IMT School for Advanced Studies, Lucca
Lucca, Italy

Space Cyber Risk: A Hybrid Analysis of Threats, Policies, and Governance

PhD Program in Cybersicurezza
Track in Software, System, and Infrastructure Security
XXXVIII Cycle

By

Francesco Casaril

2026

The dissertation of Francesco Casaril is approved.

PhD Program Coordinator: Mirco Tribastone, IMT School for Advanced Studies Lucca

Advisor: Prof. Letterio Galletta, IMT School for Advanced Studies Lucca

The dissertation of Francesco Casaril has been reviewed by:

Dr. P.J. Blount, Durham University

Prof. Dr. Kai-Uwe Schrogl, European Space Agency

IMT School for Advanced Studies Lucca
2026

Contents

List of Figures

List of Tables

Acknowledgements

Vita

December 20, 1998	Born, Rome, Italy
2020	Bachelor in Political Science Final mark: 101/110 Università degli Studi Roma Tre
2022	Master of Arts in International Studies Final mark: 110/110 Università degli Studi Roma Tre

Publications

1. Casaril, Francesco, and Letterio Galletta. "Securing SatCom user segment: A study on cybersecurity challenges in view of IRIS2." Computers & Security 140 (2024): 103799.
2. Casaril, Francesco, and Letterio Galletta. "Space cybersecurity governance: assessing policies and frameworks in view of the future European space legislation." Journal of Cybersecurity 11.1 (2025): tyaf013.
3. Tricco, G., Graham, T., and Casaril, F. "From Europe to Europa." Journal of AI Law and Regulation, vol. 2, no. 3, 2025, pp. 233–247
4. Casaril, Francesco, and Letterio Galletta. "Developing security metrics for space systems: A study considering the NIST Cybersecurity Framework 2.0 and the NIS2." International Journal of Critical Infrastructure Protection (2025): 100805.
5. Casaril, Francesco, and Letterio Galletta. "Assessing the Attack Surface of Space Organizations: A Data-Driven Analysis." Computers & Security (2026): 104848.

Presentations

1.

Abstract

Space systems support the operation of many critical infrastructures and are often considered critical infrastructure themselves. However, the cybersecurity of space remains poorly measured, inconsistently governed, and inadequately protected. This thesis investigates the gap between the actual cyber risk exposure of space-sector organisations and the governance frameworks designed to address it, combining technical analysis, empirical measurement, legal assessment, and comparative policy research.

The research first assesses the vulnerability landscape of satellite communication systems through a technical survey and the analysis of the 2022 Viasat KA-SAT attack, complemented by original reconnaissance of internet-exposed space assets using network scanning tools. The findings show that ground and user segment security is systematically neglected despite being the primary attack vector in documented incidents.

Building on this threat landscape, the thesis then evaluates the cybersecurity governance frameworks of the United States, United Kingdom, Germany, and the European Union, highlighting a consistent gap between regulatory ambition and operational effectiveness.

To support the measurement of security posture, a structured set of cybersecurity metrics is developed and validated for the space domain, mapping existing metrics against the NIST Cybersecurity Framework 2.0 and proposing new space-specific indicators introduced in a realistic satellite network architecture.

The Risk Exposure Framework is then introduced as a reproducible, data-driven methodology that quantifies the cyber exposure of space organisations by combining internet scanning data with vulnerability intelligence. Applied to eight major space organisations, it finds that approximately four percent of their combined internet-facing assets carry known, unpatched vulnerabilities, with risk concentrated in outdated web server stacks, legacy cryptographic libraries, and insufficient patch management.

Finally, a systematic discourse analysis of official policy documents from China, the United States, and the European Union reveals that the three actors operate from structurally incompatible governance models, producing divergent strategic postures and practices in space security that make international convergence unlikely in the near term.

The findings demonstrate that the space sector's attack surface is large, exposed, and exploitable, and that existing governance frameworks lack the technical specificity and enforcement capacity to produce measurable security outcomes. Creating a connection between technical vulnerability assessment and policy analysis, the thesis maps the actual threat landscape, assess whether current policy responses are adequate, and identifies what additional measures are needed to move from the recognition of risk to its meaningful reduction.

Chapter 1

Introduction

1.1 introduction

Space-based services, such as Satellite Communications (SATCOM), Earth Observation (EO), and global navigation satellite systems (GNSS) are now the backbone of essential civilian, commercial, and security functions. Space applications and services that were reserved for scientific and military use have become the connective tissue of everyday life.

Although deployed in orbit, the value of space systems is realised on Earth through terrestrial networks: satellites are operated from enterprise and public infrastructures, data is processed in cloud-based chains, and services are ultimately delivered to users via internet-connected terminals and software stacks. This ecosystem provides multiple benefits: disaster response, global connectivity, precision timing for finance, and optimised logistics, not to mention the many defence and military applications of space technologies. However, the more space systems are used and connected with multiple services and sectors, the broader the cyber attack surface extends across the ground segment, user equipment, and supply chains.

The stakes are not just abstract. On the morning Russia's army invaded Ukraine, a wiper malware named "AcidRain" disabled tens of thousands of satellite modems belonging to the Viasat KA-SAT network,

degrading command links for Ukrainian units and knocking out remote monitoring of 5.800 German wind turbines[81]. Governments in Europe and in the US later attributed the operation to Moscow and called the service loss "indiscriminate" [430]. In June 2024, the International Telecommunication Union received formal complaints from five European states detailing persistent GPS disruption and even the insertion of violent imagery into satellite television broadcasts [428].

These episodes are not isolated anomalies. Documented cyber operations against space assets predate 2022 and have become more frequent and more visible as the sector integrates cloud services, commercial off-the-shelf software, and internet-reachable ground components [60, 145].

At the same time, dependence on space is expanding at scale: estimates place the space economy at $630 billion in 2023, with projections reaching roughly $1.8 trillion by 2035, outpacing global GDP growth by about a factor of three [109, 560]. Launch cadence and on-orbit assets reflect the same trajectory: 2024 recorded more than 260 launches, and the active satellite population surpassed 8000 units [68]. Since 2015, venture capital has exceeded $60 billion, fuelling a diversified upstream–downstream ecosystem [73]. From an architecture point of view, the sector is shifting from being predominantly composed of satellites in Geostationary Orbit (GEO) to large LEO constellations that promise low latency and rapid revisit; forecasts suggest Low Earth Orbit (LEO) alone may host up to 60.000 active satellites by the early 2030s [388].

Growth increases both opportunity and exposure in equal measure, highlighting the need for effective and mature cybersecurity measures. Against this rapid growth, mounting dependency, and demonstrable adversary activity, this thesis addresses the problem of how space systems can be secured in practice. The research combines empirical measurement of vulnerabilities, comparative analysis of governance frameworks, and the development of prescriptive tools that connect legal frameworks with operational feasibility. The following section sets out the original contributions of the thesis, highlighting the advances it makes in the emerging field of space cybersecurity. Taken together, these contributions form an integrated research agenda spanning theory, evidence, and

policy.

This thesis makes four contributions to space cybersecurity research: (I) a structured conceptual framework, (II) original empirical analysis of cyber exposure in space systems, (III) an assessment of governance and regulatory implications,(IV) and methodological tools for cyber risk measurement. This Thesis, therefore, links theory, evidence, and policy, improving how cyber risks in space systems are understood and managed. These contributions are set out below and address four distinct aspects of space cybersecurity.

1. Reframing space as critical infrastructure.

   This work demonstrates that space is no longer an isolated technological domain but the backbone of modern critical infrastructures, supporting essential civilian, commercial, and security functions. Analysing space technologies and their applications, our research exposes systemic weaknesses that can cascade into failures across dependent sectors. This enriches academic debates on critical infrastructure by showing the socio-technical interdependence of space systems, also providing operators with a clearer understanding of where vulnerabilities originate and how they propagate.

2. Advancing comparative governance analysis.

   The thesis systematically compares how different countries and jurisdictions govern space cybersecurity, assessing the state, scope, and binding force of applicable requirements. It maps responsibilities, regulatory instruments, coordination mechanisms, and relevant standards and best practices, and compares them against the evolving threat landscape affecting space systems. With a particular focus on the European Union, the analysis examines how legal and policy requirements translate into operational and actionable measures for industry, evaluating their practical impact and compliance implications. This includes an assessment of the EU cybersecurity framework, the forthcoming EU Space Act, and the application of the AI Act to space-based systems.

3. Designing prescriptive and operational metrics.

   Recognising that governance requires measurable benchmarks, this thesis develops a framework of cybersecurity metrics specifically tailored to space systems. These metrics link regulatory compliance to observable technical indicators in satellite operations and ground infrastructures. Through mapping to the NIST Cybersecurity Framework 2.0 and the NIS2 Directive, the research identifies critical blind spots in current measurement practices and proposes new indicators to address them. The thesis bridges the regulatory frameworks with technical feasibility and demonstrates through a Proof of Concept (PoC) tool how metrics can support compliance assessment and continuous improvement in operational settings.

4. Quantifying cyber exposure empirically.

   To ground these normative and technical insights in the real world, the thesis introduces a data-driven methodology for measuring the attack surface of space organisations. We correlate exposed IPs, known vulnerabilities, their severity, and exploit availability into a composite risk score, developing a quantitative assessment of cyber exposure in the space sector, showing how adversaries can observe and exploit real-world weaknesses. In doing so, we enrich the empirical literature and demonstrate how technical observables can be translated into governance-relevant insights, informing both regulatory design and organisational defence priorities.

In summary, the thesis combines conceptual analysis, governance comparison, empirical measurement, and risk metrics in one study. These elements link legal and policy requirements to concrete technical conditions in space systems.

1.2 Background

The cybersecurity of space systems has emerged as a concrete operational and policy problem rather than a purely theoretical concern. Space

infrastructures rely now on standard digital technologies, software-defined components, and internet-connected ground and user segments. The expanded attack surface that these evolutions have caused exposes space to many of the same threats that affect terrestrial information systems, while retaining constraints that make mitigation more difficult, such as long hardware lifecycles, limited physical access, and complex international ownership structures.

Empirical evidence shows that cyber incidents affecting space-related infrastructure are no longer isolated events. Beyond individual incidents, several analyses suggest that cyber operations targeting space infrastructure are increasing in frequency and diversity. Recent studies identified more than two hundred cyber operations targeting space-related assets between early 2023 and mid-2025, with notable spikes corresponding to periods of geopolitical tension [412].

At the same time, official reporting mechanisms provide only limited visibility. The European Repository of Cyber Incidents records very few space-related cases each year, suggesting that underreporting or inconsistent classification remains a significant issue [205].

Technical exposure is amplified by the characteristics of space systems themselves. Many operational satellites were designed and launched before cybersecurity became a core design requirement. A substantial number of satellites currently in orbit predate modern encryption standards and secure update mechanisms, yet remain operational due to the high cost of replacement and the longevity of space hardware [451].

On the ground, satellite control networks and user terminals often rely on commercial off-the-shelf components and standard internet protocols. Research has shown that misconfigured or unpatched satellite communication devices can be identified remotely and, in some cases, exploited without sophisticated capabilities [441].

Despite these observable risks, systematic data on the cybersecurity posture of space organisations remains scarce. Unlike sectors such as finance or energy, the space sector lacks mature mechanisms for mandatory incident reporting, shared vulnerability databases, or common metrics for assessing exposure. Information sharing initiatives exist, but par-

ticipation is largely voluntary and uneven.

A second gap concerns the relationship between cybersecurity risk and governance frameworks. International space law provides little guidance on cybersecurity, and existing treaties do not address digital threats or responsibilities in cyberspace. No binding international rules explicitly govern cyber activities in space, leaving a void of clear norms and obligations for protecting space assets against hacking. In practice, this void has been filled patchily by national policies and ad-hoc guidelines, leading to a fragmented governance landscape. Different jurisdictions impose different (or no) cybersecurity requirements on satellite operators, resulting in uneven standards. Within the European Union, cybersecurity obligations relevant to space activities have emerged indirectly through broader digital and infrastructure legislation, but a binding framework addressing the entire space sector is still not in force.

Addressing these gaps is important for both practical and strategic reasons. Space systems support services that are deeply embedded in everyday activities, including navigation, communications, emergency response, and financial timing. A study commissioned by the UK government estimated that a multi-day disruption of satellite navigation services could result in economic losses of several billion pounds [498].

Addressing the identified gaps is also crucial for stakeholder confidence and strategic autonomy. For the private sector, improving cyber resilience in space assets is key to protecting huge investments and maintaining service reliability for customers. For policymakers, closing the governance gaps is important to align regulation with risk – ensuring that as reliance on space grows, laws and standards keep pace to prevent worst-case scenarios. There is also an equity and humanitarian dimension: many remote or developing regions rely on satellites. If these systems are not secure, the most vulnerable communities could lose lifeline services during crises.

The significance of this research lies in the risks of inaction. Failing to improve empirical insight into space cybersecurity means accepting potentially catastrophic threats; failing to improve governance means leaving a critical domain inadequately protected by the rule of law. Con-

versely, addressing these gaps paves the way for a more secure and sustainable space environment, which benefits all who rely on or venture into this final frontier. It ensures that space can continue to enable innovation and connectivity without becoming a new Wild West of unchecked cyber dangers.

1.3 Outline of the Thesis

Following the main themes described above, this thesis comprises seven main chapters that present published contributions in peer-reviewed journals and reviewed journals, along with additional content added to complement and update them.

- **Chapter 2** of the thesis is developed from the paper: *"Space Infrastructure as Critical Infrastructure: Rights Beyond Earth in the Digital Age"[83]*. In this chapter we discuss the relevance of space applications such as EO and GNSS for modern society and we highlight their contributions not only to technological advancements but also human rights protection, finally emphasizing the potential consequences of a disruption to space systems

- **Chapter 3** is adapted from the paper *"Securing the SATCOM user segment, a multidisciplinary study in view of IRIS²[81]"*. In this chapter, we go deeper into assessing the vulnerabilities in the ground and user segment of satellite communication infrastructure. In particular, we discuss the Viasat K-SAT attack and take some of the main challenges as lessons learned for IRIS², the satellite communication constellation that the European Union is planning to build. In this chapter, we also look at some managerial implications of implementing cybersecurity features in satellite networks, as well as the state of the art of cybersecurity standards for space.

- **Chapter 4** explores the broader policy dimension of space cybersecurity and builds primarily on the paper: *"Space Cybersecurity Governance: Assessing Policies and Frameworks in View of the Future Eu-*

ropean Space Legislation" [82] This chapter lays the basis for a comparative analysis of cybersecurity policies and governance structures in four countries: the United Kingdom, Germany, the United States, and Japan. The chapter reviews the current state of both soft and hard law in these jurisdictions, and maps the institutional responsibilities for protecting space infrastructure and networks. The chapter also focuses on the European Union legal framework, examining the current state of cybersecurity governance as well as recent legislative developments in the field, their applicability. and effectiveness.

- **Chapter 5** dervis from the paper: *"From Europe to Europa: Implications of the European AI Act for the Space Industry."[501]* and addresses the intersection between space and artificial intelligence, analysing the implications of the AI Act for the space industry—especially in light of the potential classification of space-based AI systems as "high-risk" under the regulation.

- **Chapter 6** builds on the article *"Developing Security Metrics for Space Systems: A Study Considering the NIST Cybersecurity Framework 2.0 and the NIS2 [79]"*. This chapter takes the assumptions established in the previous chapters, namely: the strategic importance of space infrastructure and its exposure to growing cyber threats, and translates them into a practical framework for risk measurement.To do so, the chapter surveys existing cybersecurity metrics from academic and professional sources and maps them to the functions, categories, and subcategories of the NIST Cybersecurity Framework 2.0. This analysis highlights significant gaps in how security is measured, and proposes new, space-relevant metrics to address these shortcomings. The chapter emphasizes how metrics can help organizations not only measure their cybersecurity posture, but also demonstrate compliance with regulations like the NIS2 Directive and the forthcoming EU space-specific rules. To support practical application, the chapter also introduces a proof-of-concept tool developed to facilitate the measurement of these metrics in opera-

tional settings. The tool is demonstrated through a detailed case study of a fictional satellite communications operator, modeled on real-world architectures.

- **Chapter 7** adopts a more technical approach to the issue of space cybersecurity and builds on the findings presented in the paper *"Assessing the Attack Surface of Space Organizations: A Data-Driven Analysis[77]"*. This chapter operationalizes many of the insights developed in earlier parts of the thesis by introducing a quantitative methodology to assess the cyber exposure of space organizations, focusing on internet-facing systems. Using open-source data and publicly accessible scanning platforms, the chapter defines and implements a framework for calculating the cyber risk associated with digital assets linked to actors in the space sector. The methodology correlates four key variables: (1) the number of publicly exposed IP addresses associated with a given organization, (2) the presence of known vulnerabilities (CVEs) on those systems, (3) the severity of those vulnerabilities using CVSS scores, and (4) the availability of known exploits linked to those CVEs. These indicators are combined to produce a composite risk score that reflects both the attack surface and the likelihood of successful exploitation.

- **Chapter 8** builds on the article "Competing Visions, Diverging Trajectories: A Comparative Study of Space Security from Discourse to Practice in China, the US, and the EU", submitted for publication, and constitutes the final analytical chapter of the thesis. This chapter represents a systematic comparative examination of how the three space actors conceptualise and govern space security across strategic, regulatory, military, and economic dimensions. Drawing on a coded corpus of official documents published between 1995 and 2025, the chapter develops and applies a technopolitical framework structured around three analytical steps: framing, materialisation, and institutionalisation. This framework enables tracing how political narratives about space are translated into concrete technological priorities, organisational arrangements,

and regulatory architectures. The central argument is that differences in space-security outcomes are not explained solely by material capabilities or technological sophistication, but by distinct governance models shaped by political institutions, threat perceptions, strategic culture, and state–market relations. The chapter identifies three ideal-typical models of space governance: a command-and-deterrence model in the United States, centred on military integration and freedom of action; a developmental and strategic-control model in China, combining state-led industrial expansion with strong political oversight; and a multilevel regulatory and norms-oriented model in the European Union, grounded in risk management, legal harmonisation, and institutional coordination. It further extends the comparison to the cyber dimension of space systems, analysing how each actor structures authority, threat models, technological priorities, and economic incentives in the field of space cybersecurity. This chapter presents a longitudinal and systematically coded comparison of the three space powers. It advances a process-oriented technopolitical framework that connects strategic studies, technology governance, and political economy. The chapter clarifies how divergent governance logics shape resilience, regulation, military integration, and market structures in the space domain, offering a coherent lens for understanding contemporary competition and cooperation in space.

The main findings of the four chapters are summarized in the conclusions in Chapter 9, where we highlight the main findings and takeaways of the thesis.

Chapter 2

The space domain and its cybersecurity implications

This chapter is adapted from the paper *Space Infrastructure as Critical Infrastructure: Rights Beyond Earth in the Digital Age[83]*, and aims to: (i) present space *use cases* as societal enablers, and (ii) trace how disruptions to space-enabled services propagate into terrestrial critical functions on which public safety, public health, and the delivery of emergency services depend. The goal is to understand the critical value space applications play in our modern societies and how potential disruptions can cause not only financial damages, but the loss of human lives. Compared to the subsequent chapters, this chapter adopts a non-technical perspective on cybersecurity and serves primarily to provide a high-level overview of why space systems are societally relevant and how deeply space-enabled services are embedded in everyday life and critical societal functions. In this chapter, we also mention Union policy instruments and their role in this framework (e.g., NIS2, CER, IRIS^2), but a more detailed legal analysis is deferred to Chapter 4 of this thesis.

2.1 Introduction

With the increasing diffusion of Information and Communication Technologies (ICTs), access to the internet has become increasingly necessary for society. ICT networks allow communication between people, governments, and companies located in any corner of the globe. Societies and communities thrive on the opportunities offered by digital connectivity, and businesses can significantly grow by accessing cross-border opportunities. In addition, different aspects of governmental services are being digitalized, requiring citizens to be connected to the web.

The digital world no longer ends at the edge of a fiber-optic cable. Every day, pictures, voice calls, and emergency signals jump from ground networks to satellites and back again. Satellites guide firefighters toward a spreading blaze, keep field hospitals online after a storm, and give remote communities access to the internet. In other words, space systems have quietly become things we rely on without thinking, much like electricity or clean water.

But the more we lean on these systems, the more we need them to be resilient against hybrid threats such as cyber-attacks. A well-aimed cyberattack on a single satellite link can scramble GNSS receivers, jam rescue radios, or cut broadband to an entire region. If that happens, people's safety, their right to information, even the health of the environment can be put on the line. In Europe, the NIS 2 Directive [169] and the Critical Entities Resilience Directive [202] now list space among the sectors covered by general resilience and cybersecurity regimes, bringing certain ground-segment operators within their scope; the precise reach of these instruments is examined in Chapter 4." The question is whether those rules are strong, and specific, enough to keep this space-enabled world safe.

This chapter aims to address the following research questions:

- How does the growing reliance on space technologies impact the protection of fundamental rights such as the right to life, health, and access to information?

- What are the risks posed by cyberattacks to space infrastructure, and how might such attacks undermine human security and emergency response operations?

- To what extent do existing legal and policy frameworks (e.g., NIS 2, Critical Entities Resilience Directive) adequately classify and protect space infrastructure as critical digital infrastructure?

To address these research questions, Section 2.2 presents the methodological framework adopted, grounded in EU law and focused on the intersection of resilience and security. Section 2.3 examines how modern space networks have become essential infrastructure, supporting several critical services on which we rely. Section 2.4 analyses two major applications: Earth Observation and Global Navigation Satellite Systems, as enablers of rights protection, illustrating through case studies how these systems support emergency management, food security, and public safety, while also introducing governance and privacy challenges. Section 2.5 explores the vulnerabilities of these infrastructures to cyber threats and their humanitarian consequences, linking technical failures to rights impacts. Sections 2.6 then assess how current and emerging EU legal frameworks, namely the NIS2 Directive, and the Critical Entities Resilience Directive address the classification, protection, and governance of space infrastructure as critical digital infrastructure. Section 2.7 synthesises the findings, demonstrating that the resilience of space systems is now inseparable from the protection of critical functions that support fundamental rights and proposing policy principles for a secure and rights-based space governance.

For this chapter, space systems are understood as the combination of space-based and ground-based components that enable the operation of services delivered through space infrastructure. They typically include spacecraft, ground control and mission operations centres, user terminals, and data processing or distribution facilities. This definition is consistent with the one adopted by the International Telecommunication Union, which refers to a space system as "any group of associated space objects, one or more of which are capable of providing space radiocom-

munication or other space functions, together with the associated ground segment ".

2.2 Methodological Framework

This chapter employs a qualitative, cross-sectoral legal-policy analysis that is grounded in the European Union's fundamental-rights framework. It examines how selected space-based services, such as EO and GNSS, contribute to the realisation of rights whose enjoyment increasingly depends on the continuity of digital and space infrastructure. These two services were chosen as they represent some of the most direct technological interfaces between space systems and human security: EO enables disaster preparedness, environmental protection, and public-health monitoring; GNSS supports emergency response, transport safety, food security, and the timing of critical services.

The analysis focuses on the Directive (EU) 2022/2555 (NIS2)[169] and the Directive (EU) 2022/2557 (CER)[202] as some of the most recent EU legislative instruments that explicitly recognise space as part of Europe's critical-infrastructure architecture and establish binding cybersecurity and resilience duties for operators. Concerning fundamental rights, the normative reference is the Charter of Fundamental Rights of the European Union [201], notably Articles 2 (right to life), 3 (integrity of the person), 6 (liberty and security), 11 (freedom of information), 35 (health care), and 37 (environmental protection), and the international right to adequate food and standard of living under Article 11 of the International Covenant on Economic, Social and Cultural Rights [524]. These rights are central but not exhaustive; they illustrate how the resilience of space infrastructure under EU law enhances the protection of fundamental human interests.

The methodological framework adopted traces the connections between governance instruments, critical-infrastructure obligations, and the protection of fundamental rights in the European legal order, providing a basis for comparative and future policy research on space resilience and human security.

2.3 Space Infrastructure in the Digital Age

Space systems played an important role from a geopolitical and technological perspective since the Cold War, where the space race between the USSR and the USA accelerated the development of space technologies. From that time, space systems have been used for various purposes: ensuring communications, distributing TV signals, observing the Earth, conducting reconnaissance, and developing navigation, positioning, and timing (NPT) infrastructures.

In the last century, space systems were mostly launched in geostationary orbit (GEO) to cover the whole surface of the Earth with one or a few satellites. They were costly, ambitious, and long-term projects. However, while such systems could offer important services, their latency was high, given the distance from Earth's surface (roughly 36,000 km). For these reasons, such systems were mostly used for specific applications and could not achieve ubiquitous use. Today, although GEO remains a cornerstone of space operations, attention has pivoted toward low-Earth-orbit (LEO) constellations.

Four interrelated factors lies behind this transition. First, access to orbit has broadened substantially: average launch costs have fallen over the past two decades, while the annual number of launches increased by more than 50% per year between 2019 and 2023, a trend likely to accelerate with reusable launchers [499]. Second, advances in component design and software-defined payloads have enabled small satellites to perform missions that previously required significantly larger payloads. Third, private investors committed more than 70 billion USD to space ventures during 2021–2022 [560], expanding the industrial base and accelerating innovation. Finally, demand is growing: LEO constellations are projected to lower wholesale data prices by about 10% between 2023 and 2035, even as global bandwidth demand rises by about 60%.

Together, these shifts have made space systems economically accessible and deeply integrated into terrestrial value chains. LEO offers low latency, resembling terrestrial connectivity metrics. Commercial SATCOM providers offer connections with latency between 20 and 40 ms [291]. In

terms of capacity, they can provide better performance than GEO satellites, though still below submarine cables. Constellations such as Starlink are now acquiring consistent portions of the market and consist of approximately 6,000 satellites, with plans to expand to 42,000 by 2035 [363][133].

Such systems can offer connectivity in rural areas and act as relays for traditional communication services that fail to provide access. A UK programme in 2024 deployed hybrid, multi-orbit terminals combining LEO and GEO capacity to feed local 5G/6G or Wi-Fi cells [522]. The objective was to bring gigabit-class broadband to communities where terrestrial backhaul is uneconomic, and to create portable networks-of-last-resort for emergencies.

Mega-constellations also enable continuous, high-resolution Earth observation (EO), supporting humanitarian and social initiatives such as hazard prediction, early warning, and property protection. With satellites becoming integral to digital society, interruptions to their functioning can breach rights to internet access, privacy, and environmental protection.

2.4 Earth Observation and GNSS as a Tool for Rights Protection

Given the expected number of launches in the next decade, the role of satellites in modern emergency response and disaster management will only increase. This section focuses on EO and GNSS as tools for protecting the environment and fundamental rights.

2.4.1 The role of Earth Observation in disaster management and emergency response

With escalating climate risks, EO satellites provide comprehensive, near-real-time data essential for environmental monitoring and disaster management [117]. Optical and radar sensors track climate indicators, inform

models, and support mitigation strategies, which makes EO data increasingly recognised as a global public good.

EO is not only a source of scientific data but an operational tool for disaster governance. After Hurricane Matthew in 2016, the Haiti Recovery Observatory used high-resolution satellite imagery to prioritise reconstruction needs rather than relying solely on on-the-ground surveys [86]. Following the February 2023 earthquake in Türkiye and Syria, the International Charter "*Space and Major Disasters*" provided imagery from satellites such as Pléiades Neo at 30 cm resolution, enabling search-and-rescue teams to allocate resources and humanitarian aid more effectively [297, 410]. These cases illustrate how EO is embedded in time-critical decision-making, and without reliable access, response coordination would be significantly degraded.

The International Charter, created in 2000 by space agencies and operators, provides a mechanism for rapid, free access to EO data during disasters. It has been activated over 800 times—more than 400 for floods—making it a central part of global emergency response infrastructure. In parallel, the Copernicus Emergency Management Service (EMS), operated by the European Commission, delivers standardised rapid-mapping products to EU Member States and international partners. Copernicus EMS is increasingly relied upon for acute events such as earthquakes and wildfires, and also for risk assessments and recovery planning [116]. Both mechanisms institutionalise the link between satellite operators, civil protection agencies, and humanitarian actors.

This institutionalisation sharpens the security stakes. If EO data flows were disrupted, whether by commercial restrictions, state interference, or cyberattacks on satellite operators and ground stations, the consequences would go beyond technical inconvenience. The reliability of humanitarian relief, the protection of affected populations, and the enforcement of human rights in crises would be directly compromised. In this sense, EO is a strategic dependency whose cyber resilience is now inseparable from environmental and human security.

2.4.2 GNSS as a Human-Rights Enabler

GNSS provides position, navigation, and timing (PNT) services that are foundational to the functioning of modern societies. Beyond personal navigation, PNT signals regulate high-frequency trading platforms, synchronise 5G networks, and support energy grid management by coordinating frequency across geographically dispersed nodes [282]. In civil aviation, GNSS enables Required Navigation Performance (RNP) and allows aircrafts to land safely in low-visibility conditions. Road transport relies on GNSS for fleet management and congestion monitoring, and agriculture uses GNSS signals for precision farming, reducing fuel use and chemical inputs while improving yields [409]. Maritime and inland waterways depend on GNSS for collision avoidance, port operations, and compliance with emissions routing requirements. But GNSS is not only used by various industries; the humanitarian value is equally significant: the Advanced Mobile Location (AML) system, mandated in the EU for emergency calls, uses GNSS to locate callers with an accuracy of a few metres, accelerating dispatch and saving thousands of lives annually [53].

Despite this centrality, GNSS remains highly vulnerable. Signals are extremely weak by the time they reach Earth and can be jammed or spoofed with relatively inexpensive equipment. Several documented incidents highlight the scale of the problem. Between 2010 and 2013, deliberate jamming around Newark Airport forced the Federal Aviation Administration to suspend tests of GPS-based landing systems after interference was traced to a truck driver using a $30 jammer to hide from his employer's tracking device [230]. In 2013, researchers demonstrated the spoofing of a 210-foot yacht in the Mediterranean, gradually misleading its navigation system without triggering alarms [51]. Civil aviation has also been affected: Eurocontrol reported more than 3,500 cases of GPS interference in 2018 across European airspace, with hotspots in the Eastern Mediterranean and Black Sea regions [188]. During the Russian invasion of Ukraine, GNSS disruption and spoofing were recorded at large scale, affecting not only military operations but also civil aviation routes over

Poland, Finland, and the Baltic states [310].

Economic assessments confirm the scale of potential loss. A seven-day outage in the UK alone would cost £7.6 billion, disrupting logistics, financial transactions, and emergency services [498] that would be hit the hardest. Emergency services, in fact capture the biggest share of GNSS benefits in the UK, and when GNSS goes down, most of the damage falls on emergency, maritime, and road—together nearly 88% of total losses in a seven-day outage (about £7.64 bn overall). Emergency services alone account for roughly £3.53 bn of that.

Two main factors are behind these numbers. First, the caller's location. Without GNSS, phones fall back to rough cell-ID, calls take longer, and some never get through. London Economics estimates about 19,000 unanswered emergency calls in a week, with a loss valued at around £1.46 bn just from that effect. Second, dispatch. Losing vehicle/personnel tracking slows response, it is estimated +2 minutes for police and fire and +4 minutes for ambulances, which accounts to around £1.97 bn for the week. This means slower rescues and people who don't get help in time. That touches rights to life, health, and timely access to essential services.

From a governance perspective, the EU recognises GNSS as part of its critical entities under the NIS2 Directive and the Critical Entities Resilience (CER) Directive. Yet regulation does not mandate specific technical redundancies. With PNT more deeply embedded into civil aviation, finance, telecoms, and emergency response, cybersecurity and signal protection are prerequisites for the continuity of rights recognised under EU law, including life, health, access to essential services, and an adequate standard of living.

2.5 The Vulnerability of Space Infrastructure: Cybersecurity Risks and Humanitarian Consequences

The Haiti and Türkiye/Syria case studies have shown how EO supports disaster response and post-crisis recovery. Space technology can provide

time-sensitive data that helps rescue teams locate survivors, assess damage, monitor displaced populations, and plan long-term reconstruction. EO systems operate as lifelines upholding fundamental rights, including the rights to life, health, and access to essential services. Yet, the very digital infrastructure enabling this life-saving functionality is increasingly exposed to cyber threats.

Space operations depend on intricate digital systems, ground control stations, data reception facilities, and cloud-based processing platforms [469]. They are part of vast, sophisticated supply chains, which increase vulnerability to cyberattacks. The growing integration of space technology with terrestrial applications has led to a rise in the number of attacks. Even a relatively simple cyberattack could have significant consequences, especially if it occurs during a humanitarian emergency.

The following scenarios introduced in this section are fictional constructs; their purpose is to demonstrate how a cyber incident affecting orbital and terrestrial components of space infrastructure could affect other critical sectors and impact fundamental rights. They are used to trace causal and regulatory relationships under existing EU resilience frameworks. This qualitative scenario method is useful to visualise interdependence and legal responsibility; however, it carries inherent limitations. Fictional cases cannot be empirically validated, their assumptions may not generalise across technologies or jurisdictions, and they simplify the complexity of cascading effects. The scenarios are presented as illustrative thought experiments whose purpose is to test whether current governance instruments, particularly NIS2 and CER, are adequate to prevent or mitigate comparable real-world incidents.

In the first case, we examine a ransomware attack on Earth Observation ground infrastructure. This highlights that space, despite being a complex and unique critical infrastructure, is not immune to other types of attacks that affect other "legacy" sectors. Particularly when we consider the ground network, it resembles similar IT infrastructures such as those of telecommunication networks.

Let's consider that in the immediate aftermath of a major natural disaster, such as a cyclone or earthquake, the International Charter "Space

and Major Disasters" is activated. Dozens of satellites are tasked to collect imagery of the affected areas, and rapid mapping services are mobilized to guide emergency responders. However, just as data from satellites begins to stream toward national authorities, a ransomware attack disables a key ground station responsible for processing and distributing the imagery.

Within minutes, emergency mapping systems go offline. Rescue teams lose access to geospatial data identifying collapsed buildings, blocked roads, or isolated communities. Vital hours are lost, not because of a lack of satellite coverage, but because the digital pipeline that delivers the data is compromised.

In this scenario, a cyberattack does not merely interrupt a technical process, but also directly endangers lives. The denial of access to EO data means a denial of essential information for delivering medical care, evacuating vulnerable populations, or distributing food and water.

Moving toward GNSS technologies, a targeted cyber-attack on GNSS, whether by jamming or spoofing, would immediately erode the capabilities described in Section 4.2. In a jamming scenario, first-responders would revert to manual location-finding techniques, adding an estimated 2–3 minutes per dispatch and potentially increasing preventable mortality in mass-casualty events. Loss of continuous AIS tracking during a spoofing attack would force search-and-rescue teams to rely on slow radar sweeps, delaying aid to mariners in distress. In the context of agriculture, GNSS signal manipulation would disrupt precision-farming equipment, such as seeding, fertilisation, and irrigation, leading to crop failures, resource waste, and volatile food prices that disproportionately harm vulnerable communities.

These scenarios highlight a pressing challenge: satellite systems must be recognized and protected as critical digital infrastructure. The security of the ecosystem is not only a matter of national interest or technological resilience; it is a matter of global solidarity and human rights protection.

Securing these systems involves multiple layers: reinforcing the cybersecurity of ground stations, ensuring the integrity of space data through-

out the processing chain, building redundancy protocols for crisis operations, and fostering transparency in how information is collected and used. This also requires stronger legal and institutional frameworks to ensure that space capabilities can withstand cyber threats and continue to serve their humanitarian mission.

While fictional, the scenarios reflect documented patterns of real cyber incidents targeting space-based systems and their terrestrial interfaces. We mentioned in the Introduction of this thesis how, the Viasat KA-SAT[537] attack disabled tens of thousands of satellite modems and caused connectivity loss for Ukrainian institutions and thousands of European energy assets, showing how a single supply-chain breach can cascade into critical-infrastructure disruption. A similar incident affected the Dozor-Teleport (June 2023)[556], which was temporarily paralysed, hindering Russian governmental communications. The attack illustrates the strategic consequences of attacking commercial SATCOM providers.

A relevant attacks on Earth-observation systems, is represented by the 2014 NOAA (National Oceanic and Atmospheric Administration) intrusion [372]. The breach forced NOAA to shut down certain data services for emergency maintenance, cutting off data vital to disaster planning, aviation, shipping and other crucial uses. For about two days, satellite data distribution was offline, which skewed weather forecasts slightly and impeded the flow of environmental information until systems were restored. Had the outage persisted, it could have seriously hampered storm tracking, hazard warnings, and climate monitoring, exactly the kind of disruption the fictional scenario envisions for disaster-response data.

GNSS spoofing incidents are amongst the most reported in recent times; data from the Baltic Sea and Nordic region illustrate a growing pattern of GNSS interference attributed to Russian jamming and spoofing, which has directly impacted commercial aviation, marine navigation and timing-dependent functions. According to Swedish aviation authorities, spoofing and jamming over eastern airspace have affected both air and sea traffic [489]. The impacts of spoofing in the region are exponentially increasing; nearly 123,000 flights were disrupted in early 2025 due

to GPS signal interference [542][183].

All these examples reinforce the scenario modelling in this section and call for governance frameworks that link space-system resilience with the protection of fundamental rights. Given the real-world scenarios, the fictional cases discussed in this chapter are plausible representations of existing threat patterns and thereby reinforce the legal and policy analysis that follows.

The incidents and scenarios discussed above demonstrate that satellite networks are now integral to the broader digital-infrastructure ecosystems. Their disruption, whether through cyberattack, interference, or cascading failure, produces effects similar to those of terrestrial digital assets. Space infrastructure forms a subset of critical digital infrastructure, extending the surface of risk and the scope of resilience obligations addressed by instruments such as NIS2 and CER. Safeguarding this ecosystem is not solely a technical or national-security concern: it is directly tied to the continuity of rights-relevant services, such as navigation for rescue operations, connectivity for hospitals, and data for environmental protection, whose interruption endangers the rights to life, health, and security. Protecting space infrastructure, therefore, advances resilience, but also human-rights protection through the continuity of essential services.

The following section discusses the classification of space as a critical infrastructure sector under EU Law, what it entails, and whether this classification is enough to guarantee the resilience of space and the services it provides.

2.6 Toward Secure Space Governance

The empirical cases discussed in the preceding sections show that disruptions of space-enabled services translate into operational consequences for emergency response, civil aviation, maritime safety, energy timing and other critical terrestrial functions. This section asks a narrower question: to what extent does the Union's general cybersecurity instruments, such as the NIS2[169],and CER [170] already engage with the entities that

provide those services, and what do they actually require of them? The fuller comparative and instrument-by-instrument analysis is developed in Chapter 4; the purpose here is to identify, what duties currently attach to in-scope space-sector entities and where the directive's text leaves gaps that the case material exposes.

NIS2 lists "Space" in Annex I among its sectors of high criticality. The entity type identified in that Annex is, however, deliberately restricted: "*Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services*." Read with Article 2 and the size thresholds in Commission Recommendation 2003/361/EC [102], this brings within scope the operators of teleports, gateway stations, satellite control centres, mission operations centres, and similar ground-segment assets above the medium-enterprise threshold. Annex I does not address space segment itself as a space entity; satellite manufacturers and constellation operators fall outside the Space sector entry, even where they are the source of the service whose continuity matters to emergency response, aviation, or energy. Two cases discussed earlier in this chapter illustrate why this scoping matters. The 2022 Viasat KA-SAT compromise (Section 2.5) operated through ground-segment infrastructure of the kind Annex I reaches. GNSS spoofing in the Baltic and Black Sea, by contrast, attacks the signal-in-space and is not addressed by Annex I at all; whatever response the Union can give to that family of incidents has to come from instruments other than NIS2.

For entities that are in scope, NIS2 prescribes a specific set of duties. Article 21(1) requires Member States to ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures "to manage cybersecurity risk, calibrated to the entity's exposure, size, and the societal and economic impact of a possible incident". Article 21(2) lists the minimum content of those measures, spanning risk analysis and information-security policies, incident handling, business continuity and crisis management, supply-chain security, secure development and vulnerability handling, basic cyber hygiene and training, cryptography, access control and asset management,

and the use of multi-factor authentication and secured communications. Article 23 layers an incident-reporting duty on top: an early warning to the competent CSIRT within 24 hours of becoming aware of a significant incident, a fuller incident notification within 72 hours, and a final report within one month.

Read against the space-sector case material developed earlier in this chapter, the catalogue is at once well-fitted and incomplete. It is well-fitted to ground-segment incidents of the Viasat KA-SAT type, where intrusion, supply-chain propagation through distributors, and insecure user-terminal firmware all fall squarely within Article 21(2)'s categories; and the Article 23 reporting cadence. It is incomplete in three respects that the case discussed before makes visible. First, the duties are framed for network-and-information-system security and do not engage with the distinctive characteristics of orbital assets: limited post-launch upgradability, narrow uplink windows, and radiofrequency-link integrity. Annex I does not reach the space segment in the first place. Second, the supply-chain duty, although broad enough to encompass the long integrator-and-modem chains characteristic of ground-segment supply, gives operators no sector-specific anchor for deciding how far into that chain due diligence must extend; the directive specifies "direct suppliers or service providers" and leaves the rest to risk-based judgement. Third, incidents that target the signal-in-space rather than ground infrastructure, of which Baltic and Black Sea GNSS spoofing is the standing example, fall outside the directive altogether.

The Critical Entities Resilience Directive (Directive (EU) 2022/2557) [202] likewise lists "Space" among its sectors but operates through a different mechanism. Member States identify "Critical entities" under Article 6 by reference to their provision of "essential services" as defined in Article 2(5), the significance of disruption, and cross-border dependence. The two directives are designed to interoperate: an entity identified as critical under CER is treated as an essential entity under NIS2. The space-sector consequences of this interaction, the parallel governance of Union Space Programme assets under Regulation (EU) 2021/696 [392], and the place of the forthcoming EU Space Act in this architecture are the subject

of Chapter 4.

Read on its own terms, then, NIS2 takes a real but partial step toward covering the cybersecurity of space-enabled services. It brings ground-segment operators above the size thresholds within a defined and demanding risk-management and reporting regime; that is the directive's contribution. What it does not do is reach the space segment, the smaller ground-segment operators that may sit below the thresholds yet sit at single points of failure for national services, or the space-specific technical questions the cases in this chapter has raised. Whether and how those gaps should be closed, through sector-specific legislation, through the EU Space Act, or through the operator-level technical governance already being developed by national or international bodies is the question taken up in Chapter 4.

2.6.1 Dual use: the solution or the problem?

The space sector experienced the convergence of commercial and military requirements in orbit. This means that most of the new constellations, whether for broadband, Earth observation, or SATCOM, have at least a defence application. This dual-use nature has long been a defining feature of the space sector, offering efficiency, innovation, economies of scale, but also generating security, legal, and humanitarian dilemmas.

From the perspective of international humanitarian law (IHL) and civilian protection, dual-use assets challenge traditional distinctions between civilian and military objects. Satellites and ground stations today often serve multiple clients and purposes at once: a single beam or transponder can relay telemedicine data for an NGO, broadband access for a rural school, and encrypted tactical communications for a defence actor. The targeting or disabling of such systems in conflict times, therefore, risks disproportionate harm to civilians.

The International Committee of the Red Cross (ICRC) warns that "the widespread dual use of space systems and the resulting entanglement of civilian and military operators magnify the risk of civilian harm" and calls for "special precautions" before the use of force against any satellite

supporting essential services on Earth [555]. This entanglement complicates proportionality assessments and challenges the implementation of IHL principles such as distinction and necessity.

A second dimension of the problem concerns governance and accountability. The control of dual-use systems is most of the time exercised by private corporations whose commercial logic does not always align with states' legal obligations under international law.

The experience of Starlink in the Ukraine War is a useful example [278]: the same commercial network enabling humanitarian coordination also carried sensitive military data. When SpaceX unilaterally restricted access in certain combat zones, both military and humanitarian operations were disrupted, demonstrating the absence of clear escalation channels and accountability mechanisms [433].

This illustrates the privatisation of strategic decision-making in space. When commercial providers can throttle, re-route, or prioritise traffic at will, they effectively exercise powers with direct humanitarian and geopolitical consequences. Yet few frameworks clarify whether such actions fall under state responsibility, corporate due diligence, or contractual discretion. This grey zone of accountability can undermine transparency and predictability in crises.

The technical architecture of modern constellations is also influenced by this dual-use paradigm, which can also increase the attack surface and affect cyber vulnerability. Software-defined payloads and shared ground infrastructure mean that a cyber-attack or kinetic strike intended for a single (military) node could cascade across civilian networks. The humanitarian implications of such spill-over effects, loss of emergency communications, disruption of navigation, and interference with disaster-response satellites are, as analysed in this chapter, profound.

Recognising these risks, European institutions and international organisations are developing governance and technological mechanisms to manage, rather than eliminate, dual-use interdependence. The European IRIS² Secure Connectivity Programme, established by Regulation (EU) 2023/588, can be seen as an attempt to separate governmental from commercial traffic. The programme aims to build a European SATCOM

multi-orbit constellation; it is structured as a public–private partnership combining commercial broadband services with a "HardGov" layer dedicated to governmental and security communications. The Regulation explicitly requires that the constellation be multi-orbital and modular, with two distinct segments: one financed by the Union for governmental use, and one privately funded for commercial services [204].

This design entails the principle of segmentation proposed by the ICRC, which shall reduce the risk that the disruption of one service could endanger others and ensure that humanitarian communications remain online in crisis conditions.

At the international level, several scholars and states have proposed establishing a "Digital Non-Interference Corridor" under the United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS) [298][525]. The corridor would assign frequency bands and orbital slots reserved for life-saving services where intentional interference would carry a presumption of unlawfulness. Transparency could be ensured by operator reports on the percentage of governmental versus commercial payload use; such a mechanism could help belligerents make informed proportionality assessments and give humanitarian actors confidence that fallback capacity exists.

The inclusion of the space sector in the EU's NIS2 Directive and CER Directive is an important step, but complementary norm-building efforts are still needed to define how operators must segment, authenticate, and protect dual-use services. The forthcoming EU Space Law should, therefore, codify the obligations of private operators concerning transparency, data-sharing, and continuity of humanitarian services during crises.

The ethical dimension must not be overlooked. Dual use is not inherently negative; it reflects the shared dependence of civilian and defence communities on the same technologies. The challenge lies in ensuring that the governance of dual-use infrastructure aligns with humanitarian needs. This can be ensured by technical segregation, contractual obligations, and independent oversight mechanisms.

2.7 Conclusion

This chapter discusses how space-based systems are a fundamental layer of Europe's digital infrastructure and key enablers of the protection of fundamental rights. The analysis of Earth Observation and Global Navigation Satellite Systems has shown that these technologies are critical infrastructures on which the realisation of rights such as life, health, food, and access to essential services now depends. Their continuous operation sustains emergency response, environmental monitoring, and the functioning of vital services, meaning that the resilience of space infrastructure has become inseparable from the protection of human security.

To address RQ1, the chapter examined how the growing reliance on space technologies affects the protection of fundamental rights. The case studies of Haiti's post-hurricane recovery and the Turkey–Syria earthquake response demonstrated that EO data have become essential for emergency management and response. Similarly, GNSS integration into Europe's emergency communications and critical service delivery systems shows that satellite navigation now safeguards life and welfare daily. The continuity of these systems ensures the effective exercise of rights guaranteed under the Charter of Fundamental Rights of the European Union and international law.

In response to RQ2, the chapter investigated the risks posed by cyberattacks to space infrastructure and how disruptions can undermine human security and emergency operations. The analysis demonstrated that cyber threats to space systems can immediately disrupt life-saving services on Earth. Interference with space systems can cascade into terrestrial crises, interrupting emergency communications, undermining disaster management, and endangering lives. Cybersecurity for space is, therefore, a direct component of human-rights protection.

Addressing RQ3, the chapter examined how the NIS 2 Directive and the Critical Entities Resilience Directive engage with the space sector. NIS 2 brings ground-segment operators above the size thresholds within a defined risk-management and reporting regime, and CER provides a complementary identification mechanism for critical entities; the two in-

struments now anchor the cybersecurity governance of space-enabled services at Union level. The directive's text, however, leaves gaps that the case material exposes relating to the space segment itself, to the boundaries of supply-chain due diligence, and to signal-in-space incidents, and motivates the sector-specific analysis developed in Chapter 4.

Building on these findings, the chapter identifies four design characteristics that any adequate cybersecurity regime for the space sector will need to address, and which are taken up in Chapter 4: (i) continuity guarantees for services on which time-critical terrestrial functions such as emergency communications, navigation augmentation, and disaster mapping depend; (ii) segmentation and isolation between traffic classes co-hosted on shared infrastructure; (iii) identification and differentiated protection of assets whose disruption produces disproportionate downstream effects; and (iv) the availability of fallback capacity, whether through multi-orbit redundancy, multi-bearer routing, or terrestrial backup, so that the loss of a single network does not entail the loss of the service. These are characteristics that any instrument, such as NIS2 as it stands, sector-specific Union legislation such as the forthcoming EU Space Law, or operator-level technical governance, will have to implement if the resilience of space-enabled services needs to match the weight terrestrial critical functions now place on them.

In conclusion, this chapter shows that safeguarding space infrastructure is a prerequisite for protecting fundamental rights in the digital age. The path forward demands the inclusion of humanitarian considerations into technical governance, ensuring that resilience frameworks serve the protection of human life, safety, and welfare.

Chapter 3

Securing SATCOM user segment: a survey on cybersecurity challenges in view of $IRIS^2$

3.1 Introduction

Building on the vulnerabilities identified in Chapter 2, this chapter moves from general infrastructure dependencies to a detailed assessment of the SATCOM user and ground segment, illustrating how abstract risks materialize technically and operationally.

Here, we focus on SATCOM and, in particular, on the vulnerabilities that the interaction between the user segment and the ground stations can generate. These segments are often neglected and rarely considered when discussing space cybersecurity policies, and only a few studies assess the cyber vulnerabilities of the user segment. Given the complexity of space infrastructure, attacks on such components have to be considered preferable for attackers, as the attack cost is significantly reduced compared to other methods that aim at disrupting SATCOM. In contrast, the results of such attacks could have the same disastrous impacts.

The advent of the so-called new space broadened the use and applications of space technologies such as SATCOM [328]; these domains, once reserved for a narrow audience, are expected to be widely employed by several users and even, to bridge the digital divide as much as concern access to the Internet. Studies in the field of SATCOM cybersecurity exist, and vulnerabilities in the field have been discovered by researchers. However, the novelty brought by the new space paradigm (of which $IRIS^2$ can be considered as an example) has not yet been extensively and deeply considered by researchers in terms of cybersecurity. Considering the actual state of space infrastructure, an assessment of what should be improved in cybersecurity is needed more than ever to build resilient future constellations. When focusing on the specific user segment, current literature is outdated or lacks a comprehensive view of different products. Moreover, little consideration has been given to understanding whether existing standards and legal requirements currently meet the threats that exist.

With this in mind, this paper aims to clearly define threats, understand how they affect these systems, and identify how they propagate to others. Then, we analyze how many such threats appear in vulnerable modems in the wild, and start mapping laws and standards in the field through a comparative approach, considering the development of $IRIS^2$ constellation as background.

More precisely, this chapter addresses the following research questions:

- RQ1: What are the most common vulnerabilities to ground and user segments in SATCOM, and what are the vulnerabilities in the field?
- RQ2: What is the State of the Art of European and American standards and regulations in the field of space cybersecurity?
- RQ3: What are the best practices that stakeholders and entities involved in the management and operation of SATCOM networks can use? Why are these practices not implemented?

We aim to provide insights into this crucial subject by drawing on existing literature and case studies. More precisely, to address RQ1 the chapter identifies the key cyber risks related to ground stations and user segments, with a special focus on satellite modem vulnerabilities, including unauthorized access, denial of service attacks, data breaches, and supply chain vulnerabilities. As a case study, the chapter analyzes the Viasat cyberattack carried out in February 2022 [538]. Moreover, we use the Shodan search engine to investigate the exposure of satellite modems and other components of satellite networks on the Internet. To answer RQ2, we present and analyze guidelines and technical recommendations in the field of SATCOM security defined by American and European stakeholders. Then, we present a comprehensive outline of the most effective practices for cyber risk management to address RQ3. Finally, the chapter concludes with a discussion of future research directions and emerging trends. It should be noted that, despite the focus of the research being SATCOM, the same considerations could be applied to different kinds of space infrastructures such as Global Navigation Satellite System [317] and Earth Observation [336] infrastructures. Our research relies on a specific case study, as obtaining real-world scenarios and empirical data on cyber incidents in the field can be extremely difficult due to underreporting by targeted organizations that prefer not to disclose cyber incidents and their consequences, especially due to the current geopolitical scenarios. We aim to address this limitation in future research.

The rest of this chapter is organized as follows. In Section 3.2, we present an overview of SATCOM describing its architecture, its main components, user and ground segments, and technology which is typical of this context. Section 3.3 presents the study of the Viasat attack, describing the vulnerabilities used by the attackers and the consequences of the attack. In Section 3.4, we provide a general overview of the common vulnerabilities and mitigations in SATCOM, focusing on user terminals. In Section 3.5, we present the results of our Shodan research about satellite network components that are accessible through the Internet and that have vulnerabilities. Section 3.6 presents and analyzes guidelines and

technical recommendations in the field of SATCOM security defined by American and European stakeholders. In Section 3.7 we discuss some lessons learned and best practices that all the actors involved in managing, administering, and functioning space infrastructure should implement. Finally, Section 3.8 compares our work with the relevant literature, and Section 3.9 draws some conclusions illustrating possible future research directions.

3.2 An overview of SATCOM technology

SATCOM could be defined as the technology that utilizes communication satellites orbiting around the Earth to transmit information, messages, voice, video, and digital data from one point to another. The communication satellites act as relays that receive signals from the Earth's terrestrial equipment, including fixed, mobile, and transportable terminals, and re-transmit them back to the receiving station on Earth without the need for physical cables or infrastructure [329]. Here, we mainly focus on SATCOM as this technology is crucial to the world's telecommunications infrastructure. Indeed, it represents most of today's satellite infrastructures, and its application ranges in various fields during the past 50 years, including radio broadcasting, weather forecasting, military, and government communications. While ground communication systems have received the majority of attention from academia and industry in recent years, corporate endeavors by top technology companies like SpaceX, Google, and Amazon have reignited interest in satellite-based systems. In particular, satellites are being used to deliver services in a range of new application domains, e.g., to reach remote areas with unparalleled connectivity (in terms of bandwidth and cost) or to support Internet of Things (IoT) devices with low power requirements [421]. Thus, recent commercial actions unmistakably point to SATCOM as one of the most significant enabling technologies for aiding the construction of the impending sixth-generation (6G) networks [438]. It thus appears to have a promising future based on its business-related driving forces. According to a specialized study report by Market Research Future (MRFR),

the SATCOM market will reach USD 41,860 Million by 2025 with an 8.40% Compound Annual Growth Rate (CAGR) [453].

3.2.1 SATCOM architecture

A SATCOM system's communication architecture can be divided into three main components (see Figure 1): the *space segment*, the *ground segment*, and the *user segment*. The space segment includes the *Satellite to Satellite* (SS) and the *Satellite to Ground* (SG) links. It can comprise *Geostationary Equatorial Orbit* (GEO), *Medium Earth Orbit* (MEO), and *Low Earth Orbit* (LEO) satellites deployed for various applications such as navigation, data connectivity, television broadcasting, radio broadcasting, imaging, and broadband Internet. Moreover, SATCOM technologies are often used in military and defense communication systems. The main difference between military and commercial can be observed in the orbits and frequencies.

The most commonly used frequency bands for SATCOM include L-band (1-2 GHz), C-band (4-8 GHz), Ku-band (12-18 GHz), Ka-band (26.5-40 GHz), and Q/V-band (30/40-50 GHz). L-band is commonly used for satellite phone and low data rate communication, while C-band is used for satellite TV broadcasting and government/military communication. Ku-band is used for high-speed Internet and satellite TV broadcasting, while Ka-band is used for high-speed Internet and military communication. Q/V-band is a relatively new frequency and is under test for future satellite communication systems. The choice of frequency depends on factors such as signal propagation, available bandwidth, and regulatory restrictions. The above-mentioned details are crucial when considering SATCOM cybersecurity, as satellite radio frequencies can be affected by various cybersecurity risks, including intentional jamming, eavesdropping, data injection, and spoofing [494]. In the case of jamming, an attacker transmits a signal to interfere with the communication between the satellite and the ground station. In contrast, eavesdropping involves attackers intercepting the data transmitted between the satellite and the ground station. Data injection attacks can also occur when attackers send

false data to the satellite, causing it to behave unexpectedly. Lastly, another cybersecurity risk that affects satellite radio frequencies is spoofing. Spoofing refers to transmitting fake signals that mimic legitimate signals to deceive the receiver. This can lead to the unauthorized access of satellite communication and the manipulation or destruction of satellite data. Spoofing can also be used to create false images or maps, which can mislead military and civilian decision-makers [250]. It is a difficult attack to detect and defend against, as the spoofed signal can closely resemble a genuine signal. The consequences of successful spoofing attacks can be severe, especially in the case of critical satellite systems such as those used in military operations or emergency response situations. However, here we do not consider satellite radio frequency vulnerabilities. We refer the interested reader to the large literature on this topic [561]. To understand the importance of a cyber-secure ground infrastructure is thus necessary to analyze the architecture of this component.

3.2.2 The ground segment

The ground segment enables communication between the satellites and user terminals. It includes dedicated Gateway stations, namely Satellite Operator, infrastructures for control, and Network Operator, such as the Network Control Centre (NCC), and the Network Management Centre (NMC) supporting the satellite access requests from users. Satellite ground systems and receivers comprise several components: the earth terminals and user receivers convert the satellite signal into useful data for the user devices, such as modems, antennas, and mobile phones. The ground segment contains the command and control system used to maintain the satellites' functionality and, in some cases, can also include the launch segment. To manage LEO and MEO satellite constellations, numerous ground stations are required across the planet to guarantee the communications between satellites and users [419]. A standard ground station requires various infrastructure and activities to ensure smooth operations, which can be represented using a simplified value chain. The ground station value chain refers to the sequence of interconnected activ-

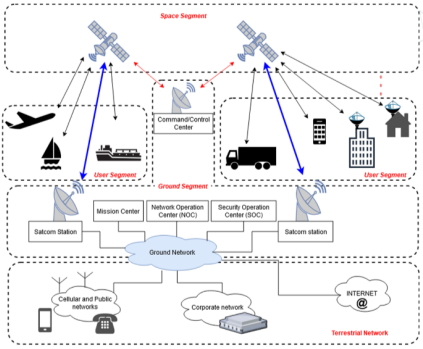

Figure 1: SATCOM architecture

ities and processes involved in the operation of ground-based infrastructure in satellite communication systems. It encompasses the entire lifecycle of ground station operations, from initial setup and infrastructure development to data reception, processing, and utilization.

The ground station value chain involves various stakeholders, including satellite operators, ground station operators, equipment manufacturers, and service providers. It encompasses a range of activities, including the construction and maintenance of ground stations, deployment and alignment of antennas, signal reception and demodulation, data processing and analysis, and the provision of value-added services based on the received data. This value chain, known as the Ground Segment value chain, comprises three primary blocks: upstream, midstream, and downstream.

The three blocks of the Ground Segment value chain are further detailed as follows [419]:

- The upstream block includes all the necessary hardware and software that facilitate mission operations, such as antennas, modems, and radio equipment, the launch facility, and the ground networks that provide connectivity among all the ground segment elements.

- The midstream block comprises all activities that support mission operations. It comprehends the control center and the IT facility,

performing spacecraft and payload Telemetry Tracking and Control, downlinking signals, and retrieving data.

- The downstream block includes all activities performed once the data is retrieved on Earth. This includes data storage, pre-processing, such as error corrections and timestamps, and services based on data analytics.

