effective satellite communication services on a global scale.

The EU's efforts in strengthening the Space Program and its navigation systems can be seen as a response to its sovereignty concerns and to achieve independence in the space domain. Ensuring reliable and precise positioning and timing in critical sectors such as transportation, emergency services, and infrastructure management, reducing reliance on external providers like the US-operated GPS enhances the EU's strategic autonomy, reducing dependence on restricted military-grade GPS capabilities and gaining complete control over its navigation system. The development of the EUSPA showcases the EU's commitment to safeguarding its interests in a coordinated manner with its member states, asserting sovereignty, and strengthening its resilience in this field.

It can be said that space is nowadays acknowledged in the European Union as an increasingly critical domain for the strategic autonomy of the EU and its Member States. It plays a vital role in achieving the EU's political agenda, supporting economic activities, and enhancing resilience. The regulatory framework for space operations in the EU has grown consistently in terms of the regulations and the classification of its organisations.[8]

Enhancing the use of space for civilian use and security and defence, is a crucial aspect of the EU's strategic autonomy. Moreover, the EU is committed to safeguarding the use of space for peaceful purposes while protecting its security interests and ensuring the competitiveness, prosperity, and security of the EU. This includes promoting norms, rules, and principles for responsible behaviours, engaging with the United Nations and third countries, and partnering with international partners for developing technologies, and NATO when it comes to space security and defence (European Commission, 2023). However, space remains an increasingly contested domain, with some countries capable of targeting critical space infrastructure (in both space and ground segments).

[8] See also: Appendix – Table: Classification of Space Organisations and Their Security Practices.

Therefore, space-based systems are also crucial for military power, with nations worldwide investing billions of dollars annually in developing and deploying advanced precision-guided weapons.

Many countries are rapidly leveraging space-based systems to enhance security and defence. In line with its defensive purpose, NATO recognises the increasing importance of space for security and prosperity, acknowledging the benefits and risks associated with space capabilities. Potential adversaries are developing counter-space technologies that could disrupt or deny Allies' access to space. NATO's approach to space focuses on integrating space considerations into core tasks, providing space support in operations, enhancing space domain awareness, ensuring deterrence, defence, and resilience, promoting capability development and interoperability, and incorporating space in training and exercises. NATO stresses the importance of responsible space behaviours, science, technology, innovation, industry partnerships, and engagement with relevant international organisations. Terminology related to space is defined to ensure clear communication within the context of NATO's space policy (NATO, 2022).

The EU's response to secure defence and resilience in space includes developing a security framework to protect space systems, sharing information, and fostering cooperation. The priorities include integrating security measures into space system design, exchanging best practices among commercial entities, and participating in standardisation organisations. The EU has recognised the increasing importance of military applications in space, as evidenced by initiatives such as the European Military Space Surveillance Awareness Network (GEODE) and the Defence of Space Assets (DOSA). These projects, developed under Permanent Structured Cooperation (PESCO) framework, highlights the EU's commitment to enhancing its military capabilities in space. In addition, the EU Radio Navigation Solution (EURAS) and the Common Hub for Governmental Imagery (COHGI) are further examples of efforts to strengthen space-based capabilities for defence purposes. The flexibility for other participating Member States to join as project members or observers further fosters cooperation and collaboration in the EU's military use of space (PESCO, 2023).[9]

The following section will assess how the EU aims to contribute to cybersecurity standards in the space domain and which are the main challenges to achieving a resilient space cybersecurity posture in the EU.

Space and Cybersecurity

Consider the ramifications of a cyber-attack undermining the control of a high-value satellite after its launch into space. The fallout could be extensive, from deviation in the satellite's programmed trajectory to potentially destroying other space assets. The concept is more plausible than it might appear. The rapid progression of space technologies has led to a surge in cybersecurity threats to space systems, encompassing jamming, spoofing, hijacking, interception, theft, data corruption, and denial-of-service attacks, with severe consequences. They compromise data accuracy, disrupt trajectory control, and result in data loss and unavailability, potentially leading to the loss of valuable assets with an impact on market share. Implementing robust countermeasures is essential to mitigate risks, safeguard space systems, and protect against these threats (Thangavel et al., 2022; Scholl & Suloway, 2022).

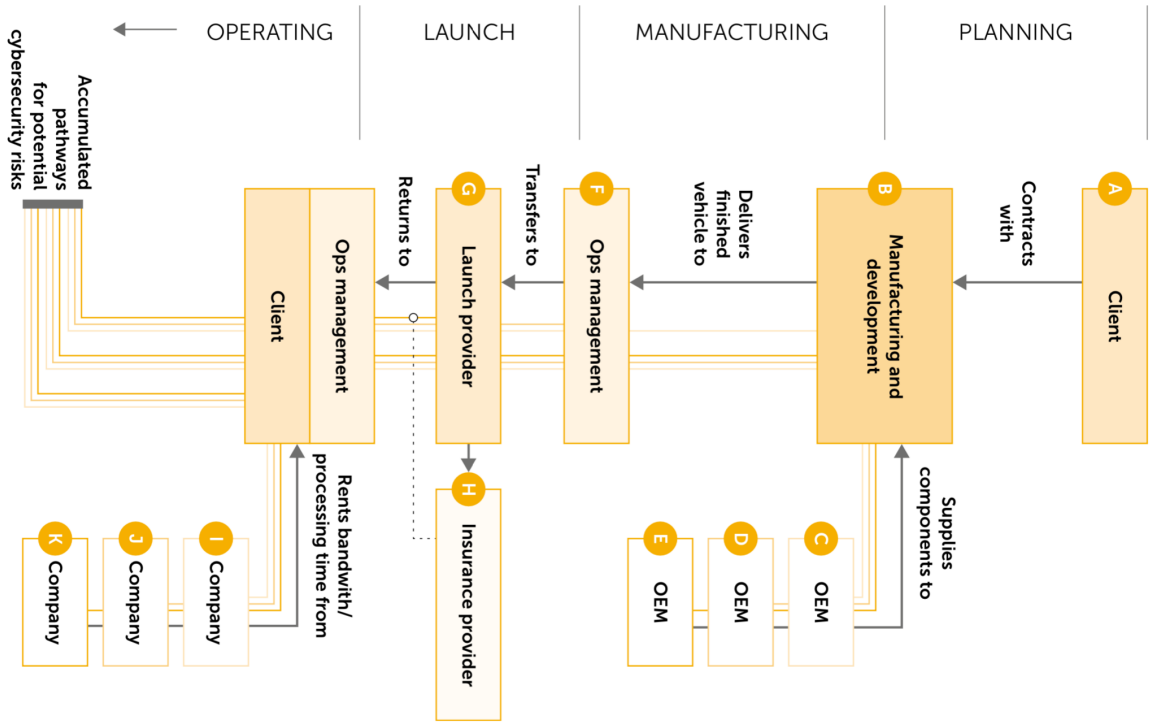
Due to the complexity of space systems segmented between upstream and downstream activities, the connected services and the whole infrastructure, and the involvement of digital platforms for handling data, the challenge of cyber-securing space systems is central to advancing this technology (Oakley, 2020). Like cyberspace, space is a security or "key war-fighting domain with critical vulnerabilities, both unintentional and intentional" (Absek, 2014). Both domains depend on technologies inside the radio and electromagnetic spectrum and Information Technology (IT). A fascinating interplay exists between space infrastructure, IT infrastructure, and cyberspace. The space

[9] See also: Appendix: Table: Security Projects Related to Space Systems in the EU.

infrastructure sets the stage for IT infrastructure development, which in turn contributes to the creation of cyberspace.

Interestingly, cyberspace then creates the conditions necessary to control the space infrastructure. This intricate relationship highlights the distinctiveness of cyberattacks in space systems, as they encompass physical, transmission, and application dimensions in a unique and interconnected manner. The chart below provides a vivid representation of the vast surface area vulnerable to threats in space systems. It highlights the multifaceted nature of these systems, involving numerous stakeholders and complex interactions.

Table 2 - Lisi, 2022



Space operations and a complex supply chain can be divided into three major segments. Orbiting satellites or constellations of satellites form the space segment, together with their payload. Orbiting objects are linked and managed from the control segment (ground segment) situated on the

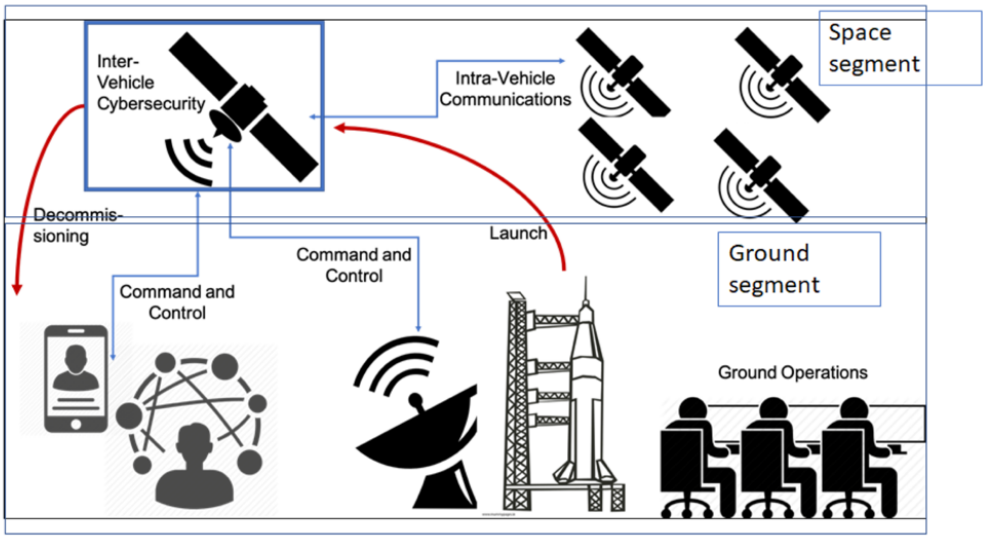


Table 3 - Space Segments (Scholl & Soloway; NISTR, 2022)

earth's surface, together with hardware and software equipment. From these facilities, technicians manage the control and operation of space assets from launch to disposal. Finally, the segment that lets users enjoy space's services, i.e., the user segment, consists of individuals, their software, and applications.[10]. This initial differentiation among various segments within space systems is crucial for determining the surface attack and which cybersecurity protocols and practices to implement at different stages within the supply chain and lifecycle of satellites and space systems (Lisi, 2022).

The security and integrity of space operations face significant risks due to vulnerabilities in satellite command and data distribution networks. Advanced actors with knowledge of these networks can exploit their cyber threats and employ offensive cyberspace capabilities. Such actions can have reversible or non-reversible effects, targeting space systems, associated ground infrastructure, users, and related links (DIA, 2022).

The software has been mentioned a few times, as it plays a vital role throughout the infrastructure, enabling data control, storage, and management. Cyber-attacks targeting software deployed in space systems substantially threaten satellite systems and their associated infrastructure. These attacks can exploit various weaknesses, including backdoors, unencrypted data, insecure protocols, software bugs, supply chain attacks, and human errors. Such attacks can have cascading effects, interrupting multiple services. Earth-bound entry points connected to the internet, weak long-range telemetry, IoT devices utilising satellite communications, and vulnerable satellite ground stations provide potential surface attacks for cybercriminals. Supply chain attacks, targeting the less secure elements in the supply chain, further exacerbate the risks. The challenges mentioned above become even more complex when considering commercial off-the-shelf (COTS) software and hardware components within the supply chain of space systems. These components introduce vulnerabilities that have the potential to impact multiple platforms (Pavour & Martinovic, 2020). Therefore, it is crucial to integrate a solid certification scheme for both software and hardware starting from the design phase to mitigate any potential risks.

The space segment is also susceptible to cyberattacks. Communication in the space segment happens between vehicles (crosslinks) and can lead to potential risks. The inter-vehicle cybersecurity plays a vital role in safeguarding against cyber threats. Again, various measures from the traditional cybersecurity domain are in place to mitigate risks, such as identification, protection, detection, response, and recovery, to ensure the integrity and resilience of the system[11]. It is worth noting that the responsibility for inter-vehicle cybersecurity primarily lies with small commercial satellite owners and operators. At the same time, other aspects of the infrastructure are typically outsourced to external suppliers and providers (Scholl & Suloway, 2022). This implies that a robust cybersecurity framework (i.e., regulations and certification scheme) is vital in assessing the capacity to protect those assets.

---

[10] In a satellite Command and Control (C2) system, multiple components work in tandem to facilitate the operations. These components include an operations centre, base station, ground network, and satellite. The base station is a central hub, enabling communication between the operations centre and the satellite. This communication involves transmitting various types of information, such as payload data, telemetry, and Command & Control instructions. Ground stations operate continuously and are remotely controlled by the operations centre. Effective data transmission is facilitated through communication protocols like the Space Data Link and Space Link Extension. The system also encompasses a user segment that contains terminals responsible for signal reception and transmission. Analysing the risks associated with space systems necessitates a comprehensive understanding of these components and their interconnectedness (retrieved from Aguilar Sanchez & Fisher, 2012).

[11] The NIST (National Institute of Standards and Technology) mitigation framework for cybersecurity provides a structured approach to identifying, assessing, and responding to cybersecurity risks. It consists of five core functions: identify, protect, detect, respond, and recover, which help organisations enhance their cybersecurity posture. The NIST framework "applies to any organisation in any part of the critical infrastructure."
. See: NIST cybersecurity framework (https://www.nist.gov/cyberframework)

Mitigation systems

In the EU context, strategic legislation, as defined in this research, guides legal frameworks toward achieving planned goals and enhancing cooperation within the internal market. Mitigation systems must be implemented as a crucial component of such strategic laws, as they safeguard crucial infrastructure, especially space-based systems, from cyber threats. This ensures system resilience and bolsters stakeholder benefits, embodying the purpose of strategic legislation.

The vulnerability of space systems to cyberattacks mainly arises from the technology used in the terrestrial segment of GNSS, which encompasses complex software programs, data processing centres, and data communication networks. Due to the extensive nature of IT infrastructures, the likelihood of internal and external cyberattacks is significantly high. To address these risks, traditional safety guidelines applied in other domains, such as the identification, protection, and detection functions, are also implemented in space systems. Various measures can be implemented to safeguard space systems, ensuring confidentiality, integrity, and availability.[12] Overall, the mitigation of risks in space is facilitated by implementing diverse technologies drawn from traditional cybersecurity measures.

Table 4 - Cybersecurity Mitigation Systems (NIST glossary, ENISA, other sources)

Strategy	Description
Encryption	Implementation of robust encryption techniques, such as Advanced Encryption Standard (AES), to ensure the confidentiality and integrity of sensitive data transmitted between space systems and ground infrastructure.
Access Control	Establishment of strict access control policies and mechanisms to restrict unauthorised access to space systems. This includes the use of strong authentication methods, role-based access control, and regular monitoring of access logs.
Intrusion Detection and Prevention Systems (IDS/IPS)	The utilisation of IDPS to identify and prevent unauthorised access attempts, detect anomalous behaviour and potential cyber threats, and trigger alerts or block suspicious actions based on network traffic analysis and activity monitoring.
Secure Coding Practices	Adherence to secure coding practices, such as following coding standards, implementing input validation, and maintaining secure configuration management, to mitigate vulnerabilities in software and firmware that attackers could exploit.
Incident Response Plan	A comprehensive incident response plan must be in place, outlining procedures for quickly identifying, containing, eradicating, and recovering from cyber threats. This plan also includes measures for preserving evidence necessary for forensic analysis.
Security Frameworks	Security frameworks, including the NIST Cybersecurity Framework, ISO 27001, and the European Union Agency for Cybersecurity (ENISA) guidelines, are implemented to guide risk assessment, security controls, and continuous monitoring.
Security Testing and Auditing	To ensure compliance with security policies and standards, periodic security audits are carried out. In addition, regular security testing, which includes vulnerability assessments and penetration testing, is conducted to identify and rectify potential weaknesses in space systems.
Training and Awareness	Training programs and awareness campaigns are employed to cultivate a cybersecurity-aware culture. These educational initiatives teach personnel best practices for handling sensitive information, common cyber threats, and social engineering techniques.

Beyond technical details, the growth of widespread cyberattacks capabilities, difficulties in implementing international norms in the field of cyberspace and the increase in the use of (cyber)space for civilian services recently forced the discussion about the security of space to the domain of strategic political theories (Pavur & Martinovic, 2019). This awareness might represent an advantage in the context of the EU regulatory procedures, contributing to shifting away the debate from a traditional military domain (Sheehan, 2015).

A tailored and comprehensive framework is necessary to strengthen cybersecurity in space operations. This framework would allow organisations to develop a profile that effectively

[12] Confidentiality measures focus on protecting cryptographic keys during uploading, securing sensitive security parameters, and optionally protecting telecommand transmissions. Integrity and authentication measures include preventing transmission errors, countering spoofing attacks, and authorising command sources. Availability is enhanced by protecting telecommand transmissions using spread spectrum, null-steering antennas, and high-power up-links. These measures collectively enhance the security and reliability of space systems.

communicates their cybersecurity posture and facilitates the organisation of cybersecurity tasks. It is a valuable tool for conveying cybersecurity requirements to suppliers and effectively managing risks associated with outsourcing space operations. Given the complexity of commercial space operations involving multiple organisations, clear communication of expectations, capabilities, and requirements is crucial for addressing cybersecurity risks. Considering factors such as changes in asset reliance, adversary capabilities, and intent is essential in determining an organisation's risk profile. Regularly revisiting the framework and regulations is vital for effective risk management practices (Scholl & Suloway, 2022).

Additional Challenges

With the rising accessibility and cost-effectiveness of space access, there has been a surge in the deployment of non-geostationary mega-constellations and small satellites, serving a wide range of applications. However, this increase in space activities has also led to a growing concern regarding space debris and its potential risks to operational satellites. Space is infinite, but the earth's orbit is quite crowded. Hence, constant monitoring and tracking of space objects remain an essential challenge to space systems. Moreover, debris and material orbiting and constantly colliding with satellites require constant assessment of techniques for minimising the risk of collision and removing debris.

Space Situational Awareness (SSA) and Space Surveillance Systems (SSS) capabilities represent a significant part of space operations. SSA capabilities enable identifying, tracking, and predicting the position of an object and, thus, potential collisions (Erwin, 2019). This means data are collected continuously, requiring robust cybersecurity measures to satisfy the requirements of the CIA triad. Malicious actors could manipulate or disrupt the data, leading to incorrect collision predictions and other negative consequences.

Developing specific cybersecurity measures for SSA and SSS can help address these risks and ensure the continuous functioning of these critical systems. Moreover, international cooperation between SSA and SSS is crucial to monitor the space environment effectively. Housen-Couriel conducted a comprehensive review of available measures under international law to address hostile acts targeting satellite systems, emphasising the importance of considering existing legal regimes and cybersecurity factors in formulating a practical framework for legal remedies (Housen-Couriel, 2016). Legislative measures should also consider the need for international collaboration and establishing common standards and norms (EUSC, 2023; ESA, 2020).

Space cybersecurity presents distinct challenges that differ from traditional practices. Current regulations and the lack of comprehensive threat modelling have faced criticism for their limitations. The complex bureaucratic structures and shared resources within the space ecosystem raise concerns about trust and compromise among stakeholders. Bridging the expertise gap is crucial, necessitating interdisciplinary knowledge. Publishing and collaboration face complexities due to the multidisciplinary nature of space technologies. Space systems surpass being mere ‘computers in the sky’, and terrestrial security practices prove inadequate. Research enhancement, particularly in systems security, is necessary for advancing space cybersecurity (Pavur & Martinovic, 2020, pp. 2-6).

Table 5 - Unique Technical Security Challenges (adapted by: Pavour & Martinovic, 2020)

Challenge	Description
Single Point of Failure	Satellites serve as singular vulnerabilities in critical infrastructures, attracting numerous attackers beyond those directly tied to mission functions.
Lack of Regulation	The absence of specific regulations for satellite cybersecurity creates uncertainty about the appropriate controls for ensuring security in space systems.
Complex Supply Chains	Elaborate supply chains in the space industry introduce challenges related to backdoor risks and allocating organisational responsibility for security practices.
COTS Integration	Integrating Commercial off-the-shelf (COTS) software and services in space systems creates vulnerabilities that can impact multiple platforms, necessitating customised patches.

Specialised Nature of Aerospace	The unique characteristics of aerospace operations present challenges in understanding and contextualising threats and defence strategies.
Resource Constraints	Satellites are resource-limited devices with constrained computational capabilities, requiring careful consideration of security-performance trade-offs.

Cyber threats targeting space systems, including satellites and ground stations, introduce distinct challenges compared to traditional cybersecurity threats. These challenges necessitate tailored measures and a holistic approach to cybersecurity in space, integrating governmental entities and the private sector. On the one hand, the interconnected nature of the complex 'system of systems' forming the space segments requires advanced technical capabilities for successful attacks, which limits the potential number of attackers. On the other hand, Paver & Martinovic (2020) identify high-risk threats from the national military and state intelligence agencies, industry insiders and suppliers. Beyond motivations, and given the extensive supply chain, the repercussions of an attack on this infrastructure can be significant and far-reaching.

In summary, addressing the unique challenges of cybersecurity in the three space segments, along with the challenges in SSA and SSS capabilities, requires tailored technical and legislative approaches to ensure the security and resilience of these systems. This entails developing specific cybersecurity measures, fostering international cooperation, and establishing common standards and norms to mitigate risks effectively. This should also involve active engagement with the private sector, given its vital role in space infrastructure and technologies.

Can the EU deal with cybersecurity issues in space?

Space cybersecurity presents distinct challenges that call for unique solutions. Despite advancements in space capabilities and protection frameworks, the evolving cyber threats and complex space-based systems pose continuous challenges. However, it is clear that there is no need to 'reinvent the wheel'. Existing cybersecurity legislation and strategies provide a strong foundation. The cybersecurity industry's role extends beyond defence to resilience and offensive capabilities. Sharing knowledge, information, and intelligence among member states on space cyber capabilities is strategic and crucial. A multi-dimensional approach, encompassing technology, regulation, cooperation, and threat adaptation, is necessary for robust space cybersecurity.

The European institutions must foster a unified approach to security standards and self-reliance, emphasising a system of systems for its space systems. The existing EU's cybersecurity framework can be extended to space. This includes the NIS 2.0, Cybersecurity Act, and Cyber-resilience Act, all facilitating specific cybersecurity requirements for space missions. Collaboration between the European Union Agency for Cybersecurity (ENISA) and space agencies is vital for this integration. A harmonised supply chain approach and member-state agreements will strengthen space asset protection, aligning with the EU's comprehensive Space Strategy.

Considering what so far described, an example of the impact of strategic regulations implemented in the context of the EU's cybersecurity of space can be found in the coordinated Space Threat Response Architecture (STRA-22). This exercise, conducted in March 2022, aimed to test the EU's response capabilities to attacks on its space assets and critical services. During this exercise, the GSMC, an integral part of the Galileo infrastructure, demonstrated the resilience of the space system in a real-case scenario. It showcased the support the GSMC can provide to ensure Galileo services' continuity. Involving political, diplomatic, and technical actors, the exercise enhanced the EU's preparedness to address space threats. This practice contributes to developing an EU Space Strategy for Security and Defence, embodying the EU's commitment to bolster its coordinate response to space-related security threats (EEAS, 2022a).

Lastly, cooperation with external and like-minded partners like the United States, United Kingdom, and Japan, frontrunners in cyberspace best practices, will further bolster the existing framework. As space challenges cannot be addressed solely at a national level anymore, the shifting

power dynamics, the evolving threats landscape, and technological developments' speed demands a broad approach.

A Question of Strategic Legislation for the EU

Historically, space security has been considered a customised add-on, resulting in diverse security requirements and numerous proprietary solutions implemented by space agencies and industries, often voluntarily. The issue of space cybersecurity has expanded the concept of security from a government or military concern to one that affects all critical infrastructure, including individual users. From a network-centric viewpoint, Satellite systems now adopt standardised and certifiable approaches to physical and cybersecurity. Overall, there has been a shift from a safety-engineering perspective towards a cybersecurity-threat perspective regarding the cybersecurity of space systems. As space missions and services became more dependent on computed data, the concept of 'data security' has been added to the traditional concept of the safety of systems and components. This led to including cyber risk in mission planning for space objects (Baylon, 2014).

The European institutions made considerable strides in the field of space technology regulation, progressively expanded its competencies, established flagship programs, and laying the foundation for a robust and sustainable space sector. The EU has also prioritised space for security and defence, developing dual-use space systems and services. The acknowledgement of the increasing significance of the space industry in Europe has highlighted the need for a robust legislative framework for space security. This area of legislation is poised to become one of the most critical and strategically essential domains in the foreseeable future due to the potential risks associated with accidents and the consequences for space services. While European competencies still need to be fully centralised, implementing regulations and certification schemes and adopting best practices at the European level will confer strategic advantages to the space industry and the broader internal market. The harmonisation of rules and the adoption of shared practices will promote a cohesive and efficient space ecosystem within Europe, bolstering the competitiveness and resilience of the region's space industry and enhancing the overall functioning of the internal market.

However, the European regulatory framework for space cybersecurity cannot be easily identified as a unified entity based on a single regulation or directive. Instead, it requires a comprehensive understanding of multiple pieces of legislation to comprehend its overall structure. This fragmented nature does not necessarily imply a lack of power in the traditional sense, as defined above. Instead, the European Union has developed a unique form of power, a '*sui generis power'*, which incorporates regulations in a balanced manner, considering technological advancements and the diverse interests of the 27 EU member states. In this complex landscape, the external dimension of Europe's strategic legislation (i.e., how Europe effectively projects its power) is just as crucial as the laws and regulations themselves. The EU's internal market remains capable to attract investors, while technologies and know-how developed in the Union are of a high standard, as are the space systems.

It is essential to acknowledge that Europe's strategic legislation on space and cybersecurity must still be fully comprehensive. However, this does not imply a lack of commitment from institutions or member states to strengthen this sector. On the contrary, there are incentives to prioritise security as one of the foundational pillars of technological advancement. Efforts are made to enhance the regulatory landscape and promote security as a fundamental aspect of Europe's technological progress. This ongoing process reflects the dynamic nature of the European Union's strategic approach to space and cybersecurity as it seeks to adapt and evolve in a rapidly changing landscape.

Conclusions

The rise of technology has reshaped global power dynamics, crucially intertwining authority, and power with the strategic dominance of cutting-edge technologies. Particularly within the domain

of space, its systems and cybersecurity, the technological prowess of the EU critically outlines the realm of its global influence. This reflects a revision of Dahl's traditional concept of power, in which technical advantages such as superior technological capabilities, data resources, and advanced infrastructure shape an actor's ability to exercise power.

In this new paradigm, *strategic legislation* of EU has emerged as a critical tool for asserting power, ensuring national security, and maintaining competitiveness. It represents the pursuit of 'smart policies' that demand agile, forward-thinking, and impactful decision-making. It aligns with the current pace of technological advancements and foresees future challenges and opportunities.

Significantly, the legislation around space cybersecurity exemplifies this shift, serving as both a security measure and a testament to the EU's strategic command over the sphere of power and influence. The EU's strategic legislation in this sector underlines its commitment to shaping policies that promote security, privacy, innovation, fair competition, and resilience in the digital age.

Moreover, the EU's approach towards strategic regulation demonstrates its understanding of technology as a driving factor for policy development. This strategic stance has found momentum with creating an updated Space Programme and establishing the EUSPA, the deployment of the EU Secure Connectivity Program and IRIS², reflecting the EU's readiness to address future security and strategic issues. This practical application of strategic regulations culminating with the STRA-22 exercise underscores the multi-dimensional approach necessary for robust space cybersecurity, with technology, regulation, cooperation, and threat adaptation as the keystones.

In conclusion, technology and strategic legislation are vital to power constituents in the EU to ensure its assertiveness and readiness in the contemporary global landscape. Their intertwined roles in shaping international relations underline the necessity for continuous adaptation and innovation in both technological and legislative domains.

Bibliography:

Absek, F. (2014), An EU View: Comparisons and Establishing Norms in the Cyber and Space Domains, in Baylon, C., Challenges at the Intersection of Cyber Security and Space Security Country and International Institution Perspectives, Research Paper, Chatham House

Aguilar Sánchez, I., & Fischer, D. (2012). Authenticated encryption in civilian space missions: context and requirements [Conference presentation]. DIAC May 7, 2012. Stockholm, Sweden.

Baylon, C. (2014), Challenges at the Intersection of Cyber Security and Space Security', Int. Secure.

Cappelletti, F., Pogorel, G., Nestoras, A. (2022), Digital Strategic Autonomy, A Crucial Imperative for Europe, in ELF Techno-Politics Series 1, ISSN: 2791-3899 (https://doi.org/10.53121/ELFTPS1) pp. VII-XV

Castells, M. and Cardoso, G, eds. (2005), The Network Society: From Knowledge to Policy. Washington, DC: Johns Hopkins Center for Transatlantic Relations

Criekemans, D. (2022), 'Geotechnical Ensembles': How New Technologies Change Geopolitical Factors and Contexts in Economy, Energy and Security, In 'Geopolitics and International Relations'. Leiden, The Netherlands: Brill Nijhoff. doi: https://doi.org/10.1163/9789004432086

Dahl, R. A. (1957), The Concept of Power. Behavioral Science, 2(3), 201-215.

Defense Intelligence Agency – DIA (2022). Space Reliance in an Era of Competition and Expansion: Challenges to Security in Space (pp. 43-45). ISBN 978-0-16-095566-2.

Erwin, S. (2019), Air Force: SSA is no more; it's 'Space Domain Awareness'. Space News; https://spacenews.com/air-force-ssa-is-no-more-its-space-domain-awareness/

European Commission. (2007, April 26), EU needs a powerful space policy to face global challenges (IP/07/575). Retrieved from http://ec.europa.eu/enterprise/space/index_en.html

European Commission (2011), Communication From The Commission To The European Parliament, The Council, The Economic And Social Committee And The Committee Of The Regions: Single Market Act Twelve levers to boost growth and strengthen confidence "Working together to create new growth" (COM/2011/0206 final)

European Commission (2021), Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme

European Commission (2022), EU Space - Factsheets. EU Space Programme. European Commission General Publications (https://defence-industry-space.ec.europa.eu/eu-space-policy/eu-space-programme_en

European Commission (2023), High Representative of the Union for Foreign Affairs and Security Policy, (2023, March 10). European Union Space Strategy for Security and Defence. Joint Communication to the European Parliament and the Council. JOIN(2023)9.

European Council (2021), Council Decision (CFSP) 2021/698 of 30 April 2021 on the security of systems and services deployed, operated and used under the Union Space Programme which may affect the security of the Union, and repealing Decision 2014/496/CFSP (see page 178 of this Official Journal).

European Parliament (2021). Legislative powers. (https://www.europarl.europa.eu/about-parliament/en/powers-and-procedures/legislative-powers)

European Parliament and Council. (2021). Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU. PE/21/2021/INIT.

European Parliament and Council. (2023). Regulation (EU) 2023/588: Establishing the Union Secure Connectivity Programme for 2023-2027. Official Journal of the European Union.

European Space Agency – ESA (2020). Space Debris. https://www.esa.int/Safety_Security/Space_Debris

European Space Agency – ESA (2023). Space for 5G and 6G, esa.int. https://artes.esa.int/space-5g

European External Action Service - EEAS. (2021). Space and defence: protecting Europe and strengthening our capacity to act. HR/VP Blog https://www.eeas.europa.eu/eeas/space-and-defence-protecting-europe-and-strengthening-our-capacity-act_en

European Union External Action Service, EEAS (2022, March 22). A Strategic Compass for the EU. https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en

European Union External Action Service, EEAS (2022a). Space: EU carries out Space Threat Response Architecture Exercise 2022 (STRA-22). EEAS Press Team, https://www.eeas.europa.eu/eeas/space-eu-carries-out-space-threat-response-architecture-exercise-2022-stra-22_en

European Union Satellite Centre – EUSC (2023). Space Situational Awareness. Retrieved from https://www.satcen.europa.eu/page/ssa

European Union (2016), Consolidated version of the Treaty on the Functioning of the European Union, Part Three - Union Policies And Internal Actions Title Xix - Research And Technological Development And Space, Article 189

European Union (2021). How EU decisions are made. (https://european-union.europa.eu/institutions-law-budget/law/how-eu-policy-decided_en)

European Union. (2021a). Council Decision (CFSP) 2021/698 of 30 April 2021 on the security of systems and services deployed, operated and used under the Union Space Programme which may affect the security of the Union, and repealing Decision 2014/496/CFSP (PE/21/2021/INIT). Official Journal of the European Union, L 170/179-182.

Falco, G. (2018). The Vacuum of Space Cyber Security. AIAA 2018-5275. In Cyber Security and Information and Command and Control Systems (Session). doi: 10.2514/6.2018-5275. Retrieved from https://doi.org/10.2514/6.2018-5275

Housen-Couriel, D. (2016). Cybersecurity threats to satellite communications: Towards a typology of state actor responses. Acta Astronautica, 128, 409-415. https://doi.org/10.1016/j.actaastro.2016.07.041

HHS Cybersecurity Program (2021) North Korean Cyber Activity. US Department of Health and Human Services.

ITU. (2021, November 12). Managing radio frequency spectrum amid a new space race. ITU News. https://www.itu.int/hub/2021/11/managing-radio-frequency-spectrum-amid-a-new-space-race/

Lewis, J., A. (2022), Technology and the Shifting Balance of Power, Center for Strategic and International Studies, Commentary, Published April 19, 2022 (https://www.csis.org/analysis/technology-and-shifting-balance-power)

Lisi, M. (2022). The Security of Space Systems: A European Perspective. In L. Martino & N. Gamal (Eds.), European Cybersecurity in Context: A Policy-Oriented Comparative Analysis (pp. 1-10). Retrieved from https://doi.org/10.53121/ELFTPS3

McLuhan, M. (1962). The Gutenberg Galaxy: The Making of Typographic Man. Toronto: University of Toronto Press.

NATO (2022). NATO's overarching Space Policy. Last updated: 17 Jan. 2022. https://www.nato.int/cps/en/natohq/official_texts_190862.htm?utm_source=linkedin&utm_medium=nato&utm_campaign=20220117_space

Oakley, J. G. (2020) Cybersecurity for Space: Protecting the Final Frontier, Apress Berkeley, CA

Palmer, J. D. (1986). Advances in Information Technology and the Redistribution of Power. IFAC Proceedings Volumes, Volume 19, Issue 8, June, pp. 153-156. https://doi.org/10.1016/B978-0-08-034915-2.50033-0

Papakonstantinou, V. (2022). Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity? Computer Law & Security Review, 44, 105653. https://doi.org/10.1016/j.clsr.2022.105653

Pavur, J., & Martinovic, I. (2019). The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space. *2019 11th International Conference on Cyber Conflict (CyCon)*, 1–18. https://doi.org/10.23919/CYCON.2019.8756904

Pavur, J., & Martinovic, I. (2020). SOK: Building a Launchpad for Impactful Satellite Cyber-Security Research. ArXiv, https://arxiv.org/pdf/2010.10872.pdf

Permanent Structured Cooperation (PESCO), Projects in Space. https://www.pesco.europa.eu

Reillon, V. (2017), European Space Policy, European Parliamentary Research Service, January 2017 — PE 595.917 (doi:10.2861/903178)

https://www.unoosa.org/res/oosadoc/data/documents/2017/stspace/stspace61rev_2_0_html/V1605998-ENGLISH.pdf

Scholl, M., Soloway, T. (2022). Introduction to Cybersecurity for Commercial Satellite Operations. National Institute of Standards and Technology. (Draft (2nd) NISTIR 8270). Department of Commerce, United States of America. https://doi.org/10.6028/NIST.IR.8270-draft2

Thangavel, K., Plotnek, J. J., Gardi, A., & Sabatini, R. (2022). Understanding and investigating adversary threats and countermeasures in the context of space cybersecurity. In 2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC) (pp. 1-10). Portsmouth, VA, USA. doi: https://doi.org/10.1109/DASC55683.2022.9925759

APPENDIX

Table 6 - Classification of Space Organisations and Their Security Practices

Class	Organisation Type	Description
1.Commercial Operators	Companies offering B2B and B2C services (e.g., Eutelsat, SES Astra, Inmarsat)	Procure satellites from European and non-European manufacturers; security requirements partially apply without adherence to standards or official certification processes.
2.National Space Agencies	Examples: CNES (France), DLR (Germany), ASI (Italy)	Promote and fund satellite programs primarily for military, governmental, or dual-use applications (telecommunications, EO, spectrum monitoring, intelligence); apply security standards and certification or accreditation processes in collaboration with national security agencies.
3.European Space Agency (ESA)	Intergovernmental organisation with 22 Member States	Aims to promote space research, technology, and applications for peaceful purposes; manage specific satellite missions conducted by European space industries; support satellite operations through ground control infrastructure; guarantee European access to space; cooperate with national and international agencies and organisations.
4.European Union Agency for the Space Programme (EUSPA)	Responsible for EU common space infrastructure development and operation	Promotes commercial downstream applications through Horizon program funding; oversees security certification and accreditation of space assets in cooperation with ESA and national security agencies of EU Member States.

Table 7 - Major Space Companies in the EU + UK

Country	Major Space Companies
Austria	RUAG Austria
Belgium	QinetiQ Space, Thales Alenia Space Belgium
Czech Republic	Czech Space Research Centre (CSRC), Iguassu Software Systems
Denmark	GomSpace, Terma
Estonia	Spaceit, Kappazeta
Finland	Reaktor Space, Iceye
France	Airbus Defence and Space, Thales Alenia Space, ArianeGroup
Germany	OHB System, Airbus Defence and Space, Rocket Factory Augsburg (RFA), IABG
Greece	Antwerp Space, Space Hellas
Hungary	Celestial Corp, C3S Elektronikai
Ireland	Skytek, Arralis
Italy	Leonardo, Avio, D-Orbit
Latvia	Ventspils High Technology Park
Lithuania	NanoAvionics, Baltic Satellites
Luxembourg	SES, Luxembourg Space Agency
Netherlands	Airbus Defence and Space Netherlands, ISISpace
Poland	Creotech Instruments, SatRevolution
Portugal	Deimos Engenharia, Critical Software
Romania	RARTEL, Romspace, National Institute for Aerospace Research "Elie Carafoli"
Slovakia	Aerospacelab, VZLU
Slovenia	SkyLabs, Cubesat Systems
Spain	Indra, Hispasat, Elecnor Deimos
Sweden	Saab, GKN Aerospace, SSC
United Kingdom	Surrey Satellite Technology Ltd (SSTL), Inmarsat

Table 8 - Security Projects Related to Space Systems in the EU (Source: Pesco: EU Commission).

Project Name	Description
GEODE	GEODE is an innovative project focusing on developing Galileo PRS-enabled PNT navigation solutions for the defence sector. It includes the creation of PRS Security Modules, PRS receivers, and Controlled Radiation Pattern Antennas. The project establishes a dedicated European PNT test and qualification facility to assess the performance and security of the developed systems. A PRS infrastructure ensures the availability of security assets for operational testing. Military field testing will be conducted on naval, land, RPAS, and timing/synchronisation platforms across multiple Member States. GEODE aims to enhance EU defence capabilities by providing secure and reliable navigation systems tailored for defence-specific applications, utilising the advanced features of Galileo PRS.
EU Radio Navigation Solution (EURAS)	The EU Radio Navigation Solution (EURAS) project aims to foster the development of military Positioning, Navigation, and Timing (PNT) capabilities within the European Union, utilising the Galileo satellite navigation system and its Public Regulated Service (PRS). EURAS promotes cooperation and collaboration among EU member states to enhance their military PNT capabilities. By leveraging the advanced features and security of the Galileo PRS, EURAS aims to support the future development of robust and reliable navigation solutions for military applications. The project aims to strengthen the EU's military capabilities and foster cooperation among member states in the field of PNT, utilising the benefits offered by Galileo and its PRS.
Common Hub for Governmental Imagery (COHGI)	The Common Hub for Governmental Imagery (COHGI) project aims to establish a centralised platform to exchange classified governmental imagery at the European level. GE coordinates the project and involves the participation of several member states, including AT, FR, LT, LU, NL, RO, and ES. The objective is to enhance the capabilities of the European Union Satellite Centre (EUSatCen) in fulfilling its core mission by leveraging the common hub. This platform enables the seamless sharing of classified imagery between member states and EU entities, promoting collaboration and information exchange in governmental imagery. By utilising the EUSatCen and taking full advantage of its resources, COHGI aims to enhance the efficiency and effectiveness of classified imagery sharing within the European Union.
European Military Space Surveillance Awareness Network	The European Military Space Surveillance Awareness Network (EU-SSA-N) project, coordinated by IT and involving members from FR, GE, IT, and NL, aims to develop an autonomous and sovereign military space surveillance and awareness (SSA) capability for the European Union. The project focuses on creating an interoperable, integrated, and harmonised SSA capability that aligns with the EU-SST Framework initiative. The objective is to enhance the protection of European member states' space assets and services by effectively monitoring and detecting natural and artificial threats. By establishing a robust SSA network, the EU-SSA-N project enables appropriate responses to safeguard the integrity and security of European space assets in the face of emerging challenges.
Defence of Space Assets (DOSA)	The Defence of Space Assets (DOSA) project, coordinated by FR and involving members from AT, FR, GE, IT, PL, PT, RO, and ES, aims to enhance the operational efficiency of the European Union in the space domain. The project optimises current and future space asset utilisation by incorporating cross-cutting space functions. These functions include reactive access to space, in-space manoeuvrability, space resilience, and training for military space operations. By developing advanced capabilities in these areas, DOSA seeks to strengthen the EU's ability to protect and defend its space assets while ensuring effective and coordinated military operations.

GLOSSARY

Term	Definition
infrastructure	The infrastructure of a space platform typically consists of the basic physical structures, mechanisms, and subsystems for propulsion, power, thermal control, attitude determination and control, and TT&C communications and processing
crosslinks	Communication between satellites
current profile	The 'as is state of system cybersecurity
downlink	Communication originating from the satellite to the ground
GNSS	Global Navigation Satellite System is a system of satellites that provides positioning, navigation, and timing services worldwide, including systems developed by different entities, such as GPS (Global Positioning System) in the US, GLONASS in Russia, Galileo in Europe, and BeiDou in China.
jamming	The intentional interference or disruption of wireless communication signals by emitting a strong signal on the same frequency causes interference and prevents the reception of legitimate signals.
payload	Mission-specific items of the overall satellite that are not part of the overall operations or "flying" of the satellite
profile	A representation of the outcomes that a particular system or organisation has selected from the Framework Categories and Subcategories
risk	The level of impact on organisational operations (including mission, functions, image, or reputation), organisational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring
satellite	Any human-made assets in space
space structures	The desired outcome or "to be" state of cybersecurity implementation
SSA	Space Situational Awareness is the knowledge and understanding of the space environment, including the location, trajectory, and behaviour of objects in space, to identify potential collisions, threats, or hazards for safe and efficient space operations.
SSS	Space Surveillance System is a network of ground-based radars, telescopes, and sensors used to track and monitor objects in space, detecting and tracking satellites, debris, and other space objects for Space Situational Awareness activities.
spoofing	The technique of deceiving or tricking a system or user by falsifying information or impersonating another entity often involves the creation of fake or deceptive signals, data, or communications.
target profile	The science of measuring a quantity or quantities, transmitting the results to a distant station, and interpreting, indicating, and/or recording the quantities measured
telemetry	During prelaunch, this cable connects the space vehicle to the launch pad to monitor the vehicle health and is disconnected or cut when the vehicle launches; enables the exchange of data with ground launch mission systems
uplink	Communication originating from the ground to the satellite
vehicle	Space operational items that include the launching items used to place the satellite, bus, and/or payload into orbit
vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source

List of abbreviations:

AES	**Advanced Encryption Standard**
CIA	Confidentiality, Integrity, Availability
DMA	Digital Markets Act
DSA	Digital Services Act
ESPA	European Union Agency for the Space Programme
EU	European Union
GSMC	Galileo Security Monitoring Centre
GNSS	Global Navigation Satellite System
IDPS	Intrusion Detection and Prevention Systems
ISO	International Organization for Standardization
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
SST	Space Surveillance and Tracking
STRA-22	Space Threat Response Architecture 2022