JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2025, tyaf013
https://doi.org/10.1093/cybsec/tyaf013

Research Paper

Space cybersecurity governance: assessing policies and frameworks in view of the future European space legislation

Francesco Casaril[*] **and Letterio Galletta**[‡]

IMT School for Advanced Studies Lucca, 55100, Lucca, Italy

[*]Corresponding author: SysMA, IMT Lucca, 55100, Lucca, Italy, E-mail: francesco.casaril@imtlucca.it
[‡]Assistant Professor of Computer Science within the SySMA research unit of IMT Luca.

Received 4 July 2024; revised 2 May 2025; accepted 14 May 2025

Abstract

The space industry has grown significantly in recent years and has become essential to our daily lives. Space applications are now critical for powering necessary infrastructure, such as energy grids and financial networks. However, as the use and value of space continue to rise, it has also become a primary target for cyber threats, posing a significant risk to the networks and their connections with critical infrastructure. As a result, policymakers in Europe and other regions are developing policies, standards, and guidelines to improve space cybersecurity and protect this crucial sector. This paper aims to analyze the responsible entities for space cybersecurity governance in the UK, the USA, Germany, and the European Union and compare existing policies and guidelines against current threats. The goal is to determine the steps necessary to make the industry more robust. Our study focuses on European legislation, with a future Space Law on the horizon. The first policies to be part of our comparative analysis are the "Technical Guideline BSI TR-03184 Information Security for Space System" established in Germany, the UK Space Agency's "Cyber Security Toolkit," and NASA's Space "Security: Best Practices Guide". Our findings highlight how governance frameworks for space security have not yet been clearly defined and we foresee a significant increase in the fragmentation of policies. We emphasize the importance of defining resilience clearly and providing tools and metrics to help industries measure their security and evaluate risk levels, to comply with upcoming policies. To achieve this goal, we suggest mapping cybersecurity requirements to practical security controls and safeguards that companies can easily understand and implement.

Keywords: space law; cybersecurity; space governance; security controls

Introduction

The security of space assets has recently become a concern for policymakers and institutions, who realized how the current level of protection of commercial satellite systems is insufficient to face the various threats that have been multiplying and increasingly targeting the multiple parts of satellite infrastructure, such as space, ground, and user segments. From 1977 to 2023, 337 cyber attacks have been reported publicly in the sector, with more than 100 in the last 2 years [1]. In response, the governments have begun developing frameworks to help and guide the industry in securing their systems, as has previously been done for other critical infrastructure sectors, such as in the field of nuclear power in the UK [2] or energy in the USA [3].

This paper aims to clarify the concept of cybersecurity governance in space and to take a snapshot of the current state of the affair in certain countries and jurisdictions, such as the UK, the USA, Germany, and the European Union. A governance framework defines roles, responsibilities, processes, and relationships among stakeholders from the private sector, public administration, and civil society [4]. It spans different topics, including economic, social, and political priorities. A clear governance framework is essential as poor governance can contribute to the emergence of cybersecurity risks in space systems, making it crucial to incorporate cybersecurity considerations into the administrative and policy frameworks that govern space operations. After analyzing the structure and functioning of cybersecurity governance, we evaluate the policies, frameworks, and guidelines that are being put in place in these regions; then, we compare them and identify any gaps. Finally, we propose some policy recommendations to address the identified shortcomings. More precisely, this paper addresses the following research questions:

RQ1. How are cybersecurity and space governance structured and organized?
RQ2. What is the relationship between cybersecurity and space governance?
RQ3. What are the policies and frameworks that countries are enacting to regulate cybersecurity in the field of space?
RQ4. Are these policies sufficient to face the current threat landscape?
RQ5. What are the gaps in these policies and how can they be addressed?

To answer RQ1 and RQ2, Section 2 focuses on cybersecurity governance in space in the selected countries. In particular, we discuss how the USA, the UK, Germany, and the European Union deal with cybersecurity and who is responsible for the security of space systems. We identify the entities involved, the strategy they developed, and the level of cybersecurity they defined for the space sector. Section 3 answers to RQ3: it analyzes how the selected countries are implementing guidelines, frameworks, and policies to secure the space ecosystem. Specifically, we analyze the proposed Satellite Cybersecurity Act and NASA's Best Practices Guide (BPG) for the USA, the Space Cybersecurity toolkit developed by the UK Space Agency, and the guidance document on cybersecurity strategies for applicants and licensees developed by the UK Civil Aviation Authority (CAA), the capabilities of the European Space Agency (ESA), and the possible future cybersecurity requirements that may be included in the European Space Law (EUSL) for the European Union. To address RQ4, we conduct a thorough evaluation of these tools and identify their limitations in addressing the actual threat landscape. In Section 4, we identify gaps in the existing instruments and provide recommendations for policymakers developing the EUSL. Finally, in Section 5 we translate some of the possible cybersecurity recommendations into actionable guidance using Center for Internet Security (CIS) Security Controls.

2 Toward stronger cybersecurity governance for space

Defining how space and cyberspace interact and how they are governed is essential for researchers and stakeholders to identify space-related cyber vulnerabilities and assess the required level of preparedness. It also helps to prepare appropriate responses in case of any disruption of space operations. The increasing dependence of space on cyberspace has made such disruptions more likely, as space capabilities now cannot exist without cyberspace. Operators use specialized computers and programs to transmit data to and from spacecraft over a computer network. The concept of software-defined satellites [5] and ground stations as a service [6] recently emerged, highlighting this trend. The dual-use nature of space and cyberspace makes defining clear governance frameworks for these fields challenging, as the links between nonmilitary and military cyberspace applications and the use of commercial space assets for military operations blur the boundaries between civilian and military usage. The creation of dual-use constellations, such as IRIS[2], confirms the willingness of institutions to increase the use of dual-use space technologies. A comprehensive architecture for space and cyberspace governance should cover both commercial and military activities and consider their strategic and dual-use nature. This section analyzes and reports on the governance frameworks of the selected countries, attempting to distinguish the complex roles, responsibilities, and duties of the various agencies in the field.

2.1 Space cybersecurity governance in the UK

Cybersecurity roles and responsibilities in the UK are divided across several government departments and agencies. The UK National Cyber Strategy, part of the Integrated Review, defines the country's cybersecurity goals. Several government departments play crucial roles in shaping cybersecurity policy and its implementation. The Cabinet Office is responsible for the formulation of cybersecurity policy and publishes the National Cyber Strategy, the first version was published in 2016 and then updated in 2022 [7]. The Department for Science, Innovation and Technology oversees the implementation of the Network and Information Systems (NIS) Regulations and domestic cybersecurity policy. The Home Office focuses on cybercrime policy, while the Ministry of Defence leads efforts to detect, disrupt, and deter adversaries in cyberspace, including oversight of the National Cyber Force. The Foreign, Commonwealth and Development Office manages international cybersecurity activities, administers the conflict, stability and security fund, and oversees the National Cybersecurity Centre (NCSC) and the National Cyber Force in collaboration with the Ministry of Defence (MoD). In case of a cyber incident, public agencies such as the NCSC [8], designated under the NIS Regulation, serve as the primary point of contact, technical authority, and Computer Security Incident Response Team. Each relevant industry sector has a different competent authority, which works with the NCSC to enforce cybersecurity requirements and produce sector-specific guidance, together with the UK Cybersecurity Council, which develops professional standards and accredits cybersecurity qualifications. On the enforcement side, the National Cyber Force conducts covert operations to counter cyber threats, while the National Crime Agency focuses on combatting cybercrime.

In the UK, critical national infrastructure operators and Relevant Digital Service Providers designated under the NIS Regulation have specific cybersecurity responsibilities; other businesses and organizations not covered by the NIS Regulation may have legal obligations derived from data protection and corporate governance rules.

Space is considered one of the 13 critical infrastructure sectors, and the UK Space Agency is responsible for ensuring its resilience [9]. In 2018, the UK Cabinet Office set out some of the key priorities for space cybersecurity, including identifying the main dependencies on space services and assets in other critical national infrastructures, identifying critical assets and services in space, and mitigating risks to increase resilience in the sector [10]. The UK Government places particular emphasis on the protection of critical infrastructure and, in the space sector, prioritizes the identification and mitigation of risks that could threaten critical assets and services. The National Protective Security Authority was created to protect the nation's critical assets, with a mission to build resilience to national security threats [11].

This highlights how the UK considered the importance of space and its dependencies in the Nation's risk strategy. In this setting, the UK Space Agency, in collaboration with space infrastructure owners and operators, is required to develop strategies to ensure the resilience of space. Companies seeking funding from the United Kingdom Space Agency (UKSA) are required to participate in mandatory engagement activities and cybersecurity planning to enhance mitigation measures and the overall resilience of space systems. Moreover, the UK Space Agency is participating in international groups working on designing cybersecurity technical standards for space systems [11].

Despite these measures, in a recent hearing the Parliament has highlighted that, although mandatory cybersecurity standards are being considered, they must be carefully balanced with the growth agenda of the commercial space industry and the need to avoid stifling innovation [11]; highlighting the possible drawbacks of overregulating the industry.

Focusing on the space sector's governance, the responsibility for space strategy, policy, and implementation is distributed across various government departments within Whitehall. While the Department for Business, Energy, and Industrial Strategy coordinates civil space policy, the National Space Strategy assigns responsibilities to 10 key government departments and agencies [12]. This fragmentation may harm the coherence and effectiveness of space policy governance, as a truly unified, agile, and decisive approach remains difficult to implement. The fragmentation between MoD and non-MoD agendas risks deviating and slowing from the UK's strategic space objectives. Recent actions are not promising regarding the coordination of the various departments, including the removal of the National Space Council from the list of Cabinet Committees and the potential restructuring of the MoD's Space Directorate. To address these challenges, the industry advocates for central leadership in the form of a Minister for Space, as exists in Japan, ideally situated within the Cabinet Office. This figure would coordinate space activities across the government and signal a strong commitment to the space industry, academia, scientific community, and international partners [12].

Despite fragmented governance, the UK has a high awareness of the cyber risks connected with the space sector. The 2023 National Risk Register [13], which is the government's assessment of the most serious risks facing the UK includes 89 risks, of which 3 are linked to space. The risks include the disruption of space-based service (moderate impact), loss of Positioning, Navigation, and Timing services (significant impact), and deliberate disruption of UK space systems and space-based services (moderate impact). The document highlights how the three risks can be caused by cyber-attacks, and mentions the need to define response capability requirements and recovery considerations in the event of an attack. Response needs would vary based on the attack's method and impact on space-based infrastructure, ground facilities, and critical radio frequency links. While measures like cybersecurity protocols, counter-jamming technology, and interference detection can mitigate electronic attacks; space domain awareness aids in attributing attacks and assessing their impact. Strengthening secure and resilient space-based services reduces the potential impact on critical defense and security functions, and exploring alternative infrastructure and service solutions, such as terrestrial-based systems, is also crucial. The document defines a recovery timeline that may depend on the attack's nature and its impact, with temporary disruptions possibly lasting minutes and permanent damage potentially taking years to recover. In the context of space security, Regulation 185 within the Space Industry Regulations 2021 [14] is an important piece of legislation that focuses on cybersecurity measures for individuals and organizations involved in spaceflight operations in the UK. This regulation applies to all licensees under the Space Industry Act and aims to ensure the security and resilience of their NIS. To be allowed to engage in spaceflight operations, companies need to comply with this regulation by developing and maintaining a cybersecurity strategy that aligns with international obligations and includes security risk assessments. This strategy must be regularly updated and reviewed. To help applicants and licensees meet these requirements, the UK CAA has developed guidance on cybersecurity, which is included in our analysis in Section 2.6.

In conclusion, even if recognized the cyber threats to space assets and started to develop space capabilities against them [15], the UK Government at the moment of writing has not yet developed and published a document defining its policy goals and strategies addressing space cybersecurity and has not yet defined clear governance frameworks for it. For this reason, this paper focuses on the only documents that define cybersecurity guidelines for the space sector in the UK. In particular, we analyze the UK Space Agency cybersecurity Toolkit (May 2020) and the Guidance on cybersecurity Strategies for applicants and licensees (UK Civil Aviation Authority, April 2023). These two documents are at the moment the only source of space cybersecurity guides and practices for the space sector in the UK.

2.2 Space cybersecurity governance in the USA

With the highest number of cyberattacks targeting its systems, the USA developed its resilience and response capabilities in every domain. Recognizing early the growing importance of safeguarding space assets, the USA established in 2019 the only independent space force existing to date, to ensure the protection of critical infrastructure beyond Earth's atmosphere [16].

The main entity responsible for cybersecurity in the USA is the Cybersecurity and Infrastructure Security Agency (CISA). CISA collaborates with various government agencies to safeguard the nation's cyber and physical critical infrastructures, supporting them in managing their cyber risk with a mission to establish a uniform level of security across the Federal Civilian Executive Branch, a part of the executive branch of the US Government that is responsible for managing and executing the policies and programs of the federal government [17]. With a budget of 3 billion for 2024 [18], CISA has at its disposal a wide range of tools to prevent, protect against, and mitigate security incidents. Within CISA, the Space Systems Critical Infrastructure working group was designed in 2021 to identify and develop strategies to minimize risks to space systems. The group is composed of institutional and private entities, but their identity and proceedings have not been disclosed. However, apart from these initiatives, no additional policy beyond Space Policy Directive-5, which will be discussed below, has been developed concerning this crucial aspect of space security.

Under the Trump presidency, the USA has prioritized the protection of its space assets by establishing the US Space Force (USSF). While cyber capabilities are integral to USSF's mission operations, the focal point of its cyber capabilities is Space Delta 6, also known as Cyber Delta, a key component of the USSF [19]. Established on 24 July 2020, Cyber Delta has dual mission objectives: ensuring continuous space access and availability through the Satellite Control Network, and safeguarding the integrity and security of all space-based mission systems and assets. Notably, Cyber Delta primarily interacts with the defense sector and does not typically engage with commercial space entities unless they are acting as defense contractors.

Despite American space assets having already been targeted by cybercriminals [20], the USA has made limited progress in integrating mandatory cybersecurity measures into policy to safeguard them. One initiative in this regard is the Space Policy Directive-5 [21], also known as Cybersecurity Principles for Space Systems. The act is a presidential memorandum, a form of order issued by the President of the USA to oversee and regulate the actions, practices, and policies of the different departments and agencies that fall under the executive branch of the US Government [22]. It carries the weight of the law and is used in this case to instruct specific government departments and the private sector to implement a series of principles. The memorandum, recognizes the importance of addressing cybersecurity concerns in space systems, offering guidelines for those involved in developing space infrastructure. The cybersecurity principles are designed to guide and serve as the foundation for the US Government's approach to the cyber protection of space systems. It can be considered as a primary attempt to define a cybersecurity strategy for space in the country and propose a programmatic roadmap for the implementation of future legislative instruments. These principles include:

a. Cybersecurity by design considerations and using risk-based engineering;
b. Implementation of cybersecurity plans that include protection against unauthorized access, physical protection, jamming, spoofing, and supply chain risks;
c. Collaboration among space system owners and operators for promoting best practices and sharing threat information within the industry;
d. Specific mission requirements, space vehicle characteristics, and orbital regimes.

SPD-5, however, does not mandate any specific space cybersecurity implementations for the sector and does not specify a governance framework for space systems cybersecurity. At the moment, the only agency that may be competent in this setting is CISA. However, the fact that space has not been defined as a critical domain makes the attribution of its resilience to CISA contradictory. The fact that space is not considered a critical infrastructure does not make it exempt from the guidelines issued by CISA, but it leaves it in a gray area compared to sectors such as energy or nuclear ones.

In July 2023, a Bill was introduced to designate space as the seventeenth critical infrastructure sector [23]. The proposal encountered significant opposition and, at the moment, it has not yet passed as there is no agreement either within institutions or in the private sector on the matter. Those against the Bill argue that the main critical infrastructure functions performed in space are already part of the 16 critical infrastructure sectors, such as communications, transportation, information technology, and government facilities; moreover, they claim that such designation would dilute policy prioritization and resources and harm industry's growth. The main question in this debate refers to identifying the responsible entity for the security of space [24]. Designating space as a critical infrastructure would entail the allocation of one Sector Risk Management Agency (SRMA). SRMAs lead government coordination and work with private-sector partners to strengthen security and resilience. Sometimes, SRMA also has regulatory duties. It also is responsible for day-to-day incident management and technical support to identify vulnerabilities in their respective sectors. However, identifying which federal agency should lead space is complex. Among the qualified entities are the Federal Aviation Administration, NASA, the Department of Defense, and the Department of Homeland Security. However, each of them has already several sectors to take care of and the allocation of space may create duplication, redundancies, and gaps in responsibilities. In 2021, CISA expressed the necessity to identify space as a critical infrastructure, suggesting that the sector is subject to risk not fully addressed through existing mechanisms, policies, or governance structure [25]. However, decisions have not yet been made for the implementation of these recommendations.

In conclusion, the USA recognizes that cybersecurity is an all-encompassing and transversal goal that applies to all domains, including space. It distinguishes between space and nonspace cybersecurity, even if there is no agency defined for its resilience yet. This particularly harms the governance of security in the sector, which is currently not well defined. The use of less secure New Space services is considered risky. However, in the civil domain, their use is not considered critical, meaning that it would not be crucial during times of crisis. Policymakers are aware of the unclear governance framework in the space domain, and they have proposed important steps to address this gap. In particular, we analyze the proposed Satellite Cybersecurity Act in Section 2.7, alongside NASA's Space Security: BPG. The Act is an essential step toward recognizing and implementing space cybersecurity, requiring the dissemination of information, and other activities to address cybersecurity risks to commercial satellite systems. On the other hand, the BPG aims to design the first actionable and usable guidelines for the private sector concerning space cybersecurity.

2.4 The German approach to cybersecurity in space

Although the scale of the attacks that affected Germany is not comparable to the ones faced by the USA, the German space industry has also been widely affected by cyber threats. In 2014, a carefully planned attack, suspected to be state-sponsored, targeted the German Aerospace Center (DLR) [26]. The systematic attack used some trojans designed to self-destruct on discovery: the malware laid dormant for several months before being activated, indicating a well-planned and stealthy attack. The available information suggests that the attackers aimed to steal confidential information and disrupt the operations of the DLR. The federal government categorized the attack as extremely serious as the center gathered and stored information on armament and rocket technologies.

The space sector in Germany is quite advanced, and many big industrial players are in the country's aerospace clusters, such as those of Bremen, BavAIRia, and e LR BW (Luft- und Raumfahrt Baden-Wurttemberg) [27]. In 2022, Germany was the largest contributor to the ESA budget with 20.8%, and in 2023, was in the top three European countries for governance space spending, with 2.286 billion euros [28]. The data clearly shows the importance of Germany in the European space sector and partially explains why Germany is one of the most advanced countries in Europe also in terms of developing cybersecurity guidelines for space.

Cybersecurity is not regulated as a unitary topic in Germany, but the policy framework is a combination of federal and European laws and regulations. The most recent law on cybersecurity is the IT Security Act 2.0 [29], which came into effect at the end of May 2023. The Act imposes several requirements, among which are establishing minimum security standards for critical infrastructures, adhering to security requirements for critical components, and complying with information obligations and reporting requirements to the Federal Office for Information Security (BSI). The Act draws upon the BSI Act of 2016 [30], which defines the German critical infrastructure sectors; even if space is not explicitly mentioned in the list, it can be considered part of telecommunication, and it shall, therefore, be in the scope of all the policies mentioned in this section.

In terms of governance, the BSI plays a key role in implementing and overseeing the IT Security Act 2.0. Acting as an ISAC, BSI is responsible for gathering and evaluating information to prevent threats, such as identifying security gaps, malware, and successful or attempted attacks, as well as methods used. It also must inform federal authorities of relevant information and facts related to IT security. Section 4 of the Act establishes the BSI Federal Office as a central hub for information sharing and coordination among federal authorities, ensuring a proactive approach to information technology security and facilitating effective response measures. The office collects information from third parties about security risks and can use it to inform the public, federal authorities, operators of critical infrastructures, and companies in the public interest.

The other main pillar of Germany's cybersecurity policy is the BSI Kritis Regulation [31]. This law has recently been updated, giving BSI more power to ensure the safety of businesses, organizations, and entities involved in critical infrastructure. Now, BSI has the authority to mandate all such entities to: conduct security audits once every 2 years, report all cybersecurity incidents and disruptions to the relevant authorities, designate a contact point for the BSI for constant availability, enforce operators of critical infrastructure to implement intrusion detection systems against cyber attacks, implement the minimum requirements of appropriate state-of-the-art organizational and technical measures for combating IT system and information system incidents.

Cybersecurity governance is, therefore, well established and regulated in the country, with the majority of the roles and responsibilities addressed to BSI. While, as much as concerns space governance, the main source to be considered is the German Space Strategy [32] released in September of 2023. On this occasion, the Federal Minister for Economic Affairs and Climate Action emphasized how space-based infrastructures are becoming increasingly critical for the security of the country. The strategy highlights the growing cyber threats to space-based systems, including their ground-based segments and data links. As a result, the document calls for an international inventory of vulnerabilities of space-based systems and continuous improvements in national and international standards and requirements for space programs

These considerations were behind the collaboration between BSI, the private sector, and the DLR, which led to the development of key objectives for cybersecurity in space infrastructures. This public–private partnership aims to establish a central coordinating body for cybersecurity in civil and military aerospace applications and systems. This unique unit focuses on information security for space infrastructures and is the first of its kind in Europe. The primary tasks of the unit include identifying minimum cybersecurity requirements in space, developing criteria and recommendations, and promoting awareness in the sector through publications and events. However, the implementation of the unit appears to be in its early stages.

One of the first outcomes of this public–private collaboration is the IT-Grundschutz Profile for Space Infrastructures, which is a guide for companies to assess and categorize the level of risks they are exposed to and to understand how to address them. In collaboration with the sector, BSI has also developed the first Technical Guidelines (BSI TR-03184) [33] on Information Security for Space Systems and the IT-Grundschutz profile for the ground segment. These documents are analyzed in detail in Section 2.8.

According to our analysis, Germany can be considered one of the most advanced European countries in terms of cybersecurity governance and policies for space. The country has clearly defined roles for its agency, the BSI, and has established guidelines for the sector and its specific segments. However, this does not necessarily mean that the space industry in the country is fully equipped to handle and mitigate actual threats. Recent studies have suggested that Germany is not adequately prepared for the increasing number of cyberattacks and lags behind other European countries in terms of cybersecurity [34]. This may be attributed to underfunding or overregulation, which can make it too expensive and complicated for companies to comply. Our analysis highlights the importance of not only having adequate policies but also the need to create the right tools for the industry to implement them effectively. The details and gaps of these policies are discussed in Section 2.8.

Table 1. Space cybersecurity governance overview.

Country	USA	UK	Germany
Address cyber threats to space in the National Cyber or Space Strategy	✓	✓	✓
Considers Space as a critical infrastructure sector	X	✓	✓
Developed a Space cybersecurity strategy/guidelines/principles	✓	✓	✓
Defined an agency for the protection of space infrastructure	X	✓	✓
Has a space ISAC	✓	X	X

2.5 An analysis of cybersecurity governance for space

The countries under analysis depend on essential space-based infrastructure for their security and economy. However, not all of them, (e.g. the UK and Germany) have a space ISAC. Furthermore, some of these countries (e.g. the USA) have either identified or created an agency with clear roles and responsibilities to protect space. A summary of the landscape of space cybersecurity governance in the countries analyzed in the first part of the paper is in Table 1.

Based on our analysis, the USA can be considered one of the most advanced countries in the field, mainly due to its military capabilities in space and the high capacity of its private sector to adapt to threats and collaborate with institutions. An example of this is the Space ISAC, a remarkable initiative that at the moment has no comparison in Europe. The center provides companies with an incredible platform for sharing intelligence, which can be leveraged to perform cyber threat intelligence reports and automated risk analysis and assessment, based on the risk profiles of companies. The ISAC comprises 64 companies, including the biggest players in the sector. However, the USA leaves space outside the critical infrastructure circle, which falls short of addressing all the vulnerabilities that affect the sector. Nevertheless, US legislators have introduced the Satellite Cybersecurity Bill [35], (analyzed in the next section) but still have failed to identify the agency that will take care of its resilience.

In contrast to the USA, the UK has recognized space as a critical infrastructure for many years. However, the UK Space Agency has not yet defined its responsibilities or created mandatory guidelines, but just a toolkit (see Section 2.6), leaving companies without clear rules to follow. While the aviation authority has developed some useful guidelines (see Section 2.6), they may not cover the entire value chain of the space sector.

In the case of Germany, the country is adapting to the risks and attempting to mitigate them with nonmandatory guidelines for the industry developed with companies, anticipating the work that the Commission is expected to do with the EUSL. In the next sections, we analyze the main frameworks, policies, and guidelines for the sector developed by these countries and, in conclusion, address any gaps they may have in terms of cybersecurity, especially when compared to current threats, and how they can be addressed in the upcoming space law.

2.6 Understanding UK space cybersecurity: insights from UK space agency and CAA

In May 2020, the UK Space Agency released a 20-page document titled the "Cybersecurity Toolkit" [36]. This document is the first of its kind in the UK and is designed to provide guidelines for the space sector. Its intended audience consists of entities involved in the supply, development, ownership, and operation of assets within the industry. These assets include facilities, systems, networks, processes, and the personnel responsible for their operation and facilitation, thus addressing almost the entire value chain. The document outlines the process that asset owners must undertake to identify their dependencies and vulnerabilities. Its goal is to assist entities in adopting appropriate cybersecurity strategies tailored to the needs of the sector. The toolkit is divided into five sections, each dedicated to guiding space asset owners and suppliers through the critical steps to secure their operations against cyber threats.

The toolkit is divided into five sections. The first section helps in recognizing potential weaknesses through detailed vulnerability mapping, providing a questionnaire to assist in identifying the level of risk and evaluating the potential impacts of the loss, whether temporary or permanent, of supplies or assets The second section provides an impact assessment framework to estimate the consequences of asset loss. Based on these assessments, appropriate mitigation measures are proposed in the third section. The fourth section defines the legal and voluntary obligations surrounding incident reporting. The final section urges the necessity of integrating cyberattack scenarios into Business Continuity Plans (BCPs), suggesting minimum requirements for BCPs, aimed at minimizing disruptions, preparing for, and documenting alternative options for maintaining operational continuity of supply chains and assets.

This toolkit is designed to assist companies in safeguarding their assets and establishing operational frameworks that can withstand and recover from cyber attacks. This toolkit, however, does not provide specific measures for physical or personnel security, nor does it prescribe technical solutions for risk mitigation. For further guidance on these aspects, the UK Space Agency recommends seeking advice from the NCSC and the CPNI. Reporting obligations that exist when cyber incidents occur are subject to thresholds. These are defined by the Information Commissioner's Office and apply to sectors within the scope of the NIS regulation. In the case of availability, a service is deemed unavailable if it exceeds 750 000 user hours. However, such thresholds may not be applied to the space sector because smaller cyber incidents may have more significant consequences than initially expected. Moreover, for threat intelligence and analytics, it should be in the interest of both companies and institutions to collect and analyze as many attacks as possible to better model and predict attack patterns.

The Space Agency is not the only entity involved in supporting the sector in its resilience. The UK CAA has developed a guidance document on cybersecurity strategies for applicants and licensees in the spaceflight industry [37]. The CAA is responsible for licensing all spaceflight activities in the UK [38] and aims to promote cybersecurity best practices for those companies willing to engage in spaceflight activities through this guidance. The document should serve as a guide for applicants who are drafting their cybersecurity strategies while applying for a license under the Space Industry Act. The document can be valuable for all those companies that, even if not planning to apply for a license, can use it to secure their assets and develop a sound cybersecurity strategy. The guidance outlines a three-part process that applicants should follow to develop their cybersecurity strategy:

1. Scoping of mission-critical processes: this step assists in identifying and documenting cyber-related mission-critical processes and the associated assets and services that support them and impact safety. In this step, as in the others, particular attention is given to the reliance on third-party systems to perform part of the applicants' mission function. Examples of information that should be included in the strategy are the command and control software utilized, network diagrams, how traffic is protected across the Telemetry, Tracking, and Command (TTC) network, how commands to the spacecraft are sent, authenticated, and received, at what stages the data is encrypted, and the standards of encryption utilized.
2. Threat analysis and risk assessment: the first should be up-to-date through systematic approaches such as STRIDE and TVRA to match the constantly evolving threat landscape, while the risk assessment should reflect the threats analyzed. Third-party technologies, software, or services should also be taken into account throughout the creation of a cybersecurity strategy and documented within the risk assessment.
3. Risk monitoring and future plan: the CAA accepts that a risk assessment is carried out for a specific period. However, applicants should conduct risk identification exercises periodically to identify and respond to evolving or new risks. As part of this activity, an applicant should document how they will manage and monitor the risks in the form of a risk management plan, which should be included within the cybersecurity Strategy.

The guidance value lies in its emphasis on third-party risks and in the examples of the information companies should consider when developing their strategies. The CAA recommends that the Cyber Assessment Frameworks designed for the aviation industry are also implemented in the space sector as they provide a comprehensive overview of good practices, along with associated standards and guidance. In contrast, the cybersecurity toolkit developed by the UK Space Agency is a helpful resource for identifying potential vulnerabilities, but an updated version is necessary to provide more detailed information on the latest threats that have emerged in recent years and the methodologies to model and analyze them.

2.7 The first attempt to regulate space cybersecurity, the US Satellite Cybersecurity Act

In May 2023, US Senators Gary Peters (D-Mich.) and John Cornyn (R-Texas) reintroduced the Satellite Cybersecurity Act [35], intending to protect commercial satellite operators from cyber attacks. The same lawmakers had introduced similar legislation in the previous year, which made progress in the Senate but ultimately failed to pass. The Act seeks to highlight the importance of commercial satellites, which are extensively utilized by critical infrastructure systems such as pipelines, water, and electric utilities [39].

The proposed Act in the US Senate aims to address and improve the cybersecurity of commercial satellite systems through several provisions. First, it mandates the Comptroller General of the USA to conduct a comprehensive study addressing various aspects of cybersecurity in commercial satellite systems. This study includes investigating resources available to federal agencies to address cyber risks, assessing the reliance on critical infrastructure, and evaluating how threats to satellite systems are included in risk analysis and protection plans. Additionally, the Act requires the creation of a commercial satellite system cybersecurity clearinghouse by the Director of CISA. This clearinghouse consolidates cybersecurity recommendations, particularly focusing on risk-based engineering, protection against unauthorized access, and supply chain risks. Furthermore, it mandates submitting a strategy by key agencies to address and improve cybersecurity, defining proposed roles and responsibilities, and addressing cybersecurity threats in critical infrastructure risk analyses.

The Act does not classify commercial satellite systems as a critical infrastructure sector. However, it acknowledges the gaps in cybersecurity within the US space industry, setting an example for other countries to follow. It highlights the importance of understanding the risks other agencies and critical infrastructure sectors face if space networks are disrupted, recognizing the significance of supporting the industry, and introducing a cybersecurity clearinghouse under CISA's supervision. Finally, the Act acknowledges the lack of clear governance for the sector and seeks to establish a strategy that can assess roles, responsibilities, and potential threats. An idea of the financial implications of the initiative is given by the Congressional Budget Office's (CBO) analysis, which foresees six full-time employees to develop and oversee the online database housing cybersecurity resources for satellite operators described in the Act. The anticipated annual costs for staff salaries and technology needed to publish safety materials are estimated at 3 million dollars. The CBO approximates an expenditure of 14 million dollars from 2023 to 2028 for implementing the bill [40].

Although the Satellites Cybersecurity Act has not yet been passed, some parts of the USA space sector have already received guidance on cybersecurity. Companies seeking to collaborate with the US MoD already have a clear set of controls and guidelines they need to comply with, particularly the Pre-Approval (IA-Pre) program, which I have extensively discussed [40]. However, until October 2023, there was not much available in terms of a cybersecurity framework for the rest of the space companies. At that time, NASA published the Space Security: BPG [41], a comprehensive cybersecurity guide designed for companies that want to collaborate with NASA on missions and for the rest of the industry. The particularity of the BPG is that it covers a wide range of essential principles and corresponding controls to strengthen the security of the space infrastructure's distinct segments. It creates three categories of controls: for governance, space missions, and ground segments. In the BPG, NASA outlines 27 distinct controls, each designed to safeguard the multidimensional framework within which space missions operate. Each principle within the BPG is designed to be applied to specific aspects of space operations, serving as tangible and actionable instruction. The cybersecurity principles outlined in the guide cover almost all the key macro areas essential for safeguarding space missions. They include risk management, access control, communication and positioning survivability, software and firmware integrity, malware protection, anomaly detection, and incident response.

In addition, the BPG introduces MITRE attack tactics together with the principles, providing potential paths for mitigation. A key novelty is that 12 tactics were taken from Industrial Control Systems (ICS) and Operational Technologies (OT) as these systems have very similar requirements for timing to space mission systems. Moreover, they represent complex ecosystems where different elements are often networked together, as happens in space-based mission systems, where there may be multiple operating systems on a variety of processors. Moreover, as in OT and ICS, widely accepted standards and architectures such as TCP/IP and UDP in spacecraft design allow for the interconnection and communication of systems, be it for government or commercial use.

The BPG represents one of the most advanced guides for space companies in the field, addressing current threats and technologies and proposing principles that can be translated into actionable controls. The guide highlights the critical need to protect communication channels, data centers, and mission control systems from cyber threats, making it an up-to-date and useful tool compared to current security risks. By focusing on general principles rather than specific directives, it can assist companies in designing security measures that suit their needs. This flexibility ensures that the guide can be widely applied to different space missions and industry requirements.

2.8 Germany's cyber guide for the space sector

In July 2023, the Federal Office for Information Security of Germany published the Technical Guideline (TR) BSI TR03184 Information Security for Space Systems [33]. This is the first European guideline of its kind and is a crucial document in the domain of space cybersecurity. The TR lays out guidelines for the security of the space segment, focusing on the satellite throughout its entire life cycle. BSI created the document in collaboration with the private sector, specifically experts from AIRBUS Germany, OHB Germany, and Secunet Security Networks AG.

The document offers two primary tools: a framework for protecting space systems against various security threats and an Allocation Table that provides detailed recommendations for security measures. In addition, BSI has defined three example attack scenarios. The Allocation Table matches potential threats with recommended security measures that are specific to different space applications. Potential threats (e.g. A218 Electrical Ground Support Equipment) have been identified for each application (e.g. G01 loss/change of information). Specific security measures (e.g. BM1 setting up a security area) have been assigned for each threat to address the associated risks. BSI stresses that this TR should be used along with a mission-specific risk analysis, which is to be prepared by the TR user. The agency has proposed a five-step methodology for conducting such analysis:

1. Identify relevant applications for the business process.
2. Identify relevant threats for the project-specific applications.
3. Perform standardized risk analysis for identified threats.
4. Assign security measures to identify threats.
5. Determine the qualitative shaping of security measures.

The user must ensure thorough identification of all potential threats and implement suitable security measures accordingly. Additionally, the TR highlights the importance of effectively managing relationships with third-party entities, which are often prime targets for malicious attacks. According to the BSI, contractors should define security requirements through contractual agreements and, if needed, conduct audits to ensure their proper implementation. The TR not only defines technical guidelines but tries with a hands-on approach to explain how potential threats could be exploited in real-world scenarios and highlights cases that can aid in the assessment of security measures. The focus is on a specific business process application (GP02 Manufacturing) and specific threats. The following scenarios are taken into consideration:

- Attack on the commissioning process through hardware/software malfunction.
- Manipulation of data from simulators.
- Destruction of equipment and media during the operation of the MGSE.

For each scenario, the guide describes the affected business processes/risk description, the persons involved, and the effectiveness of the security measures. The scenarios are realistic and well-detailed, but more of them adapted to previous attacks that affected the sector should be employed, also taking care of recently discovered CVEs and TTPs.

The last section of the TR provides some general guidelines for cryptography for space systems, crucial for maintaining the confidentiality, integrity, and availability of data. The TR suggests choosing cryptographic primitives and key lengths that correspond to a security level of at least 192 bits, acknowledging the outdated nature of current guidelines, and suggesting the use of a PTG.3 or DRG.4 as a random generator [42]. However, there is no mention of any postquantum strategy, which may require adaptation in the future.

BSI's Technical Guide for the space segment successfully provides a comprehensive framework for ensuring the cybersecurity of space systems. This framework includes identifying potential threats, establishing protection goals, implementing security measures, and providing cryptographic guidance, which significantly supports companies in securing space assets. However, some areas still require further attention and are not explicitly covered by the guidelines. Going forward, BSI plans to categorize the identified security measures into groups such as infrastructure and organizational in the next version of the guide. Additionally, BSI intends to create more reports that specialize in features related to "New Space."

Maintaining the promise, in April 2024, the BSI published a guide dedicated to the Ground Segment [42]. This time, the structure is slightly different. There is no list of threats or security measures and, therefore, no Table where security measures are assigned to threats. This is mainly because many of the threats that apply to the space segment can also affect the ground one. As for the case of the space segment, this guide was designed in synergy with the industry, and several ground segment operators were involved in its development. Similar to the BSI TR-03184, six life phases based on the life cycle of a ground segment were identified.

This IT-Grundschutz profile includes a list of relevant target objects needing protection and general requirements beyond basic protection due to space-specific processes and applications. The guide can be used to fulfill the legal requirements for operators of critical infrastructures, such as ground stations, according to the KRITIS and NIS2 Regulation.

The authors divide the ground segment into two main components: Operations Ground Segment and User Ground Segment. The Operations Ground Segment includes all processes to ensure the satellites' commanding and thus ensure the satellite's uninterrupted and safe operation. Typical components in the operational ground segment are satellite control centers and TTC ground stations. The User Ground Segment components and processes highly depend on the mission type of the space system, including communication with the payload via ground stations.

An important highlight of this BSI guide is about third-party relationships and subcontracting. The guide recommends developing specification documents that focus on a clear distribution of responsibilities and support the design of work processes between the client and the contractor. These specification documents must be converted into seamless processes and procedures and made mandatory. The document emphasizes the importance of considering external and third-party services when designing a mission. Providers must be selected based on their security requirements and audited regularly. Third-party services must be checked, and a risk assessment must be incorporated into the make-or-buy decision, taking into account the criticality of the interfaces and services. In the same way, each service provider must be assessed in terms of the trust and cyber maturity of the company. A detailed description of the interface, protocols, and data exchange must be documented. In this framework, it should be a consolidated practice to agree on templates for exchanging sensitive data such as IP addresses, port numbers, or even encryption keys, and the principles of knowledge only when necessary and least functionality must be observed.

BSI has proposed standard 200–3 for the risk management methodology of ground stations, as it considers several key steps, including identifying target objects, generating a comprehensive risk overview, evaluating frequency and damage effects, risk assessment, risk treatment, and consolidating the security concept. Interestingly, SPARTA and ESA Space Shield are also suggested as valuable standards to use. The guide not only suggests adapting the risk management framework to the mission type but also to the type of final users that will end up utilizing the commercial or state service. State missions are often geared toward providing services to citizens or safeguarding state and public interests, adhering to specific security requirements. Risk assessment and mitigation strategies for such missions may extend beyond those typically applied to commercial ones. Critical considerations include the user profile and data usage patterns, as the security posture of a system used by military personnel, for instance, may be subject to attacks from similarly sophisticated adversaries. Accordingly, each mission must tailor its security framework to align with the user profile and service type.

Business continuity is a crucial feature for ground stations. BSI suggests several best practices to ensure uninterrupted operations. These include designing critical system components redundantly in both the emergency workplace and the primary system, having redundant communication connections such as dedicated data lines or alternative frequency bands, utilizing emergency power generators and uninterruptible power supplies (UPS) for energy management assurance, designating and establishing the role of an "emergency manager" or "emergency coordinator," and forming a comprehensive emergency management organization, including a crisis team.

In conclusion, despite implementing all requirements, achieving absolute security remains unattainable, and both users and decision-makers must acknowledge the existence of residual risks. Collaboration with external organizations may entail transferring confidential information to entities over which manufacturers and operators exert limited control over security management. Even with proper training and protocols in place, employees may inadvertently or intentionally disclose such information to unauthorized individuals. Moreover, procuring services from third parties inherently carries residual risks. Promptly addressing new vulnerabilities with updates may not always be feasible, particularly in systems, where information security was not prioritized during development. The two guides are, therefore, extremely useful and of paramount importance for the sector in providing a concrete risk-assessment strategy and a high-level overview of the threats that affect space and ground segments. Moreover, the two documents provide a good foundation to assess the level of risk and establish consistent procedures to ensure the continuity of space and ground operations. However, their nonbinding nature significantly limits their impact. These guides, with their detailed risk-assessment methods proposed and threat model, could be a solid template for the design of the EUSL.

3 The European Union's approach to space cybersecurity

Exploring the governance of space cybersecurity and enhancing international and cross-sector collaboration in the space domain are crucial areas that require deeper investigation. Currently, as analyzed in Section 2, regulations related to cybersecurity for space are relatively lax, particularly, in Europe where cybersecurity requirements for obtaining launch permissions or operating spacecraft are largely absent.

Despite the fragmented regulatory landscape, there has been a growing recognition of the importance of cybersecurity among various stakeholders, prompting the implementation of targeted measures.

At the European level, the ESA and the European Union have recently emphasized the significance of space cybersecurity. ESA has adopted a dedicated cybersecurity strategy [43] to safeguard its systems and has pointed out the need to develop specialized capabilities and expertise.

The European Commission, supported by the European Union Agency for the Space Programme (EUSPA), has enacted Regulation 2021/696 [44] to establish strong security measures to protect space and ground infrastructure. However, this regulation only applies to the EU Space Programme, and not the commercial space systems. Even though the adoption of the NIS2 Directive in 2022 will extend cybersecurity obligations to operators of ground-based infrastructure that support space-based services a size cap limits its scope to medium-to-large entities (with over 50 employees and an annual turnover of over €10 million), therefore, other legislative instruments will be necessary to protect the sector.

In this section, we delve into the European Union's approach to space cybersecurity. Before exploring the regulatory approach of the Union, we describe the capabilities and frameworks developed by the ESA. Then we explore the proposal of a EUSL and the cybersecurity requirements that may be involved.

3.1 The ESA's cybersecurity capabilities

On 18 April 2011, the Computer and Communications Emergency Response Team of ESA (ESACERT) received a report that a gray hat hacker, known as TinKode [45], had claimed to have hacked into ESA's internal portal. As soon as ESA was alerted, the incident was declared as severity 1, which is the highest level of importance. Upon investigation, ESACERT found that 12 servers located on ESA's external demilitarized zones had been affected, even if no data loss or leakage occurred from the protected internal networks, the publication of usernames and passwords by the hacker was considered a serious security breach by ESA. As a response, the agency implemented a renewed rule verification process and encrypted all passwords to prevent any further security breaches.

As a Provider of expertise in the technical coordination of the European space programs and the design, development, procurement, and operation of satellite systems ESA is an attractive target of cyberattacks. This is why the agency has gradually established best practices and cyber capabilities to mitigate and counter cyber threats. In November 2023, ESA released a policy document, titled "ESA Security for Space: Shaping the Future, Protecting the Present" [43], which outlines the agency's cybersecurity resilience capabilities in the short and medium-long term, with the primary objective of safeguarding ESA's vital space infrastructure.

The document discusses the changing threat landscape in the space domain and outlines the ESA Security Framework, providing an overview of ESA's accomplishments in cybersecurity, and detailing the current and future measures and technologies available to safeguard and support space infrastructure throughout the lifecycle of a space mission.

While developing its capabilities ESA considered a new trend in space security: the increase in organized hacker groups or hacktivists actively exploiting vulnerabilities in space systems and their capabilities of launching low-tech but high-impact hybrid attacks. These attacks are often driven by a desire to experiment with new attack strategies or to gain public recognition and visibility.

In 2020, the ESA Council approved a cybersecurity framework, a major cybersecurity policy implementation that requires a robust security risk management system and integrates security engineering and security assurance into all security-critical projects from their early-stage conception and throughout their lifecycle. A group of entities is responsible for certifying this security process, including the ESA Security Authority, the Security Committee, the INFOSEC and Cyber Panel, the Industrial Security Panel, and the relevant project/program.

ESA's newest strategic document [43] outlines its present capabilities and the ones it plans to acquire in the short and long term. Currently, ESA lists three main present capabilities:

- ESEC (European Space Security and Education Centre) in Belgium, responsible for ensuring cybersecurity in the space domain through secure engineering solutions and monitoring secure operations.
- ESOC (European Space Operations Centre) in France, responsible for identifying threats and vulnerabilities from space and monitoring space missions for security purposes.
- ESRIN (European Space Research Institute) in Italy, hosting the ESACERT for forensic analysis and incident investigation, and supporting the ESA Security Office in supervising the implementation of ESA's cybersecurity Policy.

In terms of future capabilities, ESA plans to establish the following ones:

- C-POP (Cybersecurity Portable Operational Platform), which simplifies access to complex cybersecurity functions and creates a European Threat Intelligence Network. This tool can perform a variety of functions including threat and vulnerability assessment, threat modeling, threat intelligence gathering, and cybersecurity monitoring, both on Earth and in space. Its development began in 2021 and is expected to be fully operational by 2025.
- C-SOC (ESA Cybersecurity Operations Centre), which will monitor and track information and events to detect security incidents and support the readiness of ESA's defensive capabilities. C-SOC will be connected to the Cyber Portable Operational Platform and interoperable with the ESACERT.
- SCCOE (Security Cyber Centre of Excellence), an emulation platform for space missions that can perform vulnerability assessments and risk profiles throughout the system's life cycle.

Looking forward, ESA's long-term capabilities (2025–2027) include the ESA QSVP (Quantum Secure Verification Platform), an end-to-end quantum technology to support the testing, qualification, and security certification of any quantum technology applied to the security domain. To develop the QSVP ESA launched in July 2024 a public tender in order to advance quantum-based security technologies for space systems [46]. Its primary objective is to establish a comprehensive framework supporting the life cycle of quantum space-based systems, focusing on design, development, testing, verification, validation, and vulnerability assessment. This standardized evaluation platform should define certification protocols that ensure the secure implementation of quantum technologies in space missions. This initiative also aligns with the strategic goals of Member States to enhance national evaluation capabilities and provide technological reference points for assessing their national space programs. The tender, which results as classified on ESA's portal involves a significant budget exceeding 500 000 euros.

ESA's strategic goals will enable the agency to face present and future threats effectively. However, it is not clear how these capabilities can benefit the private sector instead of just ESA's operations and missions. Even though ESA's capabilities seem adequate for the current threat landscape, the implementation of the program prescribes tight deadlines that pose nontrivial challenges to its realization. Interestingly, the agency's security implementation program is set to begin with the protection of the ground segment. The agency has prioritized the protection of the ground and user segment against supply chain attacks, with the possible introduction of zero-trust architectures [47].

While it would be ideal to see similar tools developed at the European Union level, it is important to note that ESA is an intergovernmental organization with different ranges of competencies, member states, and governance than the EU. Developing similar tools for Europe and European companies should be the task of EUSPA, as the agency is responsible for the security accreditation of all the EU Space Programme components and the space sector in general. The ESA is responsible for system design, procurement of the system infrastructure (space and ground), and preparing for future system evolutions. This is why, the Commission is moving to equip the EU with a stronger policy framework for space cybersecurity.

3.2 Emerging space security standards

Policies, guidelines, and best practices are not the only tools that stakeholders are using to regulate and manage security aspects in space ecosystems. Many supranational and international organizations have begun developing and proposing technical standards to create frameworks for specific components of space networks. This effort aims to establish the foundations of a resilient space system design. In this section, we explore some of the proposed or developing standards and discuss their potential impact on the upcoming European Space legislation.

3.2.1 *The IEEE technical standard on space systems cybersecurity*

One of technical standards under development is represented by the IEEE technical standard on space system cybersecurity, by the P3349 working group. This initiative, launched in Fall 2023, responded to a joint call to action from researchers and policymakers in the USA, Australia, the UK, and the European Union [48]. The process is structured around the traditional classification of space systems: the space segment, user segment, and ground segment, as well as the link segment and integration layer, are represented in various subcommittees. The proposed IEEE standard would establish a unified framework incorporating technical requirements applicable throughout a space system's lifecycle, ensuring resilience against known and emerging threats. The proposed standard should offer a structured approach to safeguarding space missions by establishing precise technical requirements tailored to the vulnerabilities of space systems. The standard proposed to integrate cybersecurity principles at the design stage through a system-of-systems approach rooted in its core methodology: the "secure-by-component" design paradigm.

The P3349 Working Group is developing the technical framework around secure blocks, and modular security units designed to address specific cybersecurity needs across system segments. These secure blocks are built through a rigorous methodology involving Fault Tree Analysis (FTA) [49] and threat modeling, identifying potential failure points and mapping them to Common Weakness Enumerations (CWEs) recognized in cybersecurity practice. This analytical process enables the development of targeted countermeasures that mitigate specific threats, transforming abstract vulnerabilities into precise, actionable "shall" statements [50]. Each secure block is defined by a comprehensive set of security requirements that ensure compatibility and interoperability while preserving mission-specific flexibility. These blocks are organized into minimum and maximum security configurations, with the former addressing essential security needs and the latter providing enhanced protection for critical missions.

A defining feature of the IEEE standard is its reliance on a FTA process that breaks down the space system into its constituent components, identifying where and how failures could occur. Each component undergoes a detailed examination to address potential vulnerabilities linked to confidentiality, integrity, and availability. For example, components like satellite command interfaces, ground station data links, and onboard control systems are analyzed for possible failure modes, such as data interception, command spoofing, or unauthorized system access. The identified vulnerabilities are linked to specific CWEs, enabling the development of countermeasures based on secure-by-design principles such as least privilege, complete mediation, and separation of duties. These principles are taken from NIST Special Publication 800–160, Volume 2 [51], and, in particular, the UK Device Security Guidance [52].

The secure blocks are generated through a design process that considers both technical feasibility and mission priorities. Developers can combine blocks into secure architecture based on the security objectives of a given mission. For example, a mission focused on Earth observation may prioritize data confidentiality and availability, while a communication satellite may emphasize real-time command authentication. The modular structure ensures that secure blocks are interoperable and scalable, allowing system architects to adapt their designs to evolving technological and mission-specific demands.

To identify the security requirements the standard plan to apply a matrix row reduction process during secure block creation. This process reduces overlapping security requirements by optimizing the set of applicable measures, eliminating redundancy, and maintaining comprehensive coverage. This approach results in a catalog of "shall" statements that precisely define the technical requirements for each system component. These statements cover a wide range of cybersecurity functions, such as secure boot processes, encrypted data storage, hardware-based authentication, and intrusion detection systems. Each "shall" statement is directly linked to a specific fault identified through the FTA process and a corresponding CWE, ensuring both technical specificity and enforceability. This contrasts with traditional cybersecurity frameworks that rely on generalized policy recommendations or "best practices" that lack operational detail. The Working Group argues that "shall" statements transform abstract security principles into concrete, implementable technical specifications that developers can integrate directly into system designs [52].

Below is an example of how the identified minimum design approaches can be converted into minimum technical requirements for the Space Vehicle for the Attitude Determination and Control System (ADCS) for the principle A.1 Trust-Based Privilege Management:

- The ADCS components shall implement least privilege.
- Actions on and from the ADCS shall require dual authorization.

Such shall statements are a good example of linking standard provisions to direct implementable action for developers. Therefore, adopting components of the IEEE standard within EUSL could force European actors to reconsider their current top-down regulatory structures. For instance, the EU's focus could be reframed through the technical lens of modular secure blocks and minimum cybersecurity requirements proposed by the IEEE Working Group. This shift could encourage a move from general cyber principles toward precise technical obligations on satellite manufacturers, operators, and service providers.

If these detailed technical requirements were integrated into the EUSL, legislators would need to accommodate technical security audits, dynamic system certifications, and fault-tree-based compliance tests. This could lead to a rethinking of how compliance and liability are assigned in the European space sector, possibly extending responsibilities beyond operators to system integrators and component manufacturers.

The adoption of provisions designed based on the IEEE standard could transform EUSL from a policy-centric framework into a technologically grounded legal regime defined by precise, enforceable technical norms.

3.2.2 The Consultative Committee for Space Data Systems standards

The Consultative Committee for Space Data Systems (CCSDS) is a multinational forum developing standards for space communication and data systems. It includes over 11 space agencies as full members, 32 as observers, and 119 industrial associates. In addition to its standardization efforts, the CCSDS also creates a series of documents that focus on implementing security measures and space protocols, enhancing the security of data transmission in space missions [53].

Among its recent publications, the CSSDS includes the “Space Data Link Security Protocol” (CCSDS 355.0-B-2) [54], a recently proposed recommended standard, setting a technical benchmark for securing communications across space data systems. As an international standard developed by the CCSDS, it defines a framework that guides space agencies and commercial operators in implementing data link layer security. CCSDS 355.0-B-2 formalizes specific requirements for cryptographic security, including encryption, authentication, and data integrity verification. It standardizes the use of essential cryptographic constructs such as the Security Parameter Index, Security Header, and Security Trailer, ensuring consistent implementation across different mission profiles. The protocol also incorporates a well-defined structure for managing Security Associations, allowing mission planners to establish secure channels with specified cryptographic configurations.

The standard’s relevance extends beyond its technical specifications, as it also reflects evolving security concerns in space communications. The inclusion of mechanisms for antireplay protection, message authentication codes, and authenticated encryption demonstrates a forward-looking approach that anticipates future cybersecurity challenges in space environments. Its layered structure, which operates within the Open Systems Interconnection model’s Data Link Layer, ensures that the protocol can be adapted to various mission types without imposing unnecessary constraints on system design.

For European stakeholders, this standard can be used as a good reference point for improving the cybersecurity posture of space missions. Given the European Union’s broader regulatory landscape, particularly concerning cybersecurity and data protection, the CCSDS 355.0-B-2 protocol could become a reference standard for the development of legally binding requirements for space operators. The standard is already being used by governmental agencies that have developed their implementations of the SDLS protocol for their specific missions. Moreover, interoperability tests have been conducted among these implementations by ESA, the Centre National d’Etudes Spatiales, and NASA [55]. However, to enhance integration and consistency among space operators at the European level, it is essential to adopt a unified implementation of the SDLS protocol. Its recent release in 2022 indicates that industry adoption is not yet universal. This is evident due to the scarcity of market-ready solutions [56].

Therefore, the protocol can have a relevant impact on European space legislation, as ESA and national space agencies increasingly engage in joint missions and commercial partnerships. Also, the CCSDS 355.0-B-2 standard could serve as a legally mandated security framework. This could enhance technical interoperability and establish a uniform legal basis for addressing data security. In addition, CCSDS developed the recommended standard 356.0-B [57] that extends the application of the SDLS Protocol to missions utilizing the Internet Protocol (IP), offering guidance for network layer security that can be applied to a wider audience of commercial entities and users.

Another relevant recommended standard published in 2024 is the Unified Space Data Link Protocol (USLP) CCSDS 732.1-B-3 [58]. This standard concerns the transfer of mission data across space communication links. It operates at the Data Link Layer and defines how data is formatted, segmented, and transmitted between spacecraft and ground stations. USLP introduces a flexible data-handling system through structures like Transfer Frames, Virtual Channels, and Multiplexer Access Points, enabling efficient data multiplexing and service differentiation. It supports various mission types with both fixed and variable frame lengths and provides essential data transport services such as sequence control, error management, and Quality of Service configuration. The proposed modular design allows mission planners to adapt the protocol to different operational needs.

The main difference between the USLP and SDLSP is the fact that SDLSP focuses exclusively on securing data transmitted over space communication links. Unlike USLP, which deals with the structural and operational aspects of data transfer, SDLS provides encryption, authentication, and data integrity features by adding cryptographic components such as Security Headers and Security Trailers to the Transfer Frames defined by USLP. While USLP ensures that data is efficiently organized and transported, SDLSP ensures that this data remains confidential and tamper-proof. In practice, USLP can function independently for managing data flow, but incorporating SDLSP becomes essential when mission-critical data needs protection against cyber threats. Their combined use reflects a layered security approach: USLP manages the operational transport of data, while SDLSP ensures its protection, creating a secure and efficient communication ecosystem for space missions.

In addition to standards, the CCSDS developed several other types of documents for space system security such as the CCSDS 350.0-G3 [59], an informational report that outlines the application of security measures specifically through the SDLS Protocol. The report details the implementation of security services such as encryption, authentication, data integrity, and access control at different layers of the CCSDS protocol stack, including the physical, data link, network, transport, and application layers. The document also outlines security implementation points like bulk encryption, Space Data Link Security, IP Security, and application-layer cryptographic methods. It also discusses security trade-offs, protocol-specific configurations, and mission-specific security architectures.

3.2.3 Translating standards into European legislation

The adoption of space cybersecurity standards, such as those being designed by the IEEE or CCSDS presents a unique opportunity and challenge for European stakeholders in crafting future space legislation. On one side, these standards provide a technical foundation for establishing clear cybersecurity requirements through precise, enforceable obligations based on technical specifications rather than high-level policy statements. The IEEE standard, though still under development and not yet public, offers a promising model for a system-of-systems approach built on modular security blocks defined by specific threat models and linked to established CWEs. This level of detail could transform European regulatory frameworks by shifting compliance obligations from general principles to exact technical implementations. Similarly, CCSDS standards such as the Space Data Link Security Protocol (SDLS) and the USLP provide operationally proven frameworks addressing both data management and data security. However, these standards face significant challenges. They are voluntary and lack binding enforcement unless formally adopted into national or European law. Moreover, the limited industry adoption of the SDLS protocol highlights the need for greater regulatory incentives or mandates to ensure consistent implementation. Integrating these standards into EUSL would require balancing the need for harmonized technical norms with the flexibility to accommodate emerging threats and technological advances. European legislators could adopt these standards as legal benchmarks, tying compliance to technical audits, security certifications, and contractual obligations within the space supply chain. However, this would require a substantial commitment to developing a regulatory ecosystem that supports technical verification processes and fosters public–private collaboration. While not without limitations, these standards offer a pathway toward a technologically robust and internationally interoperable cybersecurity regime, ensuring Europe's leadership in secure space operations.

3.3 Toward a EUSL

There is no doubt that space security has become a crucial matter in Europe, especially with the recent increase in irresponsible and hostile behaviors such as cyber-attacks. The EU space strategy for security and defence recognizes the strategic nature of space and the need for the EU, as a global space power, to address security challenges. Even though European space assets have been the target of numerous attacks, regulation has been slow to address the issue. Policy initiatives like NIS2, which apply to space as a sector as well (but not to the space segment), may not address all the different kinds of threats and targets to the various space infrastructures.

In September 2023, the President of the European Commission, Ursula Von Der Leyen, launched the idea of an EU space law (EUSL). On 17 October 2024, the Commission published the 2024 Work Programme [60], which announced the preparation of a legislative initiative that should have been adopted during the first quarter of 2024. The EU Space Law focuses on three main pillars: safety, resilience, and sustainability. The second pillar deals with ensuring the resilience of space infrastructure against cyber threats.

In October 2023, the European Commission initiated a targeted stakeholder consultation on the Law. However, the survey received feedback from only 44 respondents, 10% of whom were from the industry. In general, they welcomed the view of the Commission and acknowledged the need for a more resilient space industry. However, companies are worried about additional financial burdens given by cybersecurity requirements and duplication of obligations because of the NIS2. The private sector, therefore suggests having mission-specific requirements and cybersecurity by design in the program management and mission operation phase.

The consultation process includes a baseline scenario [61] that describes the current state of space legislation in Europe and provides three policy options for the implementation of the future Space Law. The policy options proposed by the Commission are still in the consultation phase, and there is no concrete proposal yet. In this section, we analyze the potential cybersecurity provisions of Option 2, summarized in Table 2, and we address the shortcomings and gaps that exist in this option. We have chosen this option as it delves deeper into cybersecurity measures. While the others (Options 1, 2+, and 3), on the other hand, leave a marginal role in cybersecurity implementation.

Table 2. Cybersecurity requirements of the EUSL, Option 2.

Risk management rules	Ensure proper and coherent risk management of all space infrastructures and assets along the risk management cycle: • Management of space assets: identification and classification of assets, inventories, and documentation • Management and control of access rights for all relevant segments (space, ground, and links) • Detection of incidents: effectively activate alerts and identification of interferences, cyberattacks, spoofing, jamming, as well as incidents related to the physical infrastructures • Cyber and physical protection and prevention measures: encryption, malware protection policy, patch management, increase tolerance to noise, mitigation strategies, and back-up management • Business continuity policy, having response and disaster recovery plans • Testing the ICT systems • Reporting of significant incidents • Communication in the emergency protocols
Risk assessment	Risk assessment covering all lifecycles of the space activities and operations • Specific risk assessment [commercial off the shelf (COTS)], non-EU assets • Use of risk scenarios, threat modelling, use case
Reporting of significant incidents	Handling of all incidents • Reporting of significant incidents (cyber and noncyber related) • Establishment of national monitoring centres with the support of EUSPA
Supply chain management	• Criteria for the choice of software in the supply chain • Control ICT systems connected for maintenance • Review ICT requirements in the contracts • Non-EU assets inventory

The EU Space Law is expected to cover various aspects tailored to different stakeholders within the space industry. An initial assessment of Option 2 suggests that the Law should include comprehensive measures to address security risk assessment and management principles within space. This includes conducting security risk assessments based on various risk scenarios and implementing robust risk management principles. These principles encompass the management of assets, control rights, detection and handling of incidents, prevention and protection measures, cryptography standards, backup and patching procedures, business continuity, recovery plans, and supply chain risk management.

The law is expected to mandate the reporting of incidents to ensure transparency and accountability. Additionally, it will encourage voluntary information sharing through entities like ISAC, respecting confidentiality and competition. To accommodate the diverse needs of operators, the law will need to establish a baseline that is suitable for everyone, emphasizing the application of known risk management principles. The goal is to ensure security by design principle, maintaining flexibility in the intensity of requirements, and tailoring them based on the operator's size and phase of operation. One of the major requirements of the law is expected to be the obligation for operators to produce a security risk assessment, with different requirements for small and large companies. The aim is to promote freedom and flexibility by focusing on objectives rather than enforcing specific methodologies. However, this may pose challenges in evaluating the effectiveness of risk assessments, and a set of suggested methodologies should probably be defined.

Regarding the relationship between NIS2 and the EU Space Law, questions arise regarding the consistency between the two frameworks. Legal security and uniform rules should be the priority of policymakers, addressing all the situations where ground stations located outside the EU provide services to European citizens or are managed by European companies. It is not clear if it will be mandatory for all stakeholders, including non-EU entities, to adhere to the requirements when operating within the EU or providing services to EU satellite operators. Another gray area of the law is the so-called regime of proportionality that may be applied to SMEs and research centers, even if companies are smaller in fact, it is not guaranteed that their services may be the entry points to wider networks managed by bigger companies.

Despite the proposal for a comprehensive EU Space Law, many observers have questioned whether the EU possesses the necessary legal basis for such a policy instrument under its current constitutional framework [62]. Critics argue that Article 189 TFEU, which grants the EU competence over space policy, explicitly precludes the harmonization of national space laws, limiting the Union's ability to legislate in this field. However, the EU has adopted a "mix-and-match" legal strategy, drawing on a range of other treaty provisions to address gaps left by Article 189. For example, Articles 114 and 115 TFEU, traditionally used for internal market regulation, have been used to justify harmonization in the context of economic competitiveness and space sector development. Similarly, environmental protection mandates under Articles 191–193 TFEU have been cited to regulate sustainability aspects, including space debris mitigation and emission controls. This flexible approach allows the EU to integrate space governance with related policy domains, such as cybersecurity, safety, and sustainability, as highlighted in its 2023 Space Strategy for Security and Defence [63]. Yet, concerns persist about overregulation and potential encroachments on Member State sovereignty, particularly when national security considerations intersect with EU law. The European Court of Justice's case law, notably the Tobacco Advertising rulings [64], affirms that the EU may harmonize laws when regulatory divergence risks fragmenting the internal market—a principle the EU could extend to the space sector if, for example, cybersecurity vulnerabilities threaten the single market. Thus, while the direct competence under Article 189 TFEU is constrained, the EU's adaptive legal framework reinforces the legitimacy of its proposed space law, ensuring that regulatory efforts remain within the bounds of subsidiarity and proportionality while addressing critical challenges in space governance.

In December 2024, the Polish Presidency of the Council of the European Union published its Programme and priorities, setting the stage for its 6-month tenure from January to June 2025 [65]. Among its strategic goals, the Presidency emphasizes the need for developing a comprehensive EU space law framework. The document reflects a dual policy focus: fostering legal clarity and regulatory oversight while supporting innovation among small and medium-sized enterprises and start-ups. Notably, the proposed timeline for space law development appears linked to the Presidency's legislative agenda, suggesting that discussions and potential legislative drafts could emerge during the first half of 2025. The Presidency also prioritizes cybersecurity and environmental sustainability, ensuring that future space legislation addresses these critical concerns. This approach reflects an understanding that a robust legal framework will be indispensable in supporting Europe's ambitions in the increasingly competitive and securitized global space sector.

4 The way ahead, next steps to secure the European space sector

The fields of cybersecurity and space security are constantly evolving, and every space power is now aware of the risks associated with space. However, merely producing guidelines, best practices, and toolkits for the sector does not make it resilient. While several useful tools have been proposed, they all fall short of ensuring a resilient space ecosystem. Currently, the USA and EU are the only jurisdictions where a superior instrument, namely a space law with cybersecurity requirements, has been proposed. After carefully analyzing all the available policies, guides, frameworks, and toolkits in the field, we identified some main points and areas that should be covered and defined to have a comprehensive and effective EUSL.

In this section, after providing a systematic overview of space systems' distinctive cybersecurity risks, we refer to the policy analysis of the instruments addressed in Section 2. We identify the main elements that are not addressed by those instruments or by the future EUSL, which we consider necessary to complement and define a clearer cybersecurity strategy and policy for Europe.

4.1 Defining cyber risk in space systems

The cybersecurity frameworks and risk models governing space have come under growing scrutiny. Current cybersecurity principles and best practices have typically been derived from terrestrial ICT environments, but these conventional models cannot simply be transferred to the orbital domain without significant adaptation. The reasons for this lie in the distinct architectural, operational, and environmental factors that shape the unique threat landscape of satellite-based infrastructure.

Unlike terrestrial networks, satellite communication systems are characterized by high latency, asymmetrical links that often rely on narrowband and bandwidth-constrained radio frequency channels. These limitations impose trade-offs between performance, encryption, and resiliency. Many satellites, especially those in Low Earth Orbit, sacrifice data authentication and encryption to conserve link budget and reduce communication overhead [66]. These characteristics create direct exposure to eavesdropping, signal replay, spoofing, and integrity injection, all of which are amplified by the open nature of space radio frequency environments.

The architecture of satellite ecosystems introduces a multisegment attack surface, where vulnerabilities may be distributed across onboard subsystems, satellite-to-ground links, command and control centers, and external interfaces such as cloud APIs, GNSS inputs, and third-party mission software. The use of commercial off-the-shelf (COTS) components and open-source flight software [67] in both small and large-scale satellite programs further contributes to software monoculture risk, where a single exploit chain can propagate across missions and organizations.

Most importantly, space systems operate in an environment where physical access is impossible postlaunch, making most conventional incident response protocols unapplicable. If a system is compromised in orbit, whether through malware, misconfiguration, or remote intrusion, it cannot be physically serviced or rebooted. This increases the consequences of even minor cyber incidents, transforming software bugs or single-point failures into potential mission losses. Space assets must therefore be treated as remote critical infrastructure, subject to environmental constraints, asymmetric threats, and systemic opacity that distinguish them from any other domain of cyber defense.

In conclusion, what distinguishes the space domain from conventional ICT environments is not just its criticality, but its structural asymmetries. In summary:

- Most satellites operate on command-based architectures, with ground stations sending instructions in strict windows of uplink availability, often with minimal feedback mechanisms.
- Software updates must be uploaded during limited contact intervals, often constrained by bandwidth and energy budgets, which delays remediation of known CVEs.
- Once in orbit, compromised systems cannot be physically accessed. Remote forensics are limited, and recovery often requires risky software overwrites with no rollback capacity.
- Flight software is often open-source and reused across missions for cost and compatibility reasons, leading to cross-constellation exploitability.
- Many ground stations, GNSS systems, and cloud telemetry services are shared across operators and missions, creating lateral movement opportunities for attackers.

In the next section, we analyze how these abstract risk categories have been concretely exploited in documented incidents and simulations to illustrate the operational implications of a fragmented security architectures in space infrastructure.

4.1.2 Cybersecurity incidents in the space domain

The cybersecurity risks and threat vectors identified in the previous subsection are not merely theoretical but have repeatedly shown their applicability, as addressed in academic literature and sector-specific reports. In this section, we provide a brief overview of some empirical cases, as we believe it is required both for understanding the nature, scale, and complexity of cyber threats and for supporting tailored cybersecurity governance frameworks that reflect current threats landscapes.

One of the most famous and discussed incidents, illustrating the interconnectedness of ground and space segments, occurred in February 2022 when the KA-SAT satellite network, operated by Viasat [40], suffered a cyberattack coinciding with the start of Russia's invasion of Ukraine. Forensic investigations confirmed that attackers exploited a misconfigured virtual private network in the terrestrial management system to deliver the *AcidRain* wiper malware [68]. This malware wiped modem firmware across thousands of user terminals, causing extensive outages throughout Ukraine and parts of Europe, including the disruption of critical infrastructure such as wind farms and emergency communication systems [40]. The satellite itself remained physically unharmed, but the Viasat incident proved how terrestrial cyber vulnerabilities can cause disruptions to space-based services.

The Viasat attack showed the weaknesses of ground, but most importantly, user terminals, which are often the most exposed yet least protected elements of satellite communication networks. In this domain, researchers have demonstrated that SATCOM terminals can be exploited through both physical and software-level vulnerabilities, leading to prolonged service disruption and potential access to internal network segments. In a recent case study focused on Starlink, it was shown that the administrative interface of the user terminal lacked robust authentication controls and was vulnerable to a denial of service attack [68]. Sending a specifically crafted gRPC command via the local network, an adversary could crash the terminal's command handler, making it unresponsive. This "kill" command, if executed after forcing the terminal into a stowed state, could lead to total service loss.

These weaknesses are not unique to Starlink. Earlier research [69] revealed that several satellite broadband providers deployed terminals with default credentials, open management ports, and insecure firmware update mechanisms, making them susceptible to remote compromise. Exploits demonstrated the ability to intercept unencrypted web traffic, reroute DNS requests, and gain persistent access through firmware modifications, all without physical access to the terminal or detection by the satellite operators.

Moving up from the user to the ground segment, middleware software (software that acts as a layer between applications in the OS) emerged as a critical attack vector in March 2022, when the hacktivist group NB65, claimed responsibility for compromising the Russian space agency ROSCOSMOS [70]. Exploiting the Log4j2 vulnerability (CVE-2021–44 228) within a publicly exposed instance of WSO2 middleware (an open-source software widely used for application management, telemetry processing, and system integration). The CVE-2021–44 228 vulnerability was discovered in December 2021 in the Apache Log4j2 logging library, widely used in Java-based applications worldwide. This vulnerability allowed attackers to remotely execute arbitrary code on affected systems simply by sending specially crafted requests that included malicious payloads. Exploiting this vulnerability, NB65 allegedly gained root-level access to backend operational services, including telemetry and vehicle monitoring interfaces. ROSCOSMOS publicly disputed the severity of the breach, but independent cybersecurity analysts confirmed the presence of significant vulnerabilities consistent with NB65's claims.

This incident highlights a critical governance lesson: commercially available software can be easy to use and integrate but can also introduce substantial cybersecurity vulnerabilities when such integration is not followed by a rigorous security validation or hardening. Middleware platforms such as WSO2 or similar third-party products often become critical points of compromise, offering potential lateral movement opportunities across interconnected systems. This case makes clear why it is necessary to adopt cybersecurity governance frameworks that explicitly mandate thorough, mission-specific security assessments and validation procedures for third-party commercial software integrations.

The ROSCOSMOS breach also illustrates the links between cybersecurity and geopolitics. Claims of cyber compromise can undermine public and operator confidence, disrupt trust in critical infrastructure, and complicate crisis communication strategies. For this reason, effective space cybersecurity governance must incorporate clear protocols for transparency, incident response, and crisis communication to manage and mitigate reputational and strategic impacts. The ROSCOSMOS incident should point out to policymakers the critical importance of robust, transparent cybersecurity response mechanisms as integral components of any effective cybersecurity governance framework for space systems.

Affecting a different level of space infrastructure, the compromise and interference in satellite signals are another core component of the documented risk landscape. In this domain, many cases exist involving repeated occurrences of GNSS spoofing and jamming attacks reported by researchers and military officials. Many of these attacks were documented in Ukraine and Russia, where commercial vessels and airplanes experienced GPS signal disruption and position spoofing, [71]. Disruptions and spoofing incidents have been registered in the Black Sea region, near the Russian port of Novorossiysk, starting on 22 June 2017. According to the US Coast Guard Navigation Center, at least 20 commercial ships reported severe GPS signal losses or disturbances during this period, leading ships to report false positions, which could result in dangerous navigational errors, including collision risks and unauthorized incursions into restricted territorial waters. Likewise, Iranian military GNSS spoofing was used to manipulate or disrupt drone operations near strategic locations [72], demonstrating the practical geopolitical consequences of cyber vulnerabilities in satellite navigation signals.

Beyond real-world breaches, cybersecurity exercises demonstrated the impact of vulnerabilities inherent in satellite cybersecurity. In the WannaFly experiment [73], researchers recently explored how ransomware might be adapted to target satellites. Specifically, researchers focused on NASA's widely adopted core Flight System (cFS) [74], a modular, open-source software framework extensively utilized in low Earth orbit and other small-scale satellite missions due to its cost-effectiveness, standardization, and adaptability.

Using software injection techniques, the researchers simulated a scenario where ransomware payloads were introduced into the satellite's onboard software bus, the critical communication channel responsible for interprocess message passing among the spacecraft's software applications and subsystems. In the simulated scenario, the injected ransomware did not disable the satellite or corrupt its physical hardware. Instead, it disrupted communication pathways within the software infrastructure, isolating critical onboard applications and subsystems from one another. The spacecraft's hardware remained fully operational and physically intact, but operators lost the ability to control essential functions and perform routine tasks, effectively paralyzing mission operations.

The approach is similar to traditional terrestrial ransomware in its use of disruption without physically destroying underlying infrastructure. In this way, adversaries could demand ransom or other concessions from satellite operators in exchange for restoring command-and-control capabilities. Unlike terrestrial ransomware incidents, where backups, physical interventions, or rapid patching might provide relatively immediate recovery, satellite operators confronting similar scenarios would have severely limited response options, constrained by latency, bandwidth limitations, and the inability to physically access or reboot orbital assets.

The WannaFly simulation highlights the risk associated with standardized software frameworks and open-source solutions widely adopted in modern satellite missions. The extensive reliance on common software stacks like cFS creates potential software monocultures, where a single vulnerability could simultaneously impact numerous satellites across different missions, operators, or even constellations. In practical terms, WannaFly research underscores the need for developing enhanced software validation protocols, comprehensive prelaunch cybersecurity assessments, robust onboard isolation mechanisms, and adaptive in-orbit intrusion detection systems. This aligns directly with concerns raised by over 25 aerospace cybersecurity experts [75], which explicitly warn against software and hardware monocultures, and call for mission-specific controls, secure boot mechanisms, and supply chain transparency. The experiment therefore reinforces the need for regulatory frameworks that move beyond abstract risk awareness toward enforceable, design-stage security mandates tailored to space-specific architectures.

Collectively, these incidents, that go from ransomware simulations (WannaFly), large-scale network outages (Viasat), middleware exploitation (ROSCOSMOS), navigation spoofing (Novorossiysk GNSS disruptions), and hardware-level terminal compromise (Starlink), demonstrate the reality of space cybersecurity threats and the diversity, complexity, and scaleof attacks. Each incident is a validation of the theoretical vulnerabilities outlined previously and highlights the need for space-specific cybersecurity governance mechanisms.

The majority of the cybersecurity governance frameworks, both existing and proposed, have failed to integrate this domain specific risk perspective, remaining based on terrestrial security principles. The absence of mandatory resilience standards, the underdevelopment of enforceable cybersecurity requirements, and the general reliance on voluntary compliance or checklist-driven audits show a mismatch between the risk environment and the governance response. A cybersecurity approach appropriate for space should entail sector-specific analysis of systemic threats, adversarial incentives, and operational constraints. In the next section, we propose some of the improvements we believe are needed in terms of governance and policy development in the field.

4.2 Clarifying and assessing resilience

European legislators must prioritize resilience in the space community, but before doing so, they must define it and determine who is responsible for guaranteeing it. Currently, there is no consistent definition of resilience in the space industry. For instance, The Aerospace Corporation defines it as the ability to deliver missions despite manmade or natural interference [74]; while NATO defines it as the capability to anticipate risk, limit impact, and recover quickly through survival, adaptability, evolution, and growth in the face of turbulent change [76].

To create a European framework, the space industry has proposed specific concepts related to resilience, such as service separation, distribution, and recovery. However, a more quantitative approach is necessary to assess resilience effectively. The space sector needs a resilience assessment framework with key performance indicators (KPIs), such as recovery time, minimum performance, and functionality loss. Future research endeavors entail the definition of such KPIs and the assessment of their applicability to the space sector.

Once the definition of resilience is concretely addressed, European policymakers should define who will take care of it. Specific agencies in the USA and UK are responsible for the resilience of different critical infrastructures. They have incident response capabilities and actively support the sector. However, the EU has no defined agency for the cyber resilience of space. Although EUSPA is responsible for the sector's security, it is not clear if it has been equipped with the operational capabilities to act like CISA in the USA.

4.3 Measuring security

Resilience and security are interconnected, and measuring both is important. This is why organizations use security metrics. These metrics are crucial for policymakers to evaluate the security of space companies, and for the companies themselves to assess their preparedness against current threats. While there are security metrics available for other critical sectors [77], there are no specific ones for space systems. The space industry needs clear instructions and a standardized approach to ensure compliance with security requirements and procedures. Legislators should provide such clear guidelines. NASA's BSG and the BSI TR guides offer excellent examples of actionable security measures for the industry. Therefore, the concrete cybersecurity measures provided by the future Space Law should be translated into actionable guidelines as security controls that companies can easily understand and apply to secure their systems and better comprehend their cybersecurity posture. In Section 5, we identify some cybersecurity requirements that could be included in EUSL and map them to the latest Security Controls developed by CIS. This approach could be adopted by European policymakers to provide clear guidance to the industry on the necessary steps that need to be taken for effective cybersecurity.

4.4 Tracking global threats: information sharing and response strategies

As cyber capabilities continue to develop, it is crucial to have policies that assess current trends, which can only be achieved through active collection of threat intelligence and information sharing. Space systems are complex and require a collective defense approach. Companies should share threat intelligence and use a common lexicon for Tactics, Techniques, and Procedures.

Only a consistent database of attacks can enable the development of useful information and even the automation of intelligence collection to predict or model threat actors' activities. Based on the limited information on attacks to date, several key trends have been identified. First, the supply chain has proven to be a weak point, as intentionally faulty or backdoored hardware or software can provide access to the design schematics, physical components, and software packages of a given satellite. Second, unmanaged appliances, often edge gateway devices, SSL VPN appliances, and end-of-life hardware have also been identified as the primary entry points for attackers and the most frequently observed initial access vector for exploitation [78].

Given such a threat landscape, asset management becomes crucial, and companies should have a clear understanding of their assets, the software running on them, and which assets are managed by third parties on the same network. Another observed weakness in space systems concerns attacks targeting the critical links between satellites and ground control stations. These attacks could potentially lead to advanced attack methods such as replay or man-in-the-middle attacks. Furthermore, terrestrial command and control systems (C2), data relay stations, and ground systems processing satellite data have also been shown to be vulnerable to similar attacks. Lastly, attacks on the user segment, often via insecure network protocols for software updates of terminals or devices, demonstrated to be the most cost-efficient way to disrupt satellite communication [79]. Designing an effective EUSL requires taking into account these trends.

If the role of policymakers is crucial to address the constant emergence of new vulnerabilities in space systems, also companies need to take responsibility and a proactive approach. A sound practice would be the implementation of offensive security testing throughout the entire lifecycle of their space systems. Due to the criticality of space infrastructure, vulnerability scans, and checklists are not sufficient, and offensive security approaches complement static code analysis, especially in a white-box environment [80]. This is particularly relevant as modern space components are now accessible to almost everyone, making it easy for malicious actors to perform firmware dumping and reverse engineering techniques [81].

The launch of the EU Space ISAC is a positive step toward capturing new trends through information sharing in Europe. However, there may be gaps in the implementation of operational security measures. Detecting and defeating threats is crucial, but recovery and response are equally important. It is essential to have a plan of action in place in case a breach occurs. Intelligence gathering alone is not enough, and small and medium-sized companies cannot do it alone. To maximize the impact of threat intelligence collection, it is important to avoid duplicating efforts and foster synergy between existing information-sharing capabilities like ESA's CSOC and C-POP. One way to achieve this is by enforcing security clearance mechanisms that allow companies to trust these initiatives and become part of such networks.

5 From policy recommendations to actionable guidance

In the space industry, evaluating and ensuring security can be a complicated task. During the open consultation for the EUSL, numerous industry representatives emphasized the need for clear guidelines that CISOs and other security personnel can easily implement to comply with the new requirements. To address this issue, we have correlated the policy provisions that may be part of the EUSL with the relevant Security Controls developed by the CIS. CIS is a nonprofit organization that works to improve the online security of entities in the private and public sectors. It provides them with various cybersecurity best practices, products, and services to enhance security efficiency and effectiveness. Among them, there are the CIS Controls [82], which are a set of best practices that can be used to strengthen the cybersecurity posture of an organization. With the use of such controls, organizations can simplify their approach to threat protection, as they require users to perform a specific action to be implemented. CIS Controls have been used to help the enforcement of regulations, as to support compliance with GDPR.

To support the future implementation of the EUSL's cybersecurity requirements, we created an easy-to-use assessment mapping from CIS controls to possible EUSL requirements. The mapping provides some of the safeguards and specific actions that enterprises should take to implement the Controls. In our analysis, we included only the safeguards that apply to the implementation group (IG1). IG identifies a subset of the CIS Controls that every enterprise should apply to guard against common attacks. Group 1 is defined as "essential cyber hygiene," or the cyber defense Safeguards that every enterprise should apply to guard against the most common attacks. This group includes small to medium-sized companies with limited IT and cybersecurity expertise. These Safeguards are designed to function with small or home office COTS hardware and software. We decided to use IG1 safeguards as they are close to the commercial space sector, particularly the "new space" in terms of resources. Although exact requirements are not yet known, using CIS controls and related safeguards as a starting point can help organizations understand how far they are in their cybersecurity processes and what steps they need to take to comply with the future law. The tool is designed to help organizations identify the cybersecurity controls they need to enact and prepare for adaptation. Table 3 maps the EUSL measures to the CIS security controls v8.

For instance, the EUSL policy Option 2 provision on the Management and control of access rights emphasizes the importance of effectively identifying, classifying, and managing access to the organization's network. To align with CIS Control 6, Access Control Management, organizations can connect several safeguards that suggest to:

- Establish access granting and revoking process to enterprise assets when a new hire joins the organization or when there's a change in a user's role or permissions. This ensures that access to sensitive resources is granted/revoked in a consistent and timely

Table 3. Assessment tool, CIS controls to EUSL cybersecurity requirements.

EUSL policy provision	CIS security controls	IG1 safeguards
Management of space assets: identification and classification of assets, inventories, and documentation	CIS Control 1: inventory and control of enterprise assets	• E&M detailed enterprise asset inventory • Address unauthorized assets
Management and control of access rights	CIS Control 6: access control management	• Require MFA for externally exposed applications, remote network access and administrative access. • Establish an access granting and revoking process
Detection of incidents: alerts, identifying cyberattacks, and physical incidents	CIS Control 8: audit log management	• E&M an audit log management process • Collect audit logs and ensure adequate audit log storage
Cyber and physical protection: encryption, malware protection, and patch management	CIS Control 3: data protection CIS Control 4: secure configuration of enterprise assets and software CIS Control 7: continuous vulnerability management CIS Control 10: malware defenses CIS Control 13: network monitoring and defense	• E&M a data management process • E&M a data inventory • Configure data access control list • Encrypt data on end-user devices • Configure automatic session locking on enterprise assets • E&M a vulnerability management process • Perform automated operating system and application patch management
Business continuity: disaster recovery plans	CIS Control 17: incident response management	• Designate personnel to manage incident handling • E&M contact information for reporting security incidents • E&M an enterprise process for reporting incidents
Testing ICT systems	CIS Control 18: penetration testing	• E&M a penetration testing program (IG2) • Perform periodic external penetration tests (IG2)
Reporting of significant incidents	CIS Control 17: incident response and management	• See business continuity
Supply chain security: software selection, maintenance connections, and contract reviews	CIS Control 15: service provider management	• E&M an inventory of service providers

manner, reducing the risk of unauthorized access. Automation can streamline the process and minimize manual errors.

- Require MFA for externally exposed applications, remote network access, and administrative access. This can be enforced through a directory service or Single Sign-On provider.

By implementing these CIS Security Controls and related safeguards, organizations can effectively meet the requirements outlined in the EUSL Policy Provision related to the management and control of access rights.

These correlations demonstrate how existing CIS Security Controls can effectively address the policy provisions under different categories related to risk management, incident handling, and supply chain management in the context of space. Aligning policy provisions with CIS Controls helps organizations establish a robust security posture that accommodates all the phases of operations and compliance required by the policy.

5.1 Closing the gap: operational cybersecurity as a governance priority

One of the main goals of our research is to evaluate several policies and frameworks in the field of space cybersecurity to assess their effectiveness and identify any gaps. Additionally, we propose a methodology to connect cybersecurity requirements included in these policies to actionable items that companies can implement to ensure compliance and security in the space domain. We have observed that this approach has not yet been integrated into the lifecycle of European policies; however, other authors have emphasized the need for a more action-driven policymaking strategy.

In 2024, a consortium of over 25 aerospace cybersecurity experts, from academia, government, and industry, published a document titled: "*Minimum Requirements for Space System Cybersecurity: Ensuring Cyber Access to Space (75)*". The document was developed as a best-practice framework and influenced US policy on satellite cybersecurity, including the basis for provisions in the US Executive Order 14028 (86) and early IEEE P3349 standardization efforts [76]. The pool of experts argues that space systems require mission-specific and threat-informed cybersecurity baselines that go far beyond traditional IT security checklists. It proposes a practical framework of minimum cybersecurity requirements to protect space systems across all segments: spacecraft, ground infrastructure, link segments, and software.

The document stresses the importance of aligning cybersecurity requirements with mission-specific outcomes. The first step of the proposed methodology begins by identifying what must not be allowed to happen, for example, permanent loss of command and control, unauthorized access to payloads, or disruption of critical telemetry, and then defines the technical conditions and controls needed to prevent those outcomes. This is a fundamental shift from checkbox compliance to resilience oriented governance. In practice, this means that for each mission, the level of protection is tailored to the consequences of failure: high-risk government or defense missions must meet stricter minimums than academic CubeSats or short-lived test platforms. These categories are referred to in the document as Mission Risk Tiers.

The framework also breaks down cybersecurity requirements by segment, covering space assets, ground infrastructure, communications links, and software components. This segment-based model is particularly relevant in light of the cases discussed in Section 4.1.2. For instance, the Viasat incident showed how a vulnerability in the ground segment, not the satellite itself, can cascade into widespread disruption. The document anticipates this by including specific minimums for ground station security, such as encrypted command authentication, role-based access controls, and requirements for network segmentation. These are not abstract suggestions, but technically grounded control mechanisms that address exactly the kind of systemic vulnerabilities demonstrated in both real and simulated attacks.

The absence of such an approach in Europe is increasingly problematic. While ESA has released internal technical guidance and supported cross-national dialogues on cybersecurity, these efforts need binding force and are rarely tied to legal obligations or certification procedures. The anticipated EU Space Law may eventually introduce cybersecurity provisions, but in its current stage of development, it remains a strategic vision rather than an operational directive. There is, as yet, no indication that it will include risk-based technical mandates or harmonized requirements for lifecycle security engineering. In this vacuum, satellite operators are left either to overengineer protections at their own expense or to gamble on voluntary standards that may not be sufficient under pressure.

The Minimum Requirements for Space System Cybersecurity show what a governance model grounded in real system architecture looks like, offering policymakers the opportunity to adopt or adapt this framework as a technical backbone for upcoming legislation and regulatory guidelines.

In a policy space still dominated by declarative strategies and loose coordination, the need for operators is clarity. Space cybersecurity can be risk-based, technically specific, and enforceable, qualities often missing from Europe's developing governance model. If integrated early into the legislative process, it could help ensure that future European regulation moves beyond recognition of risk toward actual prevention.

6 Conclusions

In the first part of this paper, we discussed the approaches to space and cybersecurity governance in the USA, the UK, Germany, and the European Union. We described the approaches these countries have taken in terms of space cybersecurity, which agencies are involved, and what their roles are. We address the gaps in these approaches to provide advice to European policymakers when designing the EUSL. We emphasized the complexities of the domain and the necessary strategies for enhancing cybersecurity within the realm of space operations. We highlighted how the governance of space cybersecurity is still not well defined in most cases and call for a clear definition of roles, responsibilities, and agencies for ensuring and monitoring the resilience of the sector. We stressed the need for the definition at the European level of an entity in charge of the resilience of the space domain.

In the second section, we explored in detail the instruments the analyzed countries enacted to start providing binding or nonbinding frameworks for space cybersecurity. We highlighted how many of the current threats and trends are addressed, but still, no binding rule exists to date, leaving companies without clear obligations.

Our analysis underscored that despite the implementation of well-structured cybersecurity frameworks and protocols, their inherent limitation is their nonbinding nature often curtails their effectiveness. Hence, on one side, there is an urgent need for industry-wide acceptance and implementation of these practices to ensure higher standards of security, and for a higher instrument, namely a Regulation at the European level, to first harmonize and then enforce these frameworks.

The research highlighted the importance of incorporating attack trends and actors in new policies and frameworks. Specifically, vulnerabilities in the supply chain, user segment, unmanaged appliances, and terrestrial command and control systems should be considered. Also, the paper compared various cybersecurity frameworks, guides, and policies for the sector and emphasized the urgent need for harmonization, a common lexicon for TTPs, and the creation of common information-sharing practices for threat modeling and prediction.

Furthermore, we provided three main recommendations to European decision-makers in this historic moment where the EUSL is being designed: (i) we emphasized the need to define resilience and create quantitative indicators for its assessment; (ii) we stressed the importance of having effective security metrics that industries and institutions can use to verify and validate their security policies; and (iii) we pointed out how threat intelligence collection is useful but only partially successful if not linked to incident response capabilities.

Finally, we compared the cybersecurity requirements that may be part of the future EUSL and matched them with the Security Controls provided by the CIS. We emphasized how the industry needs actionable guidance and accurate instructions to secure its systems.

Despite addressing several gaps in current research, the present work can be further expanded. The comparative governance analysis should include nonwestern countries such as India and China, which are emerging as new space powers. Finally, future work will explore the individualization of security metrics for the domain to support companies and facilitate the assessment of their security and compliance with new requirements.

Author contributions

Francesco Casaril (Conceptualization [lead], Formal analysis [lead], Investigation [lead], Methodology [lead], Writing – original draft [equal]), and Letterio Galletta (Conceptualization [supporting], Writing – review & editing [lead]).

Conflict of interest : None declared.

Funding

This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union—NextGenerationEU.

References

1. Cyberinflight. Space cybersecurity market intelligence report. Toulouse, 2024. https://www.cyberinflight.com/?page_id=1764 (October 2024, date last accessed)
2. Department for Energy Security and Net Zero and Department for Business, Energy & Industrial Strategy. Civil nuclear cyber security strategy. London, 2022. https://www.gov.uk/government/publications/civilnuclear-cyber-security-strategy-2022(4 October 2024, date last accessed).
3. Cybersecurity Strategy. U.S. Department of Energy. 2024. https://www.energy.gov/cio/articles/doe-cybersecuritystrategy-2024(5 October 2024, date last accessed).
4. Sarri A, Fernandez Bascunana G, Gross A-K. *et al. Building Effective Governance Frameworks for the Implementation of National Cybersecurity Strategies*. Athens: ENISA, 2023.
5. Jiang W. Software defined satellite networks: a survey. *Digit Commun Netw* 2023;**9**:1243–64. https://doi.org/10.1016/j.dcan.2023.01.016
6. Cleverly G, Murray A, Mendler B. *The Evolution of Ground Stations in the New Space Industry*. Las Vegas, NV: ASCEND, 2021, 4042.
7. Montasari R. Cyber threats and the security risks they pose to national security: an assessment of cybersecurity policy in the United Kingdom. In: *Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policies*. Berlin: Springer, 2023.
8. Tarka M, Blankstein M, Schottel P. Empowering boards: how the National Cyber Security Centre Board (United Kingdom) toolkit is transforming cyber security governance. *Injury* 2023;**54**:110897.
9. UK Cabinet Office. Public Summary of Sector Security and Resilience Plans. London, 2018. https://assets.publishing.service.gov.uk/media/5c8a7845ed915d5c1456006a/20190215_PublicSummaryOfSectorSecurityAndResiliencePlans2018.pdf(4 October 2024, date last accessed).
10. UK Department for Science, Innovation and Technology. The Case for Space: Research and Analysis. London, 2023. https://www.gov.uk/government/publications/the-case-for-space(5 October 2024, date last accessed).
11. UK Cabinet Office. Written Evidence from the Cabinet Office. Science, Innovation and Technology Committee. London, 2023. https://committees.parliament.uk/writtenevidence/126643/html/cyber-resilience-of-the-UKs-Critical-National-Infrastructure-CNI(5 May 2024, date last accessed).
12. Committee, House of Commons Defence. Defence Space: through Adversity to the Stars?. London, 2022. https://committees.parliament.uk/publications/30320/documents/175331/default/(5 May 2024, date last accessed).
13. Government, UK. National Risk Register: 2023. London, 2023. https://assets.publishing.service.gov.uk/media/64ca1dfe19f5622669f3c1b1/2023_NATIONAL_RISK_REGISTER_NRR.pdf(5 April 2024, date last accessed).
14. Simmonds A. The Space Industry Regulations 2021: another giant leap?. *Covent Law J* 2021;**26**:654.
15. UK Parliament POSTNOTE. Defence of Space-Based Assets. London: Parliamentary Office of Science and Technology, 2024. https://researchbriefings.files.parliament.uk/documents/POST-PN-0654/POST-PN0654.pdf(5 October 2024, date last accessed).
16. Galbraith J. United States creates the US space command and the US Space Force to strengthen military capabilities in space. *Am J Int Law* 2020;**114**:323–6.
17. United States Government. Executive Order 14028: improving the Nation's Cybersecurity. Washington, DC, 2023. https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/information-technology-category/it-security/executive-order-14028(5 April 2024, date last accessed).
18. Agency, Department of Homeland Security Cybersecurity and Infrastructure Security. Budget Overview Fiscal Year 2024 Congressional Justification. Washington, DC, 2023. https://www.dhs.gov/sites/default/files/2023-03/CYBERSECURITY%20AND%20INFRASTRUCTURE%20S(4 February 2024, date last accessed).
19. Yonekura E, Dinicola SE, Mann S. *et al.* US Space Force personnel role distinctions. Arlington, VA: RAND Corporation, 2024.
20. Hutchins R. *Cyber Defense of Space Assets*. Medford, MA: Tufts School of Engineering, 2016, 1–18.
21. The White House, Trump PDJ (n.d.). President Donald J. Trump Is Establishing America's First Comprehensive Cybersecurity Policy for Space Systems. Washington, DC, 2022. http://irp.fas.org/offdocs/nspm/spd-5-fs.pdf(5 January 2024, date last accessed).
22. Cooper PJ. The Law: presidential memoranda and executive orders: of patchwork quilts, trump cards, and shell games. *Pres Stud Quat* 2001;**31**:126–41. https://doi.org/10.1111/j.0360-4918.2001.00160.x
23. Lieu M, Calvert M, Carbajal M, Fitzpatrick M. To Direct the Secretary of Homeland Security to Issue Guidance with Respect to Space Systems, Services, and Technology as Critical Infrastructure, and for Other Purposes, US Congress, House - Science, Space, and Technology. 2023.
24. Ellsworth JD. *We Have an Anomaly: America Is Missing a Space Systems Critical Infrastructure Sector*. Wild Blue Yonder, 2023.
25. CISA. National Defense Authorization Act Section 9002(b). 2021. United States, https://www.cisa.gov/sites/default/files/2023-01/Section_9002_NDAA_Report_FINAL_508c.pdf(5 January 2024, date last accessed).
26. The Hacker News. Spyware German Aerospace Center Cyber Espionage. Venice, CA, 2014. https://thehackernews.com/2014/04/Spyware-germanaerospace-center-cyber-espionage.html. (October 2024, date last accessed).
27. Paone M. Aerospace Clusters. World's Best Practice and Future Perspectives. An Opportunity for South Australia. San Francisco, CA: ACADEMIA, 2016.
28. Euroconsult. New Historic High for Government Space Spending, Mostly Driven by Defense Expenditures. Riyadh, 2022. https://www.euroconsult-ec.com/press-release/new-historic-high-for-government-space-spending-mostly-driven-by-defense-expenditures(October 2024, date last accessed)
29. Brzostek A. Germany's cybersecurity policy. *TKP* 2022;**15**:61–72. https://doi.org/10.32084/tkp.4793
30. Schmitz-Berndt S, Chiara PG. One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive. *Int Cybersecur Law Rev* 2022;**3**:289–311. https://doi.org/10.1365/s43439-022-00058-7
31. Vogel V, Ziegler N. Kritikalität: von der BSI-KritisV zur NIS2-Richtlinie. *Int Cybersecur Law Rev* 2023;**4**:1–19. https://doi.org/10.1365/s43439-022-00077-4
32. (BMWK), Federal Ministry for Economic Affairs and Climate Action. The German Federal Government's Space Strategy. 2023, Germany. https://www.bmwi.de/Redaktion/EN/Publikationen/Technologie/the-german-federal-governments-space-strategy.pdf?__blob=publi(4 January 2024, date last accessed).
33. Federal Office for Information Security. Technical Guidelines (BSI TR-03184). Bonn, 2023. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03184/BSI-TR-03184_part1.pdf?__blob=publicationFile&v=2(2 January 2024, date last accessed).
34. G DATA. Cybersicherheit in Zahlen. Bochum, 2022. https://www.gdata.de/fileadmin/web/de/documents/Studies/G_DATA_Cybersicherheit_in_Zahlen_2022.pdf(3 January 2024, date last accessed).

35. Satellite Cybersecurity Act. 118th Congress (2023–2024). 2023. https://www.congress.gov/bill/118th-congress/senate-bill/1425(4 May 2024, date last accessed).

36. UK Space Agency. Cyber Security Toolkit. Didcot, 2021. https://www.gov.uk/government/publications/cyber-security-toolkit(9 February 2021, date last accessed).

37. Civil Aviation Authority. Guidance on Cyber Security Strategies for Applicants and Licensees. London, 2023. https://www.caa.co.uk/publication/pid/11990(4 May 2024, date last accessed).

38. Humphreys B. The UK Civil Aviation Authority and European air services liberalisation. *J Transp Econ Pol* 1996;**30**:213–20.

39. Cilluffo FJ, Montgomery M, Cardash S. Time to designate space systems as critical infrastructure. United States. Cyberspace Solarium Commission, 2023. https://spacenews.com/time-to-designate-space-systems-as-critical-infrastructure/(5 May 2024, date last accessed).

40. Casaril F, Galletta L. Securing SatCom user segment: a study on cybersecurity challenges in view of IRIS2. *Comput Secur* 2024;**140**:103799.

41. NASA. Space Security: Best Practices Guide (BPG). Washington, DC, 2023. https://www.nasa.gov/general/nasa-issues-new-space-security-best-practices-guide/(3 October 2024, date last accessed).

42. IT-Grundschutz-Profil für das Bodensegment von Satelliten. Undesamt für Sicherheit in der Informationstechnik. 2024. https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Profil_Bodensegment-Satellit.pdf?_(5 January 2024, date last accessed).

43. ESA Security Office. ESA Cyber Security Resilience Achievement. Paris, 2023. https://esamultimedia.esa.int/docs/corporate/ESA_Cyber_Security_Resilience_Achievement.pdf(5 January 2024, date last accessed).

44. Orešković L, Grgić S. The new EU space regulation: one small step or one giant leap for the EU?. *Croat Yearbook Eur Law Pol* 2021;**17**:77–126.

45. Kallender PK. Waking up to a new threat: cyber threats and space. Transactions of the Japan Society for Aeronautical and Space Sciences. *Aerosp Technol Jpn* 2014;**12**:Tv_1–Tv_10.

46. ESA. QSVP—Quantum Security Verification Platform. ESA tender portal. 2024. Paris: European Space Agency. https://esastar-publication-ext.sso.esa.int/ESATenderActions/details/90340(14 December 2024, date last accessed).

47. Stafford VA. *Zero Trust Architecture*. Gaithernsburg MD: NIST, 2020.

48. Falco G. *An International Technical Standard for Commercial Space System Cybersecurity-A Call to Action*. Vol. **2022**. Las Vegas, NV: ASCEND, 2022, 4302.

49. Van Breukelen ED, Hamann RJ, Overbosch EG. Qualitative fault tree analysis applied as a design tool in a low cost satellite design: method and lessons learned. In: *Proceedings of STEC2006*. Noordwijk: ESA, 2006.

50. Yahia OB. Securing satellite link segment: a secure-by-component design. *arXiv* 2024.https://arxiv.org/abs/2411.12632. (October 2024, date last accessed).

51. Mailloux LO, Beach PM, Span MT. Examination of security design principles from NIST SP 800-160. In: *Proceedings of the 2018 Annual IEEE International Systems Conference (SysCon)*. Piscataway, NJ: IEEE, 2018.

52. UK National Security Center. Device Security Guidance. London, 2021. https://www.ncsc.gov.uk/collection/device-security-guidance(14 December 2024, date last accessed).

53. Wilmot J. Using CCSDS standards to reduce mission costs. In: *Proceedings of the Annual AIAA/USU Small Satellite Conference 2017. GSFC-E-DAA-TN44423*. Logan, Utah, USA: NASA, 2017.

54. Consultative Committee for Space Data Systems (CCSDS). Space Data Link Security Protocol (CCSDS 355.0-B-2). Blue Book, Issue 2. Washington, D.C., USA: CCSDS, 2022. https://public.ccsds.org/Pubs/355×0b2.pdf

55. Kazz G, Greenberg E. CCSDS Next Generation Space Link Protocol (NGSLP). In: *Proceedings of the SpaceOps 2014 Conference*. Pasadena, CA: American Institute of Aeronautics and Astronautics, 2014.

56. Masson L. Developing a CCSDS compliant platform to reliably secure current and future space data links. In: *Proceedings of the 2024 Security for Space Systems (3S)*. Piscataway, NJ: IEEE, 2024.

57. CCSDS Network Layer Security Adaptation Profile. CCSDS. https://public.ccsds.org/Pubs/356xb1.pdf(14 December 2024, date last accessed).

58. CCSDS Unified Space DATA link Protocol (USLP). CCSDS. 2024. https://public.ccsds.org/Pubs/732×1b3e1.pdf(14 December 2024, date last accessed).

59. The Application of Security to CCSDS Protocols. The application of security to CCSDS protocols 2019. https://public.ccsds.org/Pubs/350×0g3.pdf(14 December 2024, date last accessed).

60. European Commission. Commission Work Programme 2024. Brussels, 2024. https://commission.europa.eu/strategy-and-policy/strategy-documents/commission-work-programme/commission-work-programme-2024_en(3 September 2024, date last accessed).

61. DEFIS, European Commission DG. EUSL Baseline. Brussels, 2024. https://defence-industry-space.ec.europa.eu/document/download/43bfe8d3-032a-430f-b7fd-55753284d6c6_en?filename=Policy%20Options.pdf&prefLang=el(15 February 2024, date last accessed).

62. Jacobs B. Understanding the EU's competence to harmonise space law amid publication. *Delays Air Space Law* 2024;**49**:4–5.

63. European Commission. EU space strategy for security and defence. 2023. https://defence-industry-space.ec.europa.eu/eu-space/eu-space-strategy-security-and-defence_en(October 2024, date last accessed)

64. Weatherill S. The limits of legislative harmonization ten years after tobacco advertising: how the court's case law has become a "Drafting Guide". *Ger Law J* 2011;**12**:3827–64. https://doi.org/10.1017/S2071832200017120

65. Polish Presidency of the Council of the European Union. Programme of the Polish Presidency of the Council of the European Union: January 1–June 30, 2025. Brussels, 2024. https://polish-presidency.consilium.europa.eu/en/programme/programme-of-the-presidency/(14 December 2024, date last accessed).

66. Suhaimi NHS, Kamarudin NH, Khalid MNA. *et al.* State-of-the-art authentication measures in satellite communication networks: a comprehensive analysis. *IEEE Access* 2024;**12**:142241–64. https://doi.org/10.1109/ACCESS.2024.3467253

67. Wiatrek N, Burnett K, Lin SL. *et al.* Advancing spacecraft security through anomaly detection. In: *Proceedings of the 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*. Piscataway, NJ: IEEE, 2024.

68. Smailes J. Dishing out DoS: how to disable and secure the Starlink user terminal. *arXiv*. 2023. https://arxiv.org/abs/2303.00582.

69. Santamarta R. *A wake-up call for SATCOM security*. Seattle, WA: IO Active, 2014.

70. Thummala R, Falco G. *Hacktivism Goes Orbital: Investigating NB65's Breach of ROSCOSMOS*. Reston, VA: AIAA SCITECH 2024 Forum, 2024.

71. Carlo A, Obergfaell K. Cyber attacks on critical infrastructures and satellite communications. *Int J Crit Infrastruct Prot* 2024;**46**:100701. https://doi.org/10.1016/j.ijcip.2024.100701

72. Ieropoulos V. The impact of GPS interference in the Middle East. In: *Proceedings of the IEEE International Conference on Cyber Security and Resilience (CSR)*. Piscataway, NJ: IEEE, 2024.

73. Falco G, Thummala R, Kubadia A. Wannafly: an approach to satellite ransomware. In: *Proceedings of the IEEE 9th International Conference on Space Mission Challenges for Information Technology (SMC-IT)*. Piscataway, NJ: IEEE, 2023.

74. Corporation, Aerospace. *Resilience for Space Systems: Concepts, Tools and Approaches*. Chantilly, VA: AerospaceCorporation, 2017.

75. Falco G. Minimum requirements for space system cybersecurity-ensuring cyber access to space. In: *Proceedings of the IEEE 10th International Conference on Space Mission Challenges for Information Technology (SMC-IT)*. Piscataway, NJ: IEEE, 2024.

76. Vasen T. *Resiliency in Space as a Combined Challenge for NATO*. Kalkar: Joint Air Power Competence Centre, 2021.

77. Tortorelli A, Fiaschetti A, Giuseppi A. *et al.* A security metric for assessing the security level of critical infrastructures. *IJCCBS* 2020;**10**:74–94. https://doi.org/10.1504/IJCCBS.2020.108685

78. CrowdStrike. CrowdStrike 2024 Global Threat Report. https://go.crowdstrike.com/global-threat-report-2024.html?utm_campaign=brand&utm_content=crwd-brand-eur-bnlx-en-psp-x-2024. (October 2024, last accessed date).

79. Bisping R, Willbold J, Strohmeier M, Lenders V. Wireless signal injection attacks on VSAT satellite modems. Berkeley, CA: USENIX, 2024.

80. Goseva-Popstojanova K, Perhinschi A,. On the capability of static code analysis to detect security vulnerabilities. *Inf Softw Technol* 2015;**68**:18–33. https://doi.org/10.1016/j.infsof.2015.08.002

81. Boschetti N, Gordon NG, Falco G. *Space Cybersecurity Lessons Learned From the Viasat Cyberattack*. Las Vegas, NV: ASCEND, 2022, 4380.

82. Groš S. A critical view on CIS controls. In: *Proceedings of the 16th International Conference on Telecommunications (ConTEL)*. Piscataway, NJ: IEEE, 2021, 122–8.