The Ground Segment can be further divided into two main categories [571]: Ground stations for Tracking, Telemetry, and Control (TTC) and Communications Ground Stations (CGS). TTC is crucial in maintaining satellites' proper orbits and monitoring their performance. Whereas communications ground stations are responsible for processing and transmitting various types of data, such as imagery and voice, and often serve as a link to terrestrial networks. However, it is important to note that in most cases, the ground-based terrestrial network interconnections communicate with the communications ground station and not directly with the satellite.

3.2.3 The user segment

The second key element of SATCOM infrastructure is the user segment. Apart from communications ground stations, numerous commercial user terminals on the market can receive data downlinks and even transmit data uplinks in some cases. For instance, GPS navigation devices often found in cars and satellite TV dishes are examples of downlink-only user terminals. In this last category, we also include other types of equipment such as Very Small Aperture Terminals (VSAT) [110] and a new generation of user terminals, of which Starlink dishes [564] are one of the most famous examples at the moment. The cybersecurity of these components that are often closer to the end-users is the focus of this research.

ETSI's Broadband Satellite Multimedia Working Group specified a reference architecture for IP-based satellite networks [186]. However, since we focus on the user segment, we can describe the architecture of such a segment as organized into three main layers: the *Access Layer*, the

Distribution Layer, and the *Core Layer*. The Access Layer connects end-user devices, such as satellite terminals and modems, to the network and provides the physical and logical interface between the user equipment and the Distribution Layer. It may sometimes include additional equipment, such as amplifiers and filters, to optimize the signal quality and reliability. The Distribution Layer is responsible for aggregating traffic data from the Access Layer and forwarding it to the Core Layer. It may include routers, switches, and other devices providing connectivity and managing network traffic. This layer also provides security and Quality of Service (QoS) features to ensure that traffic is prioritized and routed efficiently.

Lastly, the Core Layer transports traffic between different sites and networks. It provides high-bandwidth connectivity and may use technologies such as *Multiprotocol Label Switching* (MPLS) [172] and *Virtual Private Networks* (VPNs) to optimize traffic flow and ensure security. The Core Layer also includes network management systems and other tools for monitoring and controlling network performances.

The SATCOM user segment infrastructure generally consists of various components that enable communication between the end-user and the satellite. These components include:

- Antennas [120]: An antenna is used to transmit and receive signals to and from the satellite. The antenna must be designed to operate at the satellite signal frequency and accurately pointed toward the satellite for optimal communication.

- Modems [274]: A modem modulates and demodulates the satellite signal, and it is responsible for converting the digital signal from the user's device into an analog signal that can be transmitted over the satellite and vice versa.

- Routers [562]: In a satellite communication network, routers manage data flow between different devices and networks and connect user terminals, such as modems or other devices, to the satellite network. They can also connect different networks, such as Lo-

cal Area Networks (LANs) or Wide Area Networks (WANs), to the satellite network.

- Transceivers [333]: A transceiver combines a transmitter and a receiver into a single unit and is used to transmit and receive signals over the satellite.

- Amplifiers [72]: An amplifier boosts the strength of the transmitted signal. This component is necessary to ensure the signal is strong enough to travel long distances and penetrate through obstacles.

- Terminals [72]: A terminal is the user's device connected to the SATCOM system. It could be a laptop, phone, or any device capable of sending and receiving digital signals.

- User Management Systems [367]: A user management system manages the system's users, taking care of authentication, authorization, and accounting of users.

- Operations Support Systems [163]: An operations support system monitors the system's performance, identifying and resolving any issues that may arise and ensuring that the system operates at maximum efficiency.

These components work together to provide reliable and efficient communication between the user and the satellite. They may be integrated into the same hardware, depending on the product. As mentioned above, the user segment includes terminals such as satellite mobile phones, ships, and airplanes. These devices can communicate with satellites via the link between the ground segment and the user segment, such as the forward link, whereas they can use any communication technology to interact with the gateways. The forward link consists of an uplink (base station to satellite) and a downlink (satellite to mobile user). Some constellations like Iridium, Globalstar, Thuraya, and Inmarsat [95] allow a direct connection of the user handsets to the satellites using the User to Satellite (US) link that typically uses frequencies in the L-band [95].

For this research, one of the main components to be considered is the satellite modem, which converts digital signals from a computer or another device into analog signals that can be transmitted via satellite, and vice versa. Satellite modem communication protocols are the standards and rules that govern the communication between the antenna and the satellite modem and between the modem and the Ground Station Network. Several protocols exist, the most common include [456]:

- Ethernet [338]: It is a standard communication protocol to communicate over a cabled network. In SATCOM, it allows communication between the satellite modem and other devices, such as routers or switches.
- TCP/IP [303]: They are standard protocols for exchanging data over the Internet. In SATCOM, they are commonly used to enable communication between the satellite modem and ground-based networks or devices.
- Simple Network Management Protocol (SNMP) [360]: It is a standard protocol to manage and monitor network devices. In SATCOM systems, it is often used to monitor the performance of the satellite modem and other network devices.
- Telnet [131]: It is a standard protocol to establish a remote terminal connection between a client and a server. In SATCOM, remote users can access ground-based equipment and services.
- Secure Shell Protocol (SSH) [233]: Like Telnet, SSH provides a terminal connection between a client and a server. However, unlike Telnet, SSH uses encryption and authentication to secure the connection and protect against unauthorized access and data interception.
- TR-069 Protocol [538]: Several SATCOM modems use it to manage and control remote terminals. It allows automatic configuration and management of devices, firmware upgrades, and fault diagnosis. The protocol also enables communication between the mo-

dem and a remote management system, enabling centralized control and monitoring of the modem's performance.

The protocols above are the most common ones that may be used in SATCOM modems and routers. Actually, the specific protocols used can vary depending on the specific system and application. Additionally, some proprietary protocols may be used for controlling the satellite modem and antenna, such as the iDirect protocol used by iDirect modems [309] or OpenAMIP, an IP-based protocol that facilitates the exchange of information between an Antenna Controller Unit and a satellite [255]. Other key components that are often integrated into this complex infrastructure are VPN appliances that are commonly used in the ground infrastructure to connect remote users to the network securely. These appliances are designed to provide high levels of security and reliability, but, as discussed in the following section, they are not immune to cyber-attacks.

Finally, it should be considered that attacks can be launched in any of the segments mentioned above. In light of this, the user and ground segment should be properly guarded, and all communications coming from the satellite should be kept secure, regardless of its location.

3.3 From theory to practice: the attack to Viasat

3.3.1 Chronology of the attack

On February 24th, 2022, the satellite communication service provider Viasat experienced an outage of its KA-SAT Network due to a malware wiper attack that disabled thousands of end-user terminals [538]. According to a press release published by the same Viasat, the attack was not addressed to the KA-SAT satellite, but to a "*consumer-oriented partition of the KA-SAT network*" [538], namely, Internet modems Tooway, SurfBeam2, SurfBeam2+. The attack, however, was not limited to Ukraine and had severe consequences on users, causing ripple effects across Europe. Indeed, not only thousands of customers in Ukraine, including the Ukrainian Government, army, and security services, were impacted, but

also tens of thousands of users of other satellite broadband services suffered outages. In France, around 9,000 subscribers of the satellite broadband service NordNet's [114] were affected, as well as almost 15.000 subscribers of the British broadband provider BigBlu [493] were impacted in Germany, France, Hungary, Greece, Italy, and Poland. The attack also damaged the German energy company Enercon [178], as remote monitoring and control access to its 5,800 wind turbines became unavailable due to its SCADA system relying on the KA-SAT network. Some satellite modems became unusable without the possibility of being repaired or updated remotely, resulting in thousands of customers being left without an Internet connection for weeks [432]. Weeks later, Enercon stated that there were "difficulties with the availability of the hardware" with the supplier of the modems [178]. According to Viasat, the attacker did not access end-user data and devices such as computers or mobile phones, and the KA-SAT satellite and its ground stations were not compromised, damaged, or involved in the attack. Interestingly, this part of the network is owned by the U.S. company Viasat but operated by Eutelsat's subsidiary Skylogic. In particular, the attack appears to have taken place in two main phases [432]:

- A Denial-of-Service (DoS) attack was carried out on the Viasat Internet modems located mostly in Ukraine and Germany. Attackers exploited a vulnerability in the authentication mechanism of modems, enabling them to gain unauthorized access to the infrastructure's ground and user segments. This attack disrupted satellite communication services, requiring several days to restore them fully.

- Attackers exploited a vulnerability in the VPN appliances of Skylogic, which seems to be Fortigate's [432], an American multinational corporation that develops and sells cybersecurity solutions. They entered the ground network management segment of Viasat's KA-SAT network and gained control through a lateral movement. Once into the management section, attackers executed a series of commands uploading a wiper malware in the network and erasing

the hard drive of ViaSat modems.

The attack targeted the satellite communication infrastructure's ground and user segment, affecting more than 15,000 users, including government agencies and military organizations, resulting in many users being unable to connect to the network. The alteration of the Viasat system certainly caused considerable difficulties for the Ukrainian military and government in the first hours of the conflict [62]. However, the effect on the course of the conflict is difficult to estimate. In particular, since radio signals were jammed during the first phase of the invasion, the Ukrainian military relied on satellite communications to coordinate its troops. Soldiers were thus unable to use radios, and SATCOM was considered a valuable alternative to communicate along the chain of command. Once this infrastructure was compromised, operations coordination became slower and more uncoordinated [62].

3.3.2 Analysis of the attack

The two-phase attack seemed to have been caused by vulnerabilities in the Internet modems and the VPN appliances. On one side, the DoS attack was caused by a "*misconfiguration in the management section of the satellite network*" [429]. It is suspected that the attackers were able to gain unauthorized access to a Ground Station, particularly the 'Element Management' section, which is synchronized across multiple gateways. They likely exploited a legitimate control protocol [444], such as TR-069, that seems to have been employed by Viasat, to issue a command to deliver a malicious firmware update to the terminals. One possible method for carrying out this attack is using VLAN-based attacks. However, the entity managing this *management section* has not been disclosed, as well as what exactly this management section is. Some security analysts proposed that the Viasat SurfBeam Internet modems were probably configured through the TR-069 protocol, and an unpatched vulnerability in this protocol could have allowed hackers to perform the DoS attack [432]. According to security researcher Ruben Santamarta, the TR069 'APP INSTALL' feature could have been the way through which hackers wiped

the modems [432]. Through this feature, attackers implemented functionalities that enabled the access control system to install arbitrary binaries on the modem without requiring signature verification or a complete firmware upgrade [432]. The TR-069 protocol is often used to manage Customer Premises Equipment (CPE) devices such as routers, modems, and gateways. In the case of Viasat however, it is unclear the vulnerabilities that were exploited.

On the other side, the second phase of the attack, which resulted in access to the management section, was carried out, probably exploiting already known vulnerabilities. It seems that Fortinet, the VPN appliances provider of Skylogic, has been affected by relevant data breaches [62]. In November 2021, Fortinet learned that a malicious actor disclosed around 500.000 SSL-VPN access information from 87,000 FortiGate SSL-VPN devices. These credentials were obtained from systems that remained unpatched against FG-IR-18-384 / CVE-2018-13379 at the time of the actor's scan [237]. This CVE, due to an Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal") in various Fortinet products [108] under SSL VPN web portal, allowed an unauthenticated attacker to download system files via specially crafted HTTP (Hypertext Transfer Protocol) resource requests. The credentials were leaked in two Russian-speaking forums, namely Groove and RAMP [54]. In March 2021, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) observed Advanced Persistent Threat (APT) actors scanning devices on ports 4443, 8443, and 10443 looking for CVE-2018-13379 and enumerating devices for CVE-2020-12812 and CVE-2019-5591 [229]. Thus, already in 2019, these vulnerabilities were well known, and in 2021 the FBI and CISA warned about the malicious activity of hackers targeting these vulnerabilities in a Joint Cybersecurity Advisory. Even if Fortinet promptly patched them, neither Skylogic nor Viasat signaled them to their customers. The stolen credentials of these VPN appliances were thus probably the entry point of hackers in the network [432].

3.3.3 Lessons learned

Although all the details about the attack are still unclear, the incident presents a unique opportunity for the entire sector, both commercial and governmental, to acquire useful insights and learn how to avoid similar disruptions. The attack could be considered one of the most significant publicly known against a space system so far. Furthermore, as noted by Boschetti et al. [62], the incident took place hours before the start of the Russian invasion of Ukraine in February 2022, indicating the potential utilization of a cyberattack as an initial act, having significant implications within a military context. Additionally, Viasat's dual-use paradigm, serving as both a commercial and military asset, adds complexity to the incident and indicates trends for future attacks as the space sector continues to commercialize.

The attack should be considered by European Stakeholders, especially in this historic moment since the European Union's decision to provide itself with a multi-orbit Satellite constellation for Communications, the $IRIS^2$. SATCOM and GovSATCOM, in particular, have demonstrated to be essential technologies to rely upon in critical scenarios such as conflicts, natural disasters, terroristic attacks, and in general, every time different means of communication are needed. The Viasat attack highlighted the need for a reliable SATCOM infrastructure. Still, we should not take for granted that the issues raised by the attack will be transposed in future policies and guidelines. The attack demonstrated that commercial satellites are not as reliable as military ones, even if they are often used for the same purposes as in Ukraine. Given the vulnerability of commercial satellites, an attack against these constellations could potentially provoke more disastrous consequences than an attack on a military satellite infrastructure, where risk management and risk assessment policies are always well-defined and implemented. A clear vulnerability shown by the attack is the complexity of commercial space services. In the considered case, various companies were the owners and operators of the space, ground, and user segment and were distributed in different countries and thus under different jurisdictions. Moreover, the

architecture of these systems includes different IT service providers such as Fortinet. This complexity implies different levels of not only vulnerabilities but also responsibilities regarding the security of the system. The Viasat case study shows how attackers can take advantage of trust relationships and access privileges between space companies and their IT subcontractors to gain access to networks: attackers exploited the connection between VPN provider and Skylogic, to gain access to Viasat's network.

It should be kept in mind that while regulatory compliance should serve as a baseline, relying solely on a compliance-focused security approach falls short due to minimum standards, outdated requirements, and a one-size-fits-all mentality. The SATCOM sector, like many others, necessitates a comprehensive risk management strategy, evaluating risks from various sources. The evaluation of third-party cybersecurity risks, especially IT service providers and significant suppliers, is crucial before onboarding [48]. Continuous security goes beyond initial assessments, requiring contractual obligations, ongoing monitoring, compliance management, and data use restrictions. What is needed in the industry is a shared security model that dispels the misconception that security is solely the responsibility of one of the parties involved in the architecture. The future of third-party risk management involves growing complexity, demanding automation, threat intelligence, and an always-on risk management mindset. Cyber Third Party Risk Management (C-TPRM) can involve both intrusive methods like penetration testing and non-intrusive methods that synthesize publicly available information [321]. While it is an emerging field, a range of methodologies are being explored to create an effective and efficient system for managing third-party cybersecurity risks[423].

In conclusion, the primary focus of the attack analysis should be on the possible security vulnerabilities that can arise from the intricate wholesale operations involved in a satellite infrastructure. This complexity extends down the chain to ground station operators, satellite service providers, distributors, and resellers, all requiring some level of access to provide their services. It is exactly the integration of these various components

that present the highest security challenges. This also raises legal concerns about the cybersecurity responsibilities and minimum requirements that providers must impose on their subcontractors. Commercial actors that decide to provide services to specific categories of users, such as governments and the military, should consider that their business could be significantly threatened, and their risk assessment and threat model should be reevaluated. All these considerations should translate into a higher budget dedicated to cybersecurity in cases of specific users. The concept of satellites as a single point of failure for multiple sectors is probably the most relevant issue highlighted by the attack. The propagation of the DoS to modems used in different sectors and countries showed the threat that a non-segmented network could provoke. Especially when designing $IRIS^2$, which will probably rely upon a mix of commercial already existent SATCOM infrastructures and new ones, the EU stakeholders should reconsider the dual-use of these technologies. The non-separation will automatically lead to a higher likelihood of propagation in case of attacks. Even the distinction between military and civilian when discussing SATCOM, but in general satellite infrastructures, should be considered outdated. Given the reliance of many ground-based critical infrastructures on space-based ones, not only for connectivity but also for synchronization, commercial space companies, in the case they are providing services to specific users, should grant the same security as military infrastructures and be audited in the same way. This is even more important considering the European tendency to foster the commercialization of space. In the case of Ukraine, the country relies totally on foreign space infrastructures for its military operations, this significantly reduced its capacity to implement military strategies autonomously. Various commercial satellite service providers, such as Starlink [424], Maxar [50], and BlackSky [283], allowed the country to use drones and collect intelligence for defense and attack campaigns. Nevertheless, it is advisable to exercise caution when assigning military capabilities to commercial operators, and this consideration should be extended to encompass all services that are in any way linked to civil security and defense.

3.4 SATCOM user segment: vulnerabilities and mitigations

Information regarding the technical aspects of SATCOM user segment vulnerabilities, breaches, and mitigation strategies for systems and networks are often unavailable. It appears that most of the industry and service providers have been reluctant to disclose technical details of security breaches to the public. This section aims to provide a general overview of all the common vulnerabilities in SATCOM networks, particularly user terminals, and review mitigation techniques and strategies for their reduction.

3.4.1 Context

From the viewpoint of an attacker aiming to compromise satellite networks, the user segment represents a cost-efficient attack. As the ViaSat case demonstrated, the disruption caused by compromising a small portion of the network cannot be ignored. From the user segment, an attacker can move laterally in the network and maybe even take control of the entire command-and-control system. This happened in the 90s when attackers acquired access to the flight control system of NASA's Goddard Space Flight Center [240] and exposed the ROSAT telescope sensors to the sun, causing the inoperability of the satellite. In recent years however, with the increase of commercial ground stations and with the introduction of the concept of Ground Station as a Service [62], these kinds of attacks increased in their frequency and their complexity [227]. To gain access to the component of a satellite or information about a company, attackers previously faced high barriers due to the complexity and cost. However, with the rise of new space companies, which are more communicative about their systems' supply chain, contracts, and employees, malicious actors may obtain critical information useful to support their malicious activities. Additionally, modern space systems increasingly rely on cheaper *Commercial Off-the-Shelf* (COTS) components and standardized hardware and software, making it easier for potential at-

tackers to purchase and search for vulnerabilities. This also means that if a vulnerability is found in one COTS component, all satellites using that component are vulnerable. Ground stations are thus vulnerable to cyber-attacks, which could compromise the confidentiality, integrity, and availability of critical space-based systems and operations. On January 2023, the Chief of Space Operations, U.S. Space Force Gen. B. Chance Saltzman, speaking at the Air and Space Forces Association Board of Directors meeting in Arlington, VA, highlighted that "*Satellites in space are not useful if the linkages to them and the ground network that moves the information around what you get from satellites is not assured, is not capable, is not accessible. The cyber activity that has hurt satellite operations is a reminder that we should think about cyber protection of our ground networks* [30]."

3.4.2 COTS Components and their risks

In recent years, the increasing reliance on COTS components in satellite communication systems has raised cybersecurity concerns. While COTS components can offer cost savings and improved performance because of their wide availability on the market, their integration into SATCOM systems creates a significant cybersecurity challenge. Since these components are not specifically designed for any particular application, they may not have undergone rigorous security testing and certification processes necessary for use in SATCOM systems. A list of COTS typically used in SATCOM networks follows:

- Modems: COTS modems are commonly used in SATCOM systems, however, they can be vulnerable to attacks such as denial of service, unauthorized access, and data interception. For example, attackers can exploit software vulnerabilities in the modem's firmware to gain unauthorized access to the network or launch a DDoS attack by flooding the modem with traffic. Examples of these modems are: iDirect Evolution X7, Hughes HX200, Comtech EF Data CDM-625 Advanced Satellite Modem, ViaSat MD-1366/U Advanced Extremely High Frequency (AEHF) Satellite Modem, Newtec Dialog MDM6000, Advantech Wireless AMT-75 HT Satellite Modem, Gilat

SkyEdge II-c, GRC RP-1G, SWE-DISH IPT Suitcase 1.3M Ku-Band Flyaway Terminal, Datum Systems M7S Modem, ND SatCom SKY-WAN 5G, Advantech Wireless AMT-83L High-Speed Satellite Modem.

- General Purpose Processors (GPPs): GPPs are often used in satellite payloads and ground stations to perform signal processing and data encryption tasks. However, these processors are not specifically designed for satellite applications and can be vulnerable to side-channel attacks. For example, an attacker could use a power analysis attack to extract sensitive information from a GPP by analyzing its power consumption. Examples of GPP used in Satellite Systems are: ARM-Cortex-M/R and other MMU-less devices.
- Operating Systems (OS): Common operating systems such as Windows and Linux are often used in SATCOM systems due to their wide availability and versatility. However, these operating systems are not designed with satellite-specific security considerations and may contain vulnerabilities attackers can exploit. For example, an attacker could use a buffer overflow attack to exploit a vulnerability in the OS and gain unauthorized access to the system.
- Wireless Communications: SATCOM systems rely on wireless communication links between satellites, ground stations, and user terminals. However, these wireless links are vulnerable to interception and interference by attackers. For example, an attacker could use a software-defined radio to intercept and decode the wireless communication signals or launch a jamming attack to disrupt the communication link.

The use of COTS components also poses supply chain risks. These components are often manufactured overseas, and the supply chain may not be secure. Attackers can exploit vulnerabilities in the supply chain to introduce malicious components into a system, compromising its security. Implementing robust security controls to mitigate the cybersecurity risks associated with COTS components is essential. These controls should include secure supply chain management, rigorous security

testing, certification processes, continuous monitoring, and threat intelligence. The use of COTS components in critical SATCOM systems should be limited. Government and commercial actors should prioritize using components that have undergone rigorous security testing and certification.

3.4.3 Common vulnerabilities and mitigations

The cybersecurity challenges faced by the SATCOM user segment are relatively new but require comprehensive measures to ensure the integrity and confidentiality of communications. By understanding these vulnerabilities and implementing appropriate measures, organizations can enhance the security posture of their SATCOM networks and protect against potential threats. To mitigate cyber risks, various strategies and technologies can be employed. Table 1 explores some of the most common vulnerabilities and attacks on SATCOM systems and provides some guidelines on how to mitigate them. Although the table is non-exhaustive, it describes well how exposed SATCOM systems are to cyber threats. The content of the Table 1 will be further explained in the following section.

In the last years, as costs reduced and attacks increased, several user terminals started being targeted, and vulnerabilities being actively exploited [406]. Table 2 on the other side provides some examples of vulnerabilities discovered in popular SATCOM user terminals. Understanding these vulnerabilities is essential to develop effective cybersecurity strategies to protect satellite systems from potential cyberattacks. Note that the list does not include all those vulnerabilities that affect the other components of the ground segment, such as switches, firewalls, and VPN appliances that are no less critical in the SATCOM infrastructure.

Satellite communication networks are extremely vulnerable to attacks from adversaries who target satellite user terminals, as many lack the same protections commonly found in terrestrial modems/routers. As with any networked device, satellite modems are susceptible to cyberattacks. Cybercriminals can attempt to exploit vulnerabilities in the device's firmware or software to gain unauthorized access, intercept data,

Table 1: Vulnerability/Attack and Mitigation

Vulnerability/Attack	Common mitigations/recommendations
Lack of Encryption	• Use network encryption solutions such as IPsec or TLS VPNs. • Apply mutually authenticated, encrypted TRANSEC down to vendor-proprietary protocols. • Use point-to-point communications over IKE/IPsec-encrypted VPNs.
Weak Authentication / Lack of Access Control	• Implement strong passwords and multi-factor authentication. • Employ RBAC and ABAC access controls. • Implement firewalls and network segmentation. • Change all default credentials. • Use intrusion detection and prevention systems. • Apply a need-to-know access policy.
Vulnerabilities in Software and Firmware	• Keep systems updated with the latest security patches. • Acquire updates only from trusted sources.
Cross-Site Scripting (XSS)	• Use input validation and output encoding. • Apply Content Security Policy (CSP).
Brute-Force Attacks	• Implement rate limiting. • Use strong, unique passwords. • Enforce two-factor authentication. • Use CAPTCHA or similar techniques.
Jamming	• Employ frequency-hopping techniques. • Use anti-jam antennas and polarization diversity. • Deploy commercial anti-jamming solutions.
Denial of Service (DoS)	• Deploy intrusion detection and prevention systems. • Use commercial DoS protection solutions.
Malware and Virus	• Employ antivirus and antimalware solutions. • Apply network segmentation.
Physical Threats	• Ensure physical security of SATCOM equipment and facilities. • Use tamper-evident seals and secure containers. • Deploy surveillance and monitoring systems. • Use hardened and ruggedized equipment.

or for other malicious activities (see Table 2 for some examples). Satellite routers have been known to present an attack surface through their administrator interface and have been secured through better password protection and browser policies. However, as new satellite Internet providers become more prevalent, new routers are often designed without mitigations against vulnerabilities already common in terrestrial routers. Moreover, since the router is part of a physical system that often includes the antenna, securing the admin interface is of greater importance. Attacks on the admin interface can affect the antenna's physical state, resulting in a denial of service and damage to the antenna's motors and other hardware through overuse.

Table 2: Examples of terminal vulnerabilities

Terminal	CVE	Description
Starlink Satellite Modem	See reference [463]	Fuzzing to uncover a denial-of-service attack on the Starlink user terminal
Newtec Dialog MDM6000	ZSL-2016-5359 [134]	The terminal suffers from cross-site scripting vulnerability. This can be exploited to execute arbitrary HTML and script code in a user's browser session in the context of an affected site.
Hughes Network Systems 9201, 9450, and 9502	CVE-2013-6035 [135]	The terminal does not require authentication for sessions on TCP port 1827, which allows remote attackers to execute arbitrary code via unspecified protocol operations.
NETGEAR Orbi Tri-Band Business WiFi Add-on Satellite, (SRS60) AC3000 V2.5.1.106, Outdoor Satellite (RBS50Y) V2.5.1.106, and Pro Tri-Band Business WiFi Router (SRR60) AC3000 V2.5.1.106	CVE-2020-11549 [136]	The root account has the same password as the Web-admin component. Thus, by exploiting CVE-2020-11551, it is possible to achieve remote code execution with root privileges on the embedded Linux system.
Hughes Network Systems Router Terminal for HX200 v8.3.1.14, HX90 v6.11.0.5, HX50L v6.10.0.18, HN9460 v8.2.0.48, and HN7000S v6.9.0.37	CVE-2023-22971 [137]	Cross-site scripting vulnerability in Hughes Network Systems Router Terminal allows unauthenticated attackers to misuse frames, include JS/HTML code and steal sensitive information from legitimate users of the application.

In the context of router security, the TR-069 protocol is often used to manage Customer Premises Equipment (CPE) devices such as routers, modems, and gateways. Like any network protocol, it carries potential cybersecurity risks [66], among which:

- Authentication vulnerabilities: The protocol authentication mech-

anisms may be susceptible to brute-force attacks or other forms of exploitation, which can allow unauthorized access to CPE devices.

- Malicious firmware updates: The TR-069 protocol allows to remotely update the firmware. Attackers can exploit this feature to upload malicious firmware to devices, which can be used to steal sensitive data or conduct other malicious activities.

- Network reconnaissance: The protocol allows retrieving device information, such as serial numbers, firmware versions, and hardware specifications. Attackers can use this information to conduct reconnaissance on the network and identify potential vulnerabilities.

- Denial-of-service attacks: The TR-069 protocol uses HTTP-based communication, which can be vulnerable to denial-of-service (DoS) attacks: attackers can flood the device with HTTP requests, which can overwhelm the device and render it unusable.

- Man-in-the-middle attacks: The TR-069 protocol does not provide end-to-end encryption and authentication, allowing attackers to intercept and manipulate traffic between the CPE device and the management server.

While these are potential risks, the actual exploitation will depend on the specific implementation and configuration of the TR-069 protocol within an organization's network. Proper security controls and risk assessments should be conducted to mitigate these risks.

3.5 Looking for unpatched satellite networks in the field

In this section, we perform an on-field investigation of vulnerabilities within satellite communication SATCOM systems. We exploit the Shodan search engine [232] to investigate the exposure of satellite modems and

Table 3: A summary of the vulnerable devices found by Shodan

IP	Device	Organization / ISP (Country)	Org. Revenues ($)	Country/City	Vulnerabilities	Ports
82.205.***	N/A	Horizonsat FZ LLC (UAE)	6.2 M	Germany Niederdorla	CVE-2020-15778 - CVE-2021-36368	22, 161
161.30.***	N/A	INMARSAT GLOBAL LIMITED (UK)	1.2 B	7 United Kingdom Hounslow	CVE-2022-31813 - CVE-2020-1927 - CVE-2021-4044	21, 22, 23, 443
165.220.***	Router MikroTik	ViaSat, Inc./ViaSat, Inc. (USA)	2.78 B	Germany Frankfurt	CVE-2022-22707 - CVE-2019-11072 - CVE-2018-19052	161 - 9997, 10000
219.215.***	Server	COLT Technology Services Group Limited / Viasat SPA (UK)	1.2 B	Italy/Milan	CVE-2009-4444 - CVE-2009-2521 - CVE-2008-1446	21, 80
62.145.***	Newtec DVB-S L-band Satellite Modulator NTC/2180.xA	Satellite Mediaport Services Ltd. (UK)	>5 M	United Kingdom Rugby	N/A	80, 161
80.75.***	Newtec ntc7102	YAHSAT FRANKFURT (UAE)	206 M	Germany Oberasbach	N/A	80, 161
84.11.***	Comtech EF Data CDM-570L/IP L-Band Satellite Modem	IABG Teleport GmbH (DE)	265 M	Germany Munich	N/A	161
188.***	Gilat Modem	PRIVATE JOINT STOCK COMPANY DATA-GROUP/SKYLOGIC S.P.A. (NA)	NA	Ukraine/Kyiv	CVE-2021-40438 - CVE-2022-37436	161
82.20.***	MikroTik Router	Horizonsat FZ LLC (UAE)	6.2 M	Germany Niederdorla	N/A	22, 23, 53, 80, 2000, 8291, 8728
82.205.***	N/A	Horizonsat FZ LLC (UAE)	6.2 M	Germany Niederdorla	CVE-2022-36760 CVE-2022-28615 CVE-2022-30556 CVE-2023-25690	22, 80, 443
78.41.***	Cisco ASR 1000 Series Aggregation Services Router	MPLS European Backbone 1 of Phibee-Telecom/Phibee Telecom SAS (FR)	>5 M	France/Paris	N/A	121, 161

other components of satellite networks on the Internet. Shodan is a powerful tool for exploring Internet-connected devices and their associated vulnerabilities. Shodan primarily focuses on network-level information and allows discovering devices with open ports, publicly accessible services, and exposed systems that may unintentionally disclose sensitive information or present potential security risks.

In this chapter, we use Shodan for exploratory and confirmatory purposes rather than a systematic measurement. This preliminary investigation aims to verify whether the vulnerabilities identified in the literature and technical reports are observable in real-world deployments. A more systematic, repeatable, and quantitative methodology for assessing cyber exposure—based on structured data collection, scoring, and cross-organizational comparison—is introduced in Chapter 7, where these tools are integrated into a formal Risk Exposure Framework.

By using several search terms, including the names of SATCOM service providers and names of commonly used satellite modems, we identified several SATCOM network devices that are accessible on the Internet and that are vulnerable.

We performed our research on Shodan according to the following methodology.

- We first consulted the websites of the major satellite modem manufacturers such as *Comtech* [112], *iDirect* [285], *Hughes* [281], and other databases containing technical specifications and listings of hardware.

- Then, we performed Shodan queries containing both the models of the modems and the names of the ISPs or operators that may manage the infrastructure.

- By using specific keywords related to European Satcom service providers, such as “Intelsat”, “Eutelsat”, “Iridium”, “Viasat”, “IABG”, “Inmarsat” and others, along with popular satellite modem names like “iDirect”,
  “Comtech”, “Hughes” and “Cobham”, we looked for potential vul-

nerabilities and we assessed the risks associated with the exposed devices.

We have narrowed the scope of research to equipment located in Europe and mainly in the Member States of the Union. This is because the research aims at identifying SATCOM service providers that may fall under the framework of European legislation such as NIS2 Directive.

However, as highlighted by the Viasat case study, the attack on a piece of infrastructure outside the European Union's borders can have consequences on Member States, their economies, and security. Moreover, despite these devices being located in Europe, some of the ISPs that manage them are in countries such as the UAE or the USA. This complicates the enforcement of European standards and monitoring mechanisms as well as weakens the application of fines in case of non-compliance with European laws.

We collected data about open ports, ISP information, device characteristics, and approximate location from Shodan's results. We organized the data in a tabular format to clearly overview the findings. The tabular representation allows for easy analysis and identification of potential security risks of the exposed and unpatched satellite modems. Indeed, by the open ports and signaled vulnerabilities, it is possible to assess the level of risk posed by each device and determine the potential impact on SATCOM users and industries. Identifying the device type was not always possible solely based on the collected data. However, we tried to categorize the devices whenever feasible by examining factors such as open ports, response banners, and known vulnerabilities.

A short summary of the results of our Shodan search is Table 3. The results reveal the presence of several satellite modems with unpatched vulnerabilities used by different ISPs. Our results also reflect the diversity of satellite communication infrastructure and the many vendors and technologies involved. Each found device may have unique characteristics and vulnerabilities, and various ISPs may have different approaches to managing and securing their infrastructure. Understanding this diversity is essential for implementing comprehensive security measures for specific risks and challenges associated with different devices and ISPs.

Table 3 provides a non-exhaustive list of the vulnerabilities that affect the identified hardware. The vulnerabilities with the highest score are:

- CVE-2023-25690 [39]: Certain configurations of the Apache HTTP Server from versions 2.4.0 through 2.4.55 may be vulnerable to HTTP Request Smuggling, a technique for interfering with the way a web application processes sequences of HTTP requests that are received from one or more users. The vulnerability occurs when the proxy module is enabled with certain RewriteRule or ProxyPassMatch directives. These directives involve matching and inserting user-supplied data into the proxied request using variable substitution. Exploiting this vulnerability, an attacker can split or smuggle requests, potentially bypassing access controls on the proxy server, inadvertently proxying unintended URLs to legitimate origin servers, and even poisoning the cache.

- CVE-2020-15778 [138]: the `scp` utility in OpenSSH version 8.3p1 is vulnerable to a command injection. It allows for the execution of arbitrary commands by exploiting backtick characters in the input concerning the destination address. It is important to note that this vulnerability is labeled as *DISPUTED* because the vendor has reportedly stated that they intentionally omit validation of "anomalous argument transfers" to avoid breaking existing workflows.

- CVE-2022-31813 [139]: This vulnerability is in the web-based management interface of Cisco IOS XE Software and could allow an unauthenticated, remote attacker with read-only privileges to execute arbitrary code with root privileges on an affected device.

The presence of multiple CVEs emphasizes the need for continuous monitoring, prompt remediation, and ongoing security measures to protect satellite communication and the connected infrastructure. Using such information on the vulnerabilities of each device, stakeholders can prioritize their efforts and try to introduce mitigations to protect their devices. This includes implementing regular patching and firmware updates, conducting security assessments and audits, enforcing secure con-

figuration practices, and promoting security awareness and training among users and operators.

Our results show only a partial view of devices open to potential threats, as many other modems from other SATCOM service providers may be as well on the list. The NIS2 Directive will oblige these actors to report cyber incidents and prepare business risk management strategies. However, at the moment, even if issues relating to vulnerability and patch management have been recognized as the basis for liability [324], according to standards such as ISO/IEC 27002:2022 [478], in Europe as in many other countries no explicit legal obligations exist for companies to patch their products [358]. This may cause European stakeholders to underestimate the potential impact of an attack on these networks on national security. Moreover, according to the Cyber Resilience Act [192], modems and routers that are not industrial, such as the ones used by many satellite services providers, are class I products that pose minimal security risks. However, as seen in this chapter, a lateral movement that starts with an attack on these modems may generate a non-neglectable security incident.

Based on these findings, future work could be carried out by performing a detailed vulnerability assessment of the devices identified and evaluating the potential risks that attacks such as lateral movements can have on the identified infrastructures.

3.6 Build cybersecure space links: the US and EU approaches

Operating a satellite is increasingly similar to administrating a computer network, as SATCOM often relies on IP-based space links. However, unlike servers, IP-based space systems have their "wires" open to the public. This means that space systems, as listed above, have to deal with a very broad spectrum of threats, from low sophistication as DoS/Jamming to sophisticated root access gain attempts. For these reasons, cybersecurity must be perceived as a must during the lifecycle of space systems development. This requires a cultural shift for space companies. A holis-

tic approach is needed to consider confidentiality, authentication, data integrity, and availability. The United States and, to a certain extent, the EU are moving in this direction, designing policies and recommendations to face the threats mentioned above. The following section analyzes some guidelines and technical recommendations defined by American and European stakeholders.

3.6.1 The NSA guidelines on SATCOM

According to a cybersecurity advisory published by the United States National Security Agency (NSA) in June 2022 [12], the majority of the SATCOM systems that include terminals, modems, and ground stations should be considered as unencrypted wireless networks, given their lack of encryption. These systems should not be relied upon even if they offer virtual network separation capabilities because, in most cases, they do not provide access control, separation, or confidentiality of sensitive information as the devices mentioned in Table 2. The fact that these networks can be connected to the Internet makes them easily targetable for remote attacks and exploitation. In the US, controlled unclassified information (CUI) must be encrypted at least with commercial network encryption solutions, including Internet Protocol Security (IPsec) or Transport Layer Security Virtual Private Networks (TLS VPNs) [383]. To enhance the security of network infrastructures, the US National Security Agency advises using encrypted services and recommends disabling all clear text administration services such as Telnet, HTTP, FTP (File Transfer Protocol), and SNMP (Simple Network Management Protocol) version 1/2. This measure helps prevent adversaries from easily accessing sensitive information by intercepting network traffic [382]. Administration services should be configured to use up-to-date protocols and have adequate security settings enabled. For remote access to devices, SSH version 2 is the recommended method. Additionally, HTTPS servers should be configured to accept only Transport Layer Security (TLS) version 1.2 or higher to ensure encryption.

As for encryption, the National Institute of Standards and Technol-

Table 4: CNSA Suite 2.0 Cryptographic Algorithms

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197 [377]	Use 256-bit keys for all classification levels.
CRYSTALLS-Kyber	Asymmetric algorithm for key establishment	-	Use Level V for all classification levels.
CRYSTALLS-Dilithium	Asymmetric algorithm for digital signatures	-	Use Level V for all classification levels.
Secure Hash Algorithm (SHA)	Algorithm for compute digests for information	FIPS PUB 180-4 [378]	Use SHA-384 or SHA-512 for all classification levels.
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208 [115]	All parameters approved for all classification levels. SHA-256/192 is recommended.
Extended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software.	NIST SP 800-208 [115]	All parameters approved for all classification levels.

ogy (NIST) released the guidelines SP 800-131A rev2 [380] and SP 800-56A rev3 [381] for the use of cryptographic algorithms and the choice of key lengths. These guidelines recommend that point-to-point communications over IP-based networks should use IKE/IPsec-encrypted VPNs with certificates or pre-shared keys for peer authentication and a Diffie-Hellman (DH) key exchange of at least 3072 bits or Elliptic Curve DH (ECDH) keys of 384 bits or larger (groups 14, 15, 16, 19, or 20). In the US, point-to-point communications should conform to CNSSP 15 standards [383] for National Security Systems (NSS). The CNSSP 15 is the policy regulating commercial cryptographic algorithms' usage for NSS. It is updated periodically to incorporate the latest standards and processes from CNSS and NSA. As of September 2022 (Ver. 1.0), the current version specifies the CNSA Suite 1.0, and will soon be updated to include the CNSA Suite 2.0 and Quantum Computing algorithms [118]. The CNSA Suite 2.0 is detailed in Table 4.

As much as concerns key exchange, the NSA recommends avoiding aggressive mode and using IPsec VPNs to provide mutual authentication to both ends and secure the data in transit. TLS-based VPNs should use similar cryptographic algorithms as the ones in Table 4, and

multi-point encrypted VPNs can be used in architectures where many point-to-point VPNs are unmanageable [330]. The NSA advises using mutually authenticated, encrypted TRANSEC where encryption is applied to the outermost transmission protocol using an approved pseudorandom keystream (AES 256) and key management scheme. Moreover, when using commercial satellite communications for mobile devices, best practice guidance suggests avoiding descriptive naming conventions and identifiers in device configurations to prevent external actors from easily identifying the devices and understanding their purposes.

Regarding procurement, in May 2022, the Space System Command of the United States approved the Infrastructure Asset Pre-Approval (IA-Pre) Initiative [474] in collaboration with the Commercial Services Office (CSCO). The initiative aims to enhance cybersecurity to reinforce CSCO's service evaluations and procurements for the Department of Defense (DoD). The CSCO started accepting IA-Pre applications for a restricted number of assets to perform assessments. The new initiative will replace the outdated self-assessment process where commercial companies submit their system information through a questionnaire, and CSCO evaluates it during acquisition. IA-Pre emphasizes on-site assessments for cybersecurity compliance verification by third-party assessors authorized by the U.S. Space Force Security Controls Assessor (SCA). The program also focuses on effective safeguards application and validation and weak point mitigation to decrease cybersecurity risks that may affect DoD missions that depend on CSCO for services. In the first phase, the US Space Force Authorizing Official will evaluate the cybersecurity assessments of the companies for approval as the industry progresses through the IA-Pre program. Afterward, CSCO will put the industry partner and the evaluated assets on an approved platform list. The industry partner will no longer require a cybersecurity evaluation before being awarded a contract for covered assets. IA-Pre trials started in June 2022.

This framework, however, is applied only to those operators that collaborate with the DoD. For commercial satellite operators not involved in defense initiatives, the regulatory framework is less stringent. One of

the regulatory standards that could apply to these circumstances is the NISTIR 8270 [447]. The document briefly introduces cybersecurity risk management for the commercial satellite industry to start managing cybersecurity risks in space. Developing a Cybersecurity Framework was a response to Executive Order 13636 [88], which aims to enhance the cybersecurity of critical infrastructures. It defines a Cybersecurity Framework (CSF) that adopts a risk management approach to cybersecurity and can be customized for different industries. It offers standardized terminology and methodology that organizations can implement based on their resources and operational requirements. The CSF comprises five functions: identify, protect, detect, respond, and recover. It is presented in a circular format to emphasize that cybersecurity is a continuous process that enables organizations to adapt to evolving cyber threats.

The NISTIR 8270 discusses the importance of creating and maintaining a cybersecurity program for space operations. The CSF helps to implement a cybersecurity program through seven steps effectively [447]:

- Step 1: Establish the scope and priorities of the program. This step is critical to address cybersecurity in the earliest stages of building the components of the space architecture and embedding risk-reducing measures that meet the organizational mission and business objectives into the design and supply chain.

- Step 2: Drive the organization to related systems, assets, regulatory requirements, and its overall risk approach. The organization then works to identify threats and vulnerabilities applicable to those systems and assets.

- Step 3: Create a profile to understand the organization's current cybersecurity posture. An assessment of how the CSF functions are being implemented within the organization is created by listing the subcategory activities that are currently being implemented.

- Step 4: Conduct a risk assessment, where the organization analyzes the operational environment, identifies emerging risks, and uses cyber threat information from internal and external sources to dis-

cern the likelihood of a cybersecurity event and the impact that the event could have on the organization.

- Step 5: Create a target profile by selecting the subcategories that support the organization's desired cybersecurity outcomes.
- Step 6: Determine, analyze, and prioritize gaps. The organization compares the current and target profiles to identify potential gaps. When paired with a threat, a risk assessment can be conducted to determine an overall risk rating. This will allow organizations to create a prioritized action plan to address those gaps.
- Step 7: Implement the action plan.

The Framework is an iterative process that must be repeated regularly when the impact on the organization or the cyber threat landscape changes. According to the NIST and MITRE, regularly scheduled reviews of the security profile, gap reassessment, updated action plans, and completed action plans should be conducted at least every two years and/or after relevant cybersecurity incidents or discoveries in the industry [447].

3.6.2 Defining cybersecurity standards for commercial space sector: European approach

At the European level, ENISA (European Union Agency for Cybersecurity) identified space as a sensitive domain in 2023 and acknowledged the fact that the lack of security requirements in the sector has led to a dearth of analysis and control of space-based infrastructure, which poses a significant security threat [208]. ENISA also recognized that without a broader EU-wide focus, building a strong and secure space infrastructure may take too long, leaving space-based vulnerabilities undiscovered and open to exploitation by private companies, governments, or criminal groups. Moreover, ENISA highlighted that those ground stations, which connect satellites to a central terrestrial hub, are a key element that attackers may target with denial-of-service attacks to disrupt critical military and civilian systems. Introducing space-based weapons may

further shift the geopolitical paradigm, underscoring the importance of addressing space-based infrastructure's lack of analysis and control. Attackers may remain dormant until they execute their exploits during a conflict as a means of hybrid warfare.

Despite these warnings, as of the time of writing this chapter, there is a notable absence of a comprehensive cybersecurity guideline in the EU that establishes clear technical requirements for commercial space actors. Space-based services have only recently been included in the critical infrastructure taxonomy thanks to the NIS2 Directive [169]. Given the lack of coordination, many Member States are acting autonomously, providing more or less general guidelines to commercial space companies to address the issue. In Germany, in 2021, the Federal Office for Information Security (BSI) initiated a working group consisting of experts from BSI, OHB Digital Connect, Airbus Defence and Space, and the German Space Agency at the German Aerospace Center (DLR) to jointly develop minimum cybersecurity requirements for satellites [460].

These workshops resulted in the industry-specific IT baseline protection profile in the first step. However, the document provides only general recommendations and is focused on the in-orbit part of the space infrastructure; to address the very different protection needs of various satellite missions and the other segments, it is planned to detail the requirements in various technical guidelines after the creation of the baseline protection profile and to establish them in the international context.

A recent development is represented by the Network and Information Security 2 (NIS2) [169] directive, approved in November 2022, by the European Parliament that replaces the previous NIS1. As analysed in Chapter 4, the NIS2 Directive formally includes space within the EU critical-infrastructure taxonomy. Here, the focus is on the gap between that legal recognition and the absence of concrete technical requirements for commercial SATCOM actors.

According to the European Telecommunications Standards Institute (ETSI), implementing the Open Security Controls Assessment Language (OSCAL) may be necessary to implement multiple provisions of NIS2 effectively [200]. This is especially relevant for affected essential and

important entities that must satisfy various, constantly evolving requirements across diverse contexts [200]. OSCAL is a standardized data-centric framework developed by NIST that can be used to assess the security controls application of an information system. The goal of OSCAL is to overcome the data conversion and manual efforts to describe security control's application and implementation, moving to a machine-readable format, and automating the security assessment process in several scenarios [554].

A significant step has been carried out by the EU at the end of 2022, with the Cyber Resilience Act [192], a proposed legislation aimed at establishing common standards for connected devices and services not currently covered by regulations such as the NIS2. If approved, the act would impose fines of up to €15 million (16 million $) or 2.5% of worldwide turnover on non-compliant products. The act classifies products into "default," "Class I," and "Class II" categories.

"Class I" products, such as browsers, password managers, and routers, pose, according to the proposal, minimal security risks. Manufacturers must adhere to specific standards or undergo third-party certification. "Class II" products, including software operating systems, industrial routers, and smart meters, present the highest security risk. They require third-party certification before entering the market. Approximately 90% of digital products fall into this category, even those that do not pose significant cyber threats, like photo editing software and video games. The legislation will be implemented in two phases. Within 12 months of adoption, manufacturers must report cybersecurity breaches and vulnerabilities. Within 24 months, member states and affected businesses must comply with the regulations. Some business groups and member states have raised concerns about the act. They argue that third-party judgment of security measures introduces inherent risks in the certification process. Moreover, critics fear potential delays or hindrances to the rollout of essential new technologies and services, as businesses would need to wait for certification before adopting product security measures [92].

As much as concerns Network Router Security Threat Analysis, ETSI defined in May 2022 a Threat Vulnerability and Risk Analysis (TVRA) [200]

assessment guidance that can be considered the latest European attempt to define a clear and standardized risk assessment procedure for this type of technology. However, the technical report only discusses the security of network routers that are enterprise routers or ISP routers; the home and small office routers, which forward IP packets between the home computers and the Internet, are out of the scope of the document. The approach to network router risk analysis used by ETSI involves identifying the key assets of network routers and analyzing their vulnerabilities in detail. The key assets of routers are determined by their architecture and main functions. The analysis begins by identifying the threats in different scenarios that include access-side attacks, inter-device horizontal attacks, O&M attacks, supply-chain attacks, and physical attacks. The ETSI document provides guidelines for a detailed risk assessment for a specific network, allowing the network operator to assess the threat level based on the capability and motivation of an attacker to attack these assets. The risk analysis also considers the security challenges faced by network routers, such as the protection of hardware, software, data, and protocols. It examines the vulnerabilities in these areas and provides insights into mitigating the risks associated with them. The TVRA could be considered a useful starting point to build an efficient risk management strategy for SATCOM user segment.

3.6.3 A comparison of the American and European approaches to space cybersecurity

The first point to be discussed when analyzing the two approaches is the lack of a European set of rules and laws for space infrastructure cybersecurity at the time of writing. In the US, The Satellite Cybersecurity Act [276], reported to the Senate on June 21st, 2022, addresses cybersecurity concerns about commercial satellite systems. The bill mandates that the Cybersecurity and Infrastructure Security Agency (CISA) creates and maintains a publicly available repository of resources that focuses on the cybersecurity of commercial satellite systems. Additionally, CISA must compile voluntary recommendations for developing, maintaining, and

operating these systems, which must include measures for safeguarding against cyber-related vulnerabilities, risks, and attacks. CISA must also implement its activities in collaboration with the private sector wherever possible. The bill further necessitates the Government Accountability Office (GAO) to investigate and release a report on two issues. Firstly, the federal measures taken to support the cybersecurity of commercial satellite systems, particularly in the critical infrastructure sectors, must be studied and reported. Secondly, the government's dependence on commercial satellite systems owned or controlled by foreign entities must be examined. The GAO must coordinate with designated federal agencies to conduct this study and report. In Europe, the only primary source of law dealing with space cybersecurity is the NIS2 Directive. However, how it will be applied and its consequences will be clear only at the end of 2024. Agencies such as ENISA and EUSPA have not yet clearly defined their role and contributions as much as concern SATCOM or in general space cybersecurity. Even if Member States are developing their cyber strategies and laws in the field, before developing pan-European space infrastructure, it should be determined a pan-European cyber strategy for space. Considering space as a critical infrastructure pivotal to national security interests, US agencies such as NSA, FBI, and CISA constantly produce advisories, technical reports, and recommendations about SATCOM and space cybersecurity, updating users and companies on threats and suspicious activities observed in the wild.

At the time of writing, the same activity cannot be observed at the European level, there is no equivalent of a National Security Agency in the EU, where ENISA or EDA could maybe cover such a role.

As much as concern standards in the United States, the NIST produced several resources guiding the sector as the Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services (NIST IR 8323 [47]), Introduction to Cybersecurity for Commercial Satellite Operations (NIST IR 8270 [447]), and Satellite Ground Segment: Applying the Cybersecurity Framework (CSF) to Assure Satellite Command and Control (NIST IR 8401 [345]). In Europe, the TVRA produced by ETSI should be adapted

to recent threats and scenarios, including satellite modems and routers. For this research, however, it should be considered that approaches vary according to projects and infrastructures, and $IRIS^2$ will probably be one of the first examples of Member States developing a common set of rules in the sector.

3.6.4 A wider look: The Cybersecurity Guidelines for Commercial Space Systems in Japan

The landscape of cybersecurity space policies is constantly evolving, and new standards, recommendations, and guidelines are constantly being developed by States and international organizations. To give the research a wider perspective, we analyze in this section the Cybersecurity Guidelines for Commercial Space Systems developed by the Japanese Space Industry Office, Manufacturing Industries Bureau, Ministry of Economy, Trade, and Industry (METI)[470].

The Guidelines developed by METI depict a complex scenario where more than 90 security incidents occurred both inside and outside Japan between 1986 and 2022 with a significant increase in the last 5 years. According to the Japanese authorities, the critical and challenging nature of cybersecurity for space systems is underscored by several main factors. These include the expanding roles of space systems in Japan's security, economy, and society, the proliferation of digital technology such as unmanned and automated space systems along with increased cloud services usage, the growing complexity of networks including inter-satellite communication and connections with ground communication networks, the rise in the number of satellites, ground stations, and data volume due to satellite constellations, and the increased complexity of supply chains resulting from the commercialization of space systems technology and the incorporation of consumer technology.

The purpose of these Guidelines is to collect essential information in an accessible format. Key elements covered by these guidelines encompass examining and presenting security risks associated with space systems. Furthermore, the guidelines delineate fundamental security mea-

sures that should be scrutinized by all stakeholders involved in the intricate web of space systems.

The guidelines cover satellite systems and ground systems, including satellite operation facilities, satellite data utilization facilities, and development and manufacturing facilities operated by the commercial sector. They apply to the entire lifecycle of satellite systems, including design, development, manufacturing, operation, maintenance, and disposal phases. It is important to note that the launch facility is not covered in the document.

A relevant difference between the previously analyzed approaches is that METI uses the Cyber/Physical Security Framework (CPSF) Ver. 1.0 [142] to address cybersecurity risks in commercial space systems. This is a multi-stakeholder approach that ensures the security of the entire supply chain, including affiliated companies and business partners. CPSF considers the industrial society in three layers and organizes risk sources and measures at each layer. The layers are structured as follows:

- First Layer: Connections between organizations
- Second Layer: Mutual connections between Cyberspace and Physical space
- Third Layer: Connections in Cyberspace

In the first part of the Guidelines, seven example risk scenarios are included, and for each of them, a series of measures for each of the three layers is defined. The document also defines a series of Cybersecurity requirements and basic measures connected to it to be implemented. This technical approach links each measure/requirement with the stakeholders that should be involved in it. An interesting tool proposed by METI is the Cybersecurity Management Guidelines Implementation Status Visualization Tool, a table that can be used to assess the company's efforts on 10 key items. This tool is for enterprises and organizations with 300+ employees. It has 40 questions and uses a 5-point scale to measure the status of measures taken. The Japanese approach to cybersecurity for space systems and networks is highly technical and practical. However,

the complexity of the process can be a challenge for companies that need to navigate through it. To overcome this, companies may need to develop automated checking and verification tools based on the Guidelines. This approach is one of the first attempts by a sovereign nation to develop clear guidelines for the sector. It provides non-trivial examples of threat scenarios that can affect space infrastructure and systems. It is important to note that Japan like the rest of the countries analyzed does not have any legally binding cybersecurity requirements for space companies. The guidelines provided in the document are optional, meaning that companies are free to follow them or not. However, even if they choose to follow international standards, it may not be enough to ensure the safety of space infrastructure, as we have seen in the past. The current state of space cybersecurity policies is constantly changing. In Europe, most countries and space agencies are still developing their cybersecurity toolkits. While the Union may establish a Space Law, it may be beneficial to examine the approaches taken by other countries, such as Japan, and push member states to work together to prevent any harmonization-related problems in the future. As the policy and industrial landscape continue to evolve future research should be carried out to compare the new standards, technical guidelines and policies in the field, having also a wider look and including the activities of non western countries to understand their priorities and threat perception.

3.7 Lessons learned to build a resilient European Satellite Communication Constellation

Cyber risk management for space systems is complex and challenging, as ground stations and user terminals are exposed to a wide range of cyber threats and vulnerabilities. When developing $IRIS^2$, the new space infrastructure for secure communication, the EU should consider some of the key challenges associated with cyber risk management. As the main point, the complexity of the space ecosystem should never be underestimated as it involves a large number of stakeholders, including governments, private companies, and international organizations. This

complexity makes it difficult to implement a unified approach to cyber risk management, as different stakeholders may have different priorities and resources. This is extremely relevant for $IRIS^2$ since this constellation will be implemented through the support of the private sector probably with commercial solutions already available on the market. Moreover, the space sector is subject to a rapidly evolving threat landscape, with new threats and vulnerabilities emerging regularly. Keeping up with them is challenging, particularly for organizations with limited resources. As already mentioned, a weak spot is represented by supply chain vulnerabilities as ground and user segments rely on a complex supply chain. Malicious actors may target the supply chain to gain access to the ground station, compromise the hardware or software, or steal sensitive data. In this, as in any other scenario, human error and insider threats can pose a significant risk. Staff members may accidentally introduce vulnerabilities or may be targeted by malicious actors seeking to gain unauthorized access to the system. To manage cyber risks effectively, all the actors involved in the management, administration, and functioning of space infrastructure should implement a range of best practices that we report briefly below.

3.7.1 Access control

A first best practice consists of implementing access controls to limit access to critical systems and data to authorized personnel only. Access controls should be based on the *principle of least privilege*, meaning that staff members are only given access to the systems and data they need to perform their job duties. Since network perimeter devices are crucial components in securing a network, Access Control Lists (ACLs) should be configured to make them work together and regulate inbound and outbound traffic. These access control rule sets should be specifically configured to allow only necessary services and systems to support the network's mission. It should be recommended to use a deny-by-default, permit-by-exception approach, which involves carefully selecting which connections to allow and then creating rule sets that focus on allow-

ing only those connections. This approach allows a single rule to deny multiple types of connections, reducing the need to create separate rules for each blocked connection. Failure to adopt this approach can lead to unnecessary access, increasing the risk of compromise and information gathering. If additional perimeter rule sets are needed dynamically, an intrusion prevention system (IPS) should be put in place to prevent adversaries from exploiting the network. It is also recommended to enable logging on all rule sets that deny or drop network traffic, as well as on successful and unsuccessful administrator access to critical devices. A network access control (NAC) solution should be implemented to prevent unauthorized access to a network. Such a solution prevents unauthorized physical connections and monitors authorized physical connections in the network. Port security can be implemented on switches to detect unauthorized devices connected to the network via a device's media access control (MAC) address.

3.7.2 Network segmentation

Segmenting the network is needed to ensure that critical systems and data are isolated from non-critical ones. This can limit the impact of a cyber attack, as the attacker will only have access to a limited portion of the network. Moreover, critical systems should be physically separated from other networks like the Internet. Internal routers, switches, and firewalls should be restricted to only allow necessary ports and protocols for valid mission needs. To protect against lateral movement by attackers within a network, similar systems should be grouped together logically. Network segmentation reduces the likelihood of such attacks, as it limits the ability of attackers to exploit other systems. The CISA and the NSA recommend logical grouping through isolation of similar systems into different subnets or VLANs, or physical separation using firewalls or filtering routers. This approach makes access restrictions between systems easier to manage, control, and monitor. Access control lists can be duplicated and applied directly to switches to limit access between VLANs, or they can be applied to core routers for routing between internal subnets.

3.7.3 Encryption

Encrypting sensitive data both at rest and in transit prevent unauthorized access and ensure confidentiality and integrity of data. The main guidelines for encryption have been described in the dedicated section above. The Committee on National Security Systems Policy (CNSSP) 15 has established minimum recommended settings for ensuring robust encryption in these networks. According to CNSSP 15, it is necessary to use Diffie-Hellman Group 16 with 4096 bit Modular Exponent (MODP) and Diffie-Hellman Group 20 with 384 bit elliptic curve group (ECP) for secure key exchange. Additionally, Advanced Encryption Standard (AES)-256 should be used for encryption, and Secure Hash Algorithm (SHA)-384 for hashing. At the time of writing, by adhering to these recommendations, SATCOM networks can achieve the highest levels of security and protection against unauthorized access and data breaches.

3.7.4 Continuous monitoring

Implementing continuous monitoring to detect and respond to cyber incidents can involve the use of intrusion detection systems, security information, and event management (SIEM) systems, and threat intelligence feeds. Operators should not only monitor their network but stay updated on recent CVEs and exploits published as well as password leaks. These last steps may be implemented by monitoring notorious blogs and forums on the dark web, where these data are often published.

3.7.5 Incident response

Developing an incident response plan to ensure that cyber incidents are detected and responded to in a timely and effective manner. The incident response plan should cover areas such as incident notification, escalation, investigation, and communication. The prompt detection and response of an incident are pivotal in determining the impact of an attack. In the event of detecting a breach before the deployment of wiper malware, the effectiveness of the incident response team's handling and

response to the alert can make all the difference between preventing data loss and facing complete data destruction.

3.7.6 Regular Patching and Updating

Regularly patching and updating user segment modems, and routers with the latest security updates and firmware will help to ensure that the network is protected against the latest security threats and vulnerabilities. Software must be designed to be patch friendly and provide confidence for operators to patch frequently and safely.

3.7.7 Training and awareness programs

Staff training and awareness programs are essential to ensure that employees are aware of the latest cybersecurity threats and how to identify and report potential cyber incidents. The policy should cover regular training sessions, simulated phishing exercises, and best practices for secure data handling.

3.7.8 Establishing a well-defined cybersecurity policy

Developing clear policies, procedures, and guidelines for managing cyber risks is critical for any organization. Cybersecurity policies and procedures define the rules and expectations that employees and third-party contractors must follow to maintain the security of ground station systems and data. A comprehensive cybersecurity policy should cover several aspects, including access controls, incident response, data classification, and training and awareness programs. In this context, policies should not be aimed at regulating any aspect of space systems, including technical details, but specifying what standards and requirements operators should choose when developing space infrastructure.

3.7.9 How Public Sector Support Can Help Implement Crucial Measures

Often the implementation of the basic security practices in the commercial SATCOM industry has been overlooked, primarily due to a variety of possible reasons. The complexity of SATCOM systems, involving cutting-edge technology and large-scale distributed networks, poses a significant challenge in implementing security measures. Budgetary constraints also play a role, as the cost of implementing extensive cybersecurity measures can be prohibitive for some organizations, leading them to underfund cybersecurity initiatives. In swiftly moving sectors, businesses may choose to prioritize speed-to-market over implementing strict security controls, thereby leaving security gaps. Lastly, in some instances, the regulatory environment in the satellite communications industry might not have kept pace with the rapidly evolving threats, causing an absence of mandatory security practices. These potential reasons, among others, underscore the urgent necessity for a thorough analysis of cybersecurity practices in the SATCOM industry.

As analyzed, security controls and standards in the field are starting to be developed. However, just because they exist, it does not mean they are implemented and enforced. Considering the complexity of space infrastructures and their interconnectedness with other critical domains, what emerges are the challenges arising for companies to perform extensive and effective cybersecurity risk assessments and analyses without external partners [316]. This should not be intended only as consultancy services and outsourcing but as the need to implement strong relationship and cooperation mechanisms with institutions and governmental agencies.

With this in mind, the Viasat case underscored several crucial lessons and managerial implications for companies. First of all, it showed how well public-private partnerships can work in responding to cyber-attacks. Part of Viasat's response plan involved collaborating and exchanging information with various government bodies, intelligence units, and law enforcement agencies. The National Security Agency's Cybersecurity

Collaboration Center (NSA CCC) had an established relationship with Viasat [155]. They promptly engaged after the attack, working alongside the Viasat team to discuss and analyze incoming data and insights. Furthermore, they aided in disseminating this information across different agencies. The NSA independently used the insights and data provided by Viasat, both immediately and in the subsequent months, to conduct its own analysis. This allowed them to identify connections to known threat actors, comprehend cyber threats more comprehensively, and offer additional mitigation guidance to a wider audience. For Viasat, understanding what constitutes "normal" operations proved invaluable in narrowing down their response. This knowledge facilitated the identification of abnormal actions, such as unusual file transfers or atypical toolkit usage, providing critical insight into the attack's nature. However, many companies lack a clear inventory of assets or a comprehensive grasp of their normal operations, hindering swift response strategies [390]. Automated tools for these tasks exist but have not been widely applied in the space sector [121, 544].

Taking these lessons into account, what may be lacking in Europe is a strong and established dialogue between companies and institutions, but also among companies themselves. Suppose we consider budget constraints as being one of the main barriers to standards and control implementation. In that case, these obstacles can be reduced significantly by implementing cooperative solutions or peer learning strategies.

European policymakers realized the importance of cooperation mechanisms: in October 2023 the Commission and EUSPA established the EU Space Information Sharing Centre (ISAC) [216], a collaborative initiative aimed at fostering information exchange, promoting collaboration, and advocating best practices among private organizations. Its core objectives include sharing insights on security, cyber incidents, and vulnerabilities, offering early warning systems, and enhancing cybersecurity resilience through shared knowledge and expertise. Participation is open to founding members (legal private entities from the Space sector established in the EU), academic institutions, and recognized bodies with space security expertise. Public partners, including institutions,

agencies, and national Space Agencies, are also welcome to collaborate in solving cybersecurity challenges. Such initiatives can significantly reduce the financial burden of small and medium-sized space companies, facilitating information exchange and even peer learning in the sector. However, the limits of such an initiative are clear; even if the EU ISAC will propose ready-to-use and actionable resources and tools for participants, including to guide the implementation of relevant EU regulations and shared best practices, it will not be an incident response body. Providing an answer to a security incident will remain the responsibility of each Member/company.

The Satellite Cybersecurity Act mentioned in Section 3.6.3 can be considered as a similar initiative in the US, with the sole difference that the American approach envisioned a stable office and staff to develop its tasks. An idea of the financial implications of the initiative is given by the Congressional Budget Office's (CBO) analysis [113], which foresees 6 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. The CBO approximates an expenditure of $14 million from 2023 to 2028 for implementing the bill. ENISA or EUSPA in Europe have not conducted similar estimates, and there are no indicators to suggest a similar investment in support of the European sector. This significantly limits the capabilities of the Space ISAC in comparison.

3.7.10 Navigating Regulatory Challenges: How Companies are Adapting to the Evolving Landscape

Lawmakers across Europe and the rest of the World have started drafting space laws that incorporate basic or advanced cybersecurity requirements for the sector. However, at the time of writing, the Space Law in Europe is still in its early stages. The European Commission has asked the industry to share its views on four different options [194], two of which involve the creation of binding rules and detailed technical stan-

dards developed by the European Standardisation Organisations. The proposed options would require satellite operators, manufacturers, and Member States Authorities to comply with mandatory cybersecurity regulations. The implementation of this act may have negative managerial implications that could hinder the sector's steady growth, which is expected to continue in the future. A clear assessment of the impact of this Law on the sector has not been developed, but a possible comparison with similar regulations is possible using ENISA's study on the effects of the NIS [211]. ENISA measured that the NIS had a positive impact on cybersecurity investments for many sectors. In particular, in 2023 Operators of Essential Services (OES) and Digital Service Providers (DSP) earmark 7,1% of their IT investments for Information Security, an increase of 0.4% compared to last 2022 [211]. Similar studies highlighted how the effect of NIS2 may require a 0,92% turnover as compliance cost [241], a similar increase if provoked by the future Space Law, may impact negatively the SMEs in the space sectors.

The Industry, especially the New Space sector expressed caution toward the future Space Law, encouraging the application of different cybersecurity standards tailored to each space mission's unique needs, as less stringent standards for commercial missions in LEO, and more high-security ones for those in GEO [467]. However, such an approach may be challenged by the dual use of constellations such as the Viasat one or by their multi-orbital nature as in the case of $IRIS^2$. Overall the sector seems to approve a cybersecurity-by-design process in program management, and in mission operations, but recommends introducing mission-tailored higher cybersecurity labels without applying them to the entire industry [467]. Without any doubt, adhering to certain aspects of the law will cause an increase in the costs of data, satellites, and services for companies involved in the whole space value chain. There are uncertainties as to whether any measures will be undertaken by the institutions to alleviate the costs associated with compliance, to ensure that European companies do not face any disadvantage in the global market [175].

Taking a closer look at the attitude of companies towards these new challenges, it is clear how many of them are changing their risk appetite

towards cybersecurity risks due to increased attacks. Looking at the financial reports of industry leaders such as Viasat [536] or Eutelesat [217], cybersecurity is now part of their risk factors lists. Companies realized that cybersecurity *"requires significant management attention and resources to remedy the damage that results and delay progress on business objectives and may cause companies to make payments to their customers to reimburse them for damages, pay them penalties or provide refunds; and provoke damage to their reputation with their customers (particularly agencies of the U.S. government) and the public generally"* [111].

To mitigate these risks, companies started hiring professionals such as Chief Information Security Officers, Cyber Accreditation Officers, Cyber Risk and Security Engineers, Security Operations Managers, or even engineers to comply with specific US procurement processes [217]. Space companies are also increasing the involvement of researchers and cybersecurity professionals. In the US the Department of Defense recently sponsored a competition for white hat hackers to attempt to breach an active satellite [245]. While industry leaders are opening bug bounty programs to speed up the discovery of vulnerabilities in their systems [479]. However, small and medium-sized companies in Europe may not have the resources to implement these actions.

Based on our analysis, we can conclude that the security aspect of space is facing a significant issue of fragmentation. This problem mainly concerns the stakeholders and governance of the sector, which could potentially hinder the public-private partnership essential for its growth. The European Union and national governments are finding it challenging to regulate and control the dissemination of technology in space and other sectors. The number of states with space programs has grown significantly, from the original 2 to approximately 70 in 2022 [182], and the rise of private corporations and non-governmental organizations in space has contributed to a more scattered group of stakeholders. Governance can be quite fragmented, especially in Europe and in the cyber domain. We can observe this by looking at the separation of cyberspace and space, as well as the confused interaction and role definitions among the Commission, ENISA, and EUSPA. This fragmentation can create un-

certainty, as companies are not certain about the processes they should be involved in, the standards they should implement, or the jurisdiction, harmonization, and costs of new regulations.

The complexity of space systems, high cybersecurity costs, and unclear regulations make it necessary for the public and private sectors to work together more closely. On one side, space companies need to communicate their needs and inform stakeholders about the kind of support they require. On the other hand, EU institutions and agencies need to establish clear governance and tools to not only support the industry but also develop cyber risk strategies with it. Implementing strong regulations and standards can bring about significant changes in the cybersecurity of the space industry. However, as with other sectors, there is a trade-off between security and technological progress. The EU needs to exhibit political commitment and allocate appropriate resources to support the industry without hindering growth or burdening businesses with excessive financial or regulatory demands that they cannot manage.

All in all, determining the root causes behind the lack of security measures implementation in space is not an easy task. However, research has indicated that the space sector cannot achieve a high level of security on its own and requires greater public support. Regulators need to consider the complexity and fragmentation of the sector and not increase them while designing new policies. Preliminary attempts to address security in this domain show that initiatives that involve cooperation between the public and private sectors can help enhance security measures. These initiatives include enhanced information-sharing capacities, implementation of online databases with cybersecurity resources for satellite operators, the establishment of a clear inventory of assets and normal operations, state sponsored ethical hacking competitions, bug bounty programs, enhanced hiring capacity for cybersecurity experts, and the inclusion of cyber risks in the financial considerations of companies. These actions are not to be considered just optional but essential to improve space resilience and prevent disruptions. However, the low maturity level of these initiatives (many of them are still in the early stages and not widely adopted) may partially explain the lack of security in the space sector,

together with the appearance of new, more complex, and frequent space threats.

3.8 Related work

Numerous studies have recently been carried out in the field of SATCOM cybersecurity. Tedeschi et al. [494] provide a comprehensive overview of the link-layer security threats, solutions, and challenges faced when deploying and operating satellite-based communication systems. Their work covers various domains related to satellite cybersecurity, including physical-layer security, cryptography schemes, anti-jamming strategies, anti-spoofing techniques, and quantum-based key distribution schemes. The paper highlights the most essential techniques, peculiarities, advantages, lessons learned, and future directions in each of these domains.

Benitez [49] addresses the cyber security risks present in VSAT terminals and provides methods for users to secure their data transmission through VSAT networks. The research also includes a literature review of publications about vulnerabilities in VSAT systems by cyber security organizations, VSAT service providers, and satellite communication market research.

Comprehensive and pioneering research on the field is the one by Santamarta [441] that provides an in-depth analysis of the vulnerabilities and risks associated with SATCOM security. He explains how attackers can exploit these vulnerabilities to gain unauthorized access to sensitive information, disrupt communication networks, and compromise safety. The paper also highlights the importance of responsible practices and proactive measures to prevent such attacks. The document focuses on a specific aspect of SATCOM security. Furthermore, the paper discusses the impact of SATCOM security on aviation, maritime, and military sectors. Although the white paper serves as a valuable resource for anyone interested in understanding the importance of SATCOM security and its impact on various industries, the research is focused on a limited number of terminals and is not updated, even if the majority of those terminals are still operational today.

One of the few recent works that focused on modem vulnerabilities in SATCOM is by Smailes et al. [463]. Their study focuses on the security vulnerabilities of the Starlink user terminal, a satellite modem used for Internet connectivity. The authors audit the attack surface presented by the Starlink router's admin interface and use fuzzing to uncover a denial-of-service attack. They explored the impact of this attack on different scenarios and provided recommendations to better secure satellite routers. The paper also discusses wider implications and lessons learned in terrestrial router security that can be applied in this new context.

Interesting research has been carried out in different fields such as aviation and maritime security. Dave et al. [159] discuss the increasing vulnerability of the aviation sector to cyber attacks, particularly in the areas of communication, navigation, and surveillance systems. The authors provide an overview of the aviation system and the wireless technologies used, as well as the associated security issues. They also identify threats, attack taxonomy, and existing security frameworks and solutions in the aviation domain. While the paper does not specifically focus on SATCOM cyber security, this area is included in the broader discussion of communication system vulnerabilities. In the maritime domain, Caprolu [74] developed a comprehensive investigation of cybersecurity issues associated with modern vessel systems. It analyzes the communication technologies and computer systems used within large vessels, pointing out several security issues rooted in their design and operational mode. The paper also relates these vulnerabilities with recent incidents and attacks involving vessels and identifies the weak points that any modern vessel needs to mitigate toward the enforcement of the latest IMO resolutions. The paper deals with SATCOM cybersecurity by discussing the vulnerabilities of communication technologies on vessels and the security requirements for SATCOM datalink systems for future air traffic management.

Now we compare this thesis with the papers mentioned above and summarize the comparison in Table 5. The current thesis' main novelty is that it considers the new European multi-orbital constellation for satellite communication $IRIS^2$ and the political implications of cyber risk in

the field of a European SATCOM infrastructure. Modem and router security has seldom been addressed in the field of SATCOM, while attacks on these components are revealed to be common. Lastly, the works above still lack an accurate cybersecurity assessment of commercial SATCOM networks that may be exposed to threats, this is also due to the NIS2 incident reporting requirements that are still not mandatory for the sector. Moreover, they miss a comparison with a clear set of rules and standards at the European level that can be part of the European strategy for space and defence. In conclusion, the user segment has lately been neglected by researchers as recent works on this part of the infrastructure are missing.

Table 5: Literature Source

Source	User Segment	Considers IRIS²	Legal Approach	In-field Analysis
Tedeschi[494]	✓	✗	✗	✗
Benitez[49]	✓	✗	✗	✗
Santamarta[441]	✓	✗	✗	✗
Smailes[463]	✓	✗	✗	✗
Jacobs[305]	✗	✗	✗	✓
This thesis	✓	✓	✓	✓

3.9 Conclusions and future work

In the first part of this chapter, we described the composition and use cases of SATCOM technologies, and we later focused on the user segment component. We highlighted the need for increased research in the field of cybersecurity for space infrastructures, particularly in the user and ground segments of satellite communication systems. We discussed the vulnerabilities and risks associated with these components, highlighting the lack of cyber posture in the sector. It also explored the impact of attacks on different scenarios and provided recommendations for securing satellite routers. The chapter closely analyzed the case study of the attack on the Viasat network in Ukraine, collecting important lessons and recommendations for future cybersecurity researchers and policymakers

that aim to design policies to protect the European space infrastructures such as $IRIS^2$.

The research emphasizes the importance of accurate cybersecurity assessments and the development of clear rules and standards at the European level. Comparing various cybersecurity frameworks and some of the first standards for the sector the paper addressed the urgent need for a dedicated risk assessment strategy that could focus on the last component of the SATCOM chain, the user segment. We addressed how, in this setting, the NIS2 Directive's obligations could deal with some but not all of the needs to secure the infrastructure. We highlighted the need for constant supervision and active monitoring that should be conducted by entities such as CISA in the United States.

In conclusion, the analysis of the Viasat case study highlighted the implications of SATCOM security in several sectors and the cascading effects that an attack can have on energy, transport, and civil security to cite some. The chapter highlighted the vulnerabilities that affect some of the user segment components on the field through the use of search engines such as Shodan, showcasing how a big part of the commercial infrastructure can be easily accessible by attackers. Overall, the chapter calls for a comprehensive risk assessment strategy and the implementation of guidelines to enhance the security of commercial SATCOM networks in view of the new European projects such as $IRIS^2$.

Despite addressing several gaps in the current research, the present work could be further extended, deepening the analysis carried out with Shodan, maybe using other tools or performing penetration testing on some of the assets found.

In addition, it is important for future research to focus on obtaining empirical data and real-world scenarios in the field. This can be done by creating a comprehensive dataset of vulnerabilities, breaches, and cyber incidents affecting the sector. Such a dataset can help map out threats, actors, and trends more accurately.

Moreover, future research could address the lack of a specific cybersecurity framework focused on the ground and user segment. The managerial and theoretical implications that may result from implementing

robust cybersecurity practices in the field may also be further investigated.

The comparative legislative analysis should expand to include non-western countries such as India and China, which are emerging as new space powers [484].

Finally, future work may explore the implications of AI in the field, supporting companies and facilitating the implementation and enforcement of new laws and standards. AI escalating capabilities carry the promise to bolster cybersecurity through enhanced threat detection, automated response systems, and enriched strategic protocols and procedures [76].

Chapter 4

Space Cybersecurity Governance

4.1 Introduction

Following the technical analysis of SATCOM vulnerabilities in Chapter 3, this chapter broadens the perspective by examining the governance frameworks, institutional responsibilities, and policy instruments that shape how space cybersecurity is—or is not—regulated across major jurisdictions.

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 two years. 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 or energy in the US.

This chapter draws substantially on the paper: *"Space Cybersecurity*

Governance: Assessing Policies and Frameworks in View of the Future European Space Legislation" [82] and 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 US, 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. 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 4.2 focuses on cybersecurity governance in space in the selected countries. In particular, we discuss how the United States, United Kingdom, 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 4.3 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 [376] for the US, 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, the capabilities of the European Space Agency and the possible future cybersecurity requirements that may be included in the European Space Law 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 4.4, we identify gaps in the existing instruments and provide recommendations for policymakers developing the European Space Law (EUSL). Finally, in Section 4.5, we translate some of the possible cybersecurity recommendations into actionable guidance using Center for Internet Security (CIS) Security Controls.

4.2 Towards 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 and ground stations as a service 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 non-military 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 IRIS², 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.

4.2.1 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 [370]. The Department for Science, Innovation and Technology (DSIT) 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 (FCDO) manages international cybersecurity activities, administers the Conflict, Stability and Security Fund, and oversees the National Cybersecurity Centre and the National Cyber Force in collaboration with the MoD. In case of a cyber incident, public agencies such as the National Cybersecurity Centre (NCSC) [491], designated under the NIS Regulation, serve as the primary point of contact, technical authority, and Computer Security Incident Response Team

(CSIRT). 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 (RDSPs) 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 thirteen critical infrastructure sectors, and the UK Space Agency is responsible for ensuring its resilience [517]. 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 [520]. 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 (NPSA) was created to protect the nation's critical assets, with a mission to build resilience to national security threats [518].

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 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 [279].

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 [279]; highlighting the possible drawbacks of over-regulating 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 (DBEIS) coordinates civil space policy, the National Space Strategy assigns responsibilities to ten key government departments and agencies [521]. 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.

Despite fragmented governance, the UK has a high awareness of the cyber risks connected with the space sector. The 2023 National Risk Register (NRR) [260], 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 (PNT) services (significant impact), and deliberate disruption of UK space systems and space-based services (moderate impact). The document highlights how the 3 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 [337] 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 network and information systems. 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 Civil Aviation Authority has developed guidance on cybersecurity, which is included in our analysis in Section 4.2.5.

In conclusion, even if recognized the cyber threats to space assets and started to develop space capabilities against them [7], 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.

4.2.2 Space Cybersecurity Governance in the US

With the highest number of cyberattacks targeting its systems, the United States developed its resilience and response capabilities in every domain. Recognizing early the growing importance of safeguarding space assets, the US established in 2019 the only independent space force existing to date, to ensure the protection of critical infrastructure beyond Earth's atmosphere [527].

The main entity responsible for cybersecurity in the US 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 (FCEB), a part of the executive branch of the United States government that is responsible for managing and executing the policies and programs of the federal government [261]. With a budget of 3 billion for 2024 [11], 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 United States has prioritized the protection of its space assets by establishing the US Space Force (USSF) [171]. 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. Established on July 24, 2020, Cy-

ber 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 [43], the US 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 [500], also known as Cybersecurity Principles for Space Systems. The act is a presidential memorandum, a form of order issued by the President of the United States 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 [362]. 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 United States 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:

- cybersecurity by design considerations and using risk-based engineering;
- implementation of cybersecurity plans that include protection against unauthorized access, physical protection, jamming, spoofing, and supply chain risks;
- collaboration among space system owners and operators for promoting best practices and sharing threat information within the industry;

- 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 [342]. 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 [36]. 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 structures [99]. However, decisions have not yet been made for the implementation of these recommendations.

In conclusion, the United States recognizes that cybersecurity is an all-encompassing and transversal goal that applies to all domains, including space. It distinguishes between space and non-space 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 **??**, alongside NASA's Space Security: Best Practices Guide [376] (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.

4.2.3 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 US, 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)[58]. 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 gath-

ered and stored information on armament and rocket technologies[58].

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)[397]. In 2022, Germany was the largest contributor to the ESA budget with 20.8%, and in 2023, was in the top 3 European countries for governance space spending, with 2.286 billion euros[187]. 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 [413], 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 [301], 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 author-

ities, operators of critical infrastructures, and companies in the public interest.

The other main pillar of Germany's cybersecurity policy is the BSI Kritis Regulation [5]. 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 two 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 [2] 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 pub-

lications 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)[452] on Information Security for Space Systems and the IT-Grundschutz profile for the ground segment. These documents are analyzed in detail in Section 4.2.7.

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. This may be attributed to underfunding or over-regulation, 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 4.4.

4.2.4 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., UK and Germany) have a space ISAC. Furthermore, some of these countries (e.g., the US) 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 6.

Table 6: Space cybersecurity governance overview

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

Based on our analysis, the US 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 US 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 [1], (analyzed in the next section) but still have failed to identify the agency that will take care of its resilience.

In contrast to the US, 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 4.2.5), leaving companies without clear rules to follow. While the aviation authority has developed some useful guidelines (see Section 4.2.5), 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 at-

tempting to mitigate them with non-mandatory 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.

4.2.5 Understanding UK Space Cybersecurity: Insights from UK Space Agency and Civil Aviation Authority

In May 2020, the UK Space Agency released a 20-page document titled the "Cybersecurity Toolkit" [13]. 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 Civil Aviation Authority (CAA) has developed a guidance document on cybersecurity strategies for applicants and licensees in the spaceflight industry [45]. The CAA is responsible for licensing all spaceflight activities in the UK [44] 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:

- **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.

- **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.

- **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.

4.2.6 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 [1], 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 [96].

The proposed Act in the US Senate aims to address and improve the cybersecurity of commercial satellite systems through several provisions. Firstly, it mandates the Comptroller General of the US 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 6 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 [81].

Although the Satellites Cybersecurity Act has not yet been passed, some parts of the United States 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 [81]. 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: Best Practices Guide[376] (BPG), 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 multi-dimensional 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 twelve 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.

4.2.7 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 [452]. 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 [57]. However, there is no mention of any post-quantum 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 [57]. 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[452], 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 towards 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.

Given the key function of ground stations, business continuity is particularly important; 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 ex-

ternal 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 non-binding 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.

4.3 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 European Space Agency (ESA) and the European Union have recently emphasized the significance of space cybersecurity. ESA has adopted a dedicated cybersecurity strategy [389] to safeguard its systems and has pointed out the need to develop special-

ized capabilities and expertise.

The European Commission, supported by the European Union Agency for the Space Programme (EUSPA), has enacted Regulation 2021/696 [392] 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 European Space Agency. Then we explore the proposal of a European Space Law and the cybersecurity requirements that may be involved.

4.3.1 The European Space Agency's cybersecurity capabilities

On April 18, 2011, the Computer and Communications Emergency Response Team of ESA (ESACERT) received a report that a gray hat hacker, known as TinKode [143], 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 (DMZs) 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" [389], 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 & Cyber Panel, the Industrial Security Panel, and the relevant project/program.

ESA's newest strategic document [389] 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 Germany, responsi-

ble 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 [185]. 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 non-trivial 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 [477].

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 European Space Agency 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.

4.3.2 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 ecosys-

tems. 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.

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 United States, Australia, the United Kingdom, and the European Union [225]. 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) [529] 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

[565]. 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 fault tree analysis 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 [352] and, in particular, the UK Device Security Guidance [266].

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 [266].

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 European Space Law 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 European Space Law from a policy-centric framework into a technologically grounded legal regime defined by precise, enforceable technical norms.

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 [558].

Among its recent publications, the CSSDS includes the "Space Data Link Security Protocol [3]" (CCSDS 355.0-B-2), 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 [3] 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 (SPI), Security Header, and Security Trailer, ensuring consistent implementation across different mission profiles. The protocol also incorporates a well-defined structure for managing Security Associations (Sas), 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 anti-replay protection, message authentication codes (MACs), 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 (OSI) 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 [3] 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 (CNES), and NASA [3]. 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 [356].

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[3] 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 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 [4]) CCSDS 732.1-B-3. 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 (QoS) 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 [450], 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.

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 Common Weakness Enumerations. 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 Unified Space Data Link Protocol (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 European space law 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.

4.3.3 Toward a European Space Law

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 [104] 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 October 17, 2024, the Commission published the 2024 Work Programme [103], 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 [164] 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 7, 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.

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,

Table 7: Cybersecurity requirements of the EUSL, Option 2

Risk Area	Requirement
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, links) • detection of incidents: effectively activate alerts and identification of interferences, cyberattacks, spoofing, jamming, as well as incidents related to physical infrastructures • cyber and physical protection and prevention measures: encryption, malware protection policy, patch management, increased tolerance to noise, mitigation strategies, back-up management • business continuity policy, with response and disaster recovery plans • testing the ICT systems • reporting of significant incidents • communication in 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, and use cases
Reporting of significant incidents	Handling of all incidents: • reporting of significant incidents (cyber and non-cyber 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 of ICT systems connected for maintenance • review of ICT requirements in contracts • inventory of non-EU assets

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 [306]. 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 [104]. 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 [550], 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 frame-

work 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 six-month tenure from January to June 2025 [523]. 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.

4.4 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 US 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 sys-

tems' distinctive cybersecurity risks, we refer to the policy analysis of the instruments addressed in Section 4.2.6 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.

4.4.1 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 [442]. 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 multi-segment 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 [167] 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 post-launch, 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 subsection, 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.

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 [81], 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 [81]. 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 [81]. 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 [81]. 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 [463] 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 [440]. Exploiting the Log4j2 vulnerability (CVE-2021-44228) within a publicly exposed instance of WSO2 middleware (an open-source software widely used for application management, telemetry processing, and system integration). The CVE-2021-44228 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 [502]. 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 U.S. 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 [75], 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 [290], researchers recently explored how ransomware might be adapted to target satellites. Specifically, researchers focused on NASA's widely adopted core Flight System (cFS) [6], 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 inter-process 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 pre-launch 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 [226], 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.

4.4.2 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 man-made or natural

interference [6]; 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 [119].

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 US 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 US.

4.4.3 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 [468], 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 European Space Law 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.

4.4.4 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. Firstly, 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. Secondly, 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 [293].

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 at-

tack 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 [132]. 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 [541]. 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 [543].

The launch of the EU Space ISAC is a positive step towards 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.

4.5 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 Center for Internet Security (CIS) [144]. CIS is a non-profit 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, 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 commercial off-the-shelf (COTS) hardware and software. We decided to use IG1 safeguards as they're 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 8 and 9 map 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 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 (SSO) 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.

Table 8: Assessment tool: CIS Controls mapped 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 storage
Cyber and physical protection: Encryption, malware protection, patch management	CIS Control 3: Data Protection CIS Control 4: Secure Configuration 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 lists • Encrypt data on end-user devices • Configure automatic session locking • E&M a vulnerability management process • Perform OS & 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 incidents • E&M an enterprise process for reporting incidents

Table 9: Assessment tool: CIS Controls mapped to EUSL cybersecurity requirements (continued)

EUSL Policy Provision	CIS Security Controls	IG1 Safeguards
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, contract reviews	CIS Control 15: Service Provider Management	• E&M an inventory of service providers

4.6 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 [226]: Ensuring Cyber Access to Space*". The document was developed as a best-practice framework and influenced U.S. policy on satellite cybersecurity, including the basis for provisions in the U.S. Executive Order 14028 [261] and early IEEE P3349 standardization efforts [119]. The pool of experts argues that space systems require mission-specific and threat-informed cybersecu-

rity 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 [226] 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.

4.7 Conclusions

In the first part of this Chapter, we discussed the approaches to space and cybersecurity governance in the US, 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 ana-

lyzed countries enacted to start providing binding or non-binding 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 non-binding 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 [146]: we emphasized the need to define resilience and create quantitative indicators for its assessment [179]; we stressed the importance of having effective security metrics that industries and institutions can use to verify and validate their security policies [153]; 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 Center for Internet Security. 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 non-western 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.

Chapter 5

AI in Space, implications between threats and legal requirements

5.1 Foreword

The previous chapters of this thesis showed how space systems have become critical infrastructures with growing cyber exposure (Chapters 2 and 3), and how existing governance frameworks, from national space-cyber policies to the EU's emerging regulatory architecture, remain fragmented, incomplete, or inconsistently applied (Chapter 4). At the same time, space systems are undergoing rapid digitalisation and increasing reliance on software-driven and automated functions.

In this context, the adoption of artificial intelligence does not simply introduce new functionality; it increases system complexity and autonomy, thereby adding an additional layer of security, compliance, and operational risk on top of an already vulnerable and strategically important domain.

This chapter, written based on the paper "From Europe to Europa: Implications of the European AI Act for the Space Industry" [506], examines how AI technologies are being integrated into space systems and

why their use interacts directly with the vulnerabilities and policy shortcomings highlighted earlier.

AI has long supported mission planning, onboard autonomy, data processing, and Earth-observation analytics, but its recent acceleration, driven by advances such as large-scale machine learning models and increased commercial uptake, is reshaping both the threat landscape and the regulatory responsibilities of actors in the space sector. These developments raise questions about how AI deployment intersects with existing cybersecurity requirements, critical-infrastructure obligations, and the broader regulatory goals introduced in Chapters 2 & 4.

Building on this foundation, the chapter analyses the implications of the EU AI Act for the space industry, with a focus on when space-related AI systems may be classified as "high-risk" and how such classifications interact with obligations already imposed by instruments such as NIS2 and CER. The goal is to understand how AI can enhance space operations while also introducing new forms of technical and legal exposure — and to assess whether the current regulatory trajectory addresses or exacerbates the gaps identified throughout the thesis.

5.2 Introduction

The Artificial Intelligence industry has experienced massive growth in recent years, particularly since the release of Large Language Models (LLMs) such as ChatGPT from OpenAI in late 2022. Their development and adoption have driven tremendous financial gains for the organisations involved in the AI software and hardware supply chain and promised new capabilities and productivity benefits across a vast array of industries and use cases.

AI (in the form of machine learning and other forms of algorithmic processing) has long found applications within the space sector, with adoption also accelerating in recent years. Within the space sector, AI is being used for a multitude of use cases both on Earth (e.g large-scale climate modelling, mission planning, weather and atmospheric monitoring, vegetation and ground analysis, space object detection and tracking

etc.) and in situ (e.g astronaut assistants, space healthcare, satellite data processing, selective data transmission, automated propulsion and navigation systems and real-time spacecraft monitoring etc.).

The role of AI in all of its forms is becoming pervasive throughout the space sector and will remain so in the future as the technologies and techniques continue to mature and be tailored to the requirements of particular use cases and scenarios in the space sector (e.g automated perception, tasking, navigation and operations for rovers on other celestial bodies). The growing importance of AI in the space sector is evident in the direction of the European Parliament's Regulation 696/2021 [402]which encourages the Copernicus mission to consider the European Commission's white paper on "excellence and trust" in the process of incorporating AI into its operations [105].

Due to the growing role of AI in space systems, along with the inherently international nature of the space sector emerging regulatory initiatives governing AI from around the world will become important guardrails guiding the development and deployment of AI systems in outer space. Numerous jurisdictions have begun to develop AI regulations with varying scopes of levels of complexity. For example, Australia has developed guidance that falls short of strict laws such as AI ethics principles [292], publishing a voluntary AI safety standard [258], and working towards updating existing regulatory frameworks to better handle the risks associated with AI [259].

Others such as Canada and China have gone further, enacting legislation specifically targeting harmful uses of AI [486]. The United States has also begun to develop guidance, including executive orders, the NIST AI Risk Management Framework, and various state-level laws. While these initiatives are important, the United States lacks specific AI legislation at the national level, though this may begin to change pending the results of the presidential election in November [55].

Regardless, the regulatory setting of the United States matters given its influential positions in both the space and AI sectors. However, its lack of a uniform and unified approach to AI regulation makes it difficult to glean meaningful insights as to the future of AI governance, and

even more so for the space sector specifically. This leaves the European Union (EU), with its recently finalised 'AI Act' as the most likely source of meaningful guidance for AI governance in the near future.

The EU's AI Act represents the world's most progressive and comprehensive AI regulatory framework. Not only will it apply to entities operating AI systems within the EU, but it will capture the activities of organisations providing AI services that process the data of EU citizens or are otherwise importing/supplying such systems to the EU (see below). This broad scope will capture the activities of many large-scale AI solution providers that operate across borders and has the potential to act in a quasi-extraterritorial manner akin to the EU's General Data Protection Regulation (GDPR) [401]. Beyond its broad scope, significant penalties are also attached to the contravention of certain provision of the EU's AI Act, some increasing up to 7% of the global turnover of the organisation involved (see below for more details). This makes it impossible to ignore (even for large multinational corporations), and more likely to impose de facto standards on technology companies around the world, regardless of their 'home' jurisdiction [416].

The importance of Europe's regulatory efforts to govern AI now being established, the questions become: 'How does this affect the space sector?' and 'How should organisations in the space sector prepare to comply with the EU's AI Act?'.

5.3 The impact of AI in the space industry

The space industry is undergoing a tremendous transformation. The increasing involvement of private actors, coupled with rapid technological innovation, is opening new opportunities for the sector. In particular, the growing number of space assets orbiting the Earth is unlocking a new potential in data acquisition. Satellites collect vast amounts of data that benefit various sectors. The digitalization of the sector necessitates the major involvement of emerging and disrupting technologies, such as AI, to manage the new complexity.

Safety is critical in space applications due to the high costs associated

with failure. As a result, more predictable approaches have traditionally been preferred [289]. Historically, AI was successfully applied in space for offline data processing, but it wasn't commonly adopted onboard spacecraft. The recent need for more autonomous features in orbit has led to the development of sophisticated machine learning (ML) and deep learning (DL) systems for space activities. Despite these advancements, the unpredictability of ML/DL systems has hindered the adoption of AI for onboard applications, as the 'black box' nature of these models can undermine confidence in their reliability. Moreover, running AI in outer space presents unique challenges due to the inherently complex and hostile environment, especially when considering constraints on power consumption and onboard computing capabilities [288]. However, technological advancement in software is steadily paving the way for the integration of AI on board spacecraft [287]. AI on the edge is becoming essential for future space missions. As pointed out by Madi and Sokolova, "the next generation of space missions will see software as the differentiating asset" [350]. Edge computing enables the processing of data at the source, allowing space objects to process data on board. As Varma noted, processing data near its source reduces issues associated with long-distance data transmission, minimizing the latency between Earth and space-based assets [534]. Spacecraft equipped with sensors will gather real-time data from the external operational environment, processing it onboard to perform automated decision-making and execute proper actions when required [496].

This revolution in the approach to space missions will significantly expand the capabilities of space activities. NASA is developing and deploying AI for various goals, including mission operations and planning, vehicle navigation, data communications management, anomaly detection and avoidance, human-system interaction, crew and system health management, hazard detection and avoidance, and in-situ resource utilization [373]. The European Space Agency (ESA) also recognizes AI as a crucial element for future success: "Artificial intelligence is becoming vital to handle this complexity, to operate, network, coordinate and protect our space infrastructure and to get the most out of the data acquired

by our scientific satellite missions [184]."

In navigation and exploration, AI algorithms allow spacecraft to explore complicated environments independently, avoiding obstacles, optimizing routes, and adjusting to changing conditions without human involvement. AI can analyse massive volumes of sensor data in real time in order to make intelligent judgments and navigate accurately. The incorporation of AI in autonomous navigation systems increases mission efficiency, lowers dependency on ground control, and allows spacecraft to investigate distant celestial bodies with more autonomy and agility [457].

AI is also crucial for extracting insights from the enormous amounts of data collected by satellites. In Earth observation, AI's onboard processing capabilities will allow only the most useful data to be downlinked for specific missions, filtering out unusable images. For example, many images cannot be used due to the large presence of clouds. By filtering such data, AI preserves precious bandwidth, ensuring that only images instrumental to analysis reach ground operators. This accelerates analysis and response times, which is crucial for climate disaster mitigation [177].

AI will become increasingly integrated into the governance of space ecosystems in order to sustain the management of mega satellite constellations launched in Low-earth Orbit (LEO) [505]. As the number of satellites in orbit increases, the role of human operators becomes more complicated and less cost-effective. With a certain level of autonomy, satellites will be able to acquire data, process it, and act to avoid possible collisions [14].

Additionally, AI can analyse telemetry data and detect patterns that indicate early signs of spacecraft malfunction, thereby extending the lifecycle of satellites. This is already occurring, with SpaceX employing some form of AI for its operations. An AI autopilot system for its Falcon 9 craft allows to carry out docking with the International Space Station (ISS), and AI algorithms are deployed in its Starlink constellations to avoid potential collisions [351]. However, these opportunities come with significant challenges [394]. The widespread integration of AI into

space activities will bring new risks to the industry. The advanced onboard processing capabilities of AI may make it harder to differentiate between legitimate Earth Observation (EO) operations and potentially intrusive activities that invade privacy. Indeed, satellites equipped with high-resolution cameras can analyse high-quality satellite photography, while being used to target specific objectives. The automation given by AI on edge can lead to the unintended collection of images that intrude on individual privacy [401].

While AI can improve satellite management in orbit, its integration could complicate Space Traffic Management (STM). STM refers to a set of rules, practices, and technologies to ensure sustainable and safe orbital environment. Including managing orbital traffic and space debris. Two satellites equipped with different AI systems might process the same data but arrive at different outcomes, leading to conflicting collision risk calculations. This scenario would complicate the governance of increasingly crowded orbits, rather than supporting their long-term sustainability. Other risks stem from the dual-use nature of technology. Autonomous features could be exploited for malicious manoeuvres, such as attacking satellites with national security applications, or even placing autonomous weapons in orbit. Although the Outer Space Treaty bans weapons of mass destruction [302], it does not clearly define whether autonomous weapons fall within that category [331]. Cybersecurity is another concern. Since the outbreak of the full-scale war in Ukraine, space assets have become targets of Russian attacks [531]. AI can exacerbate such risks. Systems trained to detect malfunctions in space systems could be attacked or exposed to malicious activities, leading to their failure to perform their intended functions [65]. These examples show that as autonomous capabilities become more widespread in the space environment, the potential for harm to space systems, the space environment, and the cascading effects on society will become more apparent. The development of appropriate governance systems will be crucial for the space community to ensure that space-based AI systems function accurately and adhere to legal frameworks. It is important to consider how the international regulatory framework regarding AI can guide the

responsible integration of these technologies in outer space. In this context, the AI Act can play a significant role in shaping this regulatory landscape.

5.4 The Structure and Scope of the EU's AI Act

The European Union's AI Act defines an 'AI system' as "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments" [400]. This definition intentionally aligns with other well-accepted definitions such as the OECD definition of an AI system [387].

The Act is structured around a risk-based approach, sorting AI systems into four broad categories, with each having associated regulatory obligations attached to them. Risk categories can be broadly categorized into four groups, including 'unacceptable risk' systems which will be outright prohibited, 'high-risk' systems which are allowed subject to stringent compliance obligations, 'Limited Risk' systems, which attract transparency requirements, and 'Minimal or No Risk' systems that escape compliance obligations [400].

Alongside the four risk categories, an additional section on General Purpose Artificial Intelligence (GPAI) was included following the diffusion of Large Language Models (LLMs). The former became a large focus of the discourse on AI regulation [400], however it will be less likely to be relevant in the space sector as the technical and computational requirements of space systems will prevent their deployment in situ for the foreseeable future, and for earth-bound use-cases, they would probably not fall under the high-risk category.

For space operators, the interest lies in the substantive provisions related to obligations imposed on 'high-risk' systems, which are discussed below.

The regulation applies to a broad range of parties, such as providers

placing on the market or putting into service AI systems in the EU (regardless of whether they are located within the EU), deployers of AI systems (located within the EU), providers and deployers of AI systems (located outside the EU) where the output produced by the AI system is used in the EU, importers and distributors of AI systems, product manufacturers using an AI system with their product under their own name or trademark, authorized representatives of providers (which are not established in the EU), and affected persons located in the EU [27].

This is an extremely broad scope, capturing many parties involved in the lifecycle of AI systems, including those not necessarily from the EU, but otherwise interacting with the jurisdiction through their business activities.

This is of particular importance to the space industry, given its international nature and the fact that many satellite systems (which may employ AI) provide services that span the globe, such as earth observation imagery or position, navigation, and timing (PNT) systems. Importantly, regardless of the structuring of the Act, its scope is limited by several exceptions covering a number of particular use cases and circumstances, some of which are relevant to the space sector. The most relevant examples include the 'military' and 'scientific research' exceptions, with the EU AI Act not applying to AI systems or models deemed to fall under these use cases. The 'military' exception prevents the AI Act applying to "areas outside the scope of Union law" exempting "AI systems where an in so far they are placed on the market, put into service, or used with or without modification exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities [16]."

The use of the word "exclusively" is important as it creates a strict delineation between systems being used purely for defence purposes and those that would otherwise be considered dual use. As such, AI systems that interact with space systems or data in a manner that benefits both militaries and civilians would be outside of the scope of the Act. This would possibly include (for example) AI systems that manage or enable global navigation satellite systems (GNSS). Another limit on the Act's

scope is the 'scientific research' exception, which states that the AI Act does not apply to AI systems, models, or their outputs that are "specifically developed and put into service for the sole purpose of scientific development [17]. Like the 'military' exception discussed above, the use of the phrase "sole purpose" creates a distinction between those systems, models, and outputs that are purely scientific in nature and those that may have commercial motivations as well. These exemptions are of relevance to the space industry given the long-standing dual-use nature of many space assets, as well as the prominence of scientific research throughout the sector. These exemptions will not cover AI systems or outputs used in commercial contexts, but may prompt organizations to adopt creative business structures in particular scenarios as a means of attempting to avoid obligations under the EU AI Act. Aside from relevant exemptions, the definitions of prohibited and high-risk systems must be understood as they may apply to the multitude of AI systems found in the space industry. While it is unlikely that any space-related AI systems would be classified as unacceptable/prohibited (as that classification primarily deals with social scoring, real-time biometric monitoring, and other systems that directly interfere with the rights of individuals), there may be scope for certain systems to fall under the 'high-risk' classification. This is because although space-based AI systems are unlikely to fall under the specific provisions related to safety components and third-party conformity assessments [18], they may still fall within the bounds of the provisions within Annex III of the Act, outlining other categories of what constitutes a high-risk system. Some relevant examples include AI systems which relate to migration, asylum and border control management (e.g. a system which processes satellite imagery to track people in migration contexts),[6, Annex III, Para 7] or AI systems which influence access to and enjoyment of essential private services and essential public services and benefits, particularly systems which would be used for risk assessment and pricing relating to life or health insurance, or used to evaluate and classify emergency calls for emergency services (where satellite or PNT data is used to inform this process).[6, Annex III, Para 5(c) and (d)] These examples could be considered 'Earth-

based' systems, where the data used is gathered in space, but the AI model is likely hosted by hardware on Earth. In this sense, they are all 'secondary' space AI systems, where there is little distinction between the operation of these systems and other AI systems processing input and training data gathered from non-space sources. Importantly, the list of systems included under Annex III can be modified with delegated legislation [23], meaning that this list may change with time, and stakeholders should remain cognizant of such changes given the obligations attached to high-risk systems (see below).

5.5 The Intersection of Space Technology and Critical Infrastructure Resilience

Of particular relevance to the space industry is the classification of systems that are "intended to be used as safety components in the management and operation of critical digital infrastructure [...]" as high-risk systems [10]. This could conceivably apply to both Earth-based AI systems utilizing space data and 'primary' space AI systems, those being AI systems that are located in situ, with the models being hosted aboard satellites or other space vehicles. This however, depends on whether AI systems being used in the space industry fall under the umbrella of "critical digital infrastructure" and whether they are intended to be used as "safety components" in the management and operation of such infrastructure. These terms must be interrogated to determine which use cases found within the space industry would fall within their ambit, and consequently be classified as high-risk systems under the EU AI Act.

The definition of a "safety component" is relatively clear, being "systems used to directly protect the physical integrity of critical infrastructure or the health and safety of persons and property, but which are not necessary for the system to function" where their failure "might directly lead to risks to the physical integrity of critical infrastructure and thus to risks to health and safety of persons and property." These do not include components solely related to cybersecurity purposes but would include systems for "monitoring water pressure or fire alarm controlling systems

in cloud computing centres [26]. Parallels to these examples could be seen in scenarios such as AI systems being used to control security systems at a ground station facility, or in the use of automated manoeuvring algorithms onboard satellites that may underpin critical digital infrastructure such as GNSS or PNT services. The integration of space technologies in sectors such as agriculture, finance, maritime transport, defence and aviation has increased the reliance and dependence of critical sectors on space systems. This has made space networks the single point of failure for many critical infrastructure sectors. The debate surrounding the classification of space systems as a critical infrastructure sector is both intense and multifaceted. Despite the indispensable role that space systems play in everyday life, they have yet to be formally recognized as a critical infrastructure sector by the U.S. and other major countries. This ongoing debate highlights the divergence of opinions among experts and stakeholders regarding the necessity and implications of such a designation [458].

In the U.S., advocates for designating space systems as the 17th critical infrastructure sector argue that the increasing reliance on these systems for essential economic and security functions necessitates formal protection, highlighting current policies as inadequate against unique threats such as cyberattacks and GPS jamming [319]. This approach would entail appointing a federal agency as the sector risk management agency (SRMA) to oversee risks, facilitate communication, and establish an industry-led council for cohesive threat response. However, the opposition questions the practicality and impact, noting that many space-related assets already fall under existing sectors like telecommunications and defence, potentially leading to increased regulatory burdens without added resources. The debate focuses in particular over which federal agency should serve as the SRMA, with NASA, the Department of Commerce, and the Department of Transportation being considered. In the EU, space has been considered a critical infrastructure sector for a long time. The European Programme for Critical Infrastructure Protection (EPCIP) identified space-based systems as critical infrastructure, aiming to protect them by implementing common minimum standards [418].

Directive 114/2008 and the Critical Entities Resilience Directive (CER) (2557/2022) that replaced it also recognize space as a critical infrastructure sector and emphasize the connection between the cyber and space domains [364]. Space is mentioned among the 11 sectors in the Annex of the Directive. In particular, the operators of ground-based infrastructure, whether owned, managed, and operated by Member States or private parties, that support the provision of space-based services, fall within the scope of the Directive. However, certain companies operating in the space domain or providing their services through space-based technologies or infrastructure may also be considered as digital infrastructure providers. For example, providers of public electronic communications networks and services are included in the critical sector as defined in section 8 of the Directive's annex [202]. This means that the Directive could potentially apply to all companies in the telecom sector that rely, even partially, on space-based services to provide electronic communications services or base their content delivery networks or public electronic communications networks on space architecture. The Directive, therefore, expands the scope of risk and emphasizes the connection between multiple critical infrastructure sectors. However, there may be questions about how communication between sectors, about incident reporting or other security matters, will work at both the national and EU levels. Additionally, the directive allows member states a certain degree of freedom, which could lead to different implementations, risk management and assessment approaches, potentially hindering the single market as some states may adopt less stringent approaches for their critical infrastructure operators.

To improve the resilience of Europe's CI, the CER Directive will make it mandatory for EU states to implement a series of actions by October 17, 2024. Article 4 of the CER requires Member States to define a Strategy on the resilience of Critical Entities, including strategic objectives and priorities, a governance framework, measures to enhance the resilience of CIs, and a list of the main authorities and stakeholders involved in the strategy's implementation. This strategy aligns with the risk assessment required by Member States in Article 5, which mandates Member

States to perform risk assessments taking into account relevant natural and man-made risks, including cross-sectoral or cross-border risks, accidents, natural disasters, public health emergencies, hybrid threats, and other antagonistic threats, such as terrorist offenses. Interestingly, no explicit mention is made about the risks that may arise from the application of emerging disruptive technologies such as AI. Moreover, a specific methodology for the assessment has not been defined yet. Before defining strategy and risk assessment, Member States are asked in Article 6 to identify the Critical Entities in each sector by July 17, 2026. A strict methodology for determining that an entity is critical is therefore necessary, but not yet defined. Once identified as critical, entities will have 10 months to comply with the Directive. The CER includes additional provisions such as Member States' support to Critical Entities (Article 10), the establishment of resilience measures (Article 13), and incident notification requirements (Article 15). Unquestionably, the use of AI technologies in the CI will expand the requirements set by the CER to any relevant risk in the mandatory risk assessment and strategy imposed. Another relevant EU policy in this field is the NIS 2 Directive, which entered into force in January 2023, and also listed space among the critical infrastructure sectors [304]. The Directive introduced stringent reporting requirements, mandating the disclosure of any cyber incidents that could impact space and other critical infrastructure, including ground stations, but without explicitly mentioning satellites. This presents challenges but also opportunities for the deployment of AI tools for monitoring, detecting, and responding to potential cyber threats [15]. The directive also advocates for enhanced collaboration between the space industry and regulatory bodies to identify and mitigate cybersecurity risks, requiring the sharing of information and intelligence to bolster sector-wide resilience. Supply chain security is a key focus of the NIS2, compelling space organizations to implement robust risk management practices, including due diligence and monitoring of suppliers and third-party contractors due to the sector's complex and global supply chains. Although the NIS 2 Directive does not explicitly mention AI, AI tools can support every requirement of the directive and, at the same time, critical AI operators

should be included in the scope of the act. Interestingly, Art. 9(10) of the AI Act specifies that requirements in terms of internal risk management processes may be added to those provided by the NIS 2 and CER in the case of high-risk applications. Therefore, all the aspects provided in paragraphs 1 to 9 of the Act may be part of, or combined with, the risk management procedures established by the NIS 2, CER or any other relevant EU Act [24]. Looking at the defence dimension of space as a critical infrastructure, in January 2023, the EU and NATO announced the formation of the Task Force on the Resilience of Critical Infrastructure, which aims to cover four sectors: energy, digital infrastructure, transport, and space. This initiative comes in light of recent events like the ENERCON disruption [239], highlighting the urgency of building resilience in critical infrastructure. This view is reinforced by the role of satellite megaconstellations in LEO. Such as the European Union constellation Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS2) which aims to provide secure communications for national security and military reasons for the EU and its member states. By nature, the constellation was designed with the view of constituting a strategic element for the Union, therefore, falling under critical infrastructure requirements [71].

In order to support the idea that space systems should be considered a Critical Infrastructure it is enough to consider recent disruptions to these systems and their cascading effects as well as recent studies estimating the consequences of disruptions to satellite networks. The economic impact of disrupted space services is significant. Industries reliant on satellite data, such as agriculture, transportation, and finance, could suffer substantial losses due to operational inefficiencies and delayed information. A study sponsored by the National Institute of Standards and Technology estimated the cost of a disruption of the GPS signal assessing that in precision agriculture sector farmers would lose an average of $15.5 billion in revenue if the outage occurred during the spring planting season and lasted for 30-days [243].

While, for the Telecom sector the study estimated, in the event of a 30-day outage, while the wireline networks would remain largely unaf-

fected, wireless networks would quickly begin to degrade in quality of service and would result in anywhere from $5.5 to $14.2 billion in damage over the course of 30 days. These figures give a clear idea of why space should be considered critical and adequately protected. These considerations could sway the interpretation of space systems as critical infrastructure for the purposes of the AI Act and may motivate clarification of the scope of 'critical infrastructure' as it applies to the space sector in the future.

5.6 AI in Space: Navigating High-Risk Applications

Recently, several space companies developed and marketed AI-based products that could arguably be considered as high-risk according to the AI Act. The risks and potential implications of such systems should be considered in the context of the space sector.

The German company LiveEO recently obtained funding for its proprietary solution that leverages AI to analyse satellite data for monitoring critical infrastructure, such as detecting vegetation encroachment on power lines and identifying ground deformation near railways [348] .

The product uses proprietary AI-powered algorithms to generate insights that help critical infrastructure operators manage climate risks and resilience. As this kind of product gives operators the capability for preventing disruptions and ensuring safety, it may fall under the definition of high-risk AI applications defined by Article 6(1) of the Act. In this case, AI could be considered a safety component of the EO-based product dedicated to assessing risks to critical infrastructure, due to its potential impact on public safety and infrastructure integrity.

These considerations, however, would not apply if the AI system performed a narrowed procedural task or is completing an analysis previously carried out by a human as defined in Article 6(3). LiveEO's platform is used by Europe's largest railway operator, Deutsche Bahn, to safeguard its assets, and also helps other entities, such as Nigerian pipeline operators, tackle oil theft and reduce financial losses. These

entities, when in Europe, may share with LiveEO responsibilities and may also need to comply with CER and NIS2 requirements in addition to those of the AI Act.

Similar considerations can be applied to other AI applications in the space industry, for example, SpaceX's use of AI for autonomous operations, such as docking the Falcon 9 with the International Space Station (ISS) [286]. In this case AI enhances operations by providing precise, real-time data processing capabilities that allows for automated docking processes, minimizing human error and improving mission efficiency by continuously monitoring trajectories and making necessary adjustments mid-operation.

Considering the safety dimension of AI in this context, it could be considered as a high-risk case, thus mandating rigorous testing, transparency, and accountability measures (see below). While these autonomous operations, such as docking, physically occur outside of Europe, their impacts could be felt within the EU or by its citizens, enlivening the AI Act and thus affecting organisations around the world.

In August 2021, the Federal Communications Commission of the US and SpaceX met to discuss the company's collision avoidance strategies for its Starlink satellites. In the meeting, SpaceX emphasizes the use of autonomous systems and details how satellites autonomously evaluate collision risks using data from the 18th Space Control Squadron and execute avoidance manoeuvres. However, in the documents, it is clear that behind this process, human oversight is present and reserved for coordination with other operators and high-stakes scenarios like human spaceflight. This autonomous operational model, behind the management of the Starlink constellation, could potentially face significant regulatory challenges under the EU AI Act, depending on to which extent the humans in the loop are present in operations, this is however something that is not easy to understand from official declarations and documents for the time being [253].

These examples not only highlight the potential for these activities to be classified as high-risk, but also the increasingly critical role AI is playing in monitoring, safeguarding, and operating critical infrastructures.

This advanced application of AI introduces new categories of challenges and risks.

Autonomous systems are susceptible to cyberattacks that could manipulate operational data or induce malfunctions, potentially leading to catastrophic outcomes such as spacecraft collisions or mission failures.

One key area of concern for AI applications is algorithmic vulnerability [8]. AI algorithms can be targeted by adversarial attacks that manipulate input data, deceiving the system and leading to incorrect classifications or decisions. For instance, an attacker might introduce adversarial examples into the data pipeline, causing the AI to misinterpret sensor readings and make faulty operational choices. Data integrity attacks represent another critical vulnerability [323].

Space systems rely heavily on accurate data for training AI models and making operational decisions. If the integrity of this data is compromised in AI applications for the space or other critical infrastructure sectors, the resulting outcomes can be disastrous. One method to perform such attacks is data poisoning, where attackers inject malicious data into the training set, impairing the AI's ability to interpret and respond correctly. Software exploits are also a prevalent threat, as weaknesses in the software components of AI systems can be exploited to gain unauthorized access or control [475]. This could involve taking advantage of unpatched software, executing buffer overflow attacks, or injecting malicious code to alter the system's functionality. Additionally, hardware vulnerabilities can also pose additional risks, as physical components of space systems, such as sensors and processors, can be targeted by fault injection attacks, which can cause malfunctions in the AI hardware, further impairing system integrity.

High-risk AI systems often arise in critical applications related to space. Beyond the previously discussed examples, several other AI applications in this sector may also be classified as high-risk. For instance, AI systems utilized in satellite communication equipment, in-orbit systems, and wireless network infrastructure are likely to be categorized as high-risk due to their crucial role in ensuring secure and reliable communication channels.

Similarly, AI technologies integrated into launch vehicles, drones, and high-altitude platform stations function in safety-critical environments, which would make them subject to increased regulatory scrutiny. Other scenarios that may fall under high-risk considerations include the use of AI in automated manufacturing systems for satellites or launch vehicles, as well as AI tools that ensure safety in potentially hazardous environments, such as spaceports and launch sites. Furthermore, AI systems in automated ground vehicles or transmitters used in space operations may also qualify as high-risk.

In addition to their importance as safety components, AI systems in the space sector may be classified as high-risk when they serve purposes explicitly mentioned in the EU AI Act. For example, AI systems used to monitor employee performance in mission-critical roles, as highlighted in Recital 57, fall under this classification.

Overall, AI should be utilized to enhance the operation and management of space systems, while mitigating the potential vulnerabilities that may arise from its use. As threat actors are already exploiting AI, it has become a necessity for the defence organisations to also harness AI tools to counteract these threats and strengthen defensive capabilities. Any dual use applications of these technologies must remain aware of the risks associated with their use. As we discuss the classification of high-risk systems, the above examples of AI being used in the space sector should be kept in mind to contextualize the discussion.

5.6.1 Possible Arguments Against a System Being Classified as High-Risk

Although the classification of 'high-risk' systems derives from explicit categories, the Act provides a mechanism for AI systems deemed 'high-risk' under Annex III of the Act to not be considered high-risk where they do "not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making [20]."

Providers of AI systems can justify an assessment that systems are

not high-risk by confirming that their system is intended to: "perform a narrow procedural task", "improve the result of a previously completed human activity", "detect decision making patterns or deviations from prior decision-making patters and is not meant to replace or influence the previously completed human assessment, without proper human review", or "perform a preparatory task to an assessment relevant for the purposes of the use cases listed in Annex III" [25].

Providers must document this information before the system is placed on the market or put into service and must still register the system as normal for a high-risk system and provide the documentation upon request of competent national authorities. This process of abrogating a high-risk classification does not apply to systems that perform profiling on natural persons [19].

The European Commission will, in future, provide guidelines to specify the practical implementation of this process, along with examples of use cases of AI that are high-risk and not high-risk [21].

These guidelines will undoubtedly form a crucial reference for operators in the space industry that find their AI systems otherwise falling under the 'high-risk' classification, and should be examined closely upon their publication. Worth noting is that any delegated acts modifying these rules may not decrease the overall level of protection of health, safety and fundamental rights provided for by the regulation [22], meaning that the current level of regulation is likely to act as a 'floor' with little room for abrogation of obligations. Therefore, stakeholders should consider compliance with the AI Act in its current state as a step in a longer ongoing AI assurance journey, as governance requirements will likely only increase in scope and complexity with time.

5.6.2 Regulatory Balance and Standard Setting

The prospect of increasing the scope of the Act triggers the tension between overregulation and under-regulation [407]. This debate often arises regarding new technologies, and particularly in the context of the AI Act.

Overregulation refers to an excess of legal constraints that could stifle

innovation, limit market flexibility, and impose high compliance costs on businesses. Conversely, under-regulation risks leaving critical areas unmonitored, potentially leading to the irresponsible or unsafe deployment of advanced technologies like AI. Striking the right balance is essential for fostering innovation while ensuring safety and ethical standards.

In the space sector, AI is playing an increasingly prominent role. Questions remain open on whether the EU AI Act could tip the scale toward overregulation. While the Act aims to establish a clear framework for the ethical and responsible use of AI, it may lead to a slow in innovation and deter new entrants into the space industry [533].

It is the case that AI development for space operations is guided particularly by new deep-tech start-ups and actors in the space industry that will need a nimble business environment to thrive and grow. In addition, one key aspect of EU law is the so-called Brussels Effect, in lay terms the EU's ability to set de facto global standards through its regulatory power [28]. The GDPR is a well-known example of this phenomenon, becoming the global benchmark for data protection laws [401].

Similarly, the EU AI Act, as the first comprehensive regulatory framework for AI, has the potential to shape global standards. For space operators, this could mean that even companies operating outside Europe may need to comply with the EU AI Act if they wish to engage in AI-related business with European partners or markets. Given the lack of existing global AI laws, the EU's regulatory approach could leave a significant footprint, particularly in niche sectors like space.

For this chapter, the core debate centres on whether the EU AI Act would enable a more responsible and ethical deployment of AI systems in outer space or hinder technological progress by creating regulatory hurdles. The space sector thrives on innovation, and AI will play an increasing critical role in optimizing satellite constellations, mission planning, and data management. Excessive regulation in this area could deter investment and slow down advancements in autonomous systems and AI-driven space missions. However, there are equally compelling arguments that under-regulation would leave too much room for errors, potentially leading to unsafe applications of AI in space operations. Re-

sponsible AI governance is important in the space sector, where failures can have far-reaching consequences.

5.6.3 Obligations Related to High-Risk Systems

In the event that an AI system is classified as high-risk (and avoids any abrogating factors), a number of obligations are imposed on various stakeholders of the AI system in question. The system itself must have a dedicated risk management system to identify, evaluate, and mitigate risks associated with the AI system [400] .

They must also meet data governance standards relating to training, validation and testing data sets [400]. Technical documentation must be drawn up before the system is placed on the market [400], automatic record keeping systems must be in place [400], and transparency measures must be established to provide information on the operation and governance of the system to enable deployers to interpret a system's output and use it appropriately [400]. High-risk systems must also be designed and developed to allow for effective human oversight, though this is to be commensurate with the risks, level of autonomy, and context of use of the AI system [400]. Finally, high-risk AI systems must be designed and developed to achieve appropriate levels of accuracy, robustness, and cybersecurity, though the metrics for measurement of these requirements are yet to be developed [400].

Beyond system level requirements, providers, deployers, and other parties face a number of other obligations with respect to high-risk AI systems including quality management systems [400], document keeping [400], automatically generated logs [400], taking corrective actions and disclosing information to authorities when appropriate [400], cooperating with authorities, appointing authorized representatives where needed. There are also numerous other provisions relating to notifying authorities [400], post-market monitoring [400], as well as standards, conformity assessments, certificates, and registration of high-risk AI systems [400], performing fundamental rights impact assessments, with some variation as to which exact obligations apply to a party depending on

their role in the AI lifecycle (developer, distributor, deployer, importer etc.)[400].

As can be seen through the lists above, high-risk systems carry with them many obligations that will impose an as yet unquantified (but likely significant) governance burden on the organisations involved in developing and deploying them with connection to the European market.

The exact requirements are often still vague as delegated acts will articulate the details of the required actions at a later date. Importantly, the requirements show a level of flexibility in the regulation that may provide some relief for those responsible for AI systems in the space sector. Similar to how providers can argue that their systems should not be considered high-risk (as discussed above), requirements surrounding (for example) human oversight allow for variability in the scope and depth of governance measures "commensurate with the risks, level of autonomy and context of use of the high-risk AI system" [400], and stated that high-risk systems "achieve and appropriate level of accuracy" [400]. These are important as the context of AI deployments in the space sector may necessitate alternative governance mechanisms due to the impracticality of more common governance practices being used in extreme scenarios [262]. For example, in the near to medium term future when there may be too many satellites to have their orbits managed 'by hand' by operators on Earth, and instead algorithmic management is required given the speeds of satellites in orbit, and the potential number of objects needing deconfliction and manoeuvring to avoid collisions. In such a scenario, human oversight may in fact be a source of risk rather than a mitigating factor, and so the wording of Article 14 becomes important in allowing such a modified safety practice. In summary, the exact requirements of many provisions are as yet unclear, but the flexible language in which they are couched in will allow for some degree of flexibility in achieving compliance with the Act.

5.6.4 Penalties for Non-Compliance

These obligations are paired with penalties for non-compliance. At the extreme end of the spectrum, developing or deploying prohibited AI systems (Article 5) attracts fines of up to €35m or up to 7% of an undertaking's [29] total worldwide annual turnover for the preceding year (whichever is higher) [400]. Non-compliance with provisions related to high-risk AI systems comes with fines of up to €15m or up to 3% of an undertaking's total worldwide annual turnover for the preceding financial year (whichever is higher) [400]. Even outside of prohibited and high-risk systems, contraventions of notification requirements the supply of incorrect, incomplete, or misleading information to the aforementioned notification authorities can attract fines of up to €7.5m, or up to 1% of an undertaking's total worldwide annual turnover for the preceding financial year [400]. Importantly, when applied to SMEs (including start-ups), the above penalties are the lesser of the numerical and percentage amounts stated [400].

Further, when deciding on the amounts to be fined under the previous provisions, a number of factors must be taken into account including: the nature, gravity and duration of the infringement and its consequences (taking into account the purpose of the system and how many people were affected and how badly they were affected), other aggravating or mitigating factors, the cooperation of the infringing entity with authorities, whether the infringement was intentional or negligent, any harm mitigation actions taken by the operator, and a number of other factors [400].

Together, these provisions show that the EU AI Act must be taken seriously by operators in the space industry, as the penalties can be enormous depending on the provisions infringed upon. The penalties go beyond minor fines that can be shrugged off by large entities and would significantly impact the operations of those who are penalized. Although many factors can be considered in determining the amount to be fined, these may not work in favour of operators in the space industry. This is because the scope of damage, or value of damage could be much

greater in the space sector than in other sectors. For example, an AI-enabled Earth observation platform could enable mass privacy infringements (massive scope) or an AI-enabled automated manoeuvring algorithm could cause a collision in orbit, resulting in economic damage to assets and environmental damage to Earth's orbital zones due to the generation of space debris (massive value/consequences). While Member States are responsible for the formulation of the rules surrounding these penalties and their enforcement, operators should not assume these are 'empty threats', as the EU has a track record for enforcing this type of penalty provision, with over fines amounting to a total of more than 4 billion euro being issued under its GDPR regime for privacy and data protection violations since 2018, with Meta itself attracting over €2 billion in fines [401]. For this reason, operators should be cognizant of the potential regulatory (and financial) implications of their AI projects and ensure their AI projects are compliant with the EU AI Act as both a matter of not only good AI governance and, but prudent risk management and financial planning.

5.6.5 AI Literacy

A final point to be considered is the concept of AI literacy, as outlined in Article 4 of the AI Act, represents an important disposition for the responsible use and deployment of AI systems across all sectors, including space [400]. Indeed, the provision applies to organizations involved in developing, deploying, or managing AI systems, regardless of the risk category assigned to the system. It requires providers and deployers to ensure that individuals involved in the operation and use of AI systems possess an adequate level of understanding and skill to engage with these technologies effectively and responsibly. This obligation is particularly relevant with its entry into force in February 2025. Recital 20 of the Act underscores that AI literacy should extend beyond technical proficiency, encompassing the ability to interpret outputs and understand their implications [400]. For space operators, this means not only equipping technical staff with the necessary skills but also ensuring that non-

technical staff understand the broader implications of AI, including its ethical and regulatory dimensions use in space activities and in their internal structure, such as when an AI is used as an assistant. The goals of recital 20 suggests prioritizing the adoption and the development of tailored training and educational initiatives to ensure the adoption of informed decisions regarding AI systems. Such measures could include:

- Specialized Training for Operators;
- Cross-Disciplinary Workshops;
- Awareness Campaigns for Stakeholders;
- Continuous Professional Development.

Such measures reflect the broader objectives of the AI Act to promote transparency, accountability, and public trust. While the immediate focus may be placed compliance, investing in AI literacy can offer significant long-term benefits, enhancing the sector's capacity to adopt AI responsibly and innovatively. A workforce proficient in AI and cognizant of its implications, can better navigate the complexities of deploying AI systems in both Earth-based and space-based contexts.

5.7 Conclusions

As AI technologies continue to proliferate and achieve new capabilities, their adoption throughout the space sector will continue to increase into the future. The myriad of opportunities and activities enabled by AI comes with risks to individuals, organisations, the environment, and society as a whole. These risks have spurred the development of regulatory frameworks to mitigate these risks, with the EU's AI Act leading the charge.

Use cases of AI in the space sector may be classified as high-risk systems under the Act, and in particular, provisions related to critical digital infrastructure may encompass certain current or future use cases of AI within the space sector. This, combined with the broad scope of which

parties and stakeholders are captured by the Act, necessitates that operators in the space sector be aware of the potential classifications of their system and remain vigilant regarding future clarification or changes to the relevant provisions and delegated regulations.

The space sector as a whole must understand the consequences of such classifications, including the obligations imposed on stakeholders and potential penalties for failing to meet said obligations. The heavy fines set out in the AI Act necessitate careful adherence to the requirements of the Act, as the financial (as well as legal and reputational) risks associated with non-compliance could threaten the viability of operations. Therefore, the EU AI Act, represents an important regulatory framework with which the international space sector must comply, and stakeholders in the space sector should make themselves aware of the potential implications of the EU's AI Act for their operations in order to not only achieve and maintain compliance with the Act, but also to foster good AI governance throughout the sector and prepare for other regulatory frameworks governing AI that are emerging in other jurisdictions.

Chapter 6

Security Metrics for the Space Domain

6.1 Introduction

Expanding on the regulatory and operational challenges discussed in Chapter 4 & 5, this chapter introduces a structured set of cybersecurity metrics designed to support compliance, governance, and risk assessment across diverse space-system architectures.

In today's interconnected world, cybersecurity is essential for organizations, institutions, and companies: processes like risk assessment and mitigation plans have become crucial to ensure operational services and prepare for disruptions. This is especially true for critical infrastructure sectors, where business continuity is vital not only for the functioning of companies but also for the security of nations and their citizens.

Due to the complexity of certain systems like space ones, where terrestrial and satellite networks intertwine, and the value chain comprehends a multitude of actors, it is important to establish clear parameters to measure different aspects of cybersecurity.

As a result, organizations have started developing and implementing security metrics. The National Institute of Standards and Technology (NIST) defines security metrics as tools designed to facilitate decision-

making, improve performance, and enhance accountability through the collection, analysis, and reporting of relevant performance-related data [91]. These security metrics can be seen as a tool for quantitatively measuring an organization's security posture and are essential for comprehensive network security and cyber situational awareness management. Without good metrics, security analysts cannot evaluate the effects of security measures or quantify risks.

Establishing clear and actionable security metrics is particularly important for companies as one of their objectives is to ensure business continuity and minimize business damage by preventing or mitigating the potential impact of cyber incidents. To achieve this goal, organizations need to consider all dimensions of network and information security and provide stakeholders with detailed information about their network security management and risk treatment processes.

Given the widespread use of security metrics and their importance for companies and stakeholders, their application for compliance and risk assessment as outlined by prominent EU policies, such as the NIS2, has been an area that has received little attention [275]. Previous research has mainly focused on creating new metrics for specific sectors and addressing particular security challenges with new methodologies [307]. However, the potential use of metrics to comply with EU cybersecurity policies has not been thoroughly explored, even if several regulations themselves specifically call for measures and tools to better assess security. The recently published NIS2 Implementing Regulation's Annex [190], which refers to the policy for the security of network and information systems (Article 21 of the NIS2), emphasizes the need to establish indicators and measures to monitor the implementation and the current levels of network and information security of relevant entities. Even if these documents do not provide examples of what such metrics should entail, we provide a set of proposed metrics in Section 6.6 that reflects the cybersecurity principles defined in the NIS2. Moreover, this chapter advocates for using security metrics to assess compliance with regulations like NIS2, CER, or upcoming space laws, demonstrating to policymakers that metrics can be integrated into policies to enhance their effectiveness.

While developing new metrics remains valuable for addressing emerging gaps and finding more efficient ways to assess a company's security level, not connecting their usage to practical compliance applications may make them mere theoretical tools with no real-world relevance.

This chapter addresses the issue of connecting security metrics to compliance operations, taking into account relevant regulations and standards. We quantify how the various NIST Cybersecurity Framework (CSF) 2.0 functions, categories, and subcategories are covered by existing metrics in the literature, comparing existing security metrics and mapping them according to the NIST CSF 2.0 subcategories. In addition, our work aims to demonstrate how these metrics can be used in the space sector to meet the cybersecurity requirements set forth by major EU cybersecurity policies.

In particular, this chapter aims to answer the following research questions:

- **RQ1**: How do security metrics, when organized by the NIST CSF 2.0 functions, help organizations implement and demonstrate compliance with cybersecurity requirements, especially with the EU NIS2 Directive?

- **RQ2:** In the context of critical infrastructure, especially space systems, are the existing security metrics, from both literature and key stakeholders, sufficient to cover all the functions, categories, and subcategories of NIST CSF 2.0? What are the existing gaps, and how can they be filled?

- **RQ3:** How can the selected metrics for the space sector be operationalized and evaluated in realistic scenarios?

To reply to **RQ1**, we examine how the security metrics that are aligned with the NIST CSF 2.0 functions support implementation and help demonstrate compliance with cybersecurity requirements. In our analysis, we focus particularly on alignment with EU policies, such as the NIS2. We assess similarities and differences between these instruments and highlight their common baseline for risk assessment across organizations.

To address **RQ2**, we propose a methodology to survey the current state of research in the field of cybersecurity metrics. Our approach is based on well-defined selection criteria and principles to guide the selection of security metrics applicable to the space sector, ensuring that the chosen metrics are relevant and effective. The application of our methodology results in a set of selected metrics that are then mapped to the subcategories of the NIST CSF 2.0. We identify metrics that can represent the principles and guidelines of each NIST subcategory. The mapping process is explained in detail, and its results are summarized in Table 13, 13, 14, 15, 16, 17, and 18, and online [78]. After completing this mapping, we assess the extent to which existing metrics address the NIST CSF subcategories, identifying the existing gaps in specific NIST Functions such as Respond and Recover. Based on these findings, we propose a set of new specific metrics, better suited for addressing the unique cybersecurity challenges in the space sector.

To address **RQ3**, we operationalize the identified and proposed metrics in a use case closely resembling real-world space networks and implement them in an online tool [80]. This application shows how the metrics can be mapped to NIST CSF 2.0 subcategories within a realistic scenario and used to measure and improve the security posture of space-based assets. Note that **RQ1** addresses the conceptual value of metrics structured by NIST CSF 2.0 for implementation and compliance, whereas **RQ3** focuses on their operationalization and evaluation in a realistic space scenario.

Our approach not only matches metrics with NIST CSF 2.0 but also proposes seven new metrics, bridging the gap between theoretical security metrics and their practical application in space systems. Our results highlight how these metrics can serve as valuable tools for policymakers, researchers, and industry in securing space infrastructure. By finding gaps and proposing new metrics specifically designed for space, our research advances the field and sets the foundation for more resilient cybersecurity strategies in the sector.

In the rest of the chapter, we proceed as follows. Section 6.2 clarifies the context and the motivation behind our research. In Section 6.3, we

discuss the relevant literature and compare it with the present chapter. Section 6.4 illustrates how security metrics can be used to support the implementation of NIST CSF 2.0 and to adhere to the NIS2 directive. In Section 6.5, we present our methodology to collect all the relevant security metrics from the literature. Section 6.6 maps them to the subcategories of NIST CSF 2.0, identifies gaps in the coverage of specific framework functions, and proposes new metrics to fill them. In Sections 6.7 and 6.8, we present our online tool and our case study, respectively, to show the practicality of the proposed and selected metrics. Finally, Section 6.9 draws some conclusions and discusses future lines of investigation.

6.2 Motivation and Context

Recently, policymakers have recognized the strategic need to protect space infrastructure from cyberattacks, following the suggestions of cybersecurity professionals and researchers who have long advocated for improving the security of space links and space-based and ground-based infrastructure [404].

Recent studies and analyses have shown that both the number and severity of cyberattacks have been dramatically on the rise, especially targeting critical infrastructure sectors like space [318]. One explanation is that the opportunities to perform attacks have grown, and the growing number of devices and interconnections has led to more attack vectors and vulnerabilities to be exploited [81]. Many devices that rely on space data to function, such as satellite modems and phones, GPS receivers, and PLCs, have well-known vulnerabilities that are now actively being exploited [569].

Considering the applications of space technology, a resilient space ecosystem is one of the preconditions of economic security in Europe. It is not a case indeed that several attacks against these infrastructures have been politically motivated [271]. As a result, governments started enacting policy measures to increase cybersecurity among all relevant parties [82]. These measures are usually in the form of best practices, technical guidelines, or threat reports. However, when compared to se-

curity metrics, they do not provide the same actionable and technical value from the standpoint of end users, particularly companies. To better implement these policy instruments, this chapter, therefore, proposes the development and usage of security metrics specific to space systems and the application of existing metrics from other domains to the context of space. Together with security controls, security metrics can support the implementation of security practices and measure their effectiveness. Such metrics can also be used to assess compliance with regulations and policies. We refer to metrics as tools for measuring the quality of cybersecurity management efforts, which allow for comparison with specific cybersecurity goals and evaluations at different periods of time or across organizations. In our research, these metrics are oriented toward the private sector as we consider companies to be the most vulnerable entities in the value chain, considering also the recent ENISA survey, which showed how 57% of European SMEs declared that they fear going out of business in the first week after a cyberattack [207].

When it comes to critical infrastructure protection, metrics are especially valuable, as they can provide organizations with insights into the resilience of their IT infrastructure and indicate the potential costs incurred from recovering after attacks, as well as the expenses needed for future defense against them. In our research, security metrics not only help save businesses from going offline or, even worse, going bankrupt but also assist in maintaining vital services for our daily lives.

The primary motivation for our work is the added value that metrics can provide in supporting various EU cybersecurity policies. This support extends to their implementation, evaluation, and application. A concrete example is given by Implementing Regulation of the NIS2 [190], where the European Commission mentions the need for indicators and measures to monitor the current maturity level concerning network and information security of relevant entities. This is intended to support the policies on risk analysis and information system security mandated by the Directive. Well-defined indicators and measures, such as security metrics, can be key in implementing, monitoring, and enforcing the NIS2 and other European regulations in the field. In the following sections, we

discuss relevant EU cybersecurity policies and how metrics that match the NIST CSF 2.0 can play a role in supporting them.

6.3 Related work

In recent academic literature, several studies have proposed novel security metrics for various sectors. However, to the best of our knowledge, only a limited number of research papers have specifically addressed the critical infrastructure sectors as defined in the NIS2 framework, and no specific metrics have been proposed for the space sector.

Tortorelli et al. [504] proposed a new metric for evaluating the security of complex Cyber-Physical Systems (CPSs) in a consistent and repeatable manner, helping operators take steps to improve the overall security posture of the system, the metric developed uses several elements such as component lifecycle, vulnerability criticality, and damage potential - effort ratio to measure the resilience of critical systems. Studies such as those by the Homeland Security Studies and Analysis Institute [235] developed a holistic, theory-driven suite of performance measurement metrics in the field of information sharing for critical infrastructure entities. It focuses on how these metrics can assess whether information sharing initiatives meet their goals of protecting critical infrastructure through robust data exchange among stakeholders in both the public and private sectors. Concrete examples of metrics are detailed across four categories: inputs (number of entities participating in the information-sharing initiative), processes (average time taken to disseminate threat indicators to participants), outputs (number of actionable threat reports generated), and outcomes (reduction in the number of successful cyber-attacks experienced by participating entities).

Only a few researchers have conducted in-depth studies to develop security metrics for specific sectors. Gori et al. [256], analyzed the current state of the art in selecting security metrics and proposed a novel methodology to gather, filter, and validate them. They applied this methodology to the Industrial Cyber Physical Systems (ICPS) domain, gathering almost 300 metrics from the literature. The resulting metrics are capable

of measuring the security of ICPS systems from different perspectives.

Krumay et al. [332] conducted a comprehensive study that examined the academic literature on cybersecurity management controls and metrics, specifically concerning critical infrastructures, using the NIST CSF 1.0 as a benchmark. The study evaluated the alignment of the existing literature with the framework functions and identified those gaps or areas that were underrepresented in both the academic discourse and the framework itself. The authors found imbalances in the coverage provided by the research literature, especially in the areas of detecting, responding to, and recovering from cyber incidents, and proposed potential areas for expansion within the NIST framework.

From the policy point of view, Parmar et al. [403] conducted a comparative analysis on the differences between the NIST CSF v2.0 and EU NIS2 Directive, highlighting their similarities in promoting governance and continuous risk management, and differences in regulatory enforcement and implementation requirements. The authors suggest that organizations may benefit from aligning with both frameworks to ensure comprehensive cybersecurity coverage.

Additionally, Dimakopoulou and Konstantinos [168] analyze cybersecurity in the maritime domain using the latest version of the NIST CSF 2.0 functional areas. They define a connection between research and NIST's functions and categories, identifying existing security research gaps. The primary goal of the paper is to analyze how well the maritime industry aligns with the NIST CSF v2.0 and to identify gaps in cybersecurity research and implementation. To achieve these objectives, the paper reviews existing studies and organizes its findings around the six core functions of NIST CSF v2.0. The work offers an extensive assessment of maritime cybersecurity measures aligned with the functions of the NIST CSF 2.0.

Unlike previous academic literature, which covered a broad set of metrics and controls pairing them with the NIST CSF 1.0, this chapter leverages the new NIST CSF 2.0 to advance our understanding of cybersecurity metrics for space systems. In addition, this chapter specifically focuses on the application of metrics to the space sector, an area that

has not been adequately addressed in the current literature. Indeed, to the best of our knowledge, no existing metrics that assess threats unique to space systems have been developed in the literature. Additionally, we highlight the practical value security metrics have for policymakers and decision-makers, supporting them to evaluate policy compliance, and proposes to use metrics in a way that remains underexplored in prior studies. To support our research, we also developed a tool that allows users to use these metrics and facilitate their application in concrete cases.

6.4 Supporting European Cybersecurity Policies with Data-Driven Security Metrics

In this section, we address **RQ1** and explore the role of metrics in helping organizations meet regulatory standards, enhance security practices, and ensure alignment with cybersecurity frameworks. More precisely, we provide an overview of various European policy instruments and identify how security metrics can support them. However, before diving into the specific European policies, we quickly summarize the NIST CSF 2.0 framework. We consider this framework as the cornerstone of our search for security metrics because it offers a solid foundation for any organization to improve its understanding, assessment, prioritization, and communication of cybersecurity efforts. Its predecessor, the CSF 1.0, has been used together with other standards, such as the ISO 27001 or the ISA/IEC 62443, as a reference to map security measures for Operators of Essentials Services (OES) by ENISA [210]. Similarly, CSF 2.0 can be considered a solid baseline for the NIS2 [403], because it reflects many of its principles.

6.4.1 The NIST CSF 2.0

The NIST CSF version 2.0, released in February 2024, replaced the NIST CSF version 1.1. NIST developed CSF v2.0 to help organizations understand, assess, prioritize, manage, and communicate the cyber risks that

can affect them. The Framework is suitable for use by organizations all over the world and is particularly relevant for critical entities as it reflects the content of US initiatives such as the Executive Order on Securing Critical Infrastructure [70] and the US National Cyber Strategy [32].

The Framework is presented using *functions* that describe outcomes coupled with implementation examples, and that must be achieved concurrently and continuously. While functions and outcomes can be considered relatively static, the implementation examples are rapidly changing, and are maintained separately online. In NIST CSF 2.0, each function is divided into categories related to cybersecurity outcomes. These categories collectively make up the function. Subcategories further divide each category into more specific outcomes of technical and management activities. The subcategories are not exhaustive, but they describe detailed outcomes that support each category. Table 10 illustrates an example of a function with a related category and subcategory. Since the detailed nature of subcategories, we decided to take them into account for our task of metrics matching and chose to identify at least one metric that could reflect the content or principles of each subcategory.

Function	Category	Subcategory
Identify (ID)	Asset Management (ID.AM): Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistently with their relative importance to organizational objectives and the organization's risk strategy	ID.AM-01: Inventories of hardware managed by the organization are maintained
Protect (PR)	Data Security (PR.DS): Information and records (data) are managed consistently with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-01:The confidentiality, integrity, and availability of data-at-rest are protected

Table 10: Examples of NIST CSF 2.0 functions with the corresponding category and subcategory.

Version 2.0 of the Framework features several enhancements with respect to the first version. One notable addition is the introduction of the new *Govern* function, recognizing the crucial role of governance in cybersecurity. This function integrates cybersecurity efforts with overall

business objectives and risk management strategies, providing a framework for managing responsibilities and decision-making in cybersecurity. This function is particularly relevant in the field of space, where complex supply chains involving different vendors, suppliers, operators, and end users create wide attack surfaces. Indeed, in space systems, governance is often a grey area, and this creates dangerous cybersecurity gaps; enforcing strict governance measures and accountability mechanisms could, therefore, significantly improve the security posture of the sector.

In addition to the *Govern* function, the new Framework introduces some clarifications and updates several areas to reflect the changes in the threat landscape and the emerging best practices. Moreover, CSF 2.0 uses clearer language, refines the various categories, and provides a holistic integration of privacy considerations. These adjustments have been introduced to help organizations strengthen their security posture and respond more effectively to incidents while ensuring resilience and operational continuity.

6.4.2 Operationalizing the CER Directive: The Value of Security Metrics for Critical Entities

One of the pillars in the field of critical infrastructure security policy is the European Union's Critical Entities Resilience (CER) Directive [202]. Issued in January 2023, the directive mandates that EU Member States identify critical entities in specified sectors by July 17, 2026. These entities play a crucial role in identifying essential services and conducting risk assessments, with space recognized as one of the 11 critical sectors. The adoption of the CER Directive marks a fundamental shift in the perception of the resilience of the critical infrastructure system in the European Union. The previous existing approach, based on the protection of critical infrastructure, is thus replaced by a new approach based on the resilience of critical entities that own or operate these infrastructures.

The CER Directive makes it mandatory for EU states to implement a series of actions by October 17, 2024, to enhance the resilience of Eu-

rope's critical infrastructure. In particular, it requires Member States to define a Strategy for the resilience of Critical Entities, including strategic objectives and priorities, a governance framework, measures to enhance the resilience of Critical Infrastructures and to prepare a list of the main authorities and stakeholders involved in the strategy's implementation. The CER also asks Member States to prepare a risk assessment, considering relevant natural and man-made risks, including hybrid threats, such as cyberattacks.

As there is no specific methodology for such risk assessment, security metrics can play a role in determining the level of security of entities and, therefore, also the level of risk. Moreover, the CER includes additional provisions such as Member States' support to Critical Entities, the establishment of resilience measures, and incident notification requirements, provisions that exist in the NIST CSF 2.0 frameworks and can be monitored and assessed through security metrics.

As this Directive obliges critical entities to take measures to increase their resilience but does not provide any methodological support, the use of security metrics can be of great help to companies to assess their level of security and, thus, resilience. Indeed, a necessary starting point for fulfilling this obligation is knowing the current resilience level of critical entities against incidents. The results of the resilience assessment, supported by security metrics, will enable critical entities to identify vulnerabilities, based on which adequate technical, security, and organizational measures can be defined.

6.4.3 Uncovering the relationship between the NIS2 and the CSF 2.0

This section compares the NIST CSF 2.0 with the cybersecurity risk-management requirements outlined in the NIS2. In order to reply to **RQ2**, we explore how the functions, categories, and subcategories of NIST CSF 2.0 relate to the provisions of the NIS2, particularly focusing on the requirements defined in the Implementing Regulation. We identify common areas, principles, and cybersecurity requirements, demonstrating a strong connec-

tion between the two instruments. This correlation enhances the value of metrics that can include the principles defined by CSF 2.0.

We have decided to evaluate the extent to which CSF 2.0 aligns with the requirements and provisions described by NIS2 mainly because Europe currently lacks a comprehensive cybersecurity standard that applies to all audiences, industry sectors, and organization types, regardless of their cybersecurity sophistication. If the NIS2 and other acts require sectors to adopt varying levels of stringent cybersecurity requirements and procedures, a reference framework similar to the NIST CSF 2.0 is still missing in the EU landscape. This framework should support the implementation of the Union's cybersecurity strategy and a future action plan dedicated to specific sectors.

The NIS2 Directive, analysed in detail in Chapter 4, establishes a common framework for cybersecurity risk management and incident reporting across the European Union and formally includes the space sector among the covered critical entities. In this chapter, NIS2 is treated as a regulatory baseline that motivates the need for measurable cybersecurity indicators, rather than as an object of legal analysis.

In our analysis, we have considered not only the NIS2 itself but also the Implementing Regulation [190] document. This document outlines the technical and methodological requirements for cybersecurity risk management measures and specifies the criteria for determining whether an incident is significant. Although this document only refers to certain entities such as DNS service providers, cloud computing service providers, data center service providers, content delivery network providers, and managed security service providers, similar provisions are expected to apply to all other sectors and entities affected by the NIS2.

Here, we analyze the extent to which the Commission Implementing Regulation of the NIS2 incorporates the functions, categories, subcategories, or elements defined in the NIST Framework. Our analysis aims to identify the presence of NIST CSF 2.0 functions within the Implementing Act and highlight gaps where specific elements may not be mentioned. Our goal is to emphasize how these two documents, despite their differences, address the same topics from different perspectives. This gives

us a solid basis to claim that the metrics we identify and propose in Section 6.6, addressing the CSF 2.0, are directly linked with the NIS2 and can therefore support its application and measure its compliance.

The NIS2 Implementing Regulation clarifies some aspects of the NIS2 Directive. The Commission produced two documents: the Implementing Regulation - Ares(2024)4640447 and its Annex. These documents specify the requirements for incident reporting and the technical and methodological requirements of the cybersecurity risk-management measures of the NIS2. The Commission decided to produce these documents to better clarify the content of the NIS2 and launched a consultation to ask the private sector for their opinions on such requirements. On the other hand, the NIST CSF provides a voluntary, comprehensive framework for improving cybersecurity risk management in organizations. Both documents aim to mitigate risks but differ in their main purpose, structure, target audience, and specific guidance. Both the NIST CSF and the NIS2, and its Implementing Regulation aim to establish a fundamental baseline for cybersecurity capabilities and ensure the effective implementation of these capabilities by organizations, and both emphasize the critical role of Governance and Supply Chain.

Notably, neither instrument can be fully implemented independently, but both require additional steps for full execution. NIST CSF suggests a subsequent Action Plan, while the NIS2 Directive implies the need for further frameworks, with the expectation that an additional Action Plan would also be necessary. Therefore, the need for specific metrics to support their execution is clear. Moreover, although both instruments are components of the broader process of achieving a comprehensive cybersecurity program or strategy, they seem to serve different specific purposes. While the NIST CSF offers a set of best practices and recommendations that are not obligatory, the NIS2 Directive enforces mandatory compliance with enforcement delegated to member states.

While Table 11 clarifies the key structural and legal differences between the NIST CSF 2.0 and NIS2, Table 12 highlights the alignment between the two. These dissimilarities show the complementary nature of the instruments and support our argument that CSF-based metrics can

enhance, but not replace, compliance with NIS2's mandatory requirements.

Aspect	NIST CSF 2.0	NIS2 Directive (and Implementing Regulation)
Legal Nature	Voluntary guidance framework developed by NIST; non-binding.	Legally binding EU directive with mandatory implementation for covered entities.
Enforcement	No enforcement mechanism; relies on internal governance or sector adoption.	Enforcement is delegated to EU member states, including penalties for non-compliance.
Target Scope	Applies to any organization, regardless of sector or size, on a voluntary basis.	Applies only to specific essential and important entities, defined by sector and criticality.
Structure	Organized around five Functions, Categories, and Subcategories with cross-sector applicability.	Structured around legal obligations and minimum technical and organizational requirements for risk management.
Technical Prescriptiveness	Provides high-level outcomes and flexible controls.	Specifies detailed requirements (e.g., asset inventories, backup validation, identity logging) in its Implementing Regulation.
Geographical Origin	Developed by a U.S. federal agency for domestic use, later adopted internationally.	Binding EU legislation intended for harmonization within the European Union.
Update Mechanism	Updated by NIST in public-private consultation cycles (e.g., 2.0 version in 2024).	Updated through EU legislative and delegated acts with formal regulatory timelines.
Purpose Orientation	Designed to improve risk management and maturity across organizations.	Designed to raise the minimum cybersecurity baseline across critical sectors in the EU.

Table 11: Dissimilarities between NIST CSF 2.0 and NIS2 Directive

Looking closer at the two documents, we identified several NIST functions that are covered by the Implementing Act. We report and highlight such relationships below. The Govern (GV) function of the NIST Framework includes categories such as Organizational Context (GV.OC), Risk Management Strategy (GV.RM), and Cybersecurity Supply Chain Risk Management (GV.SC). The Implementing Regulation emphasizes understanding the organizational context, including mission and stakeholder expectations, which aligns with the subcategories GV.OC-01 and GV.OC-02 of NIST. This alignment is evident in the statement: "*the policy on the security of network and information systems shall: [...] lay down roles and responsibilities [190]*". Additionally, the need for a comprehensive risk management strategy, corresponding to the category GV.RM-01, is highlighted in the Implementing Act that mandates that: "*the relevant enti-*

ties shall establish and maintain an appropriate risk management framework to identify and address the risks posed to the security of network and information systems. [190]". The Regulation also references managing supply chain risks, aligning with the GV.SC-01 and GV.SC-02 categories, stating: "*the relevant entities shall establish, implement and apply a supply chain security policy which governs the relations with their direct suppliers and service providers [190]*".

The Implementing Regulation outlines the importance of asset management, which is consistent with the category ID.AM-01 of the NIST Framework. Indeed, the Regulation states: "*the relevant entities shall establish and keep a list of all assets that are being logged and ensure that monitoring and logging systems are redundant [190].*" Additionally, the EU document details risk assessment procedures that correspond to the subcategories ID.RA-01 and ID.RA-02 of the Framework: "*The relevant entities shall perform and document risk assessments and, based on the results, establish, implement and monitor a risk treatment plan [190].*"

The Protect (PR) function through the subcategories from PR.DS-01 to PR.DS-05 addresses data security measures and aligns with the requirements of the Directive: "*the relevant entities shall lay down backup plans that include: assurance that backup copies are complete and accurate, including configuration data and information stored in cloud computing service environment*" [190]. The Regulation also discusses identity management and access control protocols, which are consistent with subcategories PR.AA-01 and PR.AA-02: " *the relevant entities shall: set up unique identities for network and information systems and their users, link the identity of users to a single person, ensure oversight of identities of network and information systems, apply logging to the management of identities*" [190].

For the Detect (DE) function, the need for continuous monitoring of systems as defined by the subcategory DE.CM-01, is underscored in the Regulation: "*ensure continuous effectiveness, monitor, maintain and test the supply of the network and information systems necessary for the operation of the service offered" [190].* Furthermore, the analysis of the detected events, similar to what prescribed by subcategory DE.AE-01, is mentioned as the Implementing Act requires for the: "*assignment of roles to detect and*

appropriately respond to incidents to competent employees" [190].

For the Respond (RS) function, the Implementing Regulation outlines incident management processes, reflecting subcategory RS.MA-01: "*The cybersecurity risk management process shall be an integral part of the relevant entities' overall risk management process, where applicable*" [190]. It also details incident response reporting requirements, matching subcategory RS.CO-01, addressing the elements defined in Section 3.5 of the Regulation.

For the Recover (RC) function, the Regulation emphasizes incident recovery plans in a way that is consistent with subcategory RC.RP-01. Moreover, Section 4.1 of the Regulation focuses on defining requirements for business continuity and disaster recovery plans.

Aspect	**NIST CSF 2.0**	**NIS2**
Main Focus	Establishing a set of best practices and recommendations for cybersecurity.	Implementing technical and methodological cybersecurity risk-management measures.
Governance	Includes categories like Organizational Context, Risk Management Strategy, and Supply Chain Risk Management.	Aligns with NIST's Governance function, emphasizing roles and responsibilities, risk management frameworks, and supply chain security policies.
Incident management	Encourages the development of incident response and recovery plans as part of the Respond and Recover functions.	Mandates incident reporting and the establishment of incident recovery plans with specific guidelines.
Supply Chain Risk Management	Emphasizes the importance of managing supply chain risks as part of the Governance function.	Requires entities to establish and apply a supply chain security policy, with detailed guidelines.
Compliance and Enforcement	Voluntary, with no enforcement mechanisms.	Mandatory, with enforcement delegated to member states, including penalties for non-compliance.
Future implementation	Suggests an Action Plan to guide implementation and assessment.	Requires further frameworks and an additional Action Plan for full implementation.

Table 12: NIS2 and NIST CSF 2.0 similarities.

Table 12 summarizes the results of comparing the two instruments. The table shows a significant alignment, especially in areas such as governance, incident management, and supply chain risk management. Moreover, it shows that the functions and categories of the NIST CSF 2.0 are well-reflected in the provisions of the NIS2 Implementing Act. This result suggests that organizations familiar with the NIST framework may find it easier to comply with European regulations.

Another similarity between the two documents concerns the need for additional frameworks and action plans to support their full implementation, highlighting the complexity of achieving comprehensive cybersecurity compliance. Indeed, the NIS2 Implementing Act requires further guidelines, while the NIST CSF 2.0 recommends an Action Plan.

We can exploit the similarity between these two documents highlighted in our analysis to provide practical guidelines to comply with NIS2. Indeed, the metrics developed for the NIST CSF 2.0 provide a measurable way to assess and ensure compliance with both frameworks, thus supporting the overall cybersecurity strategy in Europe. As reported in Table 12, such metrics can also cover the majority of the requirements laid out by European stakeholders in the NIS2 for critical infrastructure sectors such as space.

6.5 Methodological framework

After evaluating several methodologies in the literature, we decided to develop our approach to validate and verify the robustness of security metrics. Our approach synthesizes elements from various established frameworks, including Andrew Jaquith's security metrics guidelines [308], the NIST SP 800-55 performance measurement guide [91], ISACA's Guideline G41 on Return on Security Investment [545], and the PRAGMATIC approach by W. Krag Brotby [67].

Integrating these methodologies ensures a robust validation process to address the requirements of cybersecurity metrics required in the case of space systems. We decided to combine these approaches because we felt that the use of a single methodology among those analyzed, no matter how inclusive and efficient, fails to cover all the features necessary for a metric to be usable in our case study and in the field of space. The decision to develop a new methodology came from our need to not only identify and propose security metrics but also to obtain a set of metrics that could be used to comply with a specific framework and, in the future, be part of an integrated procedure to comply with EU cybersecurity regulations. Since no other methodology has been developed for this particular

purpose, we established specific validation criteria for our goal. Examples of the validation process are present in Table 19, but an extensive sample of validated metrics, and the whole set of metrics analyzed are available on the online supplementary material [80].

Our methodological approach is based on several key validation criteria extracted from the aforementioned frameworks, each contributing equally to the validation process:

- *Consistency and Objectivity (CO):* The considered metrics must be consistently measured without subjective criteria. This ensures reliability and repeatability in data collection and analysis, which is crucial for maintaining the integrity of the metrics over time.

- *Quantifiability (Q):* The considered metrics must yield quantifiable information, such as percentages, averages, and absolute numbers.

- *Availability of Data (AD):* The data supporting these metrics must be readily available and derived from repeatable information security processes, ensuring that the metrics are both practical and feasible to implement.

- *Actionability (A):* The considered metrics must be actionable and relevant to the organization's needs. They must provide specific courses of action based on certain indications, making them highly practical for decision-makers.

- *Contextual Relevance (CR):* The metrics must be contextually specific, offering insights that are directly applicable to the unique security challenges faced by critical infrastructures such as space organizations.

- *Applicability to the NIST CSF 2.0 subcategory (CSF):* The selected metrics must be related to and cover some or all the requirements, principles, or aspects of the NIST CSF 2.0 subcategory to which they are assigned.

- *Independence (IV):* The metrics must be measured independently, based on verifiable evidence, ensuring objectivity and reducing potential biases in the measurement process.

- *Cost-Effectiveness (CE):* The considered metrics must be cost-effective. They must generate more value than the cost to gather, analyze, present, and use, ensuring that the measurement process is sustainable and economically viable.

Although our approach to systematically search the literature does not follow a specific methodology such as PRISMA [395] in a formal sense, we designed our review to reflect the methodological principles that underlie PRISMA, such as transparency, filtering, and reproducibility. As outlined in Sections 6.5.2 and 6.5.3, our metric collection process followed a structured, approach composed of different phases. First, we define targeted queries using combinations of terms relevant to cybersecurity. Second, we applied clear inclusion and exclusion criteria to select sources: only papers and documents proposing concrete, measurable, and applicable metrics were retained; articles with only conceptual models or theoretical taxonomies were discarded. Third, we ensured traceability by classifying all validated metrics according to their origin (e.g., academic paper, stakeholder framework, standards body), their corresponding NIST CSF subcategory, and their compliance with our nine validation principles, including cost-effectiveness, actionability, and contextual relevance. Like PRISMA, we defined our sources a priori, documented the screening and filtering stages, and provided a replicable process flow (Figure 2) that readers can follow to reproduce our results or apply the same approach in different contexts. We combined academic literature with authoritative documents from relevant stakeholders (e.g., CIS Controls, MITRE, ISO/IEC 27004, ENISA, NIST) to build a comprehensive set of existing metrics, which were then validated and mapped using consistent criteria. Although our main search tool was Google Scholar, we used it in combination with additional academic databases such as Scopus, IEEE Xplore, and the ACM Digital Library. However, as these platforms largely overlap with the sources in-

dexed by Google Scholar, we did not identify additional relevant papers beyond those already retrieved. In this sense, our methodology respects the principles of PRISMA: systematic selection, justification of inclusion, traceable documentation.

6.5.1 Assessing the Cost of Security Metrics

While cost-effectiveness is undoubtedly an important characteristic that needs to be evaluated, assessing it can be quite challenging. Throughout our metrics selection, we justify cost-effectiveness by claiming that the information needed to evaluate the metric is already available or easy to obtain. However, this may not always be the case: it is not necessarily true that a metric requiring the collection of new data is not cost-effective.

Cost-effectiveness is treated quite differently by some of the main sources we used to collect metrics, yet their methods fit together into a single repeatable test. Jaquith opens his definition of a "good" metric claiming that it must be "cheap to gather, preferably in an automated way," making low marginal collection cost a non-negotiable gate that every candidate must pass [308]. True sustainability comes from pushing the data-gathering and calculation steps into code, which in turn permits faster sampling cycles and fresher insight without inflating labour spend [308]. The metrics-automation life-cycles extend the same economic logic: treat each metric as an engineered artefact whose design, versioning, run-time scheduling, and publication are controlled so that the human hours consumed by "care and feeding" never exceed the value of the information delivered [308].

The PRAGMATIC method [67], instead, introduces the "C = Cost" criterion, requiring the analyst to calculate the precise cost associated with a metric, the process is composed of the following steps: initial tooling, recurring collection, analytics, presentation and even the opportunity cost of choosing this measure over others, and then translate that total into a normalised score that sits beside Predictive, Relevant, Actionable and the other criteria mentioned by Brotby and Hinson [67]. Every PRAGMATIC dimension is rated on the same 0-to-100 (or 0-to-10) scale,

a high cost can be balanced by an equally high benefit; contrary, a metric that is cheap but adds little insight will still be rejected. This approach recommends banding annualised cost into broad ranges and recording the result along a brief narrative of tooling effort versus manual effort, making the arithmetic transparent and allowing managers to challenge or improve the estimate as the metric matures [67]. Cost also includes lost alternatives: prototyping two competing metrics and choosing the one with the higher net value may be cheaper than discovering too late that the first choice was uninformative [67].

Taken together, the two approaches operationalise our cost-effectiveness (CE) requirement as follows: for each candidate metric the operators should enumerate the one-off set-up effort, the licence or build costs of any tooling, the periodic run-time overhead and the opportunity cost of analyst attention, annualise that figure, and discard any metric whose score is so poor that even the most generous benefit estimate cannot lift it above zero. The surviving metrics should then be automated wherever possible to lock their marginal collection costs at the lowest achievable level; they should also be re-scored periodically as automation improves or business priorities shift. In this way, "cost-effective" is the outcome of a documented, auditable calculation. In order to make a concrete example of the practical application and validation of the cost-effectiveness criteria, we go deeper into the topic in Section 6.8.1, while discussing the metrics we used in our case study.

6.5.2 Metrics selection process

We follow a structured and multi-phase methodology to identify, filter, validate, and classify cybersecurity metrics aligned with the NIST CSF 2.0. The goal is to establish a set of metrics that reflect both the state of the literature and the needs of complex operational environments such as the space sector. Our methodology consists of four phases.

1. In Phase 1, we collect metrics from a broad range of sources, including authoritative books, official documents, and academic articles retrieved through systematic queries. The literature search

focuses on surveys and studies that aggregate or propose security metrics. In addition to general queries such as "security metrics survey," we already include targeted searches that reflect specific CSF subcategories, such as "asset management metrics", "supply chain metrics", and "incident recovery metrics."

2. In Phase 2, we perform a filtering process on the results of the previous phase to eliminate duplicates, harmonize terminology, and exclude sources that do not introduce concrete or actionable metrics. Articles that propose only conceptual frameworks, taxonomies, or general discussions without measurable indicators are excluded.

3. In Phase 3, the resulting metrics are evaluated using the nine validation principles of Section 6.5. Only metrics that meet these validation criteria are retained for further analysis.

4. Finally, in Phase 4, the validated metrics are mapped to the NIST CSF 2.0 structure. Each metric is assigned to the most appropriate Function, Category, and Subcategory based on its intended purpose and scope. This mapping allows us to assess the extent to which existing literature supports the various domains of the CSF and to identify areas of concentration and neglect.

5. Lastly, we conduct a gap analysis based on this mapping. We examine the distribution of metrics across the CSF to highlight which subcategories are most frequently addressed and which remain underrepresented. Each of the steps defined above is further discussed in the following section.

6.5.3 Selecting metrics to match the NIST CSF 2.0

This subsection answers **RQ2** by evaluating whether the existing security metrics, from both academic literature and key stakeholders, are sufficient to cover all the functions, categories, and subcategories of NIST CSF 2.0 within the context of critical infrastructure, particularly space

systems. Our findings indicate that while many metrics effectively address core areas of the framework, significant gaps remain, particularly in addressing the unique challenges posed by space systems.

We adopt a structured approach to explore the application of security metrics within space systems comprehensively and to identify the existing metrics in the literature that could match the NIST CSF 2.0 subcategories. Our methodology, the workflow of which is in Figure 2, comprised two main sources of analysis:

1. a focused examination of specific documents and books produced by relevant stakeholders and domain experts in the field of cybersecurity; and

2. an extensive literature review of academic articles.

Combining metrics from both the literature review and specific authoritative sources, our methodology aims to provide a complete assessment of the existing security metrics landscape. Here, we analyze both what the stakeholders are using and what the researchers in the field are proposing. This approach enables us to identify and recommend the most relevant and effective metrics for securing critical infrastructures such as space systems.

Concerning step (1) above, we analyzed metrics proposed by several stakeholders. The primary sources we examined are:

- *CIS Controls Measures and Metrics for Version 7* [97]: This document outlines more than 100 specific security metrics that are widely adopted for improving organizational cybersecurity posture.

- *Federal Information Security Modernization Act Chief Information Officer Metrics (FISMA CIO)* [242]: This informative document includes more than 100 metrics that can be derived from the text and supports the modernization of US federal agencies and is employed to measure and enhance information security in compliance with federal guidelines. They provide the data needed to monitor agencies' progress toward the implementation of the Administration's priorities and best practices.

- *Pragmatic security metrics: applying metametrics to information security [67]*: A comprehensive bibliographic resource that details more than 150 metrics, offering a pragmatic approach to quantifying and managing security risks.

- *Security Metrics* [308]: This book presents more than 140 security metrics examples, providing a broad overview of how metrics can be applied to evaluate and enhance cybersecurity measures.

- *ISO/IEC 27002*: an information security standard that provides a reference for a wide set of information security, cybersecurity, and privacy protection controls on which several security metrics are based.

- *NIST SP 800-55* [90]: This report focuses on developing and implementing information security metrics for an information security program. The report does not include metrics but provides guidance on how an organization can use them to identify the adequacy of security controls, policies, and procedures

- *ENISA Measurement Frameworks and Metrics for Resilient Networks and Services: Technical report* [508]: this report represents an attempt to create a single technical source of information on resilience metrics, it includes accurate information and methodologies to measure 10 security metrics and general information on 22 other metrics that can be used.

- *MITRE Cyber Resiliency Metrics Catalogue [56]*: This report presents a catalog of cyber resiliency metrics that can be used by systems engineers and cyber defenders to describe how well their efforts enable the cyber resiliency objectives to be achieved. Nearly 500 metrics are captured in the catalog.

- *ISO/IEC 27004:2016* [300]: this is the international standard specifically developed to support the measurement of information security performance and effectiveness within an Information Security

Management System (ISMS) based on ISO/IEC 27001. The standard was introduced to address the need for a systematic, auditable approach to evaluating whether security controls achieve their intended outcomes. It provides a formal measurement model, including definitions, processes, and evaluation techniques for both performance metrics (e.g., number of audits performed, training coverage) and effectiveness metrics (e.g., control impact on risk reduction). Annex B of the standard includes more than 30 example metrics mapped to specific ISO/IEC 27001 clauses, such as incident response, risk treatment, awareness training, access control, and vulnerability management. In our context, ISO/IEC 27004 is especially relevant because it illustrates how standardized measurement systems can support functions like *Identify*, *Protect*, and *Detect* within the NIST CSF. Furthermore, it provides an important benchmark for evaluating the methodological maturity of industry-developed metrics.

- *NIST SP 800-82 Revision 3*: Guide to Operational Technology (OT) Security [482]: This publication guides security professionals to secure Operational Technology (OT), including Industrial Control Systems (ICS), in alignment with the NIST Cybersecurity Framework. The document does not provide explicit security metrics, but it offers controls and recommendations, particularly in Appendix F, which maps OT security requirements to NIST CSF functions. These controls can be used to derive metrics. Despite its lack of quantifiable metrics, the report is valuable for contextualizing how cybersecurity functions can be operationalized in industrial and critical infrastructure contexts, including the space sector. However, due to the prescriptive and high-level nature of its controls, the document does not directly contribute metrics suitable for inclusion in the present metrics-based analysis.

Our analysis pays particular attention to these documents as they represent established and authoritative sources of security metrics within the cybersecurity community. In the next phase, we conduct a systematic

literature review to find cybersecurity metrics that align with the NIST CSF 2.0 subcategories. We exploit Google Scholar, in combination with IEEE Xplore and the ACM library as the main source to identify articles that include security metrics related to the five NIST functions and the related subcategories. During this phase of metric collection, our focus is on identifying relevant surveys and studies that aggregate or analyze security metrics. We aim to compile a catalog of metrics that have been recognized and validated within the academic and professional communities. We adopt search queries such as "*security metrics survey*" and "*review of security metrics*" to identify articles that provide a comprehensive overview of the existing metrics landscape. Alongside this literature review, we conduct a targeted search to identify metrics specific to key functions outlined by the NIST CSF 2.0. These functions include Access Control, Incident Response, Continuous Monitoring, Resilience, Data Security, Governance, and Risk Management. We use search queries such as "*Access control security metrics*", "*Incident response metrics*", "*Intrusion Detection Metrics*", "*Data security metrics*", "*Governance risk management security metrics*", and "*Resilience metrics for cybersecurity operations*" to ensure the retrieval of articles relevant to these domains.

Additionally, we refine the queries to match specific NIST CSF 2.0 subcategories by including targeted keywords. For example, queries like "*asset management metric*", "*risk management metric*", "*supply chain metric*", and "*incident recovery metric*" are used to retrieve articles and resources directly addressing the relevant subcategories. Through this approach, we map existing security metrics more accurately to the NIST CSF 2.0 framework and identify gaps or limitations in coverage.

These keywords and phrases are selected to obtain a comprehensive collection of metrics that is aligned with the NIST CSF and reflects the latest developments and research in the field. The search results are then filtered to include only peer-reviewed articles, conference papers, and reputable industry reports to ensure the quality and reliability of the collected metrics. For the purpose of this paper, we consider articles published between 2002 and 2024. We discard articles that do not introduce new metrics, such as those proposing new approaches, providing infor-

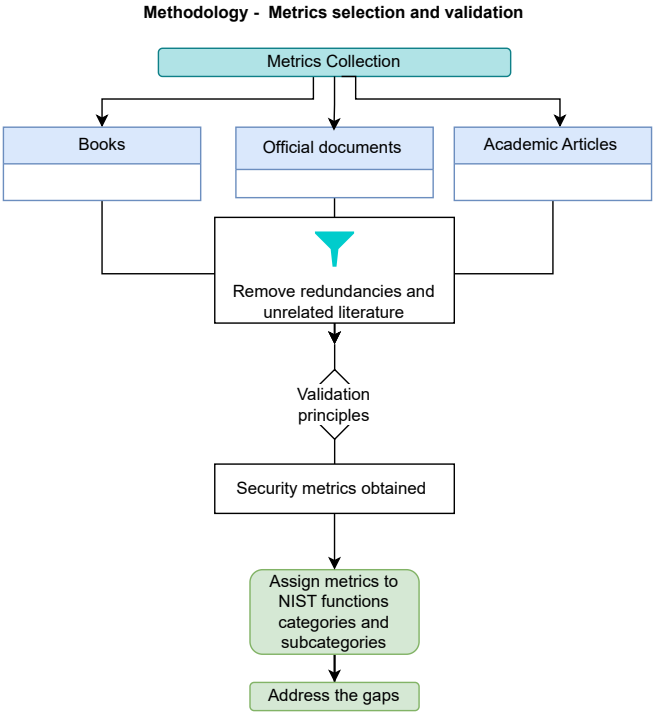

Figure 2: Metric selection methodology

mative articles, or suggesting taxonomy. We also exclude similar papers on the same metric and any non-peer-reviewed articles. Our targets are papers that directly address controls or metrics of cybersecurity applicable to critical infrastructures. At the end of this process, we obtain 48 papers that meet our criteria.

After a validation phase, we extracted 90 metrics that matched the 9 criteria we defined at the beginning of this section from the selected papers, official documents, and the books mentioned above. The next step is classifying these metrics according to the NIST functions, categories, and subcategories. In this step, we assign the 90 metrics to 45 NIST sub-

categories.

Tables 13, 14, 15, 16, 17, and 18 summarize our analysis focusing on the various functions. For example, in the case of the Govern function, we identified 14 metrics addressing 11 NIST CSF 2.0 subcategories. Our results reveal that the risk management category received the most attention from researchers. Categories, such as Organizational Context (GV.OC), which focuses on mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements, or Oversight (GV.OV), which entails the use of risk management outcomes to inform, improve, and adjust the risk management strategy, were hardly linkable to any existing security metric.

For example, one of the metrics we identified in Table 13 is *"Security policy management maturity"*, which involves measuring the organization's approach to managing information security risks. This process includes comparing the organization's risk management practices to a benchmark or standard. Despite various methods existing for performing this assessment, we considered the use of predefined criteria on a scoring scale as proposed by the Pragmatic method [67].

In the following sections, we go deeper in our analysis, show how far NIST framework functions are represented in the literature, and we present topics discussed in the literature but not covered by NIST guidelines. Finally, we address some of the gaps in the literature and provide some metrics that should be applied by the space industry.

6.6 Addressing metrics for the space sector

In our study, we focus on space systems and structure our dataset by classifying metrics based on specific characteristics that can apply to space and other critical infrastructure sectors. Space systems consist of interconnected ground-based and space-based components responsible for monitoring, managing, and supporting various space missions. Key components of space systems include satellites, ground control stations, antennas, telemetry and command systems, and various subsystems. This diversity results in high system complexity, requiring significant effort to

CSF Function	Subcategory	Metric Name
Govern	GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	• Security governance maturity (Level 1–5) [160, 353]
Govern	GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed	• Average frequency of audit records review and analysis for inappropriate activity [38]
Govern	GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders	• Security policy management maturity [67] • % critical assets/functions with cost of compromise estimated [67]
Govern	GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes	• Number of high/medium/low risks currently untreated and unresolved [67]
Govern	GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated	• % critical assets/functions with documented risk mitigation plan [67]
Govern	GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	• Proportions of systems checked and fully compliant to applicable (technical) security standards [67]
Govern	GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	• Percentage of security policies, standards, procedures, and metrics with committed owners [67]
Govern	GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies	• Information Security Budget as a Percentage of IT Budget [91] • Return on Security Investment [466]
Govern	GV.RR-04: Cybersecurity is included in human resources practices	• % BU heads with implemented operational procedures aligned with controls [308] • % new employees completing security awareness training [532]
Govern	GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	• % information systems with operational policies and controls [160]
Govern	GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	• Percentage of system and service acquisition contracts that include security requirements and/or specifications [38]
Identify	ID.AM-01: Inventories of hardware, software, services, and systems managed by the organization are maintained	• Number of orphaned information assets without an owner [40] • Proportion of information assets not (correctly) classified [67] • Information asset management maturity [67]

Table 13: Cybersecurity Metrics Aligned with NIST CSF Subcategories (First Part)

CSF Function	Subcategory	Metric Name
Identify	ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission	• Percentage of critical assets/functions residing on compliant systems
Identify	ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded	• Percentage of systems without known severe vulnerabilities [361] • Number of unpatched vulnerabilities [408] • Number of historically exploited vulnerability [408] • Weakest-Adversary [396] • k-Zero Day Safety [548]
Identify	ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources	• Percentage of participating entities reporting that the shared information they receive in a given time period informs decisions that reduce cyber risks to critical infrastructure [235]

Table 14: Cybersecurity Metrics Aligned with NIST CSF Subcategories (Second Part)

manage and mitigate potential anomalies. Given its peculiarity, metrics tailored for the space domain should consider the following characteristics:

- *Long-Term Cybersecurity Effectiveness:* Metrics should consider the long-term effectiveness of cyber defenses in space-based systems, aligning with the expected lifespan of assets in orbit.
- *Challenges in Upgrading Cybersecurity:* Metrics need to address the difficulties involved in upgrading the architecture of space-based networks, considering the significant deployment times and high costs.
- *Constraints of Small Space Systems:* Metrics should take into account the limitations related to small space systems, including their lack of integrated cybersecurity capabilities due to budget constraints and technological limitations.

From this perspective, the main security concerns within space systems include ensuring the confidentiality of sensitive mission data, maintaining the integrity of command and control signals, and ensuring the availability of communication links, all essential for the success and safety of

CSF Function	Subcategory	Metric Name
Identify	ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	• Mean-time-to-Compromise (MTTC) [339] • Probability of vulnerability exploited [573]
Identify	ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization.	• Percentage of critical assets/functions with documented risk assessment [308] • Attack Shortest Path [234]
Identify	ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated	• Risk Assessment Coverage [449]
Identify	ID.IM-03: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties	• Number of physical security devices with documented and tested security procedures [38] • Number of important operations with documented and tested security procedures [38]
Identify	ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	• Percentage of organizational units (e.g., departments) with contingency planning [422]
Protect	PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization	• Percentage of users who have undergone background checks [308] • Number of access rights authorized, revoked, reset, or changed [33] • Number and type of suspected and actual access violations [33]
Protect	PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions	• Amount of users with passwords in accordance with the password management security policy [532]
Protect	PR.AA-03: Users, services, and hardware are authenticated	• Percentage of business units that have proven their identification and authentication mechanisms [33] • Minimum Password Strength [553]
Protect	PR.AT-01: Personnel are provided with awareness and training to perform tasks with cybersecurity risks in mind	• Number of consultations with security teams by externally facing applications teams [308] • Number of customer consultations with security teams [308] • Number of security team consultations by business units [308]
Protect	PR.AT-02: Individuals in specialized roles are provided with awareness and training for cybersecurity	• Percentage of managers who have attended the organization's information security training and/or awareness program in the last 12 months [33]

Table 15: Cybersecurity Metrics Aligned with NIST CSF Subcategories (Third Part

CSF Function	Subcategory	Metric Name
Protect	PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected	• Restriction of Number of Executable Components [334] • Data transmission exposure [427] • Percentage of assets with antivirus and antispyware software [308]
Protect	PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected	• Percentage of coverage of confidentiality and integrity controls for data exchanged with customers/partners [308]
Protect	PR.PS-01: Configuration management practices are established and applied	• Rogue Change Days [63] • Mean Cost to Mitigate Vulnerabilities [361] • Patch Policy Compliance [361] • Mean Time to Patch [56] • Mean Cost to Patch [84] • Percentage of Configuration Compliance [90]
Protect	PR.PS-02: Software is maintained, replaced, and removed commensurate with risk	• % of critical assets/functions residing on compliant systems [308]

Table 16: Cybersecurity Metrics Aligned with NIST CSF Subcategories (Fourth Part)

space missions. Before presenting the space-specific metric selection, it is important to highlight the fundamental interdependence between cybersecurity and safety in this domain.

6.6.1 The Interdependence of Safety and Cybersecurity in Space Systems

In safety-critical domains like space systems, safety and cybersecurity are inherently interconnected. Failures in one area can compromise the effectiveness of the other. Safety aims to ensure that systems operate without causing physical harm or environmental damage, even in failure conditions. In contrast, security focuses on protecting systems from intentional malicious interference.

In increasingly connected and software-dependent environments, these two aspects cannot be addressed in isolation. A cyberattack can undermine safety features by disabling protective functions, injecting false commands, or manipulating the system state, thereby creating hazardous conditions. Conversely, safety gaps, such as the lack of fail-safe protocols

CSF Function	Subcategory	Metric
Protect	PR.PS-04: Log records are generated and made available for continuous monitoring	• Rate of messages received at central access logging/alerting system [308]
Protect	PR.IR-01: Networks and environments are protected from unauthorized logical access and usage	• Penetration resistance [408]
Protect	PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	• Attack Resistance Metric [547] • Mean Time to Complete Changes [327]
Protect	PR.IR-04: Adequate resource capacity to ensure availability is maintained	• Host uptime / downtime [273] • Network Resilience [89]
Protect	PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	• Security of system documentation [269]
Detect	DE.CM-01: The network is monitored to detect potential cybersecurity events	• Information access control maturity [41] • Viruses and Spyware Detected in Email Messages, websites, user files (number [#], percent [%]) [308] • Percentage of business-critical systems under active monitoring [308] • Vulnerability scanner coverage (#, %, frequency) [308] • Encounter rate [408] • Network Compromise Percentage (NCP) [181] • Attack surface [354] • Intrusion Detection Capability [265]
Detect	DE.CM-02: The physical environment is monitored to find potentially adverse events	• Percentage of critical assets/functions reviewed for physical security risks [308] • Mean-Time-To-Incident-Discovery [100]
Detect	DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events	• Administrator and operator logs [269] • Number of corrective actions [269]

Table 17: Cybersecurity Metrics Aligned with NIST CSF Subcategories (Fifth Part)

CSF Function	Subcategory	Metric
Detect	DE.AE-02: Potentially adverse events are analyzed to better understand associated activities	• Attack Impact [277] • Number of detected incidents [269]
Detect	DE.AE-02: Potentially adverse events are analyzed to better understand associated activities	• Attack Cost [435] • Cost metric [483]
Respond	RS.AN-03: Analysis is performed to establish what has taken place during an incident and the root cause of the incident	• Number of incidents handled [445] • Time per incident [476]
Respond	RS.AN-08: An incident's magnitude is estimated and validated	• Mean Cost of Incidents [264]
Respond	RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared	• Support response time (average time) [308] • Median time to initially respond to the reporter [242] • Mean blind spot metric [46]
Respond	RS.MI-01: Incidents are contained	• Mean-Time to Mitigate Vulnerabilities [549]
Recover	RC.RP-02: Recovery actions are selected, scoped, prioritized, and performed	• Mean Time between Security Incidents [445]
Recover	RC.RP-01: The recovery portion of the incident response plan is executed once initiated from the incident response process	• Mean-Time-to-Recovery (MTTR) [320] • Incidents Cleanup Cost (By business unit) [308] • Mean Incident Recovery Cost [173]

Table 18: Cybersecurity Metrics Aligned with NIST CSF Subcategories (Sixth Part)

or physical redundancies, can amplify the potential impact of cyber incidents. This mutual dependency is especially critical in space systems, where autonomous operations, communication latency, and the physical remoteness of assets necessitate that both safety and security controls be predictive, resilient, and integrated into the system design and monitoring from the beginning [535].

Developed by the European Cooperation for Space Standardisation, the ECSS-E-ST-80C [471] standard underscores this requirement by prescribing a defense-in-depth architecture, integrating protective layers that are designed to detect and mitigate cyber threats, but also to preserve the system's ability to operate harmlessly under attack or failure conditions. It explicitly distinguishes between "fail-safe" and "fail-secure" behavior requiring mechanisms that protect safety even when security controls are breached or malfunctioning. At the engineering level, space systems standards such as ECSS-Q-ST-80C [472] (software product assurance) and ECSS-E-ST-40C [473] (software engineering) require the integration of safety and security controls into configuration management, software assurance, and mission-level risk assessments.

Cybersecurity metrics, particularly those related to incident detection timing, access control integrity, system configuration consistency, and monitoring coverage, serve dual roles. They can evaluate security posture, but also act as indicators of system safety and mission reliability. Monitoring how quickly a system detects and recovers from anomalies, or how well access and configurations remain in a known-safe state, can support insights into the likelihood that safety-critical operations are still viable under stress.

In this context, the cybersecurity metrics we propose support both security oversight and operational safety assurance. Although these metrics are grounded in the NIST CSF 2.0 structure, they are relevant to safety-critical concerns, as they can help assess whether a system can withstand, detect, and recover from intentional disruptions without compromising mission safety.

6.6.2 Metrics Filtering

The purpose of this section is to explain and justify the selection of the final set of metrics. Below, we define the inclusion criteria we have established for filtering metrics based on the characteristics of critical infrastructure, specifically in the space domain:

- *Applicability:* The metric's definition must be relevant to space systems, including space-based components, e.g., satellites and payloads, ground segments, e.g., control stations and communication networks, and the protocols that enable their operation.

- *Objective Measurement:* The meaning of the metric must clearly indicate an objective measurement related to at least one of the NIST functions: Govern, Identify, Protect, Detect, Respond, and Recover.

- *Scope:* The scope of the metric must apply to categories such as "space segment", "ground segment", "communication link", or "mission operations".

As a first step, we apply our 9 validation criteria to prove the reliability and efficiency of the selected metrics. In Table 19, we provide some examples of the validation procedure and reasoning behind the selection of the metrics reported in Tables 13, 14, 15, 16, 17, and 18. Our goal is to produce a set of metrics that can be effectively applied in practical scenarios within the space sector. We do not limit our filtering process to selecting metrics merely relevant to the domain but also ensure that the chosen metrics are relevant and practical for use in other critical infrastructure sectors. To verify that each metric applies to one or more of the NIST functions, we perform a validation process for each metric before assigning it to a specific NIST subcategory.

In order to provide an example of how we applied the validation criteria defined in Section 6.5 we discuss their application in Table 19. In the first row, the metric "Percentage of critical assets/functions with documented risk mitigation plan" measures the proportion of applications crucial to an organization's operations with a risk mitigation plan.

Metric	Ref	CO	Q	AD	A	CR	CSF	IV	CE
Percentage of critical assets/functions with documented risk mitigation plan	[67]	✓	✓	✓	✓	✓	✓	✓	✓
Network Compromise Percentage (NCP)	[181]	✓	✓	✓	✓	✓	✓	✓	✓
Number of Attacks	[308]	✓	✓	✓	✗	✗	✗	✓	✓
Number of active user IDs assigned to only one person.	[308]	✓	✓	✓	✗	✗	✗	✓	✓

Table 19: Risk Mitigation Metrics for Critical Assets/Functions

This metric is consistent and objective (CO) as it systematically evaluates assets' risk mitigation plans, avoiding subjective assessments. It is quantifiable (Q), expressed as a clear percentage, allowing easy interpretation and comparison. Data for this metric is readily available (RA), as it utilizes existing records of assets and their plans. The metric is actionable (A) because it helps organizations prioritize security efforts towards the most critical applications without an established plan, enhancing resource allocation. Contextually, it is highly relevant (CR) to the unique challenges of critical infrastructures like space systems, where safeguarding key applications is essential. The metric aligns with NIST CSF 2.0 subcategories, particularly those related to asset and risk management. It is independently verifiable (IV) through documented assessments and is cost-effective (CE), as it leverages existing data with minimal additional expenses.

Similarly, the "Network Compromise Percentage (NCP)" metric in the second row of Table 19 meets our validation criteria as it provides a consistent, objective, and quantifiable measure of the percentage of compromised hosts within a network. NCP uses available data from security assessments, such as condition-oriented attack graphs, vulnerability scans, or penetration testing. It is actionable as it highlights the extent of compromise, enabling targeted interventions and resource allocation to mitigate risks. NCP is contextually relevant to critical infrastructures, directly addressing specific security challenges these organizations face, and aligns with the NIST CSF 2.0 subcategories related to protection, de-

tection, and response. The metric's independence and reliance on verifiable evidence ensure unbiased and objective results while using existing data sources makes it cost-effective.

Among the metrics extracted, some did not satisfy the full set of validation principles established in our framework and were therefore excluded from the final set of validated metrics. A more detailed overview is available on the online supplementary material [80]. The metric "Number of attacks" is quantifiable, objective, and based on available data streams (as intrusion detection systems or firewalls). However, it fails several critical validation principles: it lacks actionability (A); the raw number of attacks does not allow security teams to derive concrete courses of action. It is not clear whether a higher number of attacks reflects better detection capabilities, greater exposure, or a change in the threat landscape. Second, the metric does not meet the requirement of contextual relevance (CR), especially for highly specialized sectors such as space-based systems or critical infrastructure. The volume of attacks, without insights into their nature, success rate, or impact on mission-critical components, provides little information relevant to sector-specific threats. Furthermore, it does not fulfill the criterion of applicability to the NIST CSF subcategories (CSF). The NIST framework emphasizes control objectives, mitigation strategies, and functional outcomes – none of which are directly measurable through simple attack counts. Although the metric may offer some value as a general indicator of activity levels, it lacks the specificity and decisional utility needed for inclusion in a structured cybersecurity performance model.

Another metric excluded during the validation process is "Number of active user IDs assigned to only one person." This metric quantifies how many user accounts are uniquely associated with individual users. The metric lacks actionability (A), offers no specific guidance or decision-support beyond a generic indication of administrative hygiene. A higher or lower number may be interpreted as good or bad depending on organizational policies, making it difficult to translate the result into clear corrective or preventive actions. Furthermore, the metric lacks contextual relevance (CR) for sectors such as space or critical infrastructure,

where identity and access management is far more complex and risk-sensitive. The metric also fails in terms of applicability to the NIST CSF 2.0 (CSF). Although superficially related to subcategories like PR.AC-1 (identities and credentials are issued, managed, verified, revoked, and audited), it does not measure the performance, effectiveness, or security outcome of that control, but reflects a preference that lacks operational depth.

During our filtering process, we evaluate all the metrics based on the criteria of Section 6.5 and select the final set of metrics. This ensures that we have metrics relevant to our specific domain and are actionable and cost-effective. Although many identified metrics can be adapted or calculated using different methodologies depending on the specific case and mission, our goal is not to establish a definitive set of metrics that would be sufficient for an organization. Instead, we aim to provide a solid foundation and methodology for identifying the most suitable metrics to comply with frameworks such as NIST CSF 2.0 or to measure security based on the principles of regulations like NIS2. In the following sections, we will delve into the main findings of our analysis.

6.6.3 Metric Analysis Results

Now, we present the results of our analysis, which includes a list of the security metrics that have been selected and validated. We also analyze uncovered areas, referring to the NIST functions not thoroughly addressed by security metrics. Additionally, we compile a list of relevant metrics that can be applied to space systems.

Remember that in the NIST CSF 2.0, each Function is divided into Categories, which are related to cybersecurity outcomes that collectively comprise the Function. Subcategories further divide each Category into more specific outcomes of technical and management activities. The Subcategories are not exhaustive, but they describe detailed outcomes that support each category. Figure 3 illustrates how the selected security metrics are distributed across different NIST functions. The plot shows that most of the directly mappable metrics are related to the functions Protect

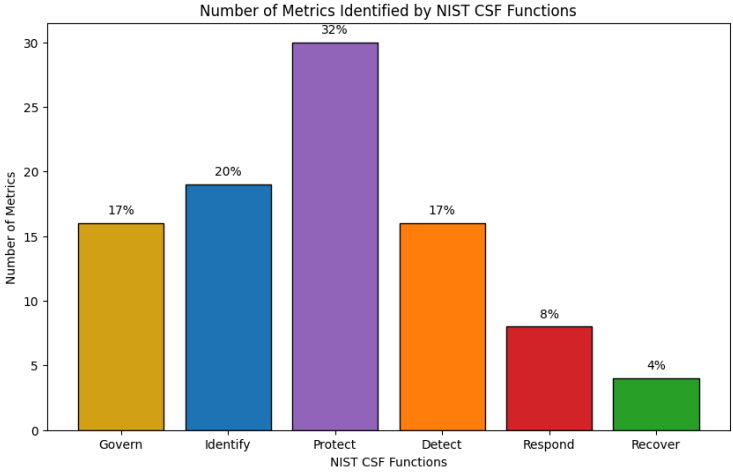

Figure 3: Distribution of Metrics per each NIST CSF Function

(32%), Identify (20%), and Govern and Detect (17%). In comparison, the functions Respond (8%) and Recover (4%) are minimally covered in the literature.

Through our research, we make significant progress in addressing many NIST CSF 2.0 Subcategories. However, there are challenges in mapping all of them, particularly within the "Respond" function. Moreover, our review of the literature identified a significant gap in metric coverage for several subcategories under the Respond and Recover functions. In particular, RS.CO (Incident Response Communications) and RS.MA (Incident Analysis) is rarely addressed through standardized or validated metrics [180, 379]

Additionally, metrics did not adequately cover subcategories and categories related to the "Govern" functions, such as Oversight (GV.OV) and Organizational Context (GV.OC). This is consistent with prior findings that governance and cultural factors are challenging to operationalize, and few existing frameworks provide quantitative metrics for evaluating oversight, stakeholder alignment, or mission-context integration [206, 141].

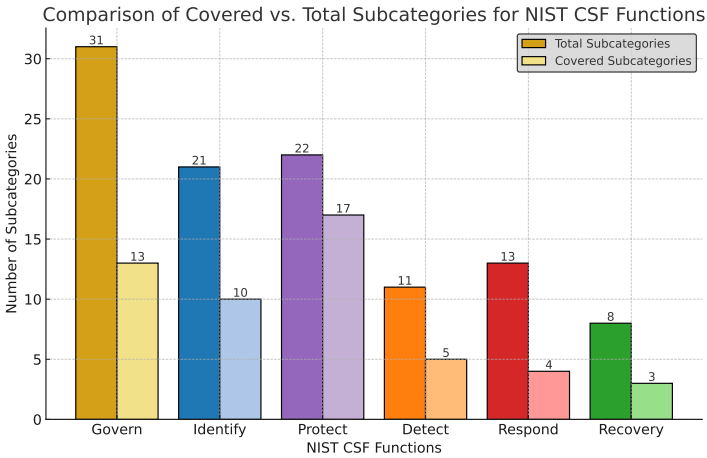

Figure 4: Metrics identified over total number of NIST CSF Subcategories

These gaps, highlighted in Figure 3, emphasize the need for further metrics development in these areas and highlight the importance of creating specific metrics to fully address the complexities of incident response, especially in the context of cybersecurity for critical infrastructure such as space systems. This is also important because incident response and reporting are some of the mandatory requirements imposed by the NIS2. Figure 4 presents the extent of metric coverage for the subcategories.

Such shortcomings, as those hilighted in Figure 3 and 4 can be linked to the difficulty of measuring certain processes and outcomes of the CSF, such as governance oversight (GV.OV). If we take three of the subcategories that compose GV.OV: GV.OC-01: *The organizational mission is understood and informs cybersecurity risk management*, GV.OC-02: *Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered*, and GV.OC-03: *Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed*, we realize how they reflect qualitative assessments that are inher-

ently difficult to quantify. Measuring an organization's understanding or alignment with such abstract concepts presents methodological challenges, especially in the absence of clear indicators or benchmarks [368, 38]. By contrast, the Respond and Recover functions, particularly categories like RS.RP (Response Planning) and RC.IM (Improvements) entail more operational, event-driven activities that are easier to quantify. For example, metrics such as mean time to detect (MTTD), mean time to respond (MTTR), or the number of incidents with documented lessons learned can be systematically tracked and analyzed. This makes it comparatively easier to assess organizational performance in these areas. Consequently, these functions may allow for a more robust and metric-driven evaluation framework, highlighting the imbalance in metric availability across the CSF functions.

Considering only the industry sources, several industry frameworks have contributed to the development of cybersecurity metrics, but their focus remains uneven across the NIST Cybersecurity Framework core functions. In particular, we see that again the Respond and Recover categories are markedly underrepresented. The CIS Controls v8, [97] for instance, emphasize asset management, identity control, and vulnerability mitigation, areas that map strongly to the Identify and Protect functions, but provide limited guidance or quantifiable metrics for incident response or recovery capabilities. Differently, the NIST SP 800-53 Revision 5 [482] presents a list of controls related to incident response (IR) and contingency planning (CP), which correspond to the Respond and Recover functions. However, these controls are primarily descriptive and do not include standardized or operational metrics that could support performance measurement or benchmarking. The MITRE ATT&CK [437] framework supports adversarial behavior mapping and threat detection, and aligns well with the Detect function, but does not propose metrication for response activities or recovery procedures. This persistent gap across industry sources shows the broader challenge of operationalizing the Respond and Recover functions in a measurable way and highlights the need for future metric development to better support incident handling, containment, and post-incident resilience.

The academic studies considered in our research overlook these dimensions, even though they should be key components of every security strategy. While NIST emphasizes that no function should be prioritized over another, is evident that there is no equilibrium in the academic work. Even if we noticed slight reductions in the detected imbalances when considering that many metrics could be applied to more than one category, some functions remained mostly uncovered. In our view, future research should focus more on addressing how to manage and assess these important areas and develop more tools to measure the soundness of cybersecurity management after a breach has occurred. If we consider metrics as a tool to support both companies and policymakers, new metrics can be developed based on analyzing policy requirements and specific expected security outcomes.

6.6.4 Analysis of Uncovered Areas

Our study also identifies uncovered areas by the NIST framework, especially in supporting the tasks of companies that are involved in critical infrastructure sectors. The monetary aspects of cybersecurity management are hardly covered in NIST, but are well mentioned in academic literature. Despite the importance of safeguarding against cyberattacks aimed at critical infrastructure, the economic consequences for the involved organizations deserve greater attention. It is widely accepted that any compliance initiative is costly, and many organizations struggle to meet the time and cost objectives of related control activities and audits. This consideration is crucial for the goal of our research, which is to support policy implementation and understand its consequences. Metrics capable of measuring the compliance costs or the financial effects of certain requirements or the non-implementation of certain requirements could be useful for both industry and stakeholders.

6.6.5 Proposed Metrics

Given the growing dependency on space technologies and the intricate structure of their architecture, traditional cybersecurity indicators might

not completely grasp the extent of the risks involved. Henceforth, new criteria are needed to evaluate security status and facilitate improved decision-making while ensuring adherence to evolving regulations, like the NIS2 Directive and the upcoming Space Law or National frameworks. We introduce a new collection of security metrics tailored to the space industry's needs, concentrating on satellite communication and space networks. These metrics aim to assess some of the cybersecurity risks encountered by entities in the sector. The value of such metrics and their practical implications are highlighted by the case study presented in Section 6.7. Moreover, these metrics can be easily integrated into the risk assessment cycle of companies through the tool we propose in the next section. As we develop the new metrics for space companies, we consider several pillars to form the basis of these metrics. These pillars can be used to develop other metrics tailored to specific companies and organizations. During the metrics development phase, we focus on the following aspects:

- *Alignment with Space-Specific Risks:* Traditional security metrics often do not account for space-specific threats like signal jamming. The proposed metrics address some of these unique challenges.

- *Focus on Resilience and Continuity:* Due to space operations' critical nature, we propose metrics that assess system redundancy, backup capabilities, and incident response coverage to ensure continuous operations and rapid recovery from disruptions.

- *Consideration of Third-Party Risks:* Recognizing the interconnected nature of the space sector, where multiple entities collaborate, we introduce metrics to assess the resilience of third-party endpoints and the security of interconnected systems.

- *Future-Proofing Against Emerging Threats:* With advancements in quantum computing, space organizations need to be prepared for future threats. We propose adopting specific metrics, such as the Quantum Cryptographic Readiness Level (QCRL), designed to evaluate readiness for such upcoming challenges.

Metric	Description	NIST CSF Mapping	Related Metric	Formula
Percentage of Critical Systems connected to satellite links without intermediate firewall	Quantifies the critical systems directly connected to satellite links without the protection of intermediate firewalls.	Identify / Asset Management (ID.AM)	Remote locations connected directly to core transaction and financial systems without intermediate Firewalls	$\%CA = \left(\frac{\text{CA-C}}{\text{TCA}}\right) \times 100$
Third party remote endpoint resilience	Measures the percentage of third party remote endpoints administered by security personnel that are subject to anti-malware and patch management controls	Govern / Cybersecurity Supply Chain Risk Management (GV.SC)	Remote endpoint manageability (%)	$3pRER = \left(\frac{\text{EPM}}{\text{TEP}}\right) \times 100$
Interconnected System Redundancy Ratio	Measures the percentage of redundant communication links and subsystems within a space network	PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	N/A	$RRR = \left(\frac{\text{RCS}}{\text{TCS}}\right) \times 100$
Signal Jamming Exposure Index (SJEI)	Measures the risk and frequency of signal jamming attempts on space communication systems.	Detect / Continuous Monitoring (DE.CM)	To calculate the jamming severity, metrics as the Error Vector Magnitude (EVM) can be used.	$SJEI = \left(\frac{\text{JAD}}{\text{TMP}}\right) \times \left(\frac{\text{JS}}{\text{TSC}}\right)$
Quantum Cryptographic Readiness Level (QCRL)	Evaluate the readiness of space communication systems to implement quantum-resistant cryptographic protocols.	Protect / Data Security (PR.DS)	N/A	$QCRL = \left(\frac{\text{QPL}}{\text{TCL}}\right) \times 100$
Incident Response Plan Coverage (IRPC)	Percentage of critical space systems and missions covered by documented incident response plans.	Respond (RS) / Incident Management (RS.MA) / RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared	N/A	$IRPC = \left(\frac{\text{CSIRP}}{\text{TCS}}\right) \times 100$
Automatic Backup Coverage (ABC)	Percentage of the organization's hardware assets configured to back up system data automatically regularly.	Recover / RC.RP-05: The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed	N/A	$ABC = \left(\frac{\text{AB}}{\text{TA}}\right) \times 100$

Table 20: Security Metrics for Space Systems with Related Metrics Updated

The proposed metrics are summarized in Table 20, and we briefly comment on them below. Table 21 defines the abbreviation used in the metric formulas. Our metrics are designed to tackle specific risks related to space operations and can be enhanced to ensure compliance with regulations and best practices. Additionally, they are adaptable, allowing for the development of additional metrics to address mission-specific or scenario-specific security concerns unique to individual companies. Tailoring the metrics to meet the specific cybersecurity requirements outlined by regulations to establish a resilient and secure space infrastructure is essential.

The first metric in the table is "Percentage of Critical Systems Connected to Satellite Links Without Intermediate Firewalls" (CSCS). Its for-

Abbreviation	Description
CA-C	Critical Assets/Functions with Cost of Compromise Estimated
TCA	Total Number of Critical Assets/Functions
EPM	Number of Third-party Remote Endpoints with Anti-malware and Patch Management Controls
TEP	Total Number of Third-party Remote Endpoints
RCS	Total Number of Redundant Links and Subsystems
TCS	Total Number of Communication Links and Subsystems
JAD	Number of Jamming Attempts Detected
TMP	Total Monitoring Period
JS	Jamming Severity
TSC	Total Signal Channels
QPL	Number of Quantum-Protected Links
TCL	Total Communication Links
CSIRP	Number of Critical Systems with Incident Response Plans
AB	Number of Assets with Automatic Backup
TA	Total Number of Assets

Table 21: Abbreviations Used in Metrics Formulas

mula is given by

$$\%CA = \left(\frac{\text{CA-C}}{\text{TCA}}\right) \times 100$$

and calculates a ratio by dividing the number of critical assets with a known cost of compromise (CA-C) by the total number of critical assets (TCA). This metric measures how many critical systems, such as core transaction and financial systems, are connected directly to satellite links without the security of an intermediate firewall. Firewalls are an essential defense in preventing unauthorized access and securing communications. In space systems, where satellites communicate with ground-based infrastructure, the absence of firewalls significantly increases the vulnerability of critical systems. This vulnerability was notably highlighted in the U.S. military's Global Positioning System (GPS) infrastructure in the late 1990s [393]. Although no breach occurred, the lack of proper segmentation between satellite links and ground-based systems made GPS infrastructure susceptible to potential attacks. This metric aligns with the NIST CSF under Identify/Asset Management (ID.AM).

The second metric, "Third-Party Remote Endpoint Resilience" (3pRER), measures the percentage of third-party remote endpoints administered by security personnel and protected by anti-malware and patch manage-

ment controls. Its formula is a percentage calculation:

$$3pRER = \left(\frac{\text{EPM}}{\text{TEP}}\right) \times 100$$

where the numerator (EPM) is the number of endpoints managed with security controls, and the denominator (TEP) is the total number of endpoints. This metric is especially relevant in space systems because they often rely on third-party contractors for critical tasks such as monitoring and maintenance. A real-world example of the need for this metric is the cyberattack on NASA's Jet Propulsion Laboratory in 2019 [295]. Attackers leveraged a third-party network vulnerability, using an unsecured Raspberry Pi device to gain unauthorized access to mission-critical systems. The breach exposed sensitive data, including information related to space missions. Our metric is aligned with Govern / Cybersecurity Supply Chain Risk Management (GV.SC) and reflects the broader importance of securing the supply chain in the space sector.

The metric "Interconnected System Redundancy Ratio" (RRR) measures the percentage of redundant communication links and subsystems within a space network. The formula is given by

$$RRR = \left(\frac{\text{RCS}}{\text{TCS}}\right) \times 100$$

and computes a ratio of redundant communication systems (RCS) to the total communication systems (TCS). Redundancy is a fundamental aspect of ensuring resilience in space systems, especially in case of failures or cyberattacks. By measuring the redundancy within the system, organizations can ensure that if one link or subsystem fails, another can take over, maintaining critical operations. This metric corresponds to PR.IR-03 in the NIST CSF 2.0, emphasizes implementing mechanisms to achieve resilience in both normal and adverse situations.

"Signal Jamming Exposure Index" (SJEI) is a metric that quantifies the risk and frequency of signal jamming attempts on space communication systems. It is computed according to the following formula:

$$SJEI = \left(\frac{\text{JAD}}{\text{TMP}}\right) \times \left(\frac{\text{JS}}{\text{TSC}}\right)$$

The formula is the ratio of detected attempts to the monitoring period by the ratio of jamming severity to total signal channels. Signal jamming is a significant threat in the space sector, where communication systems are especially vulnerable to intentional interference. In 2011 Iranian authorities were accused of jamming satellite signals from European satellite operator Eutelsat [218]. The jamming disrupted the transmission of international broadcasts, including news channels, for an extended period. Russian jamming of satellite signals during the conflict in Ukraine has shown just how critical it is to protect and measure interference. Systems like Starlink and GPS, have been targeted by Vehicular High Power Microwave Weapons like Krasukha-4 [427]. By monitoring jamming intensity, operators can respond quickly—like SpaceX did by updating Starlink systems [251]. By tracking the number of jamming attempts and their severity using SJEI, satellite operators can better prepare and respond to such disruptions. Additionally, this metric aligns with the Detect/Continuous Monitoring (DE.CM) function of the NIST CSF.

The "Quantum Cryptographic Readiness Level" (QCRL) metric evaluates how prepared space communication systems are to implement quantum-resistant cryptographic protocols. It is computed as follows:

$$QCRL = \left(\frac{\text{QPL}}{\text{TCL}}\right) \times 100$$

In the formula, QPL represents the number of quantum-protected links, and TCL is the total number of communication links. Then, The ratio is converted to a percentage. As advancements in quantum computing progress, encryption methods that currently protect satellite communications will become increasingly vulnerable. Although quantum-based attacks on space communications have not yet been reported, agencies like the European Space Agency (ESA) are already researching quantum cryptographic solutions to future-proof satellite communications [42]. This metric is crucial for measuring the readiness of space systems to adopt quantum-resistant encryption, ensuring long-term security in a post-quantum world. The metric falls under Protect / Data Security (PR.DS) of the NIST CSF.

In addition to protecting against potential attacks, space systems must be prepared to respond effectively when incidents occur. The "Incident Response Plan Coverage" (IRPC) metric measures the percentage of critical space systems and missions covered by documented incident response plans. It is computed as the ratio of systems with an incident response plan (CSIRP) to the total critical systems (TCS). Formally,

$$IRPC = \left(\frac{\text{CSIRP}}{\text{TCS}} \right) \times 100$$

The 2014 cyberattack on the National Oceanic and Atmospheric Administration (NOAA) [461], demonstrates the relevance of this metric. During the attack, intruders accessed satellite data used for weather forecasting. While the NOAA responded to the breach, the incident raised concerns about the adequacy of the organization's incident response plans for protecting critical satellite data. By adopting our metric, operators can ensure that all critical assets are prepared with detailed response protocols. This metric aligns with Respond/Incident Management (RS.MA-01) in the NIST CSF.

Finally, the "Automatic Backup Coverage" (ABC) metric measures the percentage of hardware assets configured for automatic backup. It is computed as follows:

$$ABC = \left(\frac{\text{AB}}{\text{TA}} \right) \times 100$$

The formula calculates the proportion of assets with automatic backups (AB) to the total assets (TA). Space systems handle highly sensitive and valuable data, and the risk of data loss due to system failures or cyberattacks is a constant concern. An example of its relevance is the 2014 cyberattack on the Japan Aerospace Exploration Agency [315], which compromised its systems for several months. Data recovery mechanisms played a crucial role in mitigating the damage. By measuring ABC, organizations can ensure that critical data is backed up regularly, minimizing data loss in the event of an attack. This metric aligns with the Recover (RC.RP-05) function in the NIST CSF.

We tried to link our metrics with real-world attacks and threats because we believe in the extreme value of threat intelligence in helping to design better metrics. Our proposed metrics help address specific threats to space systems and fill some of the gaps we identified in our research. However, some gaps remain, and we highlight the need for the future direction that industry, researchers, and policymakers should take. Regarding the gaps, Respond-and-Recover metrics still cover only about 12 percent of the set, leaving incident handling poorly quantified. Governance remains thin where stakeholder intent must be translated into enforceable obligations (GV.OC, GV.OV). However, the most pressing gap is along the outer edges of the mission lifecycle: Nothing yet measures launch-phase supply chain integrity, on-orbit physical resilience. Until these extremities are instrumented, the framework cannot claim full coverage of space-system risk.

A comprehensive strategy to address existing gaps would involve integrating metrics tailored for each segment of space operations: space, ground, and user segments. This could include evaluating how quickly authenticated updates are applied to flight software, assessing the completeness of the Software Bill of Materials (SBOM) [366] for space-grade components, monitoring the frequency with which telemetry, tracking, and command (TT&C) keys are rotated[572] , and verifying whether the integrity of telemetry data is maintained during its transfer across virtualized ground networks and cloud services. Furthermore, measures that tackle information sharing, cross-operator threat intelligence, would also be beneficial. Lastly, in terms of cost efficiency, improvements regarding the reduction of data collection costs related to metrics measurements should be introduced, including approaches to automate their measurement.

In future research, we aim to address the identified shortcomings further and, possibly with the help of more detailed and up-to-date threat intelligence, define further metrics.

6.6.6 The Domain Relevance of the Proposed Metrics

Some of the introduced metrics are conceptually adaptable across critical infrastructure sectors, but their formulation in this study is grounded in technical, operational, and threat-specific considerations that are particularly pronounced in the space domain. Each metric has been designed to face attack vectors, architecture-level vulnerabilities, and the asymmetrical threat dynamics that characterize space-based systems. Despite the set of new metrics we propose, being limited, their generalizability does not detract from their relevance to space; rather, it underscores the sector's need to adopt and adapt quantitative tools of analysis commonly missing from existing risk models. The metrics introduced are technology-agnostic so that they can be reused across critical-infrastructure sectors. Events of the past years show that space operators need these indicators urgently. Space systems must defend three interdependent segments: orbital, terrestrial, and radio-frequency, when operating in an environment where physical distance delays rapid intervention. Recent threat reports [490] show a steady escalation of incidents that demonstrate why quantifiable, governance-aligned metrics are indispensable for satellite missions. Considering the Percentage of Critical Systems Connected Without Intermediate Firewalls (CA), it could hypothetically be used in other domains, such as energy or finance, where high-value systems are exposed through poorly segmented networks. However, in the context of space systems, it can respond to very specific and recurring vulnerabilities, such as the exposure of satellite command-and-control channels, particularly TT&C uplinks, to direct or routable access via the public internet. A similar logic applies to the Third Party Remote Endpoint Resilience (3pRER) metric. This metric measures resilience in relation to the space sector's dependence on multi-actor supply chains and outsourced ground segment operators. In 2024, the Volt Typhoon group targeted satellite and telecommunications infrastructure in the U.S. and allied countries by exploiting remote management tools and third-party service providers [490]. Demonstrating how compromise of maintenance workstations, antenna terminal systems, or mission planning portals can

serve as privileged footholds. Supply chain compromise is for sure a systemic risk in all critical infrastructure sectors, but its implications in the space context are uniquely severe due to limited visibility, weak contractual oversight of subcontractors, and the real-time dependence of orbital assets on terrestrial uplinks.

At the architectural level resilience can be assessed through the Interconnected System Redundancy Ratio (RRR). This metric evaluates the structural capacity of satellite networks to reroute operations or shift bandwidth in the event of jamming, interception, or data corruption. The space sector's constrained redundancy is a recurrent theme in recent threat analyses, RF jamming conducted by Russian military units in Kaliningrad, and by Iranian forces in the Strait of Hormuz, disrupted satellite navigation and communication services across large areas [490]. These attacks demonstrate the urgent need to quantify systemic redundancy, in the availability of independent and survivable communication pathways within satellite constellations or hybrid ground segments.

In direct response to these developments, the Signal Jamming Exposure Index (SJEI) is introduced as a space metric. Jamming in space involves physical-layer disruption of electromagnetic signals, often from sovereign territory and targeting civilian and military assets alike. During the 2022–2023 period, more than 3,000 GNSS-related anomalies were recorded monthly over conflict zones and adjacent air corridors, many traceable to deliberate jamming operations [490]. In some cases, commercial airlines and maritime operators reported navigation failures, while satellite operators detected interference affecting uplink/downlink channels [231]. The SJEI is intended to capture the intensity and recurrence of these events, quantifying a class of threats that are highly specific to the physics and geopolitical exposure of orbital systems.

Other metrics in this set address threats that are latent yet increasingly urgent. The Quantum Cryptographic Readiness Level (QCRL) reflects the mismatch between the lifecycle of orbital assets and the cryptographic agility required in modern cybersecurity practice. Most spaceborne systems launched over the past two decades lack the hardware or software flexibility to update their encryption protocols, leaving them

vulnerable to post-quantum decryption in future threat environments. In this context, Chinese-aligned university research simulating post-quantum attacks against Starlink infrastructure and speculative targeting of LEO-based military communications in future scenarios have been recently osberved [490].

The Incident Response Plan Coverage (IRPC) metric addresses another strategic weakness. In many recent cases of space-related cyber incidents, including the Viasat KA-SAT attack in 2022 [81] and credential harvesting affecting ground segment operators, there was limited evidence of coordinated incident response procedures. IRPC intends to quantify whether response plans are defined and operationalized across different layers of the mission: from ground service operators to satellite owners and downstream users. The increasing integration of commercial assets into military command structures (e.g., the U.S. Department of Defense's use of commercial LEO constellations for tactical data relay) further increases the complexity of response planning and liability [490].

Automatic Backup Coverage (ABC) addresses the need for resilient recovery pathways. Backup coverage is often considered a baseline control in most sectors. However, in the space sector, satellite control software, operational telemetry, and user mission data are often subject to bandwidth constraints, intermittent synchronization, and proprietary ground systems that do not follow conventional backup cadences. Notably, the IntelBroker leak in early 2024 included references to configuration files and telemetry analysis platforms from multiple European space organizations [490]. In such contexts, automated and redundant backups are critical for post-incident recovery, and for maintaining continuity during partial disruptions or multi-stage intrusions.

These metrics reflect a strategic effort to quantify space system cybersecurity through indicators that are informed by real-world attacks, grounded in space-specific constraints, and applicable in operational settings. The general methodology may be extensible to other critical infrastructure domains, but its significance in the space context lies in the degree to which these threats have already materialized, and in the sector's limited capacity to reactively patch or reconfigure systems post-

deployment. In this light, the proposed framework does not generalize cybersecurity practice, it localizes it, embedding sector-wide threats into measurable, actionable indicators for risk management in the space domain.

6.7 Metrics Implementation

In the previous sections, we developed new metrics and assigned existing ones to NIST CSF 2.0 subcategories, trying to align existing and new metrics to the principles defined by NIST. However, companies may still face challenges in terms of implementing our methodology. To address this issue, we implement a Proof of Concept (PoC) tool [80] that can be used to apply some of the proposed metrics to real-world scenarios. In this section, we describe the tool, including its functionality, features, uses, and limitations.

The tool's primary purpose is to facilitate the quantitative assessment of space system security metrics. It provides a platform for users, such as CISOs, CIOs, or those responsible for risk assessment in a company, to input data related to their security parameters and to obtain as an output the values of various metrics estimating the state of the system's cybersecurity posture. The tool is designed to be extendible and to be adapted to specific company missions and risks, as well as future integration of additional metrics as new threats and cybersecurity frameworks evolve.

Our PoC is a web application organized into different sections, each dedicated to a specific security metric. We applied color schemes based on NIST CSF functions to differentiate the various categories. For the time being, our PoC calculates metrics related to the Govern function and the metrics for space systems we proposed in Section 6.6.5. A future version of the tool will include the metrics for the NIST CSF functions and others tailored to specific missions and objectives and will be aimed at space operators, cybersecurity analysts, and governmental users for the management and protection of space infrastructure. Each metric is implemented as a function that validates user inputs, applies the metric formula, and displays the results. However, despite its reduced func-

tionalities, our PoC tool can offer a solid baseline for assessing a space company's level of security, following the principles defined by the NIST CSF 2.0.

More precisely, concrete applications of the tool include:

1. *Cybersecurity Audit and Compliance:* companies can evaluate their compliance with industry standards such as the NIST CSF 2.0. The tool's alignment with NIST subcategories ensures that metrics directly correspond to compliance requirements, principles, and guidelines such as those defined by NIST. This can be further extended to other standards or policy requirements, such as those of NIS2 according to what we discussed in Section 6.4 and the upcoming Space Law.

2. *Operational Monitoring:* Space operation centers can integrate the tool into their routine cybersecurity assessments, allowing for regular monitoring of key metrics such as signal integrity and command authentication.

3. *Security Management and Resource Allocations:* By assessing metrics, organizations can better evaluate security gaps and establish better resource allocation when developing security measures.

While our current PoC offers a useful starting point for assessing space cybersecurity metrics, several limitations should be addressed in future versions. First, the current version requires manual data input, limiting its capacity for real-time monitoring and dynamic assessment, which are crucial for space operations that require continuous threat detection. Additionally, the tool currently supports a fixed set of metrics. As threats evolve, new metrics and updates will be necessary, so the tool should allow its users to add new custom metrics to maintain its relevance. The tool also relies on predefined formulas and cannot learn from past incidents or adapt to patterns, limiting its capacity for predictive analysis. A future version of the tool should be integrated with threat intelligence databases and use them with some AI algorithms to perform predictive analysis. Future research will address the mentioned limitations, including AI integration and real-time monitoring capabilities. Indeed, such

enhancements can increase its utility and provide a more sophisticated platform for defending space infrastructure against evolving threats.

6.8 Case Study: Security Metrics into Space System Design

In this section, we present a case study to validate our metrics, defined in Figure 5 modeling a fictional company in the space industry to demonstrate the relevance of metrics in supporting CSF 2.0 principles and improving the overall resilience of space systems. While developing our model, we took into consideration and based our architecture on the NIST Hybrid Satellite Network (HSN) profile [359]. According to the NIST definition, an HSN combines terrestrial and space elements owned and managed by different entities to create a comprehensive space system capable of delivering global services for various missions and connection points. Typically, an HSN architecture includes a mix of independently owned terminals, antennas, satellites, payloads, and other components that operate across different networks. HSNs can interface with government systems and critical infrastructure, providing services like satellite communications, positioning, navigation, and timing (PNT), remote sensing, weather monitoring, and imaging. The trust levels among HSN components may vary, necessitating frameworks to ensure confidentiality and integrity while maintaining the availability of shared services. HSNs allow organizations to utilize existing space capabilities and platforms through hosted payloads, ground infrastructure as a service, and virtualized satellite operation centers. Such architecture is widely used in the real world, and therefore, ensuring the security of these systems and the proper integration of its components is crucial for all the organizations involved.

In our scenario, as in the HSN, the company's architecture consists of direct and indirect systems and subsystems, including third-party components, closely resembling real-world architectures while keeping system complexity low. Our reference architecture strongly resembles space networks such as Viasat or EuroSkyPark [62], where satellite communi-

cation services are used to support or manage wind turbines. In developing our case study, we take particular care to represent aspects that closely resemble real-world scenarios while reducing their complexity for easier representation.

Our case study, named SecureSat Communications Inc., is a satellite communications company operating a fleet of satellites in Geostationary Earth Orbit (GEO) and Low Earth Orbit (LEO) to provide global communication services. The company specializes in satellite-based Internet services, telecommunications, and broadcasting. SecureSat shares the objectives and capabilities with the future European constellations IRIS^2. This choice allows us to showcase the complexity of the project and the suitability of our metrics and the NIST CSF 2.0 for future European constellations. The primary mission of SecureSat is to deliver reliable and secure communication solutions to government agencies, corporate entities, and individual consumers. While SecureSat manages the entire satellite lifecycle and production, the company relies on subcontractors for ground stations, payload control centers, and ground network operations. GroundSys, a different company, operates the ground station, including the Security operations center (SOC) and network operations center (NOC). GroundSys, in turn, relies on third-party supplier SpaceIT to manage and operate the ground network. The Ground Station includes another entity, GeoNet, that serves as the payload control center operator. Additionally, we consider a potential customer of SecureSat, WindSat, a wind energy company that relies on SecureSat's communication network to remotely control and monitor its wind turbines in the Mediterranean Sea. We believe that the entities and their relationship reflect the intricacies and dependencies that affect such complex satellite systems in the real world. To ensure robustness and security, SecureSat has developed a comprehensive cybersecurity strategy based on the NIST CSF 2.0, specifically tailored to the space sector, and decided to apply tailor-made metrics to measure some of the framework's subcategories.

As a typical space system, our architecture consists of three main segments: *Ground Segment*, *Space Segment*, and *User Segment*, with additional

roles played by third-party providers. More precisely:

1. *Ground Segment:* This includes Ground Stations, Network Operations Center (NOC), Security Operations Center (SOC), and Payload Control Center (PCC). Ground Stations handle uplink and downlink communications with the satellites, the NOC oversees network operations and ensures service quality, and the SCC handles satellite command and control.

2. *Space Segment:* This segment comprises GEO and LEO Satellites with various subsystems, including the Telemetry, Tracking, and Command (TT&C) Subsystem, Communication Payloads, and Propulsion Systems. These satellites maintain communication links and manage their orbital positions. Payload Maintenance Providers ensure the operational integrity of the satellite payloads.

3. *User Segment:* Consists of Customer Premises Equipment (CPE) and User Terminals. The CPE includes satellite modems and antennas installed at customer locations, enabling access to satellite services, and User Terminals can be mobile or fixed, depending on the application. In our case, the main user is a wind energy company. Therefore, the modems are directly connected to a SCADA system controlling wind turbines.

In our scenario, various third-party providers play crucial roles in SecureSat's operations, as described in Figure 5:

- *Payload Maintenance Providers (GeoNet):* Ensure the operational integrity and maintenance of the satellite payloads throughout their lifecycle.

- *Ground Network Operator (SpaceIT):* Manages the terrestrial network infrastructure that connects ground stations to the broader internet.

- *Ground Stations operator (GroundSys):* Manage secure communication channels between ground stations and the satellites.

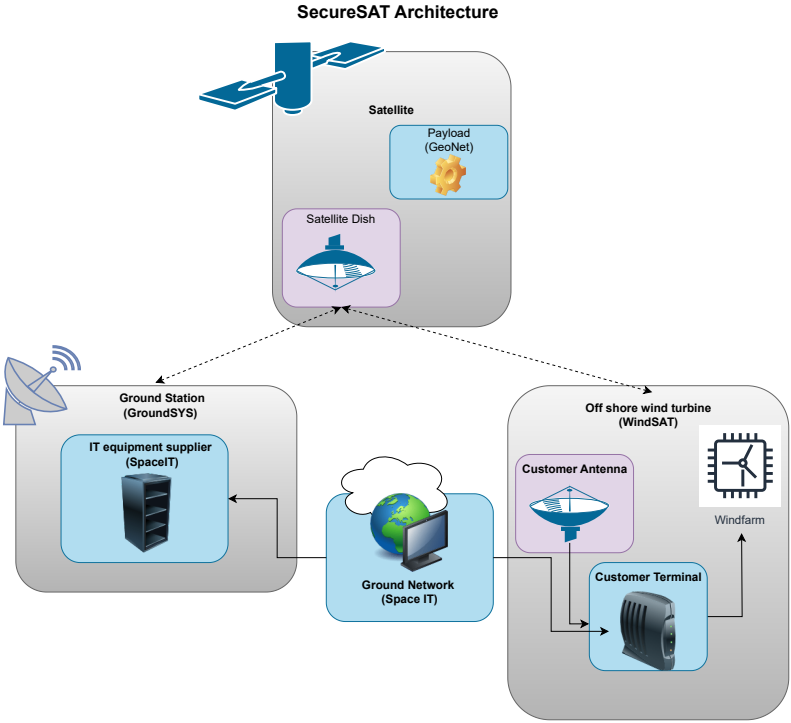

Figure 5: SecureSAT Architecture

CSF Subcategory	CSF Applicability to the Space Sector	CSF Profile Applicability to SecureSat	Related Metric
ID.AM: Physical Devices and systems within the organization are inventoried	Focus on the interfaces of the physical devices that interact with external organizations. Successful interfaces will depend on a working knowledge of physical systems owned vs leased by external organizations as well as any constraints, performance requirements, and tolerances. Collaboration with external organizations is necessary to execute a physical inventory that spans organization locations and ownership.	SecureSat, GroundSYS, Space IT and WindSAT own their assetsand perform their inventories regularly	Percentage of Critical Systems connected to satellite links without intermediate firewall
DE.CM: The network is monitored to detect potential cybersecurity events	Heighten system monitoring activities when there is an indication of increased risk to the organization or the service providers.	SecureSAT and GroundSYS monitors the availability and integrity of the RF signals to ensure their business continuty	Signal Jamming Expo-sure Index (SJEI)
GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	Ensures accountability and adherence to security policies within hybrid satellite systems (HSNs).	SecureSat defines cybersecurity roles and assigns ownership of risk management practices across its ecosystem, including GroundSys and SpaceIT.	% of security policies, standards, procedures, and metrics with committed owners
ID.RA-2: Cyber threat intelligence is received from information-sharing forums and sources	Strengthens threat awareness and response by integrating external intelligence sources.	SecureSat, constrained by resources, relies on partners like GroundSys for threat intelligence.	% of participating entities reporting timely threat intelligence
PR.AA-03: Users, services, and hardware are authenticated	Verifies external connections to prevent unauthorized access, essential in diverse network environments.	SecureSat enforces multi-factor authentication (MFA); GeoNet adds token-based access controls.	-% of users with MFA; - Number of access rights authorized, revoked, reset, or changed; - Number and type of suspected and actual access violations
ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	Helps quantify and document vulnerabilities affecting both primary systems and partners.	SecureSat and its partners, including SpaceIT, assess and record threats to their interconnected systems.	-Mean-Time-to-Compromise (MTTC); - Probability of vulnerability exploited

Table 22: CSF Subcategories and Their Applicability to SecureSat

To ensure the cybersecurity of its space architecture, SecureSat has implemented several security metrics based on the NIST CSF 2.0. SecureSat Communications Inc.'s represents an example of a comprehensive space architecture, its integration of security metrics based on the NIST CSF 2.0 subcategories demonstrates what could be the initial step to build a robust approach to cybersecurity. In Table 22, we explore how the NIST CSF subcategories apply to the space sector and specifically to the operations of SecureSat Communications Inc., GroundSys, and SpaceIT. By doing so, we can understand how tailored security metrics reinforce adherence to CSF principles and improve the resilience of their HSN. The first subcategory, ID.AM: Physical Devices and Systems Inventoried, mandates maintaining a comprehensive inventory of all physical assets, including those owned, leased, or managed by third parties. In the space domain, given the wide value chain and consequent attack surface, knowing exactly what hardware exists and who controls it, is foundational to risk management across geographically dispersed and multi-owner environments. For SecureSat, this means tracking each ground-station antenna and router (including firmware versions and lease status with GroundSys and SpaceIT), and every customer-side modem and SCADA interface at WindSat sites. One of the metrics that can complement this subcategory measures the percentage of critical systems connected to satellite links without intermediate firewall. A high value of this metric reveals that essential endpoints, whether they be TTC consoles managed by SecureSat, routing equipment operated by SpaceIT, payload control servers under GeoNet, or WindSat's SCADA interfaces, are directly exposed on the satellite link without network segmentation. The second subcategory, DE.CM, highlights the importance of continuously monitoring the hybrid network to detect and respond to potential cybersecurity events, extending that vigilance down to the RF layer. For SecureSat, this means that its SOC, working hand in glove with GroundSys, must ingest and correlate RF-link performance metrics (signal-to-noise ratios, bit-error rates), IDS/IPS alerts from SpaceIT routers, and deep-packet inspections of WindSat's SCADA flows, all in near real time. To quantify their effectiveness, SecureSat and GroundSys employ the Sig-

nal Jamming Exposure Index (SJEI), which aggregates the duration and severity of each detected interference event against total operational time. GV.RR-02, emphasizes the importance of defining roles, responsibilities, and authorities in cybersecurity risk management. In the space sector, this ensures accountability and clarity within highly interconnected systems. For SecureSat, this involves assigning specific cybersecurity responsibilities to organizational roles, such as risk management practices for its satellite fleet. The metric tracks the percentage of security policies with committed owners and quantifies this accountability, ensuring all entities adhere to clearly defined roles. Subcategory ID.RA-2, which involves the integration of cyber threat intelligence, highlights the necessity of proactive threat awareness in the space sector. Organizations like SecureSat must evaluate joining information-sharing initiatives such as the Space Information Sharing and Analysis Center (ISAC) to enhance their cyber posture. While SecureSat's smaller scale limits its direct engagement in intelligence gathering, its partner, GroundSys, actively incorporates cyber threat intelligence from manual research and cloud-based feeds. Metrics measuring the percentage of participating entities receiving timely threat intelligence supports the awareness and integration of threat intelligence into the companies' workflow. Subcategory PR.AA-03 addresses the authentication of users, services, and hardware, a critical requirement in the diverse and distributed environment of an HSN. In our model SecureSat enforces multi-factor authentication (MFA) for user access, while GeoNet, operated by GroundSys, employs token-based access controls for its payload control center. Metrics such as the percentage of users with MFA and the number of access rights changes provide measurable insights into the application of these authentication protocols. The final subcategory addressed by our analysis is ID.RA-04, and focuses on identifying and documenting the impacts and likelihoods of threats exploiting vulnerabilities. For the space sector, this requires assessing not just the primary system's risks but also those involving third-party providers. SecureSat and its partners actively evaluate potential threats and vulnerabilities, recording their findings to prioritize mitigation strategies. Metrics such as the mean-time-to-compromise (MTTC)

and the probability of vulnerability exploited help quantify these risks, guiding both immediate and long-term security efforts.

Continuously monitoring and improving its security posture through the metrics, can guarantee SecureSat the security assessment of its critical assets and the secure delivery of communication services to its clients. Our case study highlights the importance of tailored cybersecurity metrics in the space sector and provides a framework for developing security metrics based on the NIST subcategories that other organizations can use to enhance their cybersecurity strategies. In our model, we emphasize the presence of third-party providers and their roles in the interconnected nature of modern space operations, highlighting the necessity of a holistic approach to cybersecurity. In addition, using our security metrics tool can significantly ease the assessment process, and, if metrics reflect specific standards or cybersecurity requirements, such tool can facilitate the assessment of compliance with such instruments.

The applicability of selected CSF subcategories to the space sector is directly inspired by the NIST implementation of the Hybrid Satellite Network Profile (NIST TN 2272) [359], which operationalizes the NIST CSF in a realistic satellite-ground control scenario. For example, ID.RA-2 (cyber threat intelligence sharing) is mapped in the case study to functions delegated to satellite operators; ID.RA-4 is applied in risk assessment of downlink jamming; and PR.AC-3 is relevant for managing secure remote access to payload control centers. These mappings confirm that such subcategories are not merely generic but have demonstrated use cases in space system cybersecurity planning.

6.8.1 Cost-Effectiveness of the Metrics in the SecureSat Case Study

In line with the criteria defined in Section 6.5 of this paper, a metric is considered cost-effective when it generates more value than the cost required to gather, analyze, present, and use it. This principle is particularly relevant in the context of complex space systems, where budgetary constraints, long system life-cycles, and a high degree of technological in-

terdependence require efficient and sustainable measurement practices. In this section, we show how the metrics selected for SecureSat Communications Inc. meet this criterion by capitalizing on data sources, operational processes, and monitoring infrastructures that are already embedded in the company's technical and organizational architecture, our case study is the best case scenario, and we understand that the situation of SecureSAT may be ideal and different from that of many space companies, but the purpose of this case study is to reflect the best scenario in which metrics as those selected are implemented and collected.

Considering the metric assessing the percentage of critical systems connected to satellite links without intermediate firewall protection, this metric builds on system inventories and network configurations that must already be maintained for operational continuity and regulatory compliance. Since asset management and network topology information are routinely available to the ground segment operator (GroundSYS), the value of the metric derives from its ability to identify exposure points with minimal additional effort. The cost of producing the metric in this case is low because it repurposes existing data, while the insight it offers, highlighting potential lateral movement paths or misconfigured interfaces, significantly helps threat mitigation in satellite-ground communication infrastructures.

A similar cost-value dynamic applies to the Signal Jamming Exposure Index (SJEI). Signal monitoring is a core function of the ground segment supporting radio-frequency links, particularly in high-reliability services such as satellite internet or remote sensing. The SJEI leverages already captured data, such as power anomalies or out-of-band emissions, to derive a synthetic indicator of RF interference. Because the monitoring infrastructure exists independently of the metric, and because the computation relies on signal characteristics already logged for operational reasons, the marginal cost of computing and maintaining the index is minimal in the case of SecureSAT.

The metric measuring the percentage of security policies, standards, procedures, and metrics with committed owners also satisfies the cost-effectiveness criterion. SecureSat and its partners rely on policy and stan-

dards repositories to coordinate governance, and assigning responsible owners to these artefacts is a necessary part of maintaining accountability. The metric turns a compliance obligation into a management tool, quantifying the proportion of artefacts with clearly defined responsibility. The necessary data (the documentation itself and its metadata) already exists; therefore, the cost of gathering and presenting the metric is limited, while the value it provides in reinforcing clarity and accountability across organizations is significant.

In the case of the percentage of entities reporting timely cyber threat intelligence, cost-effectiveness arises from the use of existing communication channels. Information exchange between SecureSat and its partners, particularly GroundSys and SpaceIT, already includes incident reports, vulnerability notifications, and threat intelligence updates. The metric adds structure and visibility to processes that already occur, without requiring new platforms or manual reporting.

Metrics related to authentication and access control, such as percentage of critical systems connected to satellite links without intermediate firewal, or % of users with MFA; are also demonstrably cost-effective in our case study. Access control logs, authentication statistics, and identity management data are routinely collected as part of security operations in SecureSAT and GroundSys. The metrics merely require aggregating and analyzing this data in a structured way to monitor adherence to access management policies. Their value lies in enabling SecureSat and its partners to detect lapses in identity governance (unused privileged accounts or failure to revoke credentials), without incurring new monitoring costs. For identity and access-control reporting, commercial studies flagged a 159% ROI and net customer savings of over $3 million in credential protection and support costs [236]. These benefits primarily stem from enforcing MFA, detecting outdated privilege assignments, and lowering help-desk calls, exactly the capabilities SecureSat gains from its IAM metrics.

Finally, metrics assessing vulnerability exploitation potential, such as mean time to compromise (MTTC) and probability of exploit, are also rooted in data already gathered by security teams at SecureSAT. Vul-

nerability scanning, threat intelligence, and risk assessment are essential components of modern SOC operations, particularly in regulated environments. The marginal cost of transforming existing vulnerability logs and intelligence feeds into risk indicators is small, especially when compared to the operational impact of addressing the wrong vulnerabilities or misjudging exposure.

Across all examples, the metrics selected for SecureSat satisfy the cost-effectiveness requirement because they do not introduce new data collection burdens, require minimal transformation of existing operational data, and provide concrete decision-support value. Although it is true that the assessment method applied in this article relies on a qualitative balance between cost and benefit, the same metrics would also rank favorably in structured evaluation frameworks, such as the PRAGMATIC method [67], which explicitly score metrics based on the implementation effort, the automation potential and the relevance of the decision. This alignment reinforces that the SecureSat set of metrics delivers sustained information value at a justifiable cost.

6.9 Conclusions

This chapter evaluated the current state of security metrics in the literature in comparison to the functions, categories, and subcategories outlined in NIST CSF 2.0. In doing so, we assessed how many NIST subcategories were covered by security metrics addressing aspects outlined in the NIST framework. After establishing a detailed methodology to identify and allocate metrics to NIST subcategories, our analysis revealed significant gaps in specific functions such as Respond and Recover, as well as certain gaps in particular subcategories related to the Govern function. Furthermore, subsequently to the identification of these gaps, we proposed specific metrics that could be developed and utilized by companies in the space sector.

To support existing and upcoming European policies in the field of critical infrastructure cybersecurity, particularly in the space sector, our research identified a solid legal basis in EU policies such as NIS2 and

CER for the necessity of developing and applying security metrics to assess risk better and measure compliance with such policies. Additionally, by presenting a case study based on real-world space architecture, we demonstrated the need for such metrics and their implementation. While the case study demonstrates the applicability of the proposed metrics in a realistic context, we acknowledge the limitation of not having validated the framework using real-world company data. Future work will aim to address this gap by collaborating with industry partners to test the metrics in operational environments.

Considering the practical obstacles and difficulties that companies may have in implementing and monitoring these metrics, we have developed and proposed a PoC tool that allows for the calculation and easy visualization of the security status of various metrics. Despite the invaluable nature of the research, we highlighted specific limitations in terms of matching metrics to NIST subcategories, as such matching is not always straightforward and feasible. We acknowledge that the proposed metrics only partially cover the assessment needs of companies operating in the space sector, which will require tailored, specific metrics for their respective scenarios. Nonetheless, the research illustrated how metrics can be practically utilized and how frameworks such as the NIST CSF 2.0 can provide a solid foundation for defining key actions that companies should implement. Although we provided a comprehensive mapping and evaluation of cybersecurity metrics relevant to the space sector, we recognize a gap in the current landscape: the lack of OT-specific metrics.

Given that space systems are often cyber-physical and integrate both IT and OT components, future work should aim to incorporate more metrics tailored to operational technologies, particularly those that address system availability, control integrity, and industrial protocols. Bridging this gap remains a priority for future research and is key to providing a truly integrated cybersecurity assessment framework for space infrastructure. Additionally, future research will focus on addressing the identified gaps in more detail and testing the implementation of the selected and proposed metrics in companies willing to experiment with them to assess further needs and potentially expand the catalog of metrics for the

space sector.

Chapter 7

Assessing the Attack Surface of Space Organizations: A Data-Driven Analysis

Following the development of security metrics for space systems in Chapter 6, this chapter moves from conceptual measurement to empirical assessment. While earlier chapters demonstrated why space systems qualify as critical infrastructure (Chapter 2), how vulnerabilities manifest in practice, particularly in the SATCOM domain (Chapter 3)—and where current governance frameworks fall short (Chapter 4), the next step is to understand how these issues materialize in real-world, internet-facing infrastructures. This chapter addresses that gap by introducing a data-driven methodology to evaluate the cyber exposure of organizations active in the space sector, operationalizing several insights developed earlier in the thesis.

The aim is to quantify exposure at scale, identify patterns of vulnerability across the sector, and assess how publicly observable attack surfaces relate to existing regulatory obligations such as NIS2 and the forthcoming EU Space Law. Building on the conceptual risk model and met-

rics introduced in Chapter 6 the Risk Exposure Framework (REF) provides a concrete and repeatable way to measure how space organizations appear to adversaries scanning the public internet.

7.1 Motivation and objective

Space technologies are vital to modern societies, from navigation and communication to weather forecasting and defense operations. Many of the services we rely on depend on satellites and space infrastructure. Recently, the European Union has started treating space not just as a technical field, but as a core part of its security and defense strategy. This approach is expressed in several strategic documents. The "Strategic Compass for Security and Defence" [197], adopted in 2022, was one of the first EU documents to frame space as a contested domain, and calls for stronger tools to detect and respond to threats targeting space infrastructures. The "EU Space Strategy for Security and Defence" [191] builds upon the previous document by stressing the need to protect space assets and systems from sabotage, espionage, and cyberattacks. More recently, the "White Paper for European Defence – Readiness 2030" [191] has clearly stated the centrality of space to European security, highlighting again the need for better protection of satellites and ground stations, especially from cyber threats.

These strategic moves come at a time when the threat landscape for space is becoming more serious. The 2022 cyberattack on Viasat during the early days of the war in Ukraine showed how space systems can be disrupted with major consequences [62, 81]. Attacks on undersea Internet cables, like those in the Baltic and Mediterranean, have added concerns about Europe's digital backbone [446]. In this context, secure space infrastructure becomes even more important as a backup and as a way to stay connected when other systems fail.

Despite the growing attention to cybersecurity in the space sector, there is still a significant gap in the ability to empirically measure the cyber exposure of space organizations. Current frameworks tend to be qualitative, relying on expert judgment, or focused on threat modeling

without incorporating real-world data from Internet-facing systems. At present, there is no standardized methodology for assessing and quantifying this exposure across the space industry. Consequently, policymakers and operators lack actionable metrics to evaluate risk levels, prioritize mitigation efforts, and align with the evolving cybersecurity requirements within the European context.

Given the strategic importance of space technologies in our society, this paper aims to address the above gaps. Specifically, we aim to answer the following research questions, each of which is motivated by a specific driver:

RQ1 How can we effectively measure cyber risk in space-sector organizations in a way that supports both technical and policy decision-making?

The need to address this research question originates from the existing gap between high-level cybersecurity obligations, such as those imposed by EU policies, and specific, automatable technical measures that can be directly verified for effectiveness.

RQ2 Is it possible to measure cyber risk exposure in a clear and repeatable way?

This question stems from the need for a clear and repeatable method to quantify cyber-risk exposure, which supports cross-organizational comparison as internet-facing assets continue to grow and oversight becomes mandatory.

RQ3 How much exposed are space-sector organizations to cyber risks, especially those that come from Internet-connected systems?

This question comes from the evidence indicating that successful intrusions in the space domain often originate from Internet-connected systems within ground and user segments, highlighting the need for an assessment of the resulting exposure at a sector-wide level.

RQ4 Can we connect this kind of measurement to existing European cybersecurity policies and frameworks?

This question is driven by the development of European space cybersecurity policies, particularly the NIS-2 directive and the proposed EU Space Act, which increasingly require continuous risk assessment at both the organizational and sector levels.

To answer these research questions, we introduce the *Risk Exposure Framework (REF)*, a risk assessment methodology that aims to measure two aspects: (i) how much is an organization visible to potential attackers (*exposure*), and (ii) how likely it is that known vulnerabilities in the organization's attack surface might be exploited (*likelihood*). REF is designed to be flexible and can be applied in different contexts, but in this paper, we focus on space organizations. More precisely, this paper provides the following contributions. To reply to **RQ1** and evaluate the level of exposure of space-sector organizations, we collect data on the Internet-exposed assets of both public and private space entities, identifying connected devices and known vulnerabilities. To determine how to measure cyber risk effectively, we utilize REF to generate a risk score based on observable data. Then, to answer **RQ2** and to test whether our approach is clear and repeatable, we apply REF to a representative group of space organizations and evaluate its consistency across different entities. Finally, to reply to **RQ3** and **RQ4**, we examine whether the framework can connect to existing European policies: we interpret our findings in light of strategic documents such as the EU Space Strategy for Security and Defence and current NIS2 obligations, showing how REF can complement policy-driven approaches to cyber risk governance. Our goal is to offer a simple but useful way to think about cyber risk in space, using a method that is practical, repeatable, and aligned with where European policy is heading. To support reproducibility and further research, a Python implementation of the REF methodology is available in a public GitHub repository [80].

Note that REF specifically focuses on the ground segment and on supporting digital infrastructure and other Internet-facing assets discoverable through network reconnaissance tools. This ground-segment focus is particularly relevant since several recent cyberattacks against space systems originate through these externally accessible entry points [537].

REF does not directly assess the space segment itself (onboard spacecraft systems, satellite subsystems, or orbital infrastructure), which typically operate in more isolated, proprietary, or air-gapped environments that are not visible through Internet scanning methodologies.

The rest of the paper is organized as follows: Section 7.2 presents some background information about Internet Connected Device Analysis, space-enabled critical infrastructures, and the relevant literature for our work. Section 7.3 explains how REF works and the metrics it uses. In Section 7.5, we apply the REF framework to a group of space-related organizations and illustrate the results of our analysis. Section 7.6 discusses how REF can be used to fulfill some requirements prescribed by current policies. Finally, Section 7.7 wraps up the findings and outlines possible future research lines.

7.2 Background

7.2.1 Internet-connected device analysis

Internet-connected devices (ICDs) include a great category of devices such as industrial control systems, satellite modems, or energy management systems [349] that are exposed to the public Internet, either by design or misconfiguration. The analysis of these devices is a key activity to understand the evolving cybersecurity posture of modern digital infrastructures.

ICD exposure creates an expanded attack surface that can be monitored and evaluated using a specialized class of search engines. Among the most widely used engines, there are *Shodan* [357], *Censys* [174], *ZoomEye* [341], *Fofa* [347], *BinaryEdge* [158], and *Netlas* [386]. Each engine has its own scanning strategies, indexing models, and coverage scope, which affect the consistency and granularity of its results. Below, we briefly review the main features of these platforms to clarify the motivation for our choice:

- Shodan is one of the most used IoT search engines. It systematically scans IP address space and indexes data based on service banners,

open ports, software versions, geographic information, and organizational ownership. It integrates vulnerability databases like the National Vulnerability Database (NVD) [59], and associates identified services with Common Vulnerabilities and Exposures. It also supports advanced filters (e.g., organization, open ports, and presence of vulnerabilities), allowing advanced targeting.

- Censys focuses on the protocol level and provides highly expressive query capabilities. It collects detailed X.509 certificates, TLS configurations, and other protocol metadata. It offers less direct vulnerability tagging compared to Shodan, but it can fingerprint cryptographic settings and web infrastructure.

- ZoomEye and Fofa are widely used in Asia [341] and provide extensive metadata tagging and visualization features. These engines often surface device types and service families using machine learning classifiers.

- BinaryEdge offers detailed metadata exports, including packet capture-level summaries, and often identifies honeypots, behavioral patterns, and unusual ports. It can be very useful for correlating IoT device behavior with cloud infrastructure exposure.

- Netlas is a more recent platform that combines banner search, certificate transparency logs, and passive DNS information. The vulnerability integration and query complexity of the tool are still evolving.

Each of these engines contributes to the global reconnaissance landscape, but they are rarely interchangeable. Their coverage is often non-overlapping, meaning that a device visible in Shodan may be completely invisible to Censys or BinaryEdge. For the structured cybersecurity assessment of REF, which involves quantitative risk scoring, we consider Shodan as the most operationally relevant platform: its direct CVE tagging, historical scan database, and support for Boolean logic queries allow us to track the evolution of exposure across organizations, sectors, or geographic re-

gions. In particular, it can associate each retrieved IP with known vulnerabilities and CVEs, a feature that is fundamental to our REF framework. Furthermore, Shodan's API is reliable, well-documented, and supports advanced filters that help target devices with specific characteristics during the risk quantification at the organizational level. Other platforms, like Censys or BinaryEdge, offer complementary perspectives, but their output is less consistent in tagging vulnerabilities or associating results with organizational identifiers.

To complement Shodan's exposure data with exploit intelligence, we integrate REF with the Vulners API [509]. Vulners is a vulnerability intelligence platform that aggregates data from multiple sources, including the National Vulnerability Database [59], Exploit-DB [528], Metasploit, and vendor advisories, checking for CVEs against public exploit sources. It also parses information from vendor advisories and security bulletins, including references to known exploitability. Vulners provides access to structured information about vulnerabilities, including their CVSS scores, CWE classifications, publication dates, and, most importantly for our research, exploit availability. Within REF, Vulners is used to query each CVE identified by Shodan to determine whether known exploits exist in the wild. Automating this enrichment process, REF can scale across hundreds of devices and IP addresses, mapping the real-world exploitability. The result is a more actionable measure of risk, grounded in adversarial capability and opportunity.

The ultimate goal of ICD analysis in our research is not merely to catalog devices but to assess their security posture. This includes evaluating the likelihood of exploitation based on exposed services, the impact of potential breaches based on system criticality, and the presence of known software vulnerabilities. As such, ICD analysis is used to perform cyber risk assessment workflows, particularly in sectors like space infrastructure. While the detailed methodology behind REF and our framework is described in Section 7.3, the next section describes instead some of the research that has already been carried out in this domain.

7.2.2 Space-enabled services as interdependent critical functions

Space infrastructure is embedded within critical sectors as a set of enabling functions whose failure degrades terrestrial systems in several ways. Satellite communications provide wide connectivity for operational technology and enterprise backhaul (teleports, gateways, cloud-hosted ground functions), as well as broadcast and broadband services to public services, and mission Telemetry, Tracking, and Command (TT&C). As operators externalise ground functions (commercial teleports and cloud-based ground segment as a service), misconfigurations or common vendor vulnerabilities become increasingly present as points of weakness across otherwise independent organisations. Positioning, Navigation and Timing (PNT/GNSS) provides absolute time and position to power grids, telecommunications, and finance, and anchors aviation and maritime navigation; jamming and spoofing thus propagate beyond navigation to timing-dependent processes when holdover and multi-source strategies are weak [417, 176, 516]. Earth Observation (EO) and traffic services (sat-AIS/ADS-B) feed situational awareness and logistics, moving through partner APIs and commercial clouds into emergency response, defence, and supply chains; their integrity and availability constraints translate directly into the quality of downstream public services. These structural ties explain why cyber incidents in the space domain typically materialise first at organisational boundaries (reachable management portals, VPNs, provider APIs) and then radiate into energy, transport, telecoms, finance, and public safety rather than remaining confined to the space sector [209].

7.2.3 Risk propagation across organisations and sectors: evidence and how to address it

Cyber incidents in the space domain demonstrate that attacks often affect multiple organizations. The interconnected nature of space requires understanding and measuring each organization's exposure to cyber threats. Quantifying external exposure, specifically the number of systems that

are reachable and vulnerable, can help anticipate and mitigate these propagation effects. The following examples illustrate how failures in the space layer can lead to systemic risk and emphasize the importance of measuring exposure to prevent such incidents.

The KA-SAT incident of 24 February 2022 [81] demonstrated how a compromise of the management plane enabled the deployment of a wiper against satellite modems, rendering terminals inoperable. The attack cascaded from the satellite operator to telecommunications providers and ultimately to the energy sector, where Enercon temporarily lost remote monitoring and control of approximately 5,800 wind turbines relying on SATCOM backhaul for operations [455, 178, 537, 147]. The propagation path in this case ran from a vendor's ground management environment to customer equipment, and onward into geographically dispersed industrial assets.

In 2025, a similar attack targeted the maritime sector, exploiting a supply-chain compromise that disrupted fleets using satellite connectivity. Reports and technical analysis attribute the campaign to the group Lab Dookhtegan [299]. The threat actor attacked an Iranian shipping company by exploiting vulnerabilities in their provider of satellite communications and related services (Fanava Group) [140]. The attackers compromised Fanava's central infrastructure and disabled iDirect Falcon, the network management and control platform that coordinates Very Small Aperture Terminal (VSAT) communications between ships and shore stations. By disrupting Falcon's control processes, used for link allocation, modem authentication, and configuration updates, the attackers were able to wipe storage partitions and sever multiple ship-to-shore links simultaneously. Public reporting indicates that communications were interrupted on more than 60 vessels (39 tankers and 25 cargo ships) in one wave, with two subsequent waves affecting up to 116 vessels overall, extending the impact from maritime communications into associated corporate IT and operational monitoring systems [154]. This incident illustrates how a provider-level supply-chain attack can compromise a satellite service intermediary, rendering it a single point of systemic failure for multiple operators and fleets.

Space-derived positioning and timing services have also been targeted. Aviation regulators warned of persistent GNSS jamming/spoofing near conflict zones, and maritime reporting from the Strait of Hormuz linked dense interference episodes to abnormal tracks and a high-profile collision and fire between tankers near Khor Fakkan on 17 June 2025 [176]. Regulators and analysts have emphasized that GNSS interference in constrained waterways can disrupt traffic separation and port scheduling and, when timing distribution depends on satellite signals, can cascade into logistics and other timing-sensitive operations [516, 503, 431, 417].

These cyber-incidents demonstrate how Space disruptions can propagate because many terrestrial services rely on shared dependencies for connectivity, data, and timing. The practical way to secure these links is to organize operations so that no single satellite link, one provider's control plane, one timing source, or one ground site can take a whole service with it.

For communications, this means building real diversity and automatic failover across independent paths: where terrestrial backhaul exists, keep it as a live alternative; where it does not, combine more than one satellite constellation and provider, and place ground sites in different locations so a fault or compromise at one teleport or cloud region does not become a sector-wide outage.

Management channels should remain accessible even during periods of primary service degradation. This ensures the ability to reconfigure or quarantine fleets of terminals and remote sites, thereby reducing the impact of modem-fleet "wipe" effects and outages on the provider's infrastructure. These principles are consistent with ground-segment security guidance such as NIST IR 8401 [344], which identifies external management planes and shared service providers as high-impact risks requiring appropriate instrumentation and isolation [151, 519].

Since many cascading failures originate between the space and user segments, it is essential to strengthen both the ground and supplier layers while ensuring link diversity. Best practices include isolating command and mission operations from enterprise IT, maintaining strict con-

trol over remote administration, employing modern authentication mechanisms, and staging signed updates with safe rollback capabilities. These requirements should be included in contracts with ground-segment and cloud-based service providers, together with obligations for transparency regarding software provenance. This way, if there is a compromise at an intermediary level, it cannot silently affect dozens of customers, as we have seen in cases of supply-chain breaches.

Positioning, navigation, and timing need specific protection measures because problems with satellite signals affect more than a single vessel or aircraft; they impact air and sea traffic management, port operations, and any activity that depends on precise timing. The goal is to reduce the effect of disruption: use receivers that combine multiple constellations and frequencies; verify the integrity of the received signals (for example, through Galileo's Open Service Navigation Message Authentication [214]); detect jamming or spoofing and respond through pre-defined operational actions [98]; and maintain accurate timing even during signal loss through holdover techniques [215]. Aviation and maritime guidance on PNT interference also adds the procedural layer: planned alternate routes, backup navigation modes, clear reporting channels, and conservative operational defaults when signal trust is uncertain [514].

Detection and coordination should also match how failures actually spread. Keep a living map of external dependencies, such as teleports, cloud regions, remote-access and identity providers, and terminal vendors. Exercise what happens when the largest nodes in that map fail. REF here can genuinely help identify shared, internet-visible weaknesses across different organisations (such as the same exposed administration portal or the same vulnerable version appearing in many places). Those are the points where one exploit can move fastest across an ecosystem; prioritising them creates the biggest reduction in propagation risk.

Finally, propagation is also a problem of information flow. Incident contacts and formats with satellite and ground providers, as well as aviation and maritime coordinators, shorten the window in which an outage in one place becomes a major disruption. Technical and organizational interconnections can cause failures to spread across different operators

and sectors. This highlights the importance of exposure measurement approaches. Before delving deeper into the REF framework and its features, the next section discusses some of the major contributions in the fields of space cybersecurity and in the analysis of internet-connected devices.

7.2.4 Related Work

Several recent publications have explored the role of cybersecurity in the space domain, and the increase in scientific production on this topic highlights the relevance and timeliness of the subject.

Pavur and Martinovic [405] map satellite security into four arenas (RF links, in-orbit platforms, ground segment, and mission/ops), catalog threat actors and attack classes, and propose a research agenda to bridge the gap between policy and technology. The author highlights that the constraints of space systems make IT security insufficient.

Khan et al. [322] provide a holistic review of space cyber-attack vectors spanning ground, space, communications, user, cloud, and supply chain, with a matched set of mitigations and research needs (space-tailored IDS, zero-trust, crypto/keying, blockchain access control, and regulatory/standards work). Their work presents a useful current landscape of cybersecurity risks and a roadmap.

Manulis et al. [355] frames how New Space changes the threat landscape: historically, most incidents hit ground and RF links, but the widespread development of large constellations created new vulnerabilities in other segments. The article surveys past incidents, adversary motivations, and likely attack classes, and also walks through enabling technologies and where they open or close attack surfaces. It represents an orientation map tying architectural choices to concrete risks.

Yu et al. [570] carry out an analysis of nine commodity modems, building a taxonomy across Satellite Communication Interface (SCI), Ground Network Interface (GNI), and hardware, and find numerous issues in standard services (web/Telnet/FTP), unprotected control paths, and hardware/bootloaders, plus ICDs at scale. Their work demonstrates practi-

cal exploit chains, and catalogs new categories alongside known ones. It also proposes concrete mitigation (service hardening, signed updates with rollback, securing debug interfaces) and provides tooling for analysis. Strong, device-level evidence that user-segment weaknesses can enable wide-area impact.

These contributions provide a solid overview of vulnerabilities and their underlying reasons, highlighting how different segments of the space infrastructure serve entry points for attacks. However, their focus differs from our study; they discuss threats and suggest mitigation strategies, but they do not introduce a framework for measuring the risks faced by space organizations through their internet-connected devices. Additionally, while they address vulnerabilities and propose mitigations, they overlook the policy dimension of space cybersecurity; while our work includes aims to bridge cybersecurity requirements to operational frameworks to address them.

Another part of the literature connected to our work concerns the analysis of ICDs and their attack surface. Shodan has been widely studied for its role in identifying and indexing ICDs, including critical industrial control system (ICS) components. Alsmadi et al. [34] has explored Shodan's ability to reveal vulnerabilities in ICS environments, demonstrating its potential as both a reconnaissance tool for attackers and a valuable resource for cybersecurity professionals. Researchers examined how Shodan indexed programmable logic controllers and proposed service banner manipulation as a mitigation strategy to limit exposure to Shodan queries.

Genge and Enăchescu [246] went beyond basic device discovery supported by Shodan and proposed ShoVAT, a Shodan-based vulnerability assessment tool capable of automatically identifying vulnerabilities using service-specific banner analysis. Through the testing on 1501 services across 12 different institutions, ShoVAT identified 3922 known vulnerabilities, showing the potential of Shodan-powered tools for cybersecurity assessments.

Similarly, Williams et al. [557] leveraged Shodan to assess vulnerabilities in consumer IoT devices, collecting a large dataset of indexed devices

and analyzing their security posture using Nessus vulnerability scans. Their results revealed a significant number of consumer IoT devices vulnerable to exploits that could compromise user data and privacy, underscoring widespread security concerns associated with the growth of IoT.

Liu et al. [346] showed that an organization's breach likelihood can be predicted purely from externally observable network properties, achieving around 90% accuracy in forecasting data breaches without any internal data. In the industrial domain, Gourisetti et al [257]. propose a risk assessment framework for energy delivery control systems that leverages Shodan-derived device fingerprints and publicly known vulnerabilities; their method correlates externally gathered device information with threat intelligence to produce risk-based scores for exposed critical assets.

Harry et al. [272] developed quantitative attack surface indices by combining Internet-wide scan results with CVE data to measure the "size" and "severity" of an entity's exposure. Their framework analyzes thousands of internet-facing devices (using platforms like Shodan/Censys) and computes metrics such as service diversity and aggregated vulnerability severity, which were found to correlate with certain risk factors (e.g. population served) while revealing gaps (e.g. weak correlation between sheer CVE counts and actual exploit likelihood).

These studies show that data from Internet-exposed devices can support cyber risk assessment, but they usually address the problem in a partial way, for example, by focusing on statistical correlations, single-device scores, or specific domains. The analysis is often limited to counting exposed services or vulnerabilities, and does not clarify how these findings map to standard risk concepts or how they can be combined at the organizational level. The Risk Exposure Framework makes links externally observable services and vulnerabilities to exposure, accounts for the availability of exploits in estimating likelihood, and aggregates these elements into an organization-level score. REF goes from data collection to scoring and interpretation, and provides inputs that can complement existing risk management processes. Our work further differs by grounding the use of REF in European cybersecurity policy require-

ments, by explicitly comparing it with existing risk assessment frameworks, and by showing how it can be used in a complementary way rather than as a replacement. In this paper, we extend this research line to space cybersecurity by focusing on space-sector organizations and by considering the impact of exposed assets in light of the critical role of satellite and aerospace infrastructure.

Although numerous risk-assessment methodologies exist across IT, OT, and space domains, including general-purpose models and sectoral threat-modelling approaches, such as those we discuss in Section 7.4, these frameworks do not quantify an organisation's externally observable attack surface. They rely primarily on expert judgement, architectural assumptions, or mission-centric threat scenarios, and therefore cannot capture real-world Internet exposure, persistent vulnerabilities, or the availability of exploits affecting ground-segment systems. The contribution of REF lies in addressing this specific measurement gap. With REF we introduce a reproducible, data-driven methodology to assess the externally visible cyber posture of space organisations.

7.3 Introducing the Risk Exposure Framework

Our *Risk Exposure Framework* (REF) is a structured, quantitative methodology designed to assess the extent of an organization's exposure to cyber threats and translates it into a quantitative risk assessment. Our goal is to understand how organizations such as aerospace manufacturers, satellite service providers, and space agencies are potentially vulnerable to cyber threats. By defining REF, we also aim to study how this type of assessment can be automated and beneficial to private companies and other actors involved in the space value chain.

7.3.1 Framework design and risk metrics

REF is designed to be automatic and data-source agnostic, meaning that it can be implemented using any dataset that provides relevant information about exposed digital assets, known vulnerabilities, and a broader

threat landscape.

Indeed, it supports different tools or cyber intelligence sources depending on availability and context. Although REF can be implemented using various sources, in Section 7.5, we use Shodan for identifying publicly exposed services and IPs, and Vulners for retrieving exploit availability and vulnerability severity.

The REF framework is built upon three metrics: *Exposure* (E), *Likelihood* (L), and the *Overall Risk Score* (R). Below, we introduce them.

Exposure (E) aims to measure the breadth and depth of an organization's visible attack surface, considering not only the number of publicly accessible IP addresses but also the concentration of vulnerable services exposed. Specifically, we retrieve the list of accessible IP addresses for the organization under analysis. For each IP address $a \in IP$, we compute the number of vulnerable services it exposes, denoted as $\mathcal{V}(a)$, which is proportional to the number of ports on that host affected by known CVEs. These represent potential entry points for adversaries attempting to compromise the system. The Exposure metric aggregates these values over all IP addresses and normalizes the result by the total number of exposed IPs, capturing both intensity and proportionality of exposure across the organization's infrastructure.

Formally, let IP be the set of accessible IP addresses for a given organization, and let $\mathcal{V}\colon IP \to \mathbb{N}$ be a function mapping each IP address to the number of vulnerable services it exposes (i.e., ports associated with known CVEs). Then, the Exposure score E is defined as:

$$E(IP) = \frac{1}{\#IP} \sum_{a \in IP} \mathcal{V}(a) \tag{7.1}$$

where $\#IP$ denotes the total number of publicly exposed IP addresses, and the numerator accumulates the total number of vulnerable services across those addresses. The resulting value reflects the average density of vulnerabilities per host, emphasizing infrastructures where exposure is not only broad but also concentrated in weak points. This formulation ensures comparability across organizations of different sizes while retaining sensitivity to localized high-risk configurations.

Whereas Exposure focuses on what is achievable, the Likelihood metric (L) estimates the danger that an attacker will succeed in exploiting these weaknesses. Likelihood is composed of multiple factors and is formalized by combining *adversary interest* (A), *exploit availability* (EA), and the *severity of the vulnerabilities* (VSI) themselves.

More precisely, adversary interest (A) is a multiplicative constant that represents the attacker's motivation to target a particular space organization. This might depend on political and economic incentives or the strategic value of the satellite or service at hand. We assigned this value to 1 (low interest) for the reasons we explain in Section 7.3.4.

Exploit Availability (EA) measures the ratio of public exploits known for the vulnerabilities identified. It is the ratio of total exploits available for an address and the total number of unique vulnerabilities. Formally, let $\mathcal{E}$ be a function that returns the number of exploits available for a vulnerability v on an host a, we define Exploit Availability as a function $EA\colon IP \to \mathbb{R}$ from a set of IP addresses to a numeric value as follows:

$$EA(IP) = \sum_{a \in IP} \frac{\mathcal{E}(v, a)}{\mathcal{V}(a)} \tag{7.2}$$

Vulnerability Severity Impact (VSI) represents the exploitation probability through the CVSS v3.0 scores, ensuring that even if exploit code is available, the real impact and complexity of each vulnerability are included. We model $VSI\colon IP \to \mathbb{R}$ as a function from a set of addresses to a numeric value, and we discuss in detail its calculation in Section 7.3.3.

The combination of A, EA, and VSI measures how much risky a successful cyberattack may be, given the attacker's motivation, the presence of readily exploitable weaknesses, and the seriousness of each vulnerability. Thus, we defined the Likelihood metric $L\colon IP \to \mathbb{R}$ as a function given by the following formula:

$$L(IP) = A(EA(IP) + VSI(IP)) \tag{7.3}$$

Once Exposure (E) and Likelihood (L) are computed, they are combined to produce the *raw Risk Score* (RR). As done above, $R\colon IP \to \mathbb{R}$ is

a function from a list of IP addresses to a real number. We propose two methods for computing it. The first averages Exposure and Likelihood, treating the two dimensions equally:

$$RR(IP) = \frac{E(IP) + L(IP)}{2}$$

The second uses a weighted coefficient C to tune the importance of Exposure versus Likelihood, allowing decision-makers to highlight either how large the attack surface is or how probable exploitation might be. In either case, the result is a single Raw Risk Score that informs analysts about the magnitude of the organization's overall cyber risk posture.

$$RR(IP) = CE(IP) + (1 - C)L(IP)$$

Large space organizations, such as those included in our analysis, can have thousands of exposed IPs and hundreds of potential vulnerabilities. Therefore, Raw Risk Scores can inflate to very large values. To address this, we applied a logarithmic scaling to the Raw Risk Score, obtaining the *Overall Risk Score* (R). Formally, we define $R\colon IP \to \mathbb{R}$ as follow:

$$R(IP) = \log_2(1 + RR(IP)) \tag{7.4}$$

The log-based approach preserves the relative ordering of risk values while containing the otherwise unbounded numbers in a more comprehensible range, representing risk scores that are easier to interpret, making it simpler to highlight which organizations or missions deserve priority attention and resources.

Applying the REF framework means computing R above. Our method is flexible enough to account for differences in entity size or complexity, while still allowing detailed analysis of vulnerabilities and exploit feasibility. With the REF, we obtain a clear vision of how many real, exposed attack vectors are present and what impact exploits could cause. REF can be used by security engineers, risk managers, and decision-makers as a practical means of identifying risk and prioritizing defenses in an environment where many components are mission-critical and where reliable operation can be essential to national and commercial interests. In

the following sections, we dive deeper into the various components of REF and discuss their applications and limitations.

7.3.2 Derivation of REF from the General Risk Model

REF derives directly from the risk model

$$Risk = Impact \times Likelihood$$

a formulation adopted in cybersecurity frameworks such as NIST SP 800-30 and ISO/IEC 27005. In the context of Internet-facing infrastructure, we operationalize Impact through the Exposure (E) metric, which quantifies the breadth and depth of an organization's attack surface, measuring the number of publicly accessible hosts and the concentration of vulnerable services they expose. A higher Exposure score indicates that the potential impact of a successful breach is amplified, as more entry points and vulnerable services translate into greater opportunities for unauthorized access, data exfiltration, or service disruption.

Secondly, we operationalize Likelihood through the Likelihood (L) metric, which estimates the probability that identified vulnerabilities will be successfully exploited. This probability is determined by three factors: adversary interest (A), which reflects the motivation to target specific organizations; exploit availability (EA), which measures the existence of weaponized exploits for discovered CVEs; and vulnerability severity impact (VSI), which incorporates CVSS scores to account for both the complexity of exploitation and the extent of potential damage.

When Computing $Risk = f(E, L)$, E represents impact, and L represents likelihood. REF maintains consistency with the general risk model and grounds each component in observable, quantifiable data drawn from Internet scanning platforms and vulnerability intelligence sources. Figure 6 illustrates this derivation, showing how the risk formula is mirrored into measurable cybersecurity indicators.

7.3.3 Assessing Vulnerabilities' Severity

The Vulnerability Severity Impact (VSI) is a metric we developed to assess the criticality of an organization's vulnerabilities by evaluating both

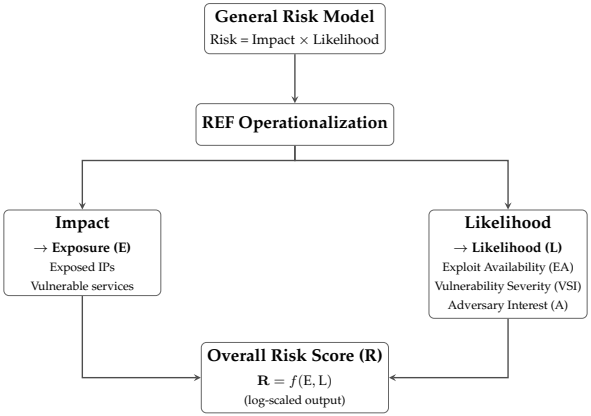

Figure 6: REF derivation from the general risk model (Risk = Impact × Likelihood).

their frequency and severity, as established by the CVSS v3.0 framework. VSI reflects the real-world impact and ease of exploitation for each vulnerability.

The CVSS v3.0 framework is used for the calculation of VSI and categorizes vulnerabilities based on their exploitability, impact, and environmental factors. This ensures that vulnerabilities that are both severe and frequently observed within an organization have a significant influence on the likelihood calculation. VSI evaluates how severe an organization's vulnerabilities are, using CVSS v3.0 principles. To calculate VSI, we first calculate the Average CVSS Score of observed CVEs as follows:

$$\text{avgCVSS}(IP) = \frac{1}{\#IP} \sum_{a \in IP} \sum_{v \in \mathcal{V}(a)} \frac{\text{CVSS}(v)}{\#\mathcal{V}(a)}$$

where $\text{CVSS}\colon V \to \mathbb{R}$ is a function mapping a vulnerability to its CVSS score. Then we define $VSI(IP)$ by cases as follows:

$$VSI(IP) = \begin{cases} 1 & \text{if avgCVSS}(IP) < 5.0 \\ 3 & \text{if } 5.0 \leq \text{avgCVSS}(IP) \leq 8.0 \\ 5 & \text{if avgCVSS}(IP) > 8.0 \end{cases}$$

In our approach, the CVSS v3.0 framework is used to evaluate vulnerabilities by considering both how easy they are to exploit and how damaging they could be. The VSI score captures this by averaging the CVSS scores of an organization's most common vulnerabilities. In this research, VSI values were derived using observed Common Vulnerabilities and Exposures extracted from public internet-facing services, combined with corresponding CVSS v3.0 scores from Shodan and Vulners. The Integration of VSI into our broader Risk Exposure Framework, gives a better visibility to organizations on their security posture. A higher VSI score means an organization has vulnerabilities that are both frequently observed and highly exploitable, making it an interesting target for cyberattacks.

In defining the thresholds of VSI, we adopted the CVSS severity bands, balancing sensitivity and robustness. CVSS outlines qualitative severity bands (*Low*, *Medium*, *High*, and *Critical*) with numeric boundaries (for example, High is defined as a score between 7.0 and 8.9) that serve as reference points. Specifically, we adopted these thresholds to ensure consistency with established practices. However, we also understand that vulnerabilities may tend to cluster in mid-range scores, so it is important that our thresholds do not overly compress the higher severity categories. For this reason, we selected thresholds that maintain clear distinctions among more severe vulnerabilities and also avoid the inflation of the highest category due to small differences in CVSS scores. We use standard CVSS brackets but interpret them with sensitivity to our domain. REF incorporates VSI solely as a component of the Likelihood metric, rather than as a standalone classification for assessing risk. Its role is to calibrate the contribution of exploitability within the overall metric. Finally, we are aware that CVSS has its limitations, such as inconsistencies among evaluators, a lack of contextual awareness, and a static approach to evolving threat conditions [280]. For this reason, any thresholding process must acknowledge the need for some degree of interpretive discretion.

7.3.4 Assessing Adversary Interest in the Space Sector

Adversary interest (A) is a critical component of the Likelihood (eq. 7.2) calculation, as it directly reflects the motivation attackers have in targeting a particular sector. Intuitively, a higher adversary interest suggests that cyber threats against the sector are more persistent.

Accurately estimating this metric is very challenging, since an attacker's interest towards a given target is influenced by a wide range of factors, including economic, political, and geopolitical considerations. Defining a precise, objective, and quantifiable metric that incorporates all those aspects is not feasible in practice. Therefore, we must adopt an under-approximation strategy, which by its nature comes with certain limitations. In this paper, we under-approximate this measure using data on historical incidents and trends, taking their frequency into account. Specifically, to objectively estimate the adversary's interest, we analyzed the number of cyberattacks against the space sector compared to other critical infrastructure sectors. We considered the following data for our historical investigations and comparison:

- The ENISA Threat Landscape Report 2024 [209].
- The European Repository of Cyber Incidents (EuRepoC) [199] in the period 2000-2025. This repository is maintained by an independent research consortium dedicated to better understanding the cyber threat environment in the European Union and beyond.
- Threat intelligence from Cyberinflight [145], which is one of the founding companies of the EU Space ISAC and a leader in CTI in Europe. We considered a threat intelligence report from 2022.

By analyzing this data, we assign a score to the adversary's interest in the space sector. Here, we let the adversary interest (A) score range from 1 (low) to 3 (high). The idea is that A should take the value 3 (high interest) for those sectors that are among the top targets for cyberattacks, with a significant share of total incidents. The value 2 (moderate interest) should be given to those sectors that experience moderate but consistent

targeting, accounting for around 5-10% of incidents. The value 1 (low interest) should be assigned to those sectors that are rarely targeted, with a share of less than 3% of total incidents.

We use our historical data as follows. First, we analyze the data from ENISA Threat Landscape (period July 2023 – June 2024), shown in Figure 7. We observe that approximately 100 cyber incidents targeted the space sector, while the number of incidents across all sectors was estimated at 9,900. This means that the space sector accounted for about 1.01% of all cyber incidents within the timeframe considered.

To determine how significant this percentage is, we compare it to the following high-target sectors:

- Public Administration: 1,880 incidents (19% of total)
- Transport sector: 1,110 incidents (11% of total)
- Finance: 900 incidents (9% of total)
- Space: 100 incidents (1.01% of total)

The analysis clearly suggests that the space sector is not yet a primary target for attackers when compared to sectors such as public administration, finance, and transport.

Then, to supplement the previous data, we examine historical records from CyberInflights 2023 threat reports, which document more than 60 cyberattacks against the space sector within 2023, as shown in Figure 8. The results of the plot align closely with our observations above and indicate that attacks against space assets have remained relatively infrequent so far when compared to other high-risk sectors.

Finally, to achieve a broader perspective, we analyze data from EuRepoC, shown in Figure 9, which provides the following insights into cyber incidents targeting critical infrastructure:

- Space Sector: 18 incidents (0.51% of all reported cyber incidents globally), representing 1.3% of all incidents targeting critical infrastructure.

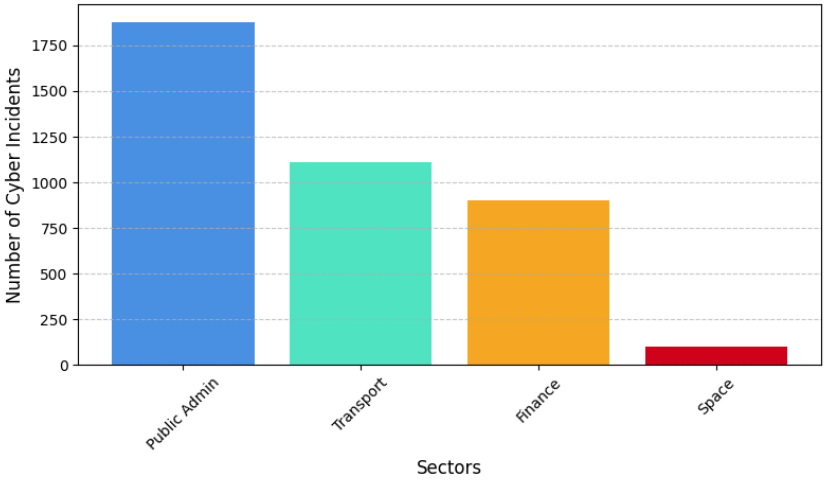

Figure 7: ENISA Threat Landscape: Attacks against critical sectors 2023-2024

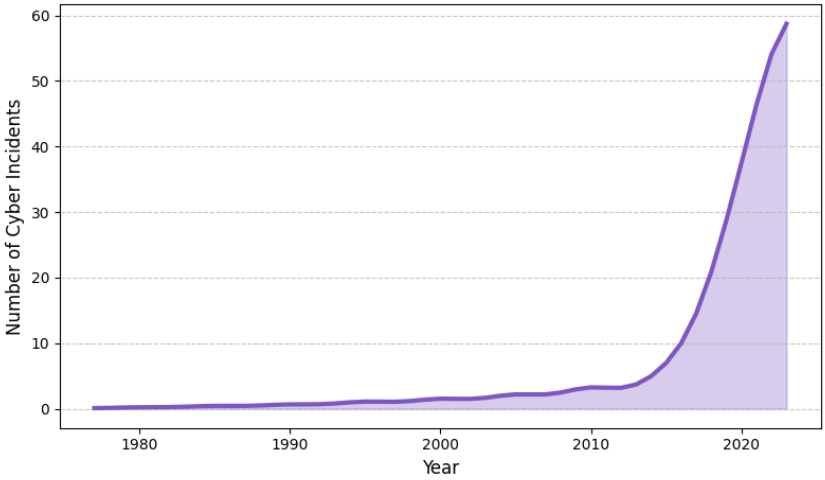

Figure 8: Evolution of cyberattacks on Space (1977-2023)

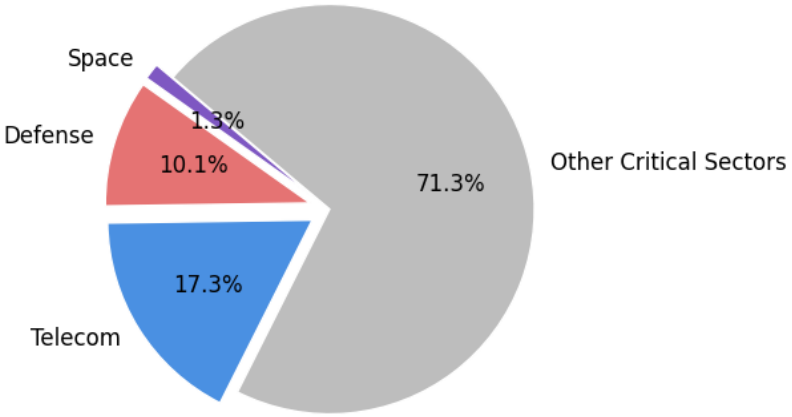

Figure 9: Cyber Incidents in Critical Infrastructure (2000-2025 EuRepoC)

- Defense Sector: 141 incidents (4.03% of all incidents globally), representing 9.8% of all incidents targeting critical infrastructure.
- Telecommunications: 243 incidents (6.94% of all incidents globally), representing 16.9% of all incidents targeting critical infrastructure.

To assign a score to the space sector, we make the following considerations. The space sector represents 1.01% of incidents (2023-2024 data), 1.3% of critical infrastructure attacks (2000-2025 EuRepoC data), and historically low attack volumes (CyberInfilights 2022 data). This percentage is significantly lower than high-priority targets like public administration (19%), defense (9.8%), and telecommunications (16.9%). Thus, based on our scoring model, the space sector falls into the low interest ($A = 1$) category.

As said above, we are approximating the attack interest through the frequency of past incidents. However, while cyberattacks on the space sector are relatively less frequent compared to other critical infrastructure sectors, this may be related to the nature of the threat actors involved rather than the sector's lack of strategic importance or attractive-

ness, or to the classification of such attacks. Space assets and networks are widely targeted by state-sponsored hackers and advanced persistent threats (APTs) [284, 391, 568]. These types of cyber operations are quite different from the more frequent financially motivated attacks observed in sectors like public administration, finance, healthcare, or retail, often requiring months or even years of reconnaissance, exploitation, and operational execution. The complexity and resource demands of these operations explain why they are less observed if compared to financially driven attacks, which can be cheaply automated. It is only by assigning the same value and characteristics to the threat model across sectors that we conclude that while space assets are targeted by highly capable adversaries, these attacks are less frequent due to the nature of their execution, justifying an A = 1 classification.

Another important consideration that should be included in our discussion is the recent upward trend in attacks against the space sector [415]. The past few years have seen a notable increase in cyber incidents affecting space infrastructure, suggesting a growing adversary interest, but the overall volume remains significantly lower than in sectors such as telecommunications, defense, and public administration.

Additionally, we have to consider that many cyber incidents affecting space assets might not be explicitly categorized as space-targeted attacks in existing cybersecurity databases. Space systems are an integral part of telecommunications, energy, and defense networks, and cyber intrusions into these sectors could have originated through vulnerabilities in space-based infrastructure. This interconnectivity creates a blurred boundary in incident classification, and some attacks exploiting space assets as entry points may be recorded under other categories, such as energy or communications. Therefore, the actual impact of cyber threats leveraging space infrastructure is likely underestimated.

In conclusion, the A = 1 classification does not imply that the space sector is not a relevant target, but rather that the frequency of cyberattacks – when considering all attackers on the same level – remains low due to the nature of the adversaries involved and the resources required for such operations. The observed trends suggest that this classification

may need to be revised in the future as cyber threats against space systems continue to evolve.

7.3.5 Data Collection: Identifying Exposed Space Assets

Our methodology for quantifying cybersecurity exposure within space-sector organizations combines Shodan for host and service discovery with Vulners for exploit intelligence. To provide a clear overview of the methodology, Figure 10 illustrates the step-by-step process of the Risk Exposure Framework. The framework follows a linear workflow from initial organization identification through data collection, vulnerability analysis, and final risk score computation.

The first step concerns the identification of space manufacturers, satellite operators, space agencies, and other potentially interesting entities operating in the space sector. This stage involved consulting public lists [213] or referencing known space companies to compile an initial list of relevant organizations. Despite our focus on the space sector, some organizations included in our list are involved in vertical sectors such as defense and aerospace. In Table 23, we summarize some of the information related to the companies we identified in our analysis. The information on the organization name is crucial in our analysis to identify its Internet attack surface. Indeed, during data collection, we leverage Shodan's `org:"<OrganizationName>"` filter to isolate ICDs that appear to be associated with each targeted entity's domain or IP block.

After mapping an organization's potential footprint, we refine our search with the `has_vuln:"true"` filter to query hosts labeled by Shodan as containing known vulnerabilities (CVEs). Shodan tags these vulnerabilities based on observed service banners or software fingerprints. This filter narrows our list to IP addresses that simultaneously belong to the organization's network space and host at least one exposed service carrying a known CVE. For each IP address returned by the query above, we retrieve host data using the Shodan API. This data includes open ports, service banners, potential CPE (Common Platform Enumeration) strings, and CVE references. This host-level information is used for linking each

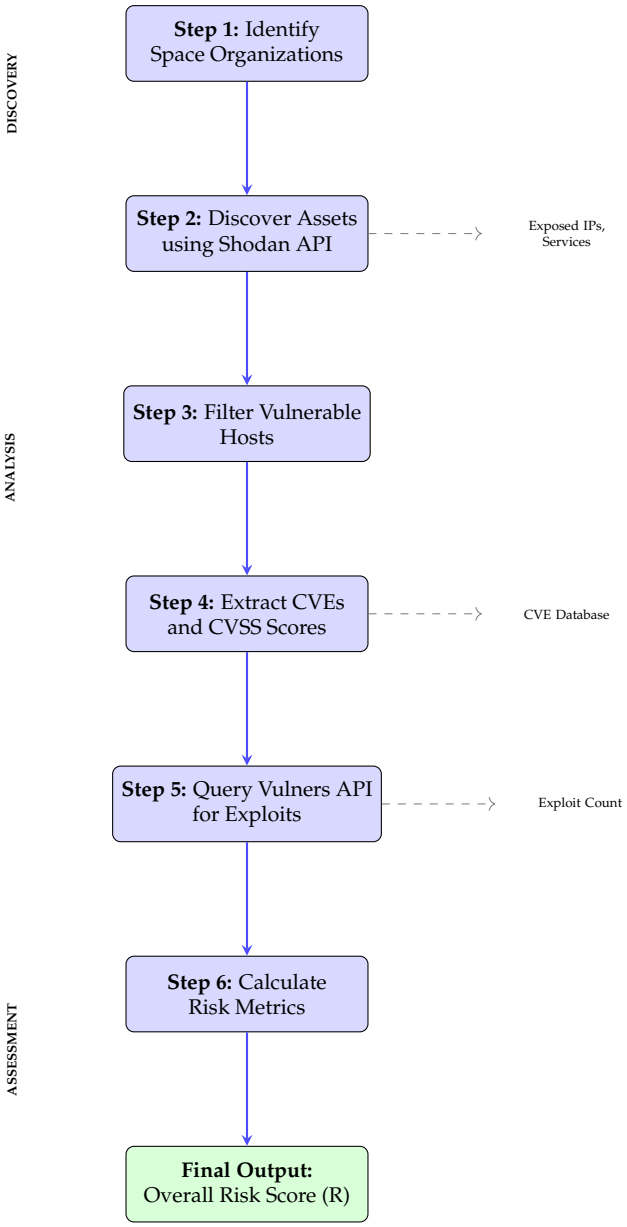

Figure 10: REF Methodology Workflow

Algorithm 1: Risk Exposure Framework (REF) for Space Organizations

Input: Organization name org_name
Output: Risk metrics and vulnerability report

// Step 1: Data Collection
Initialize Shodan and Vulners APIs;
$shodanResults \leftarrow Shodan.query(org : org\_name \wedge has\_vuln : true)$

// Step 2: Vulnerability Analysis
$hostInfo \leftarrow \emptyset$; // Info on vulnerable hosts
// Collect data for each host
foreach *host* h *in* $shodanResults$ **do**
    Extract CVEs, CVSS scores, CPEs, and vulnerable ports;
    Store vulnerability data for host h in $shodanResult[h]$;

// Step 3: Exploit Intelligence
Collect unique CVEs from all hosts;
Query Vulners API for exploit availability (parallel);
Build the function $\mathcal{V}$ associating each host with its exploit counts;

// Step 4: Risk Calculation
$IP \leftarrow \{hostInfo[h].ip$ for each host $h\}$;
// Exposure score
Compute $E(IP) = \frac{1}{\#IP} \sum_{a \in IP} V(a)$;
Compute $EA(IP)$ using exploit availability ratio;
Compute $VSI(IP)$ from average CVSS scores;
// Likelihood
Compute $L(IP) = A \times (EA(IP) + VSI(IP))$;
// Raw Risk
Compute $R_R(IP) = C \cdot E(IP) + (1 - C) \cdot L(IP)$;
// REF score
Compute $R(IP) = \log_2(1 + R_R(IP))$

// Step 5: Report Generation
Generate summary with risk scores and metrics;
Rank top vulnerable IPs by exposure and exploitability;
Identify most common CPEs and CVEs;
return *Risk assessment report*;

Table 23: The companies and organizations analyzed in our study. For each company, we report its main domain of activity, its estimated revenue, the main region of operations, and whether it produces dual-use technology and is a government service provider.

Organisation	Domain	Estimated Revenue	Primary Region	Dual-use	Government Service Provider
AIRBUS	Aerospace, Defence, Space	€ 69B [31]	Europe	Yes	Yes
Telespazio	Satellite Services, Space Operations	0.7 [495]	Europe	Yes	Yes
Viasat	Satellite Communications	€ 4.28B [539]	USA	Yes	Yes
SpaceX	Launch Services, Satellite Internet	€ 8.3B [436]	USA	Yes	Yes
ESA - Villafranca Satellite Tracking Station	Satellite Tracking / Space Operations	N/A	Europe	Yes	Yes
GMV Aerospace and Defence S.A.	Aerospace, Defence, Space Software	€ 0.3 B [252]	Europe	Yes	Yes
Gilat Telecom Ltd	Satellite Communications	€ 0.3B [249]	Middle East	Yes	Yes
Eutelsat	Satellite Broadcasting	€ 1.5B	Europe	Yes	Yes

service or port to its reported vulnerabilities and for listing unique characteristics such as version strings or protocols.

From the data retrieved from Shodan, we analyze each IP and store the following information for each of them that allows us to compute the functions $\mathcal{O}$, $\mathcal{V}$ used in the definition of Exposure and Likelihood in Section 7.3.1:

- The number of vulnerable ports on that IP (ports that Shodan specifically tied to at least one CVE).
- The total number of vulnerabilities detected for that IP.
- A list of those vulnerabilities and any relevant details—like CVSS scores—when available.
- The set of CPE strings, if reported, indicating software or operating systems in use.

Each discovered CVE across all IPs is used to perform a query to Vulners to retrieve how many public exploits, namely, proofs of concept,

exploit scripts, or modules, exist for that specific CVE. The result is used to build the mapping $\mathcal{E}$ we used in the definition of Exploit Availability (EA) metric of Section 7.3.1. This data allows for estimating how readily attackers can capitalize on the discovered vulnerabilities. Once for each IP, we have the number of open vulnerable ports, the total number of vulnerabilities, and exploit information, we compute the total count of vulnerable IPs belonging to the organization, the global set of unique CVEs across all hosts, and the overall average CVSS score as described in Section 7.3.3.

With the per-IP data assembled, we apply the Exposure formula and derive the Likelihood from the aggregated exploit information and the average CVSS score. This calculation yields a measure of how probable it is that these exposed assets could be successfully compromised if targeted.

We then calculate a raw risk value by weighting Exposure and Likelihood, and then apply a logarithmic transformation to maintain interpretability. The final result is direct evidence of publicly visible attack vectors and existing exploit modules, going from a simple port-scan perspective into a more comprehensive threat picture.

Having established the theoretical and mathematical foundations of the Risk Exposure Framework, we operationalize it in Algorithm 1. The pseudocode provides a high-level procedural overview of the REF methodology, delineating how data about organizations' attack surface is systematically collected and processed to derive quantitative risk assessments.

7.3.6 What REF sees in the space domain

REF focuses on Internet-exposed assets. Therefore, it captures ground-segment and enterprise risks and offers limited visibility on deliberately isolated links or flight software. However, space-specific characteristics often leave observable signals at network boundaries:

- *Isolated environments.* When segmentation and cross-domain controls are effective, externally visible exposure is small or null; con-

versely, misconfigurations and reachable remote-access paths (e.g., VPN gateways, web management, cloud ground services) appear in REF's exposure and banner data, precisely the pattern ENISA highlights in "Scenario 3 of its space threat assessment: network intrusion due to lack of security protocols and misconfiguration." [209]

- *Limited compute / RT constraints.* Space-qualified/rad-hard processors and deterministic RTOS constraints push conservative change policies and cryptographic agility on adjacent systems; at the boundary, this often shows up as older protocol stacks or slower remediation. REF does not measure on-board resources, but it does register persistent, externally reachable vulnerable versions and weak protocol fingerprints that can be a downstream effect of such constraints [375, 254, 247, 530].

- *Firmware/update limitations.* Tight windows and signed over-the-air (OTA) requirements can lengthen patch latency for equipment interfacing with space systems. REF cannot attest to firmware assurance, but when those processes slow remediation, it will observe longer-lived external vulnerabilities on boundary services [398, 343].

In conclusion, REF reports what a remote adversary can see. It cannot prove air gaps, evaluate flight software integrity, or inspect internal trust zones: those require a mission-internal assessment. Our results and policy mapping already utilize REF in this "first-line triage" role [209].

7.4 Integrating REF into existing risk assessment methodologies

This section illustrates how REF can be incorporated into some of the existing risk assessment frameworks and processes for space systems. Specifically, we examine the Notional Risk Score developed by the Aerospace Corporation, the Cybersecurity Risk Assessment for Space Systems created by Honeywell, a case study developed by ENISA, and general-purpose frameworks for or other quantitative risk models such as the

NIST SP 800-30 (Risk Assessment Guide)[294], the FAIR (Factor Analysis of Information Risk)[313]. While other frameworks exist, including those developed by NIST, we chose to focus on these due to their operational practicality and relevance. We show that REF can enhance different stages of any risk assessment methodology related to space or other organizations.

7.4.1 REF and SPARTA NRS

Many ICT risk assessment methodologies often fall short in addressing the dynamic and complex nature of cyber threats in space systems. To bridge this gap, industry and policymakers have requested threat-based risk assessment approaches tailored to space. These methodologies prioritize the identification and analysis of specific threats, such as signal jamming, spoofing, DDoS, or unauthorized access to satellite control systems, to inform the development of targeted mitigation strategies. Focusing on the most probable and impactful threats should allow organizations to allocate resources more effectively and enhance their defensive measures.

One of these frameworks is *Space Attack Research and Tactic Analysis* (SPARTA), developed by the *Aerospace Corporation* [497], an American nonprofit that operates a federally funded research and development center (FFRDC), and provides technical guidance and advice on all aspects of space missions to military, civil, and commercial customers. The SPARTA framework defines a taxonomy of potential cyber threats that are specific to spacecraft and space missions. Its primary goal is to support organizations in identifying, understanding, and addressing vulnerabilities across different stages of an attack. The framework organizes threats into high-level tactics, such as *ST0001 – Reconnaissance*, which refers to the phase where threat actors gather information to support future operations, or *ST0002 - Resource Development* that represents the phase where they try to establish resources to support operations. Each tactic is associated with multiple techniques, which describe how an adversary achieves a tactical objective. For instance, a technique might in-

volve exploiting trusted relationships to gain initial access. These techniques can be further broken down into sub-techniques, which represent more specific or granular behaviors. Sub-techniques are variations of the parent technique and often reflect a particular implementation of a threat action, such as compromising mission collaborators (e.g., academic or international partners) to achieve initial access. This hierarchical structure helps organizations trace the progression of potential attacks and design targeted countermeasures accordingly. To quantify and manage cyber risks in space systems, the Aerospace Corporation introduced the *Notional Risk Score* (NRS) within the SPARTA framework. The NRS should provide a metric to evaluate the potential impact and likelihood of cyber threats, assigning numerical values to various threat scenarios. The NRS can be considered a general-purpose framework for its adaptability to assess the cybersecurity risks associated with space systems. It assigns risk scores based on system criticality, likelihood of exploitation, and potential impact. These scores are calculated through a subjective analysis that considers expert assessments of adversary capabilities, system vulnerabilities, and operational priorities. Three elements determine the likelihood of an attack: (i) adversary motivation, which is linked to system criticality and assumes that more critical assets attract more attention from threat actors; (ii) exploitation difficulty, which considers the complexity of executing an attack technique; and (iii) adversary capability, categorized into seven tiers ranging from script kiddies to the most sophisticated state actors. The likelihood assessments are combined with an impact evaluation, which considers potential mission disruption, data integrity loss, or availability concerns. The final risk score is placed on a 5×5 risk matrix, where impact and likelihood scores are assigned values from 1 to 5, producing a risk score that falls into a *low*, *medium*, or *high-risk* category.

In practical terms, organizations can employ REF to rapidly identify which Internet-accessible assets are most at risk and derive a specialized Exposure (E) metric. That data can then be fed into an organization's broader application of NRS by becoming part of the "threat likelihood" factor specifically for externally reachable software or systems. There-

fore, NRS might be applied to multiple mission segments, and REF provides verified details on real-world, network-facing vulnerabilities. Integrating the two can increase overall risk assessment efficiency, ensuring that the security posture of a specific entity is properly informed by actual vulnerabilities visible on the public internet. While REF focuses on a narrower slice of infrastructure, it can offer an enriched perspective on how easily such vulnerabilities might be exploited, insight that is often lacking in purely theoretical frameworks.

7.4.2 The REF as part of Honeywell's Security Risk Assessment

In order to give a more comprehensive view of how REF can be integrated into the risk assessment process of space organisations, we considered an additional framework employed by the industry, developed to be applied to space systems [535]. We summarized the contributions that REF can give to Honeywell's Risk Assessment in Table 24.

Honeywell's Security Risk Assessment is designed for evaluating security risks in safety-critical systems, including aerospace and space systems. This methodology focuses on identifying, assessing, and managing cybersecurity risks through a clearly defined set of procedures. The first step entails the creation of a comprehensive security architecture, which involves establishing system boundaries, identifying key assets, attackers, vulnerabilities, and possible points of entry. The second step comprehend the definition of security risk elements — assigning quantitative values based on severity, occurrence likelihood, and prevention capability. The methodology involves constructing detailed security models such as threat trees and security ontologies, which help to visualize and analyze the relationships and potential impact of threats. The last step regards the definition of the acceptability of risks according to predefined criteria, guiding decisions on necessary mitigation measures.

In this context, one area where REF provides substantial value is in supporting the creation of security architecture. Traditional risk assessment methodologies require a clear understanding of an organization's

attack surface, including vulnerabilities and potential points of entry. REF automates the discovery and quantification of Internet-facing assets and vulnerabilities, directly informing the security architecture and providing empirical evidence on entry points. The integration of REF can help risk assessment teams base their architectural decisions on current and actionable intelligence rather than assumptions or generic risk profiles. Furthermore, REF enhances the process of defining security risk elements. In various methodologies, risk elements — such as attackers, access vectors, and vulnerabilities — are identified and assigned severity, occurrence, and prevention values based on expert judgment. REF can complement and refine this expert judgment by contributing quantitative, empirically derived metrics related to exposure and exploit availability. Additionally, REF can help refine security risk models. Honeywell's risk assessment uses threat modeling techniques such as threat trees and security ontologies to represent possible attack paths and outcomes. REF provides concrete, data-driven input for these models, identifying actual vulnerable ports, associated CVEs, and the existence of known exploits, which can be used as inputs to threat trees and scenario analyses. A REF augmented risk analysis can better depict real-world threat scenarios and identify previously unrecognized attack vectors.

7.4.3 REF and ENISA Space Threat Landscape Report

In March 2025, ENISA [150] published the Space Threat Landscape report to drive cybersecurity efforts across the European space sector. The Report outlines threats and realistic attack scenarios that space operators and ground segment entities might face, supporting the development of mitigation strategies. The importance of this report lies in its sector-specific focus, as it addresses the specific challenges that come with managing space assets, both in orbit and on the ground.

One of the critical scenarios highlighted by ENISA is "Scenario 3: Network Intrusion Due to a Lack of Security Protocols and Misconfiguration." This scenario demonstrates how weaknesses in network configuration, such as default settings, the use of unsecured protocols, or miss-

Table 24: Integration of Honeywell Risk Assessment Steps with REF Contributions. For each step and activity of the Honeywell Risk Assessment, we describe how the REF elements can contribute to or complete them.

Risk Assessment Step	Honeywell Risk Assessment Activities	REF Contribution	REF Elements
Security Architecture Creation	Establish system boundaries, identify assets, vulnerabilities, and entry points.	Provides identification and quantification of external attack surfaces and exposed assets.	Exposure (E), Vulnerable IPs, Ports
Definition of Security Risk Elements	Identify risk elements; assign Severity, Occurrence, and Prevention values.	Supplies empirical metrics for exploit availability, vulnerability severity, and adversary interest.	Exploit Availability (EA), VSI, CVSS
Security Model Development	Create security ontologies and threat trees based on identified vulnerabilities.	Offers precise data-driven inputs (CVEs, exploitability) for constructing detailed threat scenarios.	CVEs, Exploit Data (Shodan/Vulners)
Risk Scenario Identification	Aggregate vulnerabilities into structured threat scenarios.	Enables realistic and granular risk scenarios informed by real-world vulnerability and exploit data.	Likelihood (L), Real-world Exploits
Determining Risk Acceptability	Evaluate risk scenarios against acceptance criteria.	Provides quantitative scoring for better-informed risk decisions and clearer acceptability analysis.	Risk Score (R), Risk Scaling (Log)
Continuous Risk Monitoring	Periodic assessment and updates based on new vulnerabilities or threats.	Enables continuous, automated monitoring and updating of the external cybersecurity posture.	Real-time data feeds (e.g., from Shodan)

ing access controls, can open the door to unauthorized intrusions. The ground segment, a complex web of mission control centers, data relay stations, and tracking infrastructure, is particularly vulnerable to such issues, especially when operational services are inadvertently exposed. REF can support risk evaluation in this specific scenario. Even if it cannot be used as a full forensic audit or to emulate an intrusion detection system, it can flag areas of concern by assessing exposure and estimating the likelihood of exploitation based on known vulnerability data. This process can be useful in the early stages of risk assessment, where broad visibility into the organization's digital footprint is necessary to identify possible weak spots. Applied to Scenario 3, REF helps identify where misconfigurations might be leading to increased risk, without needing access to internal configurations or administrative policies.

With Scenario 3 ENISA wants to highlight that default settings, insufficient segmentation of networks, and the use of outdated or unencrypted protocols are common among ground operators especially in legacy or multi-tenant environments. REF aligns with this threat landscape because it focuses on externally observable data, such as exposed IP services using weak protocols or devices with known CVEs, which ENISA describes as prime enablers of such intrusions. In this context, REF does not replace internal configuration audits, but identifies publicly visible risk indicators that ENISA flags as early-stage vulnerabilities in cyber kill chains. For instance, if a ground station's control interface is exposed over an unsecured protocol, something ENISA considers as plausible in shared infrastructure scenarios, REF can flag this exposure even without privileged access to the system. Furthermore, REF assigns a dynamic risk score based on exposure and exploitation likelihood that mirrors ENISA's recommendation for continuous risk posture assessments, especially given how quickly threat actors can pivot from reconnaissance to exploitation. ENISA also calls for proactive vulnerability management and improved network hygiene, and here too, REF can provide a scalable first line of analysis by identifying likely misconfigurations, insecure remote access points, and threat-exposed services that deserve in-depth review. The data-agnostic architecture of REF also ad-

dresses ENISA's observation that space operators rely on a fragmented toolset and diverse supply chains, offering a platform-neutral method of initial risk triage. In conclusion, REF operationalizes several of ENISA's recommendations: exposure monitoring, risk quantification, and prioritization of mitigation efforts, within a framework capable of automated and continuous external scanning.

7.4.4 Contextualizing REF within the existing Risk Assessment Landscape

This section analyzes other general-purpose security frameworks and methodologies to better understand how REF fits into them. More specifically, we consider the following:

- NIST SP 800-30 (Risk Assessment Guide) [294] provides a comprehensive methodology for conducting risk assessments within information systems. This framework employs a structured approach that identifies threat sources, threat events, vulnerabilities, likelihood determinations, impact analysis, and risk determination. It operates primarily through qualitative assessments supported by semi-quantitative scales (from Very Low to Very High), requiring extensive organizational knowledge and expert judgment to evaluate risks across the full system lifecycle.

- FAIR (Factor Analysis of Information Risk) [313] represents a quantitative risk assessment model that attempts to standardize risk terminology and measurement. FAIR decomposes risk into discrete factors: threat event frequency (contact frequency × probability of action) and loss magnitude (primary and secondary losses). Contact represents the frequency at which a threat agent encounters a vulnerable asset, while action refers to the likelihood that the agent, having made contact, decides to attack. FAIR uses probabilistic methods and Monte Carlo simulations to generate risk estimates in monetary terms, making it particularly valuable for business decision-making and cyber insurance contexts.

- CVSS (Common Vulnerability Scoring System) provides a standardized method for rating IT vulnerabilities. Version 3.0 calculates scores based on three metric groups: Base (exploitability and impact characteristics), Temporal (current exploit techniques and remediation levels), and Environmental (modified base metrics considering local requirements). While CVSS excels at individual vulnerability assessment, it does not inherently provide organizational or system-level risk aggregation.

- ENISA Risk Assessment Frameworks encompass multiple specialized matrices designed for European critical infrastructure operators. ENISA has developed several complementary assessment frameworks, including the 5G Security Controls Matrix [148], the Interoperable EU Risk Management Framework, and the PETs Control Matrix [149]. Each framework addresses specific technological domains while maintaining alignment with EU cybersecurity directives and supporting standardized risk evaluation across member states. The 5G Security Controls Matrix consolidates technical and non-technical controls relevant for 5G network security, mapping various technical controls to an established EU supervisory framework for telecoms. The Interoperable EU Risk Management Framework evaluates interoperability features of risk management frameworks using a four-level scale and provides a methodology for assessing potential interoperability among different frameworks. The PETs Control Matrix includes systematic assessment criteria for privacy-enhancing technologies, distinguishing between generic criteria (applicable to all tools) and specific criteria (assessing particular functionalities).

REF represents a distinct niche within this ecosystem of risk assessment frameworks, functioning as an automated, data-driven exposure quantification tool rather than a comprehensive risk management system. Unlike the frameworks mentioned above, REF specifically targets the observable external attack surface, providing empirical measurements that can feed into broader risk assessment processes. Table 25 compares

our framework with the other mentioned above, focusing on their main characteristics.

Table 25: Comparative Analysis of Risk Assessment Frameworks

Framework	Scope	Methodology	Automation	Data Requirements	Output Type	Space-Specific	Integration with REF
REF	External attack surface	Quantitative (E × L)	Fully automated	Internet scan data, CVE/exploit DBs	Numerical risk score	Adaptable	N/A (baseline)
NIST SP 800-30	Full system lifecycle	Qualitative/ Semi-quantitative	Manual	Internal documentation, expert judgment	Risk levels (VL-VH)	No	REF provides data for Steps 2-2, 2-3
FAIR	Information risk (monetary)	Quantitative probabilistic	Partially automated	Historical loss data, threat intelligence	Financial risk ($)	No	REF informs Contact Frequency, Vulnerability
CVSS	Individual vulnerabilities	Quantitative scoring	Manual/Semi-automated	Vulnerability characteristics	Severity score (0-10)	No	REF aggregates CVSS scores
ENISA Matrices	Sector-specific threats	Qualitative (5×5 matrix)	Manual	Threat scenarios, impact assessment	Risk categories	Sector-dependent	REF quantifies likelihood dimension
SPARTA NRS	Space mission threats	Semi-quantitative	Manual	Adversary analysis, system criticality	Risk matrix placement	Yes	REF supplies exposure metrics
Honeywell SRA	Safety-critical systems	Model-based (threat trees)	Partially automated	System architecture, threat models	Risk acceptability	Yes (aerospace)	REF populates asset inventory

Rather than replacing the above frameworks, REF should be positioned as a complementary tool that enhances their implementation through empirical data injection at specific assessment phases. Organizations implementing NIST SP 800-30 can leverage REF outputs as empirical inputs for likelihood estimates, particularly during the vulnerability identification and threat-vulnerability pairing phases, transforming what would typically be expert judgment into data-backed assessments. Within FAIR models, REF's exposure metrics can inform Contact Frequency calculations with actual reconnaissance data, while its exploit availability statistics support Probability of Action estimates with real-world exploit prevalence rather than theoretical assessments. REF's aggregated vulnerability view complements individual CVSS scores by providing organizational context for prioritizing patch management efforts, helping security teams understand not just which vulnerabilities are severe, but which severe vulnerabilities are actually exposed and exploitable in their infrastructure. For organizations using ENISA risk matrices, REF enables dynamic updates to likelihood assessments through continuous measurement, transforming static annual assessments into living risk documents that reflect the current threat landscape.

The radar chart in Figure 11 compares the four major risk assessment frameworks discussed above with REF across eight critical capability dimensions. Each framework displays a distinct capability profile, reveal-

ing strategic positioning rather than direct competition. The chart compares the REF to other established risk assessment frameworks across eight capability axes. The comparison is based on a structured qualitative–quantitative evaluation; the methodology builds on established practices of comparative evaluation of risk assessment frameworks [462, 314].

Scores were assigned by mapping each framework's published features, scope, and methodological constructs to the eight axes defined in the figure. For each dimension, a definition and observable criterion were established (e.g., presence of automation, use of external data, and financial quantification). We examined each framework to verify whether these characteristics were explicitly implemented, partially addressed, or not addressed at all. Each axis was rated on a discrete 1–5 scale, where 1 means minimal or implicit capability and 5 denotes full integration. The axes represent eight dimensions of cybersecurity assessment capability. Automation Level reflects the degree to which data collection and risk computation occur without manual intervention. External Visibility measures reliance on externally observable data such as exposed IPs or services. Continuous Assessment captures whether the framework supports periodic or real-time reassessment of risk. Space Domain Specificity indicates explicit adaptation to the space domain. Regulatory Alignment evaluates consistency with formal risk management standards (e.g., NIS2, NIST SP 800-30). Vulnerability Detail expresses the depth of vulnerability modeling, including CVE/CVSS integration. Financial Quantification refers to the framework's capacity to express outcomes in economic or loss-expectancy terms. Internal Coverage assesses inclusion of organizational, procedural, and human-factor controls beyond the technical perimeter.

Our analysis results in the following main takeaways:

- *REF's Distinctive Strengths*: REF demonstrates good performance in three interconnected areas: Automation Level (5/5), External Visibility (5/5), and Continuous Assessment (5/5). REF achieves moderate scores (3/5), Regulatory Alignment, and Vulnerability Detail, indicating its ability to support specialized applications while

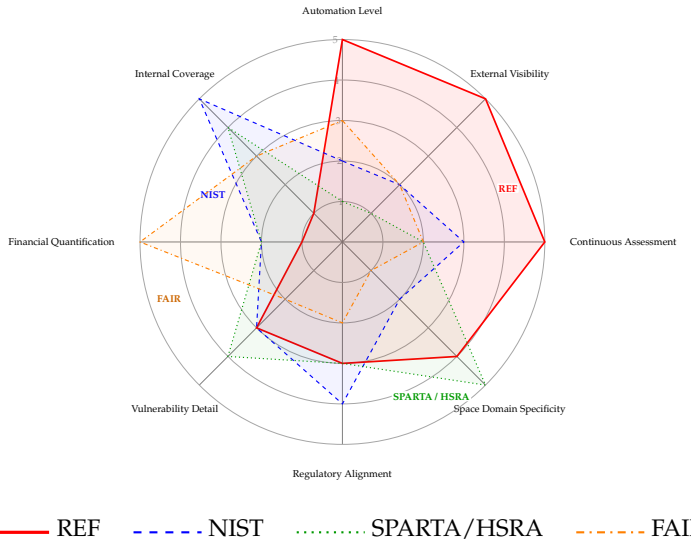

Figure 11: Radar comparison across eight capability axes

maintaining broad applicability.

- *Complementary Framework Profiles*: NIST RMF excels in Internal Coverage (5/5) and Regulatory Alignment (4/5) while showing limited automation and external visibility capabilities. SPARTA/Honeywell frameworks achieve maximum Space Domain Specificity (5/5) and strong Vulnerability Detail (4/5), reflecting their specialized focus on space-specific threats and attack scenarios. FAIR's strength lies in Financial Quantification (5/5).

- *Strategic Integration Implications*: The non-overlapping capability profiles suggest that these frameworks function as complementary rather than competing solutions. REF's capabilities can feed quantitative data into NIST's comprehensive internal risk management processes, while SPARTA/Honeywell's space-specific expertise can provide contextual interpretation of REF's vulnerability findings. FAIR's financial quantification can translate REF's technical risk scores into economic impact assessments for decision-making.

- *Coverage Gaps and Synergies*: Systematic coverage gaps emerge when frameworks are used independently. REF's minimal Internal Coverage (1/5) and Financial Quantification (1/5) scores indicate clear boundaries for its application scope. However, these limitations become strengths in integrated approaches where REF provides automated external assessment while other frameworks address internal risks, sector-specific threats, and economic impacts.

The comparison supports the integration strategy we defined above and demonstrates that effective cyber risk management requires the coordinated deployment of specialized frameworks. In the following section, we show in detail how REF can be operationalized in practice.

7.4.5 REF operationalized

This section presents the example of an operational playbook to show how organizations can act on REF outputs in concrete, repeatable ways. A playbook, in this context, is a structured procedure that translates REF's empirical measurements into operational decisions, responsibilities, and evidence. The purpose is to demonstrate that REF can be a decision-support tool that guides remediation and compliance.

Playbook A aims to operationalize a weekly REF run into vulnerability management. The REF outputs are used to prioritize exposed assets, create remediation tasks with fixed deadlines (service-level agreements, SLAs), and generate audit-ready evidence of risk reduction. Table 26 encodes the prioritization policy: each row describes the condition under which an exposed asset is classified (e.g., public exploit available, high CVSS severity, weak management protocols), the action required, the deadline, and the accountable owner.

In the first row (P1 – Critical), the policy addresses assets whose exposure is either actively exploitable (EA > 0), or carries a high technical severity (CVSS ≥ 8.0), or is accessible by an administrative/control interface over a weak protocol. The required action is immediate patching or removal of the exposure. The SLA is 72 hours, reflecting the urgent threat level. The asset owner is accountable, and in the meantime, the

SOC should place the IP:port on the SIEM watchlist and enforce blocking via IDS/EDR.

In the "Containment override" row, the trigger is any Internet-exposed control plane or clear-text management protocol (such as Telnet or HTTP admin). In this case, the threshold is not a CVSS score alone, but a weak control mechanism providing attacker access. The required action is de-exposure followed by a scheduled protocol replacement; the SLA is 24 hours because the risk of compromise via exposed control interfaces is very high. Interim controls include network blocks and protocol-specific IDS signatures. The treatment here aligns with prioritisation frameworks that stress exploitability, exposure context, and business risk over severity alone.

Figure 12 then lays out the weekly loop: five ordered steps from measurement to remediation and reporting. The aim is to make the process explicit for security personnel, demonstrating how weekly REF runs drive prioritization, remediation, SOC monitoring, and measurable risk reduction.

In Step 1 REF recomputes all exposure and risk metrics using Shodan data, CVEs, and exploit information. This produces an updated REF report and a baseline change in the overall risk score (ΔR). Step 2 classifies the results: assets are grouped into priority tiers (P1–P3) depending on exploit availability, CVSS score, or weak protocols.

In Step 3, these classified findings are converted into remediation tickets, each with a clear SLA and assigned owner. Step 4 runs in parallel within the SOC: critical assets (P1) are added to watchlists, and temporary defences such as IDS rules or EDR blocking are applied while fixes are underway. Finally, Step 5 collects all progress data, how many vulnerabilities were closed, how fast containment happened, and produces the weekly risk burndown report.

7.5 Experimental Results and Discussion

In this section, we describe how we applied the methodology defined in Section 7.3 to conduct a risk assessment based on the exposure of the

Table 26: Playbook A — Prioritization policy for weekly REF runs. Each row specifies how an exposed asset is classified, what must be done, and within what deadline.

Priority tier	Trigger condition (REF evidence)	Required action	Deadline (SLA)	Accountable role	Interim SOC control
P1 — Critical	Exploit available (EA $>$ 0) **or** CVSS $\geq$ 8.0 **or** exposed admin/control over weak protocol	Immediate patch or de-expose; emergency change permitted	72 hours	Asset owner	Add IP:port to SIEM watchlist; enforce IDS/EDR blocking
P2 — High	5.0 $\leq$ CVSS $<$ 8.0, EA = 0	Patch or harden configuration; document exceptions	7 days	Asset owner	Targeted anomaly detection; monitor exposure persistence
P3 — Medium	CVSS $<$ 5.0, EA = 0	Patch during maintenance cycle	30 days	Asset owner	Baseline monitoring
Containment override	Any Internet-exposed control plane or clear-text management protocol (e.g., Telnet, HTTP admin)	Immediate de-exposure; schedule protocol replacement	24 hours	Asset owner	Temporary network blocks; protocol-specific IDS signatures

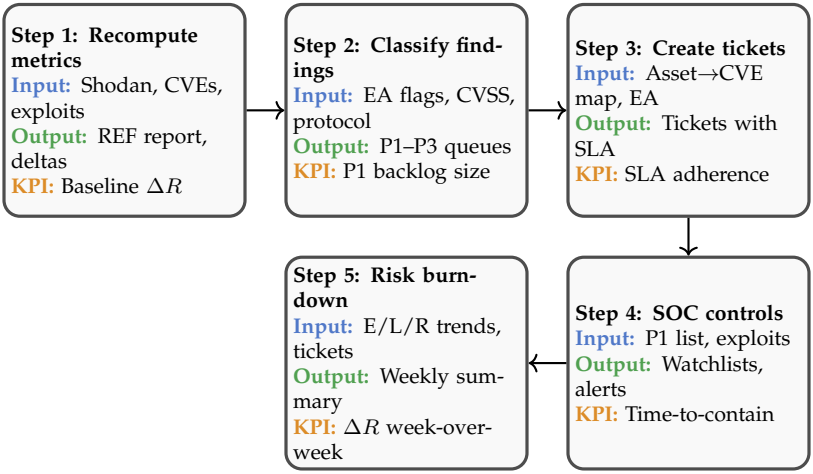

Figure 12: Playbook A — Weekly REF loop. A horizontal process pipeline: each step has standardised Inputs, Outputs, and KPIs.

eight companies of Table 23. The code for reproducing our experiments is available in the online repository [80]. However, in the description of our results below, we anonymize the name of the organization for security reasons. We then present and discuss the results of our analysis of the major CVEs identified across the various organizations, highlighting key findings and summarizing the main takeaways. Finally, we validate the methodology on synthetic data and discuss the threat to validity of our results.

7.5.1 Identification of Vulnerable Space Organizations

Our assessment provides insights into the security posture of the space industry and organizations in the sector at large. Our analysis considers eight leading organizations operating globally, resulting in a combined total of 99,957 publicly exposed IP addresses, among which 4,102 were identified as vulnerable, having known associated CVEs. This represents 4.1% of vulnerable hosts over the total exposed ones. The combination of the Shodan and Vulners APIs gives us a snapshot of the industry's current cybersecurity posture, underlining widespread and organization-specific vulnerabilities. A comprehensive summary of the quantitative results from this analysis is available in Table 27. To contextualize our analysis, we present the ranges and trends observed in the main elements of REF. Exposure scores, which reflect the scale and visibility of ICDs, span from as low as 8.22 (Company 1) to nearly 96.48 (Company 5), with a mean value of approximately 37.78. This indicates substantial variability in the online footprint of different organizations, from tightly segmented infrastructures to those with highly exposed configurations. Likelihood scores, which estimate the probability of exploitation based on CVE severity and exploit availability, vary between 6.84 and 7.40, with a mean of 7.17. The distribution remains relatively narrow, suggesting that most organizations share a comparable level of latent vulnerability once exposure is established. The average CVSS score for the vulnerabilities found ranges from 6.67 (Company 7) to 7.08 (Company 3), reinforcing the trend that most exposures involve high-severity vulnera-

bilities according to standardized scoring. The Overall Risk Score ranges from a low of 3.13 (Company 1) to a high of 5.72 (Company 5), with an average around 4.48. Entities such as Company 5 (5.72), Company 2 (4.87), and Company 8 (4.56) fall into the higher risk bracket, combining moderate-scale exposure with a notable concentration of high-severity vulnerabilities and available exploits. Conversely, Company 1 shows the lowest Overall Risk Score, reflecting a relatively modest footprint and reduced vulnerability context. Looking specifically at the examined organizations, Company 5 demonstrates the highest Overall Risk Score, with a value of 5.72. Despite having only 163 publicly exposed IPs, 72 of these were found to be vulnerable, with a total of 547 unique CVEs and 417 available exploits. This leads to an exceptionally high Exposure Score of 96.48, by far the largest in our sample. The average CVSS score associated with these vulnerabilities is 6.77, further underscoring their severity. This entity shows that even compact infrastructures when characterized by concentrated exposure and poor mitigation, can carry critical levels of cyber risk. Company 2 follows with a scaled risk score of 4.87. It has a moderate number of exposed IPs (1,042), among which 73 are vulnerable, linked to a striking total of 699 CVEs and 717 known exploits. The Exposure Score of 49.32 is second highest overall, indicating that the organization's digital footprint, although not the largest, is heavily loaded with accessible and potentially exploitable services. The average CVSS score is again high (6.77), reinforcing the critical nature of the exposure. The Likelihood Score for this organization is also significant, contributing to its high risk positioning. Company 8 ranks third, with a total of 2,000 exposed IPs and only 34 of them vulnerable. However, those 34 IPs correspond to 725 unique CVEs and 590 known exploits. This density of vulnerabilities results in an Exposure Score of 37.96 and a Likelihood Score of 7.37, one of the highest in our dataset. Combined with an average CVSS score of 7.03, also above the mean, this positions the organization in a high-risk tier despite a seemingly small vulnerable surface. Company 6 presents an illustrative case of risk intensification in smaller infrastructures. With only 44 exposed IPs and 15 vulnerable ones, it would normally be classified as low-exposure. How-

ever, the 70 CVEs identified, and 101 exploit matches raise the Exposure Score to 29.62. The organization's Likelihood Score of 7.36 and average CVSS of 7.07, among the highest across the dataset, result in a Risk Score of 4.28. This confirms that compact infrastructures are not inherently safer and may pose comparable levels of risk when vulnerabilities are severe and easily exploitable. Company 4 holds a unique position due to its large-scale online presence. It records the highest number of exposed IPs (62,598) and vulnerable IPs (2,533), with 560 unique CVEs and 671 available exploits. However, its Exposure Score is relatively moderate at 25.28. The Likelihood Score of 7.10 and average CVSS of 6.84 still contribute to a notable Overall Risk Score of 4.10. This organization's vast scale inherently raises the stakes, as a small percentage of vulnerable assets can translate into a significant attack surface. Company 7 shows an Overall Risk Score of 4.09, with 5,420 exposed IPs and 125 vulnerable. These are associated with 810 CVEs and 784 exploits, generating an Exposure Score of 25.11. The CVSS average is slightly lower at 6.67, but the concentration of exploits and elevated Likelihood Score of 6.99 contribute to its risk profile.

Table 27: Cybersecurity risk metrics for space organizations under test sorted by the value of the Overall Risk Score.

Org	Exp. IPs	Vuln. IPs	CVE Count	Exploits	E. Score	L Score	Avg. CVSS	Overall Risk
Company 5	163	72	547	417	96.48	6.84	6.77	5.72
Company 2	1042	73	699	717	49.32	6.99	6.77	4.87
Company 8	2000	34	725	590	37.96	7.37	7.03	4.56
Company 6	44	15	70	101	29.62	7.36	7.07	4.28
Company 4	62598	2533	560	671	25.28	7.10	6.84	4.10
Company 7	5420	125	810	784	25.11	6.99	6.67	4.09
Company 3	25537	881	572	662	24.25	7.40	7.08	4.07
Company 1	1253	269	233	380	8.22	7.33	6.87	3.13

Company 3, despite its relatively large footprint (25,537 exposed IPs), registers a lower Risk Score of 4.07. With 572 CVEs and 662 matching exploits, the Exposure Score is 24.25. Notably, Company 3 records the highest Likelihood Score in the entire dataset (7.40) and the highest average CVSS score (7.08), pointing to particularly exploitable vulnerabilities. Finally, Company 1 registers the lowest Overall Risk Score at 3.13. It has

1,253 exposed IPs and 269 identified as vulnerable, linked to 233 CVEs and 380 exploits. Although the CVSS average is a mid-range 6.87, the relatively low Exposure Score of 8.22 keeps the risk profile limited. This analysis represents a snapshot of the cybersecurity state of specific space organizations but also highlights broader implications for the industry at large. The variability in cybersecurity risk profiles across entities reflects the inconsistent maturity levels in vulnerability management practices and cybersecurity governance. Organizations with expansive and complex digital infrastructures, such as Company 4 and Company 3, face distinct challenges in continuously mapping and securing their digital assets, leading to significantly elevated exposure scores and higher exploitability. Smaller entities with fewer digital assets, like Company 6 or Company 5, face risks that are fewer in number but potentially equally impactful, emphasizing the need for tailored, context-specific cybersecurity approaches.

7.5.2 Analysis of Exposed Services and Critical Attack Surfaces

A substantial part of our analysis involves examining the most prevalent exposed services and vulnerabilities. In practice, we extract the most observed Common Platform Enumerations (CPEs) and CVEs from Shodan data. CPEs are structured naming schemes for information technology systems, software, and packages. Through this process, we identified technological assets and vulnerabilities that are particularly widespread, highlighting the most critical areas needing attention in the snapshot of companies we considered. Given the size of our sample, we expect that such findings reflect weaknesses present in the whole space sector.

By aggregating the results globally across all organizations, we identify some clear patterns regarding commonly exposed technologies and their unpatched vulnerabilities. These results are in Table 28.

The table displays the scan results for the ten most common CPEs identifiers across all organizations, along with the number of separate hosts associated with each identifier. A CPE string follows the NIST for-

Table 28: Top observed CPEs by organization and occurrence count

Organization	CPE	Count
Company 1	cpe:/a:f5:nginx	81
Company 1	cpe:/a:sendmail:sendmail:8.15.2%2f8.15.2	80
Company 2	cpe:/o:canonical:ubuntu_linux	18
Company 2	cpe:/o:linux:linux_kernel	16
Company 3	cpe:/a:f5:nginx:1.5.1	15
Company 3	cpe:/a:getbootstrap:bootstrap	14
Company 4	cpe:/a:jquery:jquery:3.5.1	22
Company 4	cpe:/a:openbsd:openssh:9.3	21
Company 5	cpe:/a:apache:http_server:2.4.6	40
Company 5	cpe:/a:openssl:openssl:1.0.2k	34
Company 6	cpe:/a:f5:nginx:1.18.0	25
Company 6	cpe:/o:canonical:ubuntu_linux	25
Company 7	cpe:/a:openbsd:openssh:7.4	25
Company 7	cpe:/o:canonical:ubuntu_linux	19
Company 8	cpe:/a:getbootstrap:bootstrap	6
Company 8	cpe:/a:f5:nginx:1.10.3	4

mat `part:vendor:product[:version]`. The initial letter indicates whether the entry represents an application (a), operating system (o), or hardware (h). The next two fields specify the supplier and product, with an optional fourth field that indicates the version. For example, the identifier `cpe:/a:f5:nginx` refers to the Nginx web server application maintained by F5, regardless of the version. In contrast, the identifier `cpe:/o:canonical:ubuntu_linux` encompasses every release of Canonical's Ubuntu operating system.

Among the most frequently observed software were servers such as Apache HTTP Server, Nginx, and OpenSSH implementations, as well as widely-used operating systems like Ubuntu Linux, FreeBSD, and Microsoft Windows. But also, client-side frameworks and libraries such as jQuery and Bootstrap showed a significant presence across multiple organizations.

Table 29 summarizes the most frequent CVEs detected by our analysis: we observe a consistent presence of outdated HTTP servers and their associated vulnerabilities. For instance, Company 5 notably shows

a heavy dependence on legacy software stacks, particularly older Apache HTTP servers (e.g., version 2.4.6 and 2.4.37) coupled with outdated OpenSSL versions (1.0.2k). Specifically, the Apache vulnerability CVE-2013-4365 appeared 49 times in Company 5 systems. This vulnerability also appears 11 times in Company 8. These vulnerabilities enable attackers to perform denial-of-service (DoS) attacks or execute arbitrary code. CVE-2024-11233 appears 81 times within Company 1's infrastructure alone, making it one of the most frequent critical vulnerabilities in the dataset. CVE-2024-11233 and CVE-2024-11234 are particularly recent and critical, associated with PHP version 8.2, indicating that some organizations, such as Company 1, continue to use vulnerable and potentially unpatched web frameworks.

Open-source libraries and client-side frameworks such as jQuery represent another significant risk area. Notably, vulnerabilities CVE-2020-11022, CVE-2020-11023, CVE-2019-11358, and CVE-2015-9251 appeared 22 times each. These vulnerabilities, prominently found in the digital infrastructures of Company 4, Company 3, and Company 7, primarily enable Cross-Site Scripting (XSS) and client-side injection attacks, potentially compromising web interfaces or allowing attackers to exfiltrate sensitive operational data. The presence of vulnerable versions of jQuery and Bootstrap suggests insufficient monitoring of software supply chains and inadequate update processes, meaning that automated dependency management tools and regular software composition analysis are still scarcely present.

Vulnerabilities related to cryptographic libraries, particularly outdated versions of OpenSSL are also widespread. For instance, vulnerabilities CVE-2023-48795, CVE-2023-38408, and CVE-2007-2768 were detected 42 times in Company 7 systems. Their presence underscores the neglected updates of security-critical components.

In addition, Table 29 shows a high prevalence of old versions of Nginx (notably, 1.18.0 and 1.10.3) in companies like Company 6 and Company 7. While Nginx itself is widely regarded as secure, outdated versions expose companies to known exploits. Specifically, CVEs associated with older Nginx versions, like CVE-2021-36368, emphasize the urgent

Table 29: Top CVEs by organization, including frequency, severity, and type.

Company	CVE	Occurrence	CVSS Score	CVE Description
Company 1	CVE-2013-2220	81	7.5	Buffer overflow / PHP
Company 1	CVE-2024-11233	81	9.8	Buffer overflow / PHP
Company 2	CVE-2009-0796	22	5.0	Cross-site scripting (XSS) / Apache HTTP Server
Company 2	CVE-2013-4365	49	7.5	Heap-based buffer overflow / Apache HTTP Server
Company 3	CVE-2020-11022	22	6.1	jQuery / Arbitrary code execution
Company 3	CVE-2020-11023	22	6.1	jQuery / Arbitrary code execution
Company 4	CVE-2008-3844	35	6.8	Externally introduced modification / Red Hat Enterprise Linux
Company 4	CVE-2023-51767	35	7.8	OpenSSH / Authentication bypass
Company 5	CVE-2009-0796	22	5.0	Cross-site scripting (XSS) / Apache HTTP Server
Company 5	CVE-2013-4365	49	7.5	Heap-based buffer overflow / Apache HTTP Server
Company 6	CVE-2009-0796	22	5.0	Cross-site scripting (XSS) / Apache HTTP Server
Company 6	CVE-2013-2765	8	4.3	Apache HTTP Server / DoS
Company 7	CVE-2008-3844	42	6.8	Externally introduced modification / Red Hat Enterprise Linux
Company 7	CVE-2021-36368	42	7.2	OS
Company 8	CVE-2013-2765	11	4.3	Apache HTTP Server / DoS
Company 8	CVE-2013-4365	69	7.5	Heap-based buffer overflow / Apache HTTP Server

need for the sector to implement strict patch management policies.

From the broader industry perspective, these frequently recurring vulnerabilities and exposed services represent significant attack surfaces, increasing the potential impact of cyber incidents. The space sector's unique operational context intensifies the risk implications. Compromise or disruption to satellite tracking stations, telemetry data centers, or satellite communication networks could lead to severe operational, economic, and potential safety implications. Specifically, for tracking stations, reliance on vulnerable systems exposes critical satellite operations and sensitive telemetry data, thereby risking operational continuity and strategic assets. Mitigation strategies must combine different approaches, targeting not just technical remediation but also organizational processes and cybersecurity culture. The organizations should first implement a robust and automated patch management lifecycle, ensuring swift deployment of security patches across all software stacks and prioritizing systems that directly interface with satellite control or telemetry operations. Second, they should implement continuous vulnerability management programs, integrating automated vulnerability scans and dependency tracking, in order to ensure organizations maintain real-time visibility into their cybersecurity posture. The ongoing presence of critical vulnerabilities in key software components highlights significant cybersecurity gaps within the space industry. Addressing these vulnerabilities through timely patch management, continuous vulnerability monitoring, and proactive security measures is the only way forward. These targeted cybersecurity strategies will greatly reduce the attack surface, thereby enhancing the industry's overall security posture and resilience.

7.5.3 Result Validation

To validate our REF methodology, we perform two evaluations. The first consists of applying REF on a synthetic dataset to study how the REF score varies under the variations of the variables. The second evaluation is a sensitivity analysis based on a tornado diagram. In Table 30, we

Table 30: REF metrics and corresponding formulas

Metric	Formula	Ref.
Exposure (E)	$E(IP) = \frac{1}{\#IP} \sum_{a \in IP} \mathcal{V}(a)$	(7.1)
Exploit Availability (EA)	$EA(IP) = \sum_{a \in IP} \frac{\mathcal{E}(v,a)}{\mathcal{V}(a)}$	(7.2)
Vulnerability Severity Impact (VSI)	$VSI(IP) = \begin{cases} 1, & \text{if avgCVSS} < 5.0 \\ 3, & 5.0 \leq \text{avgCVSS} \leq 8.0 \\ 5, & \text{if avgCVSS} > 8.0 \end{cases}$	(7.3.3)
Likelihood (L)	$L(IP) = A\,[EA(IP) + VSI(IP)]$	(7.2)
Raw Risk (RR)	$RR(IP) = \frac{E(IP)+L(IP)}{2}$	
	$RR(IP) = C\,E(IP) + (1-C)L(IP)$	–
Overall Risk (R)	$R(IP) = \log_2[1 + RR(IP)]$	(7.4)

summarize all the formulas used in REF for clarity and reference during validation.

Synthetic dataset

We generated and analyzed a synthetic dataset [80], designed to test how the metrics respond under controlled variations of key variables. Through this process, we aim to empirically demonstrate the consistency, sensitivity, and reliability of our approach. The dataset of the synthetic organization, named *SpaceTes*, is structured into 4 separate scenarios (identified with letters from 'A' to 'D'), and is designed to isolate and examine the impact of specific variables on the Exposure Score and subsequently on the Overall Risk Score.

In Scenario A, we vary the average number of vulnerabilities per IP, keeping the total exposed IPs and vulnerable IPs constant. The results in Figure 13 show again a linear growth in Exposure, as expected.

In Scenario B (Figure 14), while we let every host expose ten vulnerable services, we progressively add more vulnerable IP addresses, letting the total address-space size grow. Exposure rises with the square of the vulnerable-IP tally. The red dashed curve in Figure 14 therefore climbs

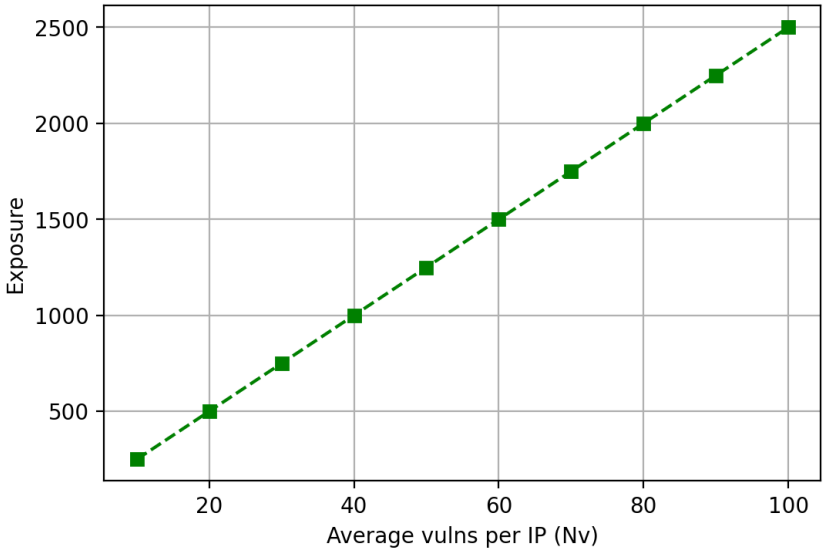

Figure 13: Scenario A: Exposure vs. Avg. N of Vulnerabilties per IP

steeply: doubling the vulnerable surface from 20 to 40 hosts quadruples Exposure, and moving from 50 to 100 hosts multiplies it by four once again. The plot confirms that even modest expansion of an exploitable footprint drives a non-linear surge in Exposure, underscoring how quickly overall cyber-risk balloons when a network is allowed to sprawl without hardening each additional node.

Finally, in Scenario C, we examined the variations in the likelihood (L). Here, we keep the technical attack surface constant, the exposure is fixed at 500, and we increase only the likelihood score from 1 to 15. Because the raw-risk formula is a weighted formula, every unit step in L adds exactly 0.5 to the total. The blue dashed line in Figure 15, therefore, increases with perfect linearity, moving from about 250.5 when $L = 1$ to roughly 257.5 when $L = 15$. This confirms that, once the vulnerable footprint has been set, our metric remains proportionally sensitive to shifting threat likelihoods.

Lastly, we over-laid the results from the two experiments in which

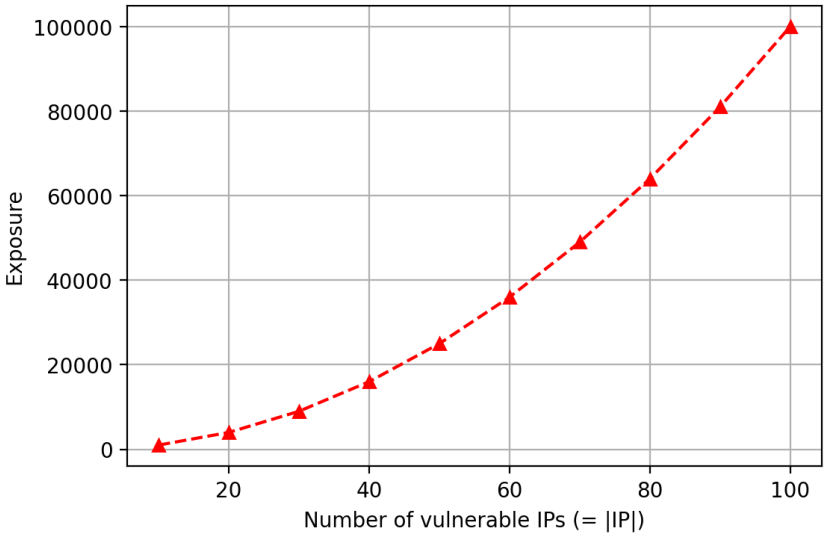

Figure 14: Scenario B: exposure vs. TotalVulnIPs

Exposure changes, Scenario A (varying the number of vulnerabilities per IP) and Scenario B (varying the count of vulnerable addresses), and plotted the corresponding Risk Raw (RR) values against the resulting Exposure scores. As shown in Figure 16, the points from both scenarios fall on the same straight line: regardless of whether Exposure grows because each host becomes more vulnerable or because the vulnerable footprint becomes "wider" (more affected IPs), the raw risk rises in exact proportion to the Exposure term in the formula. Scenario C is omitted from this overlay because its Exposure is held constant while Likelihood is swept. The joint plot confirms that our metric responds to any of the technical drivers in a linear way.

Sensitivity Analysis

To validate the robustness of our methodology and identify the weight of our metrics on the Overall Risk Score, we conducted a sensitivity analysis using the tornado diagram approach. With this analysis we aim to

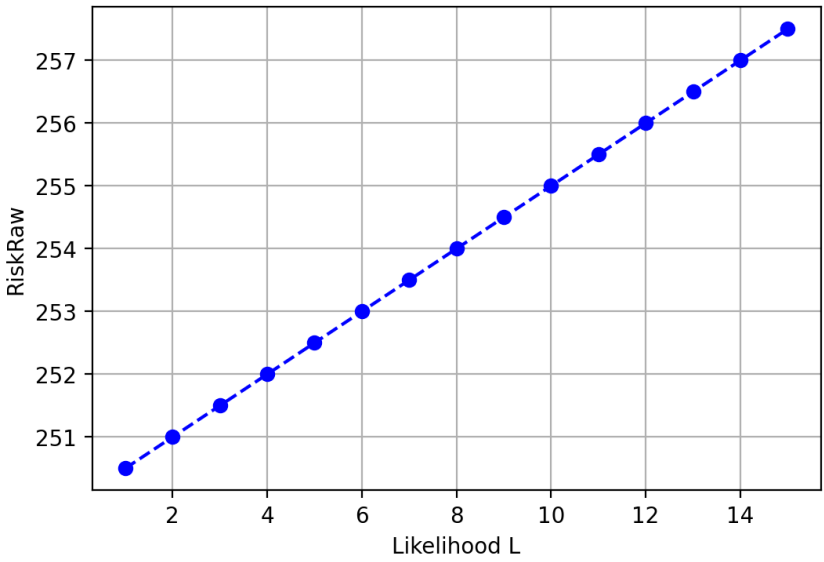

Figure 15: Scenario C: Risk Raw vs Likelihood

demonstrate how REF responds to variations in input parameters, establishing confidence in the REF's reliability and discussing the key drivers of cybersecurity risk assessment outcomes.

The tornado diagram method evaluates the impact of each input parameter on the output by varying one parameter at a time while holding all others constant at their baseline values. For each parameter, we calculated the Overall Risk Score using lower bound (10th percentile), expected value (50th percentile), and upper bound (90th percentile) estimates. This one-at-a-time (OAT) approach allows us to isolate and quantify the individual contribution of each parameter to overall risk score variability, following established sensitivity analysis practices in risk engineering [61].

We selected three representative organizations from our dataset: Company 2 (high risk, R=4.87), Company 3 (moderate risk, R=4.07), and Company 1 (lowest risk, R=3.13). These organizations represent different vulnerability profiles, through which we can assess whether sensitivity pat-

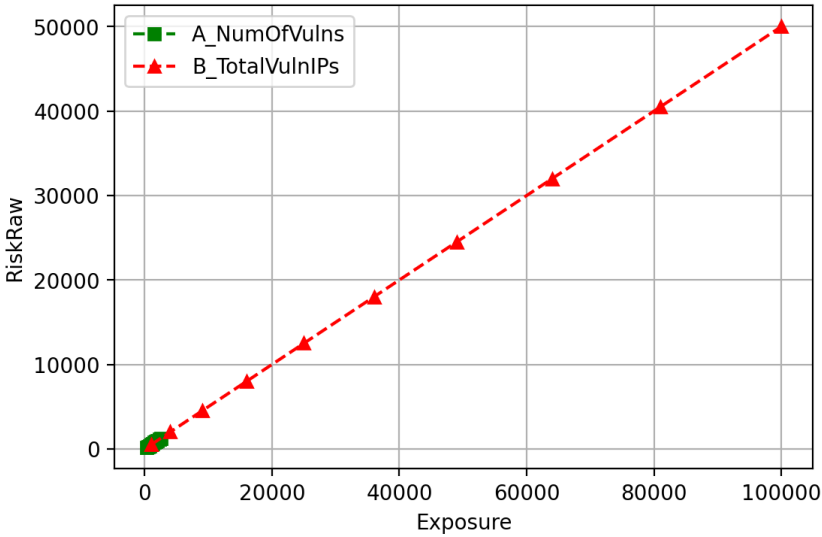

Figure 16: Risk Raw vs exposure

terns remain consistent. For each organization, we varied the following six key REF input parameters from the observed baseline value: Total Exposed IPs: ±50%; Total Vulnerable IPs: ±50%; Total CVE Count: ±40%; Total Exploits Available: ±30%; Average CVSS Score: varied between 5.0 (medium severity threshold) and 9.0 (critical severity), reflecting the range observed in our dataset; Adversary Interest (A): varied between 1 (low targeting motivation) and 3 (high strategic value).

Figure 17 shows the tornado diagrams for Company 2 (the other diagrams are on our online repository [80], with parameters sorted by decreasing influence (widest bar at bottom, following standard tornado diagram approach). The horizontal bars illustrate the range of risk scores achievable by varying each parameter between its lower and upper bounds, while the vertical red dashed line indicates the baseline risk score calculated using observed values. The width of each bar directly represents that parameter's sensitivity: wider bars indicate parameters that, when varied, produce larger swings in the Overall Risk Score. The sensitivity

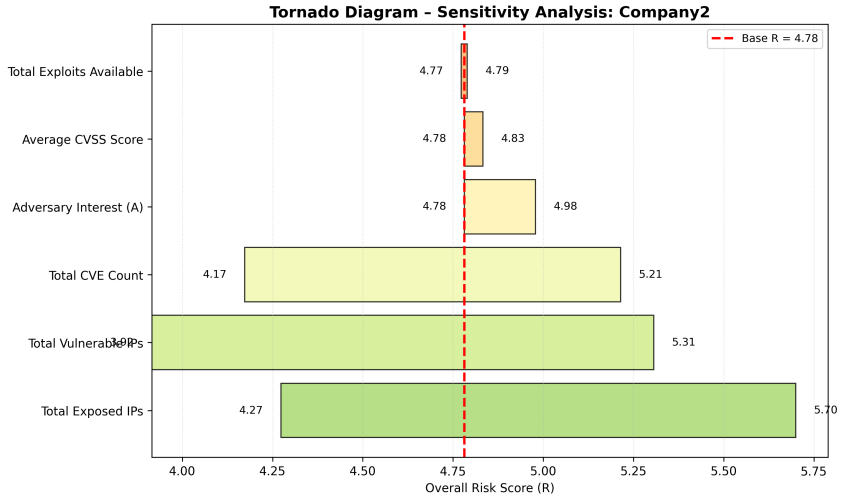

Figure 17: Sensitivity Analysis Company 2

analysis reveals consistent patterns across all three organizations, providing useful information about REF's behavior and validating our design decisions.

The sensitivity analysis highlights several consistent patterns across all organizations. The size of the external attack surface emerges as the most influential factor: variations in the number of exposed IPs cause the largest absolute changes in the Overall Risk Score, confirming that the span of an organization's externally visible infrastructure is the main driver of cyber risk exposure. Closely following, the concentration of vulnerable hosts is almost equally critical. Increases in the number of unpatched or misconfigured systems amplify risk. Parameters related to individual vulnerability characteristics, such as the total CVE count, average CVSS score, and the number of available exploits, have a moderate but consistent influence. These factors matter, yet their impact remains secondary to the structural properties of the attack surface itself. Adversary interest is modeled uniformly as A=1 in our main analysis. Sensitivity tests show that variations of A between 1 and 3 affect the resulting

risk score, demonstrating that refining the estimation of adversary intent, using sector-specific threat intelligence or geopolitical indicators, could improve the accuracy of REF, especially for organizations operating in contested domains or managing strategically valuable infrastructure.

This sensitivity analysis demonstrates that REF responds predictably and proportionally to input variations, with no evidence of unstable behavior. The most influential parameters, attack surface size and vulnerable host concentration, align with established cybersecurity principles, and the framework maintains consistent sensitivity patterns across organizations of different scales and risk profiles, supporting generalizability.

Finally, our analysis validates REF's design choices, particularly the emphasis on attack surface breadth and vulnerable host concentration, and demonstrates that the framework responds predictably to realistic parameter variations.

7.5.4 Threats to validity

REF offers a structured and reproducible way to assess cybersecurity risk in space organizations, but its validity is subject to several important considerations. These limitations do not invalidate our findings, but they do highlight areas where further refinement is needed.

First, our data collection is based on Shodan and on its filter `org:"..."` tag. This filter is extremely useful for attributing assets to specific entities, but it does not guarantee that the assets identified are part of the core or mission-critical infrastructure. Organizations may operate services under different registered names, third-party domains, or through partners and subsidiaries that may not be captured by this filter. Not all assets captured by the org filter may actually belong to the organization, especially in cases of dynamic IP assignment or misattributed metadata. This can create uncertainty in the completeness and precision of the dataset. However, although the tag may not accurately reflect the true boundaries of an organization, it still provides a consistent and reproducible view of exposed services. Allowing exposure levels to be compared across many entities in the space sector.

Shodan operates through periodic scans that provide only partial, time-bound snapshots of the public Internet. The exposure data is therefore ephemeral: an IP found vulnerable today may be patched tomorrow, or entirely removed from service. Longitudinal sampling over several months can mitigate volatility and reveal persistent misconfigurations or the regular emergence of the same weaknesses, which is a valuable signal of systemic risk.

Another limitation lies in the simplification used when assigning adversary interest. In the current implementation, the adversary interest factor is set uniformly to 1 across all organizations. This assumes an equal level of attractiveness to threat actors, which does not reflect real-world geopolitical or economic dynamics. Some organizations, such as those operating in defense, launch capabilities, or dual-use technologies, may be significantly more targeted than others, especially in certain countries.

Additionally, the framework does not assess the intent, capability, or behavior of specific threat actors. The presence of a known vulnerability does not imply imminent exploitation, and the existence of an exploit does not confirm attacker interest. Without telemetry data, incident logs, or threat intelligence integration, the REF approach remains at the level of potential risk rather than realized threats.

The methodology also presumes a consistent link between vulnerability exposure and organizational impact. A small number of exposed, yet highly sensitive, assets could pose a greater risk than hundreds of low-impact devices. REF does not incorporate contextual factors such as asset criticality, system isolation, or compensating controls, all of which play a significant role in actual risk realization. By highlighting the quantity and severity of internet-facing vulnerabilities, our methodology provides asset owners with essential data that they can easily cross-reference with their own criticality inventories and compensating controls. REF is not designed to replace internal risk models; instead, it enhances them with externally verifiable evidence.

Finally, the vulnerability scoring itself relies on public CVSS data, which is a generalized and often conservative estimate. CVSS scores may

be outdated, incomplete, or misaligned with specific configurations used in operational systems. However, it remains the most widely adopted severity measure, keeping our results comparable with vulnerability management practices already established across the space industry.

In summary, while the REF is a scalable and repeatable approach to quantifying exposure and likelihood, its outputs should be interpreted in light of these limitations. Future work may improve the framework's validity by integrating more contextual signals, refining attribution methods, and incorporating live threat intelligence data.

7.6 Policy and Security Implications

REF is primarily a tool for assessing the cyber exposure of organizations based on a series of observable data, but it can also support the implementation of broader cybersecurity strategies and regulatory frameworks for critical infrastructure protection. Governments and institutions around the world are adopting more strict cybersecurity policies to address the evolving threat landscape in the space domain, and this requires new operational tools that can assist in translating these policies into measurable actions. In this respect, REF contributes by providing a method to assess external risk exposure, making it a building block within a comprehensive, multi-layered cybersecurity policy implementation.

In this section, we discuss how REF can support some policy provisions of the EU's NIS 2 Directive, which establishes harmonized requirements for risk management, incident reporting, and supervision across critical sectors, including space, and of the USA Executive Order Strengthening and Promoting Innovation in the Nation's Cybersecurity.

7.6.1 REF for NIS2 Cybersecurity Requirements

Analyzing the NIS 2 Directive makes it clear how REF aligns with its emphasis on risk management and visibility over the digital infrastructure of essential and important entities. In particular, REF can assist in

fulfilling the requirements outlined in Article 21 of the Directive, which obliges organizations to adopt technical and organizational cybersecurity risk-management measures. REF mechanisms help continuously monitor and evaluate the exposure of an organization's network-facing assets. This complements policy requirements for entities to maintain updated inventories of vulnerabilities, to assess the severity of known weaknesses, and to identify systems that are directly exposed to the Internet.

REF can also contribute to operational cybersecurity obligations under Articles 23 and 24, which mandate timely incident notification and coordinated vulnerability disclosure. Helping organizations identify exploitable vulnerabilities in real time, REF can support earlier detection of potential entry points for breaches or risky configurations that might otherwise go unnoticed until exploited. Moreover, REF can also support the implementation of sectoral cybersecurity policies and coordinated risk assessments as required by Article 13. Since REF is designed to scale across multiple organizations and rely on online available data, its results can be aggregated and compared to reveal trends across different entities or sectors. Supervisory authorities and national competent authorities could use REF-based insights to perform comparative exposure analysis or prioritize oversight and audit activities.

However, REF is not a comprehensive cybersecurity solution, and it does not replace the broader suite of measures required by NIS 2. For example, it does not account for internal controls, organizational governance, supply chain risks, staff training, physical security, or encryption standards. It cannot address strategic, legal, or contractual dimensions of risk, nor does it include mechanisms for managing incident response, crisis communication, or business continuity. In short, REF does not satisfy the full scope of Articles 21–24 on its own.

Instead, our methodology should be understood as a practical tool that complements broader compliance and risk management strategies, an effective early-stage mechanism for identifying and quantifying externally visible risks. It can be integrated into wider risk assessments, such as those required by Article 20, to ensure that organizations begin their

cybersecurity work from a clear and empirical understanding of where they are most exposed. Alongside asset classification, threat modeling, and penetration testing, REF supports an organization's ability to comply with the NIS 2 Directive in a data-informed way.

7.6.2 REF supporting the European Space Act

The EU Commission released the EU Space Act proposal on 25 June 2025 [106]. The Act aims to consolidate previous strategies into a unified legal framework for all space activities within the European Union.

The Act is built on three key pillars: safety, resilience, and sustainability. Safety is prioritized through improved space traffic management (STM), enhanced traceability of space objects, and a well-defined strategy for managing space debris. Resilience is achieved by implementing binding cybersecurity requirements to better protect European space assets and infrastructure. Sustainability is promoted by making environmental impact assessments mandatory for space missions and encouraging compliance and innovation in areas such as in-orbit servicing technologies and satellite end-of-life management.

The Act introduces a sector-specific cybersecurity framework tailored to space infrastructure, addressing gaps left by existing legislation such as the NIS2 Directive, which sets cybersecurity requirements for medium and large-sized public electronic communications networks and certain ground-segment operators, but it does not cover key areas of the space sector. This includes spacecraft, Earth Observation and Space Situational Awareness satellites, micro-operators, launch services from outside the European Union, and critically, Union-owned constellations.

The proposal calls for a dedicated risk management regime for space operators. Under Article 75, the Act identifies itself as *lex specialis* over NIS2: for any operator already classified as an *"essential"* or *"important"* entity, the space-specific requirements outlined in the Act take precedence over the more general provisions of Article 21 of NIS2. Overall, this means that operators will be required to conduct thorough risk assessments, implement security measures proportional to the criticality of

their missions, and maintain continuity protocols across all operational phases (Articles 78-88). A new Union Space Resilience Network (EU-SRN) will facilitate coordinated responses to major cyber incidents and further support harmonization across member states (Article 94) [106].

Article 78 obliges operators to identify, reassess, and treat vulnerabilities throughout the lifecycle of space missions, and it empowers the Commission to issue delegated acts that standardise threat-modelling methods and ensure comparability of risk assessments [106]. Our REF framework can help operators to fulfill such obligations: indeed, it generates the evidence, such as delegated acts, that are needed: a time-stamped map of exposed services, the CVEs linked to each host, exploit maturity, and a composite Risk score.

Asset governance under Article 80 depends on inventories that are drawn up by individual space missions and include the origin and current physical location of assets, including the identification of a cloud-based service. Again, our REF framework can support these activities through its discovery phase, which collects some of this data, pulling ASN, geolocation, and hosting-provider data.

Article 88 makes Threat-Led Penetration Testing mandatory before launch and every three years thereafter, with the scope to be chosen considering the risk assessment referred to in Article 78(2) [106]. Our REF framework can support organizations with the requirements of this article. Indeed, the ranked list of Internet-facing hosts produced by REF lets security teams transform that legal wording into a concrete test plan: start with the endpoints sitting in the highest-risk decile, verify whether the theoretical exploit paths can be demonstrated in practice, and document the results against REF's baseline so improvements show up as a measurable downward risk.

Article 92 introduces a formal supply-chain risk-management framework and instructs operators to inventory "critical assets of non-Union origin" and collect their dependence on those suppliers [106]. Our REF framework can narrow that task by flagging which external libraries, SaaS consoles, or third-party services account for the largest share of exploitable CVEs in the mission, helping procurement teams channel their

due diligence and their contract clauses towards the vendors with less exposure. These provisions, even if just part of a proposal, point toward a continuous, evidence-based risk quantification from best practice to legal requirement. REF can deliver and support some of these measurements that Chapter II calls for.

7.6.3 Applying REF to the Cybersecurity Oversight of U.S. Space Infrastructure

By examining other recent policies where REF can contribute, we identified an interesting initiative in the U.S. that represents one of the first policies explicitly demanding and designing some cybersecurity requirements for the space sector. In January 2025, before the end of his mandate, the 46th President of the United States issued the "Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity". The Order aims to strengthen the cybersecurity posture of the United States across multiple critical infrastructure sectors, including space. This document follows up on prior cybersecurity strategies and executive orders, expanding regulatory oversight, strengthening security standards, and emphasizing the role of government agencies and private sector stakeholders in reducing cyber threats.

The U.S. government recently responded to the increasing cyber threats to national security by implementing stricter cybersecurity frameworks, including Executive Order 14028 [219] (Improving the Nation's Cybersecurity) and the National Cybersecurity Strategy. However, "*the rapid expansion of digital infrastructure, the emergence of new attack vectors, and the growing importance of space-based assets* [219]" needed further policy advancements, leading to this 2025 Executive Order.

A section of the Executive Order focuses specifically on the space sector, acknowledging the rising cybersecurity risks associated with satellite networks, space-ground communication systems, and federal space programs. The document explicitly states that "as cybersecurity threats to space systems increase, these systems and their supporting digital infrastructure must be designed to adapt to evolving cybersecurity threats and

operate in contested environments", underscoring the need for continuous assessment, rigorous vulnerability management, and secure software development in all aspects of space operations.

Among the primary requirements set forth in the Executive Order for the space sector, the following stand out:

1. *Mandatory Cybersecurity Assessments*: The order requires federal space agencies and their contractors to perform continuous cybersecurity assessments of their space-based infrastructure.

2. *Enhanced Procurement Security*: The directive compels NASA, the Department of Commerce, and the Department of the Interior to review and update cybersecurity requirements within the Federal Acquisition Regulation (FAR) to ensure that space-related contracts enforce stricter cybersecurity controls. This measure aims to prevent vendors with inadequate cybersecurity postures from supplying critical space technologies.

3. *Protection of Satellite Communications and Space-Ground Links*: A major aspect of the Order is the security of satellite communications. Indeed, it requires "all new civil space systems to incorporate risk-based, tiered cybersecurity requirements to protect command and control functions, detect and mitigate anomalous activity, and ensure secure software and hardware development practices."

4. *Creation of a Space Cybersecurity Oversight Framework*: The National Cyber Director is tasked with submitting a comprehensive study on space ground systems managed by Federal Civilian Executive Branch (FCEB) agencies, including an inventory of systems and recommendations to improve cyber defenses. This initiative seeks to enhance oversight, provide cybersecurity benchmarks for space agencies, and promote cross-agency cooperation in cybersecurity efforts.

5. *Strengthening Secure Software Development in Space Systems*: Given the increasing reliance on commercial and open-source software

> in space operations, the Executive Order mandates that software providers follow strict cybersecurity guidelines and demonstrate compliance with secure software development standards. The order states that "software providers must also address how software is delivered and the security of the software itself, with the Federal Government identifying a coordinated set of practical and effective security practices for space system software development."

Our REF methodology closely aligns with several cybersecurity concerns outlined in the Executive Order. Specifically, it addresses the need for continuous assessments, testing, and exercises to verify the cybersecurity capabilities of federal space systems and their supporting infrastructure. REF can be adopted to evaluate the external attack surface of space-related assets, particularly focusing on ground segment infrastructure and Internet-connected components. REF can therefore aid in fulfilling the continuous assessment mandate by identifying externally exposed and potentially vulnerable services across space system operators.

Additionally, the Executive Order mandates that agencies review and update cybersecurity requirements in civil space contracts, using a risk-based, tiered approach (Section 3(e)(i)) [219]. REF could be part of this process as a monitoring mechanism to support the implementation and enforcement of such requirements. For instance, REF-derived metrics could be used to validate that Internet-facing components of space systems comply with security baselines over time. It can therefore be used as part of a verification layer in contract compliance monitoring. REF's methodology could inform risk tier assignments as it is able to identify systems with a high number of exploitable services or critical CVEs.

However, REF should not be considered as a standalone solution for fulfilling policy requirements. Instead, it offers a data-driven monitoring component that can be integrated into a wider risk assessment and cybersecurity management process. In particular, it can be the first layer for detecting exposure and identifying organizations or systems that may need deeper inspection and additional safeguards. Its applicability to ground components of space infrastructure makes it a practical addition

to the cyber resilience toolkit outlined in the policies described in this section and in others that will come, such as the European Space Act [82].

7.7 Conclusion and Future Research

Our framework stems from the need to quantify cyber risk in the space sector (**RQ1**) and to do so in a clear and repeatable way (**RQ2**) from observable data on the external attack surface of space sector organizations (**RQ3**). With the Risk Exposure Framework, we built an indicator that combines Exposure (size of the exposed infrastructure) and Likelihood (probability that vulnerabilities are actually exploited), thus mapping to the requirements of major cybersecurity policies (NIS 2 in the EU, Executive Order 14144 in the US) (**RQ4**).

Addressing **RQ1**, this paper measured cyber risk through the Risk Exposure Framework (REF), which combines data on exposed Internet assets and known vulnerabilities into a quantifiable indicator. Our approach responds to the need for a measurable link between high-level policy requirements and concrete technical assessments. Translating exposure and vulnerability data into a single metric, REF can allow organisations to monitor the effectiveness of cybersecurity measures and to support both technical and governance decisions.

RQ2 focused on repetability and clarity: REF proved both clear and repeatable, as the same data collection and computation process was applied across several space-sector organisations, allowing for direct comparison of their risk levels. The resulting distributions showed consistent patterns of exposure and exploitability, confirming that the method can be reused for longitudinal studies. The reproducibility of the metric and the transparency of its components address the need for a standardised way to track cyber risk across organisations.

Through **RQ3**, we aimed to investigate the level of exposure of the space sector. The results showed that space organisations remain significantly exposed to risks originating from Internet-connected systems. Out of roughly 100,000 identified assets, about 4% contained known vulner-

abilities, with risk levels varying widely depending on how those vulnerabilities were concentrated. As previous attacks have demonstrated, the most critical exposure originates from the ground and user segments, confirming their likely role as entry points in space-related incidents.

RQ4 inquired about the possibility of connecting security measures to policy requirements. We demonstrated how REF can be directly related to European cybersecurity policies, as REF's indicators correspond to the continuous risk assessment and vulnerability management obligations defined under NIS2, and to the monitoring and oversight provisions foreseen in the proposed EU Space Act. Our framework, therefore, provides a concrete technical foundation to support regulatory compliance and sector-level supervision, and can easily link empirical evidence to policy objectives.

From our experimental results, we learned several key lessons. First, the high number of unpatched CVEs highlights how velocity and consistency in patching outrank perimeter breadth; large operators accumulated extreme Exposure scores, probably due to update cycles lagging behind service deployment, whereas limited infrastructures moved into high-risk territory only when critical patches remained outstanding. Second, data shows how the weakest technical layer is still the basic web and cryptographic stacks: Apache HTTP Server, Nginx, OpenSSL, jQuery, demonstrating that dependency management rather than exotic satellite-specific code is the leading attack vector. Third, small does not equate to safe: entities with a few dozen public hosts nevertheless posted high Overall Risk scores, because exploit availability magnified each remaining flaw.

REF should be understood as a complementary tool within a comprehensive cybersecurity assessment strategy for space, rather than a standalone solution. While REF excels at identifying and quantifying ground-segment exposure, where most cyberattacks originate, it does not replace other essential security assessment methodologies such as onboard system audits, hardware security testing, or mission-critical system penetration testing. Organizations implementing REF should integrate its findings with broader security assessments that cover space-

segment vulnerabilities, insider threat analysis, and mission-specific risk factors that cannot be captured through external network reconnaissance.

The framework's ground-segment focus aligns with current threat landscapes and policy requirements; however, space operators should ensure that REF-based assessments are part of a comprehensive security program that addresses all mission segments and operational phases.

7.7.1 Future Research Directions

Future research should build upon the methodology proposed in this study. One option involves integrating additional tools for identifying and characterizing ICDs beyond Shodan. Platforms such as Censys, ZoomEye, or GreyNoise could be combined to provide broader visibility into exposed space infrastructure and validate findings across different data sources. Additionally, vulnerability data could be enriched with threat intelligence feeds, including indicators of compromise (IOCs), active exploit tracking, or ransomware group targeting patterns, which would support the estimation of likelihood.

Asset criticality is one measure that is not completely addressed in REF. This would enhance the risk model by weighting exposures not only by technical severity but also by their potential mission impact, helping prioritize remediation across infrastructures. Another underexplored domain is the temporal analysis of exposure trends, which would assess how organizational risk evolves over time and how effectively vulnerabilities are being mitigated. While offering insights into the cybersecurity exposure of space sector organizations, our approach has several important limitations. First, it relies solely on publicly accessible information, meaning that only internet-facing systems are captured. Internal infrastructure, assets protected by firewalls, VPNs, or hidden through filtering techniques, are excluded from analysis. As a result, the risk scores produced here reflect only a subset of the true attack surface, what is externally visible, and may underestimate risks tied to internal system vulnerabilities or insider threats. Future work should therefore widen the observation perimeter by fusing external scan re-

sults with data drawn from internal vulnerability scanners, EDR agents and industrial inventories, so that the model also captures risks tied to non-internet-facing assets. Second, the framework's dependence on CVE identifiers, while useful for standardization and comparison, overlooks operational context. The methodology does not consider the business or mission criticality of the exposed systems, nor whether compensating controls, segmentation, or isolation mechanisms are in place. Two hosts with the same vulnerability may pose vastly different risks depending on how they are deployed and secured. Similarly, this approach cannot account for custom or proprietary configurations that might either mitigate or amplify the vulnerability impact. A second research track should therefore aim to link business or mission-criticality to every host by linking CVEs to impact scores derived from business-impact assessments.

A further limitation lies in how we infer exploitability. The presence of an exploit in public databases such as Vulners is a necessary but insufficient condition for actual threat activity. The framework does not detect ongoing attacks, zero-day vulnerabilities, and it assumes that all exploits are equally likely to be leveraged, which may not reflect the strategies of sophisticated threat actors. Exploitability estimates can be refined by combining real-time threat-intelligence feeds, measurements of exploit weaponisation in the wild and machine-learning models that rank the effort required to abuse each vulnerability.

In addition, the reliability of service-level data, especially from Shodan, requires careful consideration. Shodan may label a host as "vulnerable" even if no specific open port is visibly tied to a CVE, due to how its scanning engine interprets software banners and metadata. For example, a host running an outdated operating system may be marked as vulnerable even when only non-vulnerable ports are open. Shodan's scans are periodic and port-limited: not all ports are checked at every scan cycle, and not all responses yield full banner data. As a result, an IP might be listed with vulnerabilities but show no active services, or vice versa. In this regard, the reliance on banner-based services such as Shodan can be mitigated by cross-checking multiple scanners or similar tools.

Chapter 8

Competing Visions: A Comparative Study of Space Security from Discourse to Practice in China, the US, and the EU

8.1 Introduction

"*America innovates, China copies, Europe regulates*" has become a convenient catchphrase for describing the technological competition dynamics in the world. The space sector seems, at first glance, to reinforce this narrative: Chinese reusable launch concepts remind SpaceX's Falcon 9, while the European Union advances an ambitious Space Act centered on safety, resilience, and sustainability. However, these claims describe just outcomes while hiding the political, institutional and strategic processes through which space powers arrive at them.

Existing literature on space security and governance reflects this limitation, as a substantial part of the literature examines national space strategies, military doctrine or commercial programmes in isolation, while

another part focuses on specific policy instruments or technical risks. As a result, we lack a systematic understanding of how major space powers conceptualise space security, how these conceptualisations are embedded in governance structures, and how institutional arrangements shape regulatory and strategic choices over time.

Space has become integral to economic activity, critical infrastructure, and military operations, while the number of actors and objects in orbit continues to grow. At the same time, the concept of space security is evolving, acceptable thresholds of risk and interference are changing, and the balance between military, civil, and commercial activities is blurring. Space security is articulated differently across political systems, reflecting divergent priorities, threat perceptions, and state–market relations.

This chapter is adapted from the paper "Competing Visions, Diverging Trajectories: A Comparative Study of Space Security from Discourse to Practice in China, the US, and the EU" (working paper, co-authored with Thao Pham, Centre for Security, Diplomacy and Strategy, Brussels School of Governance, VUB). The chapter addresses the concept of space security through a comparative analysis of China, the United States, and the European Union. It argues that differences in space security outcomes are best understood not as simple expressions of power or technological capability, but as the product of distinct governance models and strategic doctrines. These models are shaped by political institutions, strategic culture, and techno-industrial objectives, and they condition how risks are identified, managed, and regulated across the space domain.

The analysis is guided by four research questions:

- **RQ1** How do China, the United States, and the European Union conceptualise space, and space security in particular, in their official strategic documents?

- **RQ2** What governance arrangements do they use to organise space security, and how do these arrangements affect approaches to resilience, risk, and regulation?

- **RQ3** How is space security governed in practice across military, civil, and commercial domains?

- **RQ4** To what extent do the political, technological, and economic dimensions of space cybersecurity governance differ across the three actors, and what does this divergence reveal about broader patterns of technopolitical ordering in contested domains?

The paper advances the claim that each actor has developed a distinct space doctrine governance model. In the United States, space security is structured around military command, deterrence, and the protection of freedom of action, with commercial actors increasingly integrated into national security objectives. In China, space security is embedded within a developmental framework that combines technological advancement with strong state oversight and strategic control. In the European Union, space security is approached primarily through regulatory harmonisation, risk management, and the external projection of norms, reflecting the Union's broader governance logic.

The chapter proceeds as follows. The first section reviews the relevant literature and positions the contribution within existing debates on space security and technology governance. The second section outlines the methodological approach and comparative framework. The subsequent sections analyse China, the United States, and the European Union in turn. The final section compares the three models, highlighting their implications for international cooperation, commercial regulation, and strategic stability, as well as emerging areas of convergence, including resilience, dual-use systems, and closer ties between military and commercial space activities.

8.2 Literature review

Space development and governance arrangements in the US, China, and the EU have been studied extensively, from inventorising technological assets to how space power is exercised through institutions, norms, and

regulatory influence [165] [311]. These studies offer dive into asymmetries in influence, divergent institutional trajectories, and the growing salience of space as a domain of geopolitical competition.

A prominent strand of research focuses on material power and rule-shaping capacity, particularly in the context of US-China rivalry. Several case studies tracked the evolution of American and Chinese space capabilities from their inception, showing how China rapidly narrowed technological gaps, while the US has remained a step ahead in part due to export controls, alliance structures, and the success of its commercial sector [552][369]. More recent work shifts the focus to its soft power. Morin & Tepper, for example, investigate a large dataset of space organisations and agreements to assess how an extensive global network of partnerships has enabled the US to diffuse its norms globally [371]. As impressive as how China has elevated its capabilities, it has not been able to translate them into equivalent influence over the rules of the game.

In addition, Freeman's analysis of evolving narratives of "global commons" highlights the fluidity and strategic use of norms [238]. Her work shows how the US and China have effectively reversed their traditional positions on the framing of outer space, crystallising these shifts in competing initiatives such as the Artemis programme and the International Lunar Research Station [464].

Klimburg-Witjes traces the process of securitization in European space policy, showing how space shifted from being framed as a civilian, economic domain to a security domain [326]. The author describes this as boundary work, the process of redefining which issues belong to security versus which belong to economics or science. Her work shows how framing changes are never neutral; they involve reshaping institutions, bureaucracies, and who has authority over decisions. In Europe's case, the securitization boundary work shifted authority from civilian agencies toward military and defense actors.

Burke-White and Williams provide a comprehensive mapping of space governance frameworks used by the US, China, and Russia, arguing that existing international rules from the 1967 Outer Space Treaty are no longer adequate for managing modern competition [69]. The authors

show that these competing models reflect incompatible views on property rights, military activities, and who should govern celestial bodies. Their work demonstrates that space governance is not stalled because countries lack technical knowledge, but because they fundamentally disagree on what the rules should be.

A parallel literature examines Europe's distinct trajectory of space governance. Brandenburg and Lieberman attribute Europe's fragmented space governance to path-dependent decisions and constrained geopolitical positioning [64]. In other words, Europe's secondary position in the global power hierarchy (relative to the US and former USSR) constrained its development of a military space role, regardless of institutional design. This suggests that governance capacity in space security is partly a function of power distribution. However, changes are underway as many observations point to securitisation of EU space policy, marked by the erosion of traditional civilian-military boundaries and the creation of new security-focused agency restricted to EU member states [326]. This development might signal a reconfiguration of Europe's vision of space governance, bringing it closer to state-centric models seen in the US. Beyond Brandenburg & Lieberman, scholars in comparative politics and international relations have examined how different regime types produce different institutional solutions to similar problems. Varieties of Capitalism literature, by Hall et Al. [270] and work on "institutional complementarities" by Amable [35] show that institutional choices in one domain (e.g., labor markets, innovation systems) reinforce and stabilize choices in others. Similarly, space governance institutions do not stand alone, they interact with broader national innovation systems, defense procurement processes, and diplomatic strategies.

These contributions share a limitation that motivates this paper. They tend to explain divergence primarily at the level of outcomes rather than the processes through which those outcomes are assembled. This gap can be addressed by examining the intermediate steps of which priorities are articulated and translated into practices. Doing so makes it possible to assess how similar vocabulary can co-exist with markedly different governance models, and how they accumulate into durable patterns of

divergence.

8.3 Theoretical framework

This chapter examines how space security is conceptualised and governed differently across China, the United States, and the European Union. The central premise is that differences in strategic discourse and policies come not only from different threat environments but also from different problem definitions. How an actor defines space security, what it understands the threat to be and which solutions are appropriate, shapes institutional arrangements and governance choices.

Problem definition is considered mainly as a political act, and a culturally mediated process reflecting deeply rooted assumptions about security, sovereignty, and the proper role of the state [312]. How an issue is defined depends partly on objective data: space is congested, contested, and cyber incidents are increasing, but more importantly on how problems are socially constructed. The interpretation of the same empirical phenomenon varies across actors, reflecting different assessments of risk and different institutional narratives [335].

The United States operates within a strategic culture that privileges military primacy and freedom of action. Its narrative centres on the United States as the lead actor in space, utilising frameworks to maintain American dominance. This shapes how threats are identified (challenges to technological superiority) and which solutions are preferred (military deterrence, export controls, technology leadership).

China operates within a strategic culture anchored in historical memory and technological aspiration. Its narrative positions China as reclaiming its position as a leading power. Space is framed as critical to undoing historical wrongs and demonstrating China's legitimacy. This shapes threat identification (challenges to rising status and sovereignty) and preferred solutions (state-directed development, centralised control, technological self-reliance).

The European Union operates within a strategic culture focused on rules, harmonisation, and negotiated governance. Its narrative empha-

sises space as a domain for common benefit, requiring regulatory frameworks that balance security with market access. Threats are defined as fragmentation and uneven risk treatment across member states, and solutions emphasise standards harmonisation.

Problem definitions develop and crystallise over time through policy discourse and institutional practice. An actor's first successful framing of a problem creates a first-mover advantage. As actors invest resources in capabilities aligned with their problem definition, those investments create path dependencies that make shifting course increasingly difficult. What begins as a difference in framing gradually becomes embedded in budgets, institutions, and technical standards.

This framework treats policy language as evidence of genuine problem definition. Discourse analysis examines what actors emphasise in official documents, and reveals the underlying problem definitions that drive policy choice. Analysing how actors articulate their understanding of space security, we can map the underlying strategic cultures that shape divergent governance models.

This chapter employs problem definition analysis as its core theoretical lens, and examines how space security is conceptualised and framed rather than treating it as an objective threat with self-evident solutions. The central premise is that policy divergence emerges not from different threat environments but from different problem definitions. How an actor defines space security, what it understands the threat to be, whose interests are at stake, and which solutions are appropriate, shapes institutional arrangements and governance choices.

To understand why the three actors pursue such different space strategies, we analyse their official policy documents. What they emphasise repeatedly reveals how they define the problem. Discourse becomes evidence of underlying problem definition.

8.4 Methodology

This chapter follows a qualitative comparative design, examining policy document with the interpretation of themes and discourse. This ap-

proach draws inspiration from established traditions in qualitative content analysis [448] and thematic coding in policy research [439]. Additionally, it borrows from strategic discourse analysis [224] to capture what is said and how it is said.

The analysis is based on a corpus of official policy, strategic, and regulatory documents published between 1995 and 2025. Each document was selected because it reflects the actor's institutional voice in shaping the governance of space, or its broader view of space as a strategic domain. The corpus of policy documents is presented in Table 31.

All texts were analysed in their official English versions, and, in the case of China in their translated versions, to ensure comparability. These documents form a balanced corpus of 38 sources, representing both legislative and strategic instruments.

The analytical process combined three layers of interpretation: thematic classification, cluster mapping, and sentiment analysis. Each document was divided into analytically meaningful paragraphs and manually coded in a table format. Each row represented a paragraph, and the columns recorded the assigned macro-theme, cluster, and sentiment label.

The coding scheme was developed iteratively and is presented in detail in the Codebook (Annex A), which includes definitions, inclusion criteria, and examples for each theme and cluster.

The analysis began with thematic coding, organised around eight broad macro-themes that capture the main dimensions of space governance and policy:

1. Internationalism and Global Governance
2. Peaceful Development and Normative Framing
3. National Development and Technological Advancement
4. Space Infrastructure and Capability Building
5. Military Modernisation and Civil–Military Integration
6. Commercialisation and Industry

Actor	Document	Citation
China	China's Space Program: A 2021 Perspective (State Council Information Office, 2021)	[481]
	National Defence White Papers (From 1995 to 2019), with a total of 10 papers	[480]
	The Regulations on the Administration of Terminal Equipment Directly Connected to Satellite Services (Cyberspace Administration of China, 2025)	[93]
United States	Space Policy Directive-4: Establishment of the United States Space Force (2019)	[222]
	Space Policy Directive-5: Cybersecurity Principles for Space Systems (2020)	[223]
	Defense Space Strategy Summary (Department of Defense, 2020)	—
	Space Capstone Publication: Spacepower (United States Space Force, 2020)	[526]
	National Space Policy of the United States of America (White House, 2020)	[221]
	United States Space Priorities Framework (White House/National Space Council, 2021)	[384]
	A Strategic Framework for Space Diplomacy (U.S. Department of State, 2023)	[513]
	Executive Order: Enabling Competition in the Commercial Space Industry (White House, 2025)	[220]
European Union	EU Shapes its Future Space Policy Programme (Council of the EU, 2019)	[130]
	Council conclusion on "Space as an enabler" (28/05/2019)	[128]
	Council Conclusions on Key Principles for the Global Space Economy (Council of the EU, 2020)	[127]
	Regulation (EU) 2021/696 Establishing the EU Space Programme	[402]
	A Strategic Compass for Security and Defence (Council of the EU, 2022)	[124]
	Joint Communication: An EU Approach for Space Traffic Management (European Commission and High Representative, 2022)	[195]
	Council Conclusions on an EU Approach to Space Traffic Management (2022)	[125]
	Council Conclusions on Copernicus 2035 (2022)	[126]
	European Parliament Resolution on an EU Approach to Space Traffic Management (2022)	[198]
	Regulation (EU) 2023/588 Establishing the Union Secure Connectivity Programme (IRIS²)	[203]
	Council Conclusions on the EU Space Strategy for Security and Defence (2023)	[129]
	Proposal for a Regulation on the Safety, Resilience and Sustainability of Space Activities (EU Space Act) (European Commission, 2025)	[106]

Table 31: Corpus of policy documents analyzed across China, the United States, and the European Union.

7. Space Governance, Law, and Standards

8. Geopolitical Positioning and Strategic Image

The selection of macro-themes was guided by the chapter's research questions and capture space governance as a multidimensional process. Addressing these questions requires an analytical structure that captures both security and military concerns, but also development goals, regulatory practices, economic strategies, and international positioning.

The eight macro-themes, reflect recurring dimensions identified in the literature on space policy, technopolitics, and global governance, and remain aligned with the empirical material.

Internationalism and Global Governance and Peaceful Development and Normative Framing (1-2) capture how actors justify their space activities externally, articulate legitimacy claims, and position themselves within international norms and institutions. National Development and Technological Advancement and Space Infrastructure and Capability Building (3-4) capture space policy and state capacity, industrial strategy, and investments in infrastructure. These themes follow strategic priorities and how they are translated into concrete capabilities, looking at how governance models are enacted in practice.

Military Modernisation and Civil–Military Integration (5) captures how security concerns are included in technological and institutional systems. This theme reflects the growing recognition that contemporary space governance is shaped by blurred boundaries between civilian, commercial, and military uses. It is connected to the second research question and reveals how different actors manage dual-use technologies and security risks through distinct institutional arrangements.

Commercialisation and Industry (6) reflects the increasing centrality of private actors, market mechanisms, and industrial policy in space governance. This theme is necessary to compare how the three cases structure public–private relations, regulate commercial activity, and integrate industry into national or supranational space strategies.

Space Governance, Law, and Standards (7) captures formal regulatory instruments, legal frameworks, and standard-setting practices. This

theme addresses governance in its narrow sense and reflects how authority is exercised through rules, compliance mechanisms, and institutional oversight.

Finally, Geopolitical Positioning and Strategic Image (8) captures how space policy is used to signal status, leadership, and strategic intent. The eight macro-themes provide a necessary structure to organise the corpus and ensure comparability across cases, but many paragraphs address multiple issues or contain highly specific policy discussions that could not be meaningfully distinguished at that level. Relying exclusively on macro-themes risked flattening important variations and obscuring how particular topics were articulated and prioritised within broader categories. For these reasons, an additional layer of categorisation was introduced in the form of thematic clusters. Clusters operate as a finer-grained analytical tool nested within each macro-theme, and deepen the analysis to capture the capillarity of the corpus.

Each macro-theme therefore was further divided into a second-order of 36 clusters, such as cluster 4.1 – Satellite Systems and Applications, 5.2 – Civil–Military Integration, and 7.4 – Debris Mitigation and Space-Traffic Management. The complete list of the clusters is available in the Appendix A. Beyond content, the research also assessed the tone in which space is discussed. Each paragraph was labelled with one of five sentiment categories, capturing how the actor's discourse positions itself strategically, as described in Table 32.

In this analysis, sentiment reveals whether a document seeks to reassure, deter, or project strength. Each paragraph's sentiment was determined through close reading and then cross-checked to ensure consistency.

After coding was completed, the results were aggregated and compared across the three actors. Thematic and sentiment data were used to construct comparative matrices, which helped us to identify the focus of each document. To ensure comparability across documents, actors, and time periods with different corpus sizes, all indicators were normalised. Each thematic or sentiment category was expressed as a proportion of the total number of coded units within the relevant analytical scope (docu-

Table 32: Sentiment Coding Scheme: Tone Analysis Categories

Label	Description	Typical Expressions
Conciliatory	Cooperative and inclusive tone promoting mutual benefit	”peaceful purposes”, ”shared development”, “mutual understanding”
Cautious	Balanced or prudent tone, acknowledging risks or uncertainty	”take effective measures”, ”ensure safety”, ”monitor closely”
Neutral	Descriptive, factual, or technical without evaluative tone	”the mission launched”, ”the system provides data”
Assertive	Confident tone projecting leadership or capability	”will lead”, ”strengthen capacity”, ”enhance deterrence”
Combative	Confrontational or competitive tone	”oppose interference”, ”defend national interests”, ”combat threats”

ment, actor, or year). This normalisation prevents longer documents or larger corpora from dominating the analysis and allows observed differences to be interpreted as relative variations and discursive orientation rather than artefacts of corpus size.

Formally, the normalised share of a category was calculated as:

$$\text{Normalized\_share}(i, u) = N(i, u) / \sum_i N(i, u) \tag{8.1}$$

Where i denotes a coded category (sentiment or thematic cluster), u the unit of analysis, $N(i, u)$ the number of occurrences of category i in unit u, and $\sum_i N(i, u)$ the total number of coded occurrences within that unit.

Frequencies of themes, sentiments, and clusters were treated as indicators of discursive salience; in this framework, the prominence of a theme or tone reflects its importance within an actor's broader strategic narrative. The integration of thematic, cluster, and sentiment layers made it possible to identify both what each actor prioritises (the issues) and how they articulate those priorities (the tone).

Coding is in itself a subjective process, depending on the analyst's familiarity with the policy, legal, and strategic language of each jurisdiction; therefore, minor variations in interpretation may influence thematic classification and sentiment labelling. To mitigate this, a detailed codebook was developed and used consistently throughout the process. Cross-checks and iterative revisions were carried out to ensure conceptual stability and interpretive coherence.

Concerning comparability across political systems. Policy and strategic texts issued by China, the United States, and the European Union vary in institutional style, rhetorical convention, and purpose. This study addresses these discrepancies through contextual interpretation rather than literal comparison, ensuring that coding reflects intent rather than linguistic form.

The following analysis examines how China, the United States, and the European Union articulate space security through strategic discourse and how these framings translate into material capabilities and institutional arrangements.

8.5 China: Space, Strategic Development and State Control

Chinese space governance is framed predominantly as a state-led project of modernization, with space conceptualized as: (1) national development infrastructure essential to state capacity and technological self-reliance, and (2) a venue for legitimizing great-power status through international cooperation and norm-engagement. The tone across official documents is mixed: 46.9% of paragraphs employ assertive language, 24.8% are conciliatory, with minimal use of cautious or combative rhetoric, reflecting a coherent communicative strategy.

In the theme frequencies, shown in Figure 18, Space Infrastructure and Capability Building (Theme 4) accounts for 25% of Chinese discourse, Internationalism and Global Governance (Theme 1) for 22%, and National Development and Technological Advancement (Theme 3) for 17%. The entire space system and its benefits are integrated into a nationalist-

modernization narrative; satellites, launch systems, and interplanetary missions are linked to state capacity, sovereignty, and technological self-reliance.

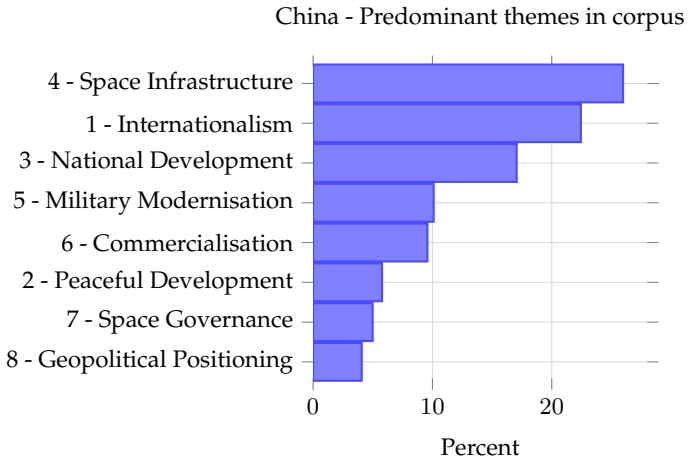

Figure 18: Thematic Distribution in Chinese Space Policy Documents.

The prevalence of Internationalism and Global Governance (23%, increasing by 45 percentage points from 1995 to 2022) redefines sovereignty-driven objectives in the language of responsibility and multilateralism. Temporal tracking suggests space is a domain especially sensitive to external perceptions, particularly from the United States.

Before 2000, Beijing signaled restraint and legitimacy-building through defense white papers employing tags like ”disarmament”, ”arms control”, and ”legal compliance” alongside ”development-oriented” language. Sentiment analysis reinforced this, with disproportionate use of conciliatory (46.8%) and cautious (22.5%) language. During a period when space development risked interpretive escalation, this framing legitimized China’s sustained space interest as a development necessity within prevailing peaceful-use norms.

A pronounced inflection occurred during 2004-2006. Although only two policy documents were published, assertive sentiment rose to 69%, with joint development and security theme coding approaching 89.7%.

This should be seen as an outlier; such rhetoric did not persist in subsequent versions. However, the prominence of capability-signaling, "technological leapfrogging," "independent development," and "strategic importance" showcased China's readiness to scale advanced systems.

In the subsequent decade, the core developmental-capability narrative persisted, but shifted from capacity-building to ecosystem-building, eventually to space governance. Commercialization and Industry (Theme 6) themes rose markedly, accounting for 20% of the 2016 corpus. Language relating to commercial value-chains expanded to 8.3% from 1.1% in 2011.

By 2022, Internationalism and Global Governance reached 45.3% of yearly corpus, with a markedly shifted internal composition. Earlier periods relied overwhelmingly on International Cooperation; however, 2022 data showed remarkable expansion in Multilateral Governance and Treaties, surging to 15.8% of all texts, paralleled by Space Law and Standards reaching 12.3%. This transformation signals a significant shift in China's space diplomacy toward institutional participation and norm-making.

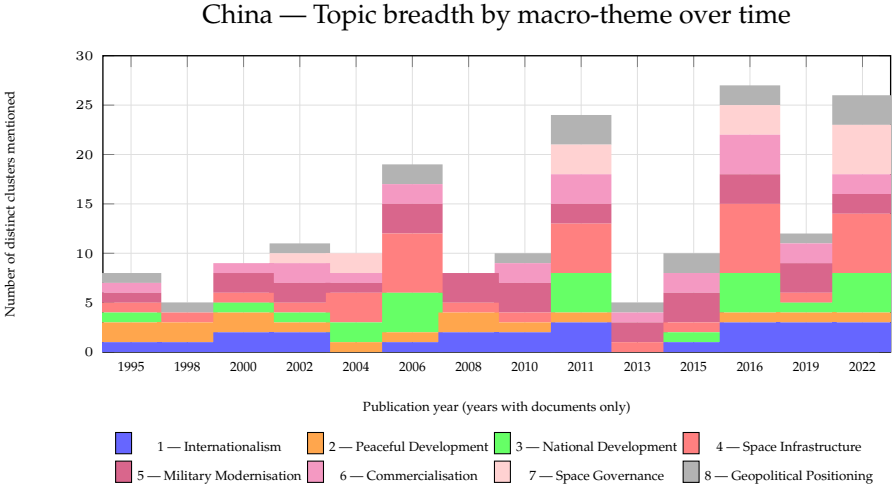

Figure 19: Thematic Breadth in Chinese Space Policy Discourse (1995–2022).

Technopolitical arrangements achieve durability through institutionalization, manifested most clearly in the consolidation of the CCP's space governance under direct Party authority. China's space bureaucracy historically replicated the Soviet model, separating civilian exploration from military operations. This division changed under Xi Jinping. The 2015 military reforms abolished the old structure and created the People's Liberation Army Strategic Support Force (SSF), unifying space, cyber, and electronic warfare under single command.

However, in 2024, the SSF was dismantled and its functions redistributed through a more tightly supervised structure: space operations assigned to a newly constituted PLA Aerospace Force and cyber operations to a PLA Cyberspace Force, both subordinated to an Information Support Force responsible for joint networks and C4ISR integration. All three report directly to the Central Military Commission, chaired by Xi himself, preserving direct Party oversight and preventing excessive technostrategic autonomy accumulation in any single actor.

Beyond the military chain of command, strategic directions flow from Xi-led Party bodies and ad hoc "leading small groups" such as the Central Commission for Integrated Military-Civil Development (established 2017). Policy codification is handled by the State Council, primarily through the Ministry of Industry and Information Technology, which allocates funding, sets technical standards, and approves sensitive exports. Programme execution rests with state-owned conglomerates such as the China Aerospace Science and Technology Corporation, whose leadership appointments are ultimately controlled by the CCP.

In recent times, the strategic outlook broadened to incorporate private industry, and another layer was added with the creation of China Satellite Network Group in 2021, with the goal to build the Guowang mega-constellation (12,992 LEO satellites by 2030). Although framed as a commercial broadband project, Guowang is part of the military-civil fusion ecosystem. Launch coordination, spectrum allocation, and data governance remain under political oversight. Private "New Space" firms operate under licensing regimes requiring the support of the PLA under China's 2017 National Defence Transportation Law.

The Cybersecurity Law and Data Security Law further define space-related assets and data links as critical information infrastructure subject to localization, security review, and real-time monitoring. Regulations extend this logic to user terminals, ensuring ostensibly civilian satellite connectivity remains "secure and controllable". In essence, space in China is an expression of CCP rule where control over orbit, infrastructure, and data reinforces both external strategic autonomy and internal political order.

8.6 The US: Space as a Contested Domain

Across the US corpus from 2019 to 2025, space governance is anchored in a consistent conception of outer space as a contested strategic terrain. This discourse is linked to efforts to preserve domain usability and predictability, upon which the US and allies depend. Space is described as critical high ground. Congestion, commercial scaling, and infrastructural vulnerability are treated as security problems requiring governance tools beyond purely military solutions.

These views are visible in both language and thematic structure (Figure 20). Space Combat and Weaponization (cluster 4.7) remains among the most frequent clusters (approximately 18% across the corpus), and it is often paired with usability governance themes: Debris Mitigation and Space Traffic Management (7.4) accounts for 9%, Technical and Safety Standards for 0.5%, Multilateral Governance and Treaties (1.2) for 2.5%, and Responsible Leadership (8.2) for 1.5%. The dual framing results in militarized readiness paired with managerial sustainability and responsibility vocabulary.

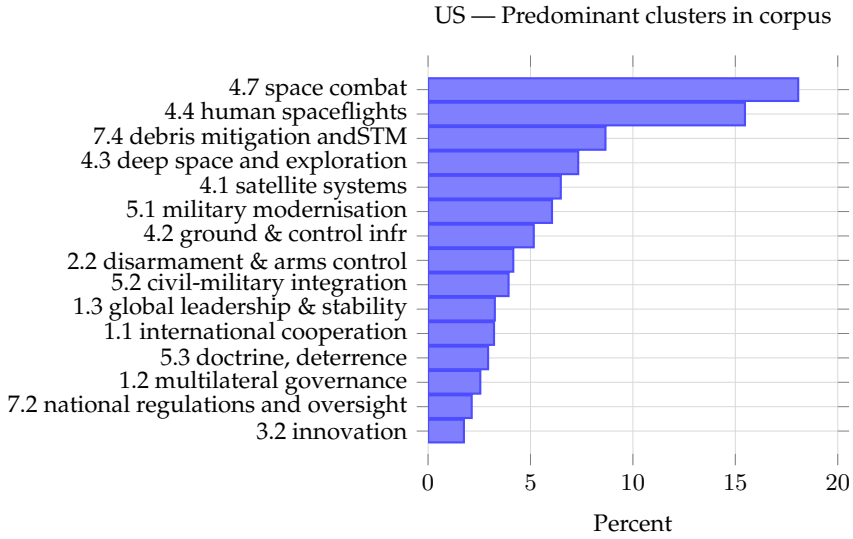

Figure 20: Predominant Clusters in US Space Policy Discourse.

Across time and administrations is narrated and operationalized differently, for different audiences with different goals.

Under the first Trump administration, framing focused on reclassification. Space Policy Directive 4 (SPD-4, 2019) [222] was written in a legal-administrative register, with roughly three-quarters of its paragraphs coded as neutral. This apparent neutrality normalized the idea that space now requires a permanent military organization. By tasking the new Space Force with familiar defence functions of "organise, train, and equip military space forces to ensure unfettered access to and freedom to operate in space," SPD-4 integrated space into existing defence bureaucratic grammar [222].

In this period, documents displayed higher concentrations of combative and assertive language (around 25% and 10% respectively), emphasizing that competitors are developing counterspace capabilities and that the US must be prepared to "deter and defeat" hostile actions [512]. This was not framed solely in terms of counterforce options but of usability and sustainability. Debris Mitigation and Space Traffic Management (7.4)

emerged quite frequently, alongside infrastructure and resilient themes. Congestion, debris, and cyber vulnerability were also treated as threats requiring governance addresses.

Under Biden, the framing was broadened and repackaged in more diplomatic and ally-friendly terms. The US Space Priorities Framework (2021) [384] reaffirmed that space is vital to national security and deterrence but reframed these priorities through alliances, norms, and innovation. Combative language dropped markedly, suggesting a shift away from blunt threat description towards signaling intentions and priorities.

The rhetorical shift was even more pronounced in the Strategic Framework for Space Diplomacy (2023) [513]. In this document, conciliatory sentiment jumped to 60% of coded paragraphs with an emphasis on "partnership, economic prosperity, diversity, equity and inclusion, and scientific and technological progress" [513]. For the first time, the role of space diplomacy is spelled out as a tool to maintain US leadership, promoting norms of interoperability and responsible behaviour. It was aimed at countering the expanding international space footprint of China through soft-power instruments.

By 2025, framing under the second mandate of Trump expanded into political economy. The Executive Order on Enabling Competition in the Commercial Space Industry [220] adopted a confident, directive tone dominated by assertive and neutral language. It focused on regulatory reform, industrial policy, and the removal of barriers to private-sector activity like market entry and export controls [220]. The most significant cluster within this period is National Regulations and Oversight (7.2), which accounts for about 18% of all thematic mentions. The variations of the macro themes over time are shown in 21.

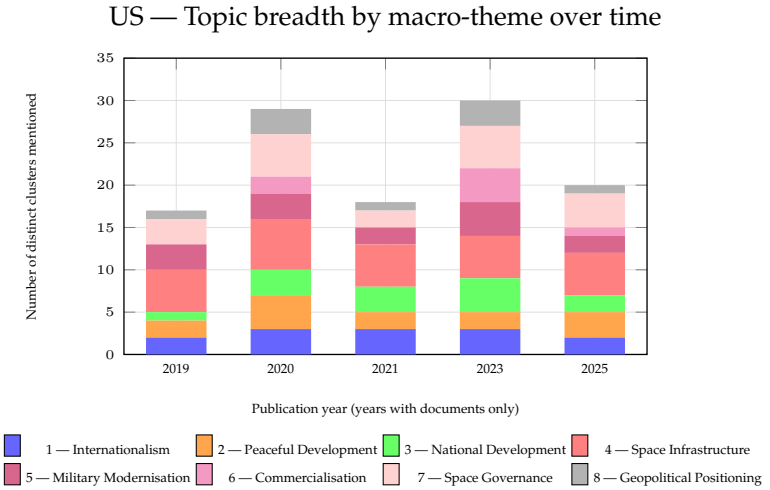

Figure 21: Thematic Breadth in US Space Policy Discourse (2019–2025).

These trends have been and will further be stabilized through institutionalization, which makes the US space posture locked-in and durable across political cycles. The establishment of the Space Force and reconstitution of US Space Command were the most visible expressions of this process. Texts under prominent clusters like Doctrine (5.3) or Military Modernization and Reform (5.1) professionalized space, defined core missions, and aligned space operations with joint and combined warfare.

The US's consistent understanding of space as a contested strategic terrain transcribed into a stable technopolitical order. The dual framing of deterrence and usability materialized through various capabilities, which we discuss in Section 8.13. These choices created path dependencies and were made durable through institutionalized military reforms, diplomacy, and market regulation.

8.7 The European Union: Space Regulation and Strategic Autonomy

During the period subject to this study, the EU increasingly framed space as a strategic domain integral to security, resilience, and autonomy while retaining a distinctive self-understanding as a regulatory and multilateral actor. In general, space is framed both as an economic asset driving growth and competitiveness, and a strategic but vulnerable ecosystem whose disruption would have immediate security consequences. Unlike China or the US, the framing is not organized around military preparedness but around governance capacity, resilience, and the management of systemic risk.

From 2019 to 2022, the EU saw space mostly through the economic and civilian lens. The earliest documents in 2019 positioned space policy at the intersection of industry strategy and economic development while calling for greater political steering and institutional coherence. More than 57.1% of paragraphs were coded as assertive, signaling an elevated ambition and moving this issue higher up in the political agenda. At the same time, the thematic profile, shown in Figure 22 is distinctly governance-heavy, with National Regulations and Oversight (7.2) accounting for one-fifth of the text. This trajectory was complemented with prominent language in Economic Development and National Rejuvenation (3.1), Market Development and Commercial Expansion (6.1), and State-Led Planning and Policy Support (3.5). Key debates about balancing competitiveness with long-term sustainability were constantly carried out through diplomatic means. Texts clustering in Multilateral Governance and Treaties (1.2) and International Cooperation (1.1) showed how the European approach centered on consensus rule-making and the embedding of space within international legal frameworks.

The shift towards explicit security framing became clear after Russia invaded Ukraine in February 2022. In the Strategic Compass for a stronger EU security and defence [123], space was formally designated as a strategic domain, linking hostile activities to malicious interference and destabilizing behaviour that could trigger a Union-level response.

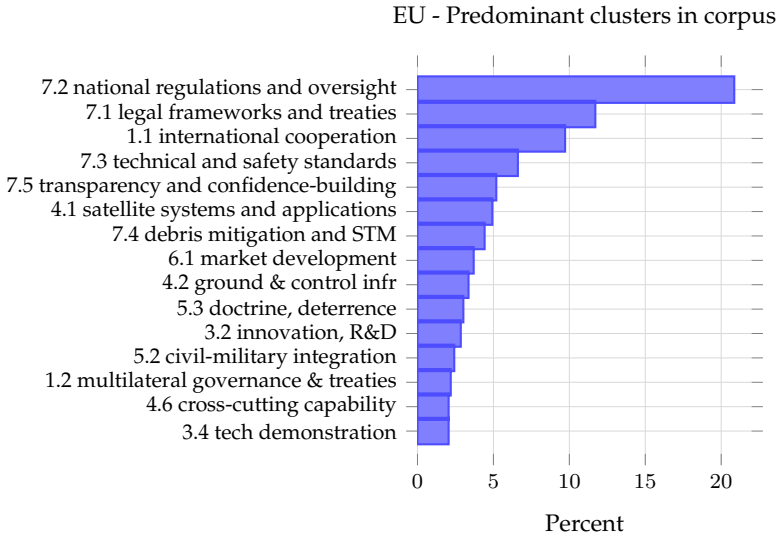

Figure 22: Predominant Clusters in EU Space Policy Discourse.

This discursive change is mirrored in the sentiment analysis. 2022 was the most assertive year in the corpus, with more than 56% of paragraphs coded as such, and was the first year in which a measurable share of combative language appeared.

The thematic centre of gravity also changed markedly. Clusters like Military Modernization and Reform (5.1), Military Doctrine (5.3), and Strategic Competition and Regional Focus (8.4) were on the rise. All indicated growing anxiety from systemic vulnerability and geopolitical pressures in the space domain. The EU, however, still opted to prioritize its risk management through collective action and oversight rather than moving openly to weaponization. This was confirmed by looking at the minimality of Space Combat and Weaponization (4.7) and stable patterns of governance-related themes visible in Figure 23.

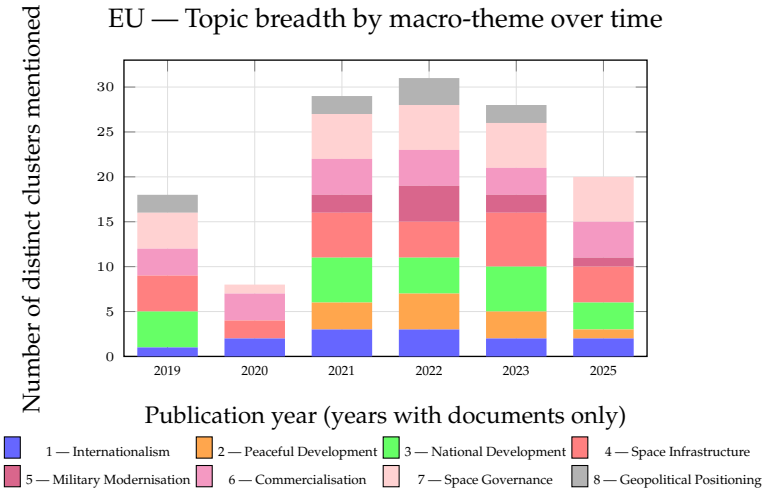

Figure 23: Thematic Breadth in EU Space Policy Discourse (2019–2025).

The security framing stabilized in subsequent years. International Cooperation (1.1), especially with NATO, was most frequently mentioned with notable use of Dual-Use Integration (5.2) and Confidence-Building Measures clusters. This perception was finally crystallized in the language of regulation and compliance expressed through the EU Space Act proposal. Once again, a governance-centric vocabulary was completed by a neutral legislative tone. Vulnerability and security concerns have now materialized into tangible policy choices and institutions.

8.8 Space Cybersecurity as Security, Market, and Infrastructure: China, the EU, and the United States

Previous sections examined the discourse surrounding space and the securitization of this domain by the European Union, China, and the United States. As a central aspect of security in space is closely associated with its cyber dimension, this section examines how the EU, the

US, and China conceptualise and address cybersecurity in the space domain. In our analysis space, cybersecurity is not a purely technical problem, but a political and economic one, shaped by institutional authority, technological choices, and market incentives. In this section, we adopt a comparative approach centered on common analytical questions. This analysis draws on official regulatory and policy material, technical threat assessments, and industry-oriented sources, including policy consultation inputs and market analyses.

The section is organised into three sub-sections according to three main concepts. The first examines political and governance logics: how space cybersecurity is framed, where authority is located, and whose interests are represented. The results of this analysis are shown in Table 33. The second analyzes technological priorities and dominant threat models, and this analysis is shown in Table 34. The third addresses economic perceptions, focusing on costs, incentives, and distributional effects. The analysis's summary is presented in Table 35. A final synthesis shows how these dimensions combine into distinct models of space cybersecurity. Across all three actors, space cybersecurity is a matter of public interest; however, the meaning of that public interest, the location of authority, and the role and perception of the industry differ markedly.

In the Chinese case, space cybersecurity is part of a broader doctrine of cyber sovereignty and national security [420]. The Cyberspace Administration of China frames satellite connectivity as a security-sensitive extension of national cyberspace, requiring political oversight and technical control [93]. Satellite internet is, on one side, a commercial service, but on the other, a potential channel for information flows that could bypass domestic controls or expose critical infrastructure to external interference [93].

In the Measures for the Administration of Terminal Equipment Directly Connecting to Satellite Services, a CAC document published in 2024 [93], Chinese authorities treat satellite modems and user terminals as a key source of risk in space-based communication systems. These devices are first seen as technical weak points whose disruption can affect military operations and critical infrastructure, a concern reinforced by

the KA-SAT/Viasat cyberattack during the war in Ukraine, which temporarily disrupted communications for military and civilian users. At the same time, satellite terminals are understood as enabling forms of internet access that may bypass existing domestic control mechanisms. The Measures, therefore, focus on regulating terminal-level access through cybersecurity requirements, licensing, and usage restrictions, to reduce both operational vulnerability and uncontrolled information flows.

Chinese regulators assert the right to determine which satellite systems may operate within national territory, to license terminal equipment and service providers, and to impose mandatory security and data-protection obligations [93]. In China, operators are expected to prevent the transmission of information deemed harmful to state security or social stability. Here, the industry appears primarily as an implementation layer; companies are encouraged to contribute to industrial development and innovation, but within parameters set by the state. There is little evidence of an autonomous industry voice shaping regulatory objectives; alignment, rather than negotiation, is the dominant mode.

In the European Union, space cybersecurity is framed through the lens of internal market integration and risk management. The European Commission identifies fragmentation across national space laws and uneven treatment of safety and cybersecurity risks as obstacles to a functioning market for space-based data and services, and uses this as the main justification for a EU Space Act [107], the first legal instrument to introduce industry-wide requirements in the sector. Space cybersecurity goes alongside safety and environmental sustainability as a condition for market integration rather than as an expression of national sovereignty.

Therefore, in the EU, multiple voices are involved in the consultation process. When it comes to new cybersecurity requirements, such as those that will probably be introduced by the Space Act, many different actors contribute to the political discussion, trying to push for their position. European standardisation actors emphasise the importance of harmonised standards and resist approaches that would bypass established consensus-based processes [85]. Downstream service providers accept the need for cybersecurity obligations but highlight the risk that

upstream compliance costs will cascade through the value chain [563]. From the upstream industry perspective, cyber resilience is framed as a strategic asset: clear, predictable, and harmonised requirements are seen as necessary to preserve European industrial credibility, avoid market fragmentation, and sustain cross-border supply chains. However, this segment of the industry also warns that overly prescriptive or rapidly evolving rules risk constraining innovation and disproportionately affecting system developers.

This negotiated, market-oriented approach contrasts with the United States, where space cybersecurity is framed less as a regulatory coordination problem and more as a core national security imperative. The US, in fact, frames cybersecurity in strongly securitised terms, linking it to national security, critical infrastructure protection, and deterrence in a contested domain [500]. Space systems are indispensable to both military operations and civilian life, and their disruption is treated as a serious strategic risk.

Rather than relying on a single, comprehensive regulatory framework, the US implements cybersecurity requirements through agency-specific rules, procurement practices, and program-level standards. US space companies describe this landscape as fragmented, with requirements varying across civil and defence programmes and often derived from generic IT frameworks ill-suited to space systems. Industry voice is clearly present and influential, but it is channelled primarily through consultation, contracting, and feedback loops rather than through formal regulatory negotiation [122].

8.9 Technological Priorities: What Is Secured and According to Which Threat Models

All three actors converge on a basic technical consideration: space systems are complex, multi-segment architectures in which vulnerabilities in ground infrastructure, links, user equipment, or on-board systems can undermine the whole. Divergence emerges in which segments are prioritised and how threats are translated into design and regulatory choices.

Table 33: Cybersecurity governance framing in China, the Eu and the US

Actor	Core framing	Authority structure	Role of industry
China	National security and cyber sovereignty	Highly centralised state control	Implementer aligned with state objectives
EU	Safety, resilience, and internal market	Shared, fragmented and negotiated	Active participant shaping implementation
US	Mission assurance and deterrence	Decentralised, agency-driven	Strong consultative and contractual voice

The summary of the analysis of this section is shown in Table 34

Chinese technical and regulatory approaches place a distinct focus on terminal devices and ground-based infrastructure [93]. Regulators focus on controlling user endpoints to prevent unregulated connectivity and unauthorised data flows, and technical assessments highlight persistent weaknesses in the cyber posture of ground-segment systems [492]. Exposed services, legacy software, and insufficient network segmentation are identified as the recurring problems across space-related organisations. The implicit conclusion is that formal regulatory control must be complemented by significant improvements in operational cybersecurity practices.

From an industrial perspective, Chinese market actors adopt a system-wide threat model encompassing communication links, ground systems, satellites, supply chains, and terminals. Threats such as jamming, link hijacking, malware insertion, and component-level compromise are used to justify the expansion of a dedicated satellite internet security sector. The enumeration of threats serves as a diagnostic function, but also an economic one; cybersecurity supports investment narratives around integrated, end-to-end security solutions.

Technical assessments of Chinese space-related organisations focus on the ground segment as the weakest link [492]. Exposed web services, remote management interfaces, legacy software stacks, and insufficient network segmentation are recurrently identified as sources of risk [492].

These weaknesses are considered empirically observable conditions affecting aerospace manufacturers, satellite operators, and research institutes. Ground systems are understood as attractive targets because they concentrate command, telemetry, and data processing functions while often relying on conventional IT infrastructure that lacks space-specific hardening.

In the European Union, technological priorities are shaped by a lifecycle-based and asset-centric understanding of risk. Threat modelling explicitly distinguishes between space assets, ground infrastructure, user segments, and human and organisational components, and maps vulnerabilities across design, manufacturing, launch, operational, and end-of-life phases [212]. Cybersecurity is inseparable from system engineering choices made early in the lifecycle, rather than as a set of controls applied post-deployment.

European threat assessments place particular emphasis on ground-segment exposure and interdependencies [212]. Ground stations, mission control centres, cloud-based data processing environments, and third-party service providers are consistently identified as high-risk nodes due to their connectivity, reliance on commercial IT services, and integration with non-space networks. At the same time, link-level threats such as jamming, spoofing, and interference are analysed alongside cyber intrusions, reflecting an understanding of space systems as hybrid cyber-electromagnetic environments rather than purely digital systems [212].

Rather than prescribing specific defensive technologies, the European approach seeks to translate these threat models into risk-management obligations. Harmonised standards and certification schemes are expected to operationalise cybersecurity requirements in a manner proportionate to mission profile, system criticality, and operator capacity. The underlying design philosophy treats space systems as critical cyber-physical infrastructure embedded in wider digital ecosystems, requiring structured, auditable risk management across the full lifecycle rather than bespoke or purely reactive security measures.

The United States adopts a similar threat-informed and operationally grounded approach to space cybersecurity, shaped by the assumption

that space systems will be targeted by capable state and state-sponsored adversaries. U.S. policy and technical guidance seem to prioritise the protection of critical space system functions, particularly command-and-control, telemetry, tracking, and mission data integrity, because their compromise could result in loss of positive control, mission failure, or cascading physical effects in orbit [500]. Cyber threats are therefore framed less in terms of data confidentiality and more in terms of system integrity, availability, and assured command authority, reflecting the role of space assets in military operations and critical civilian infrastructure.

Recent vulnerability assessments identify the ground segment and interface layers as primary points of exposure [152]. Ground stations, mission control networks, cloud-based data processing environments, and software-defined radios are treated as particularly vulnerable due to their connectivity, reliance on commercial IT infrastructure, and integration with non-space networks [515]. At the same time, U.S. sources emphasise risks associated with long-lived on-orbit systems that were designed before contemporary cyber threat models were fully developed [515].

The U.S. private sector often points out the disparity between terrestrial cybersecurity frameworks and the unique challenges of space systems. These challenges include limited processing power, intermittent connectivity, and lengthy development and deployment cycles. These factors complicate the implementation of standard security measures, such as continuous monitoring, regular patching, and intrusion detection [443]. These constraints reinforce a technological emphasis on secure-by-design engineering, where cybersecurity considerations are embedded early in system architecture rather than after the launch. Encryption, authentication, segmentation of critical functions, and protection against unauthorised command injection are prioritised over comprehensive compliance with generic cybersecurity checklists [447].

As a result, the technological debates in the US increasingly focus on architectural resilience; disaggregation, redundancy, and proliferated constellations are promoted as ways to limit the operational impact of successful cyberattacks by reducing single points of failure and enabling

controlled degradation rather than catastrophic loss. Cybersecurity is a practical engineering and mission-assurance problem, closely tied to system design choices and operational concepts, and not as a standardisation-driven exercise aimed at uniform control implementation across all space assets.

Table 34: Technological Priorities in China, the Eu and the US

Actor	Technical emphasis	Dominant threat model	Design logic
China	Terminals and ground control	Loss of control and information leakage	Secure, controllable ecosystems
EU	Lifecycle and system-wide risk	Multi-segment disruption	Risk-based standardisation
US	Critical functions and resilience	State-level adversaries	Threat-informed pragmatism

8.10 Economic Perceptions: Costs, Markets, and Incentives

This section examines how space cybersecurity is framed economically across the three actors, focusing on whether cybersecurity requirements are understood as regulatory costs, strategic investments, or market opportunities.

In the European Union, space cybersecurity is currently primarily a regulatory cost with a measurable economic impact, which is quantified through formal ex ante assessments, such as the Commission's impact assessment for the EU Space Act [107], which estimates that cybersecurity and resilience requirements will generate non-negligible but bounded cost increases across the space value chain, particularly for satellite manufacturing and ground systems.

According to the Commission's modelling, cybersecurity-related obligations contribute to satellite platform manufacturing cost increases in the range of 3–10% [196], depending on mission type and system complexity. When aggregated across affected segments, these increases translate into an average price rise of approximately 2.7% [189] across the EU

space industry.

Despite these costs, EU institutions frame cybersecurity expenditure as economically justified by its long-term benefits, including reduced regulatory fragmentation, lower systemic risk, increased trust in space-based services, and improved conditions for cross-border operations. The private sector, however express concern about fixed compliance costs and administrative burden, particularly in the early phases of implementation.

In China, cybersecurity requirements are widely framed as an industrial opportunity rather than a regulatory burden. Market analysts interpret mandatory security obligations as demand-generating mechanisms that support the emergence of a domestic satellite internet security industry [296]. Fixed per-satellite security expenditures are treated as predictable inputs into national constellation programmes, providing a stable revenue base for firms aligned with state priorities. Regulation is thus understood as a tool for market creation and industrial consolidation rather than as a constraint on innovation.

Economic studies estimate [296] that the domestic satellite internet security market, including secure ground infrastructure, terminals, and network protection, will reach approximately RMB 8–10 billion annually by 2030, driven by the rollout of state-backed and commercial constellations. Cybersecurity expenditure is treated as a predictable and stable revenue stream for domestic firms aligned with national programmes, rather than as a factor constraining investment or demand.

Notably, no official Chinese documents attempt to quantify cybersecurity requirements as incremental costs imposed on operators. Economic risk is instead associated with delays in constellation deployment or policy execution, while cybersecurity requirements themselves are assumed as a baseline condition of participation in the market.

In this setting, firms with strong ties to state programmes and domestic supply chains are positioned to benefit, while foreign providers and unaligned actors face significant barriers to entry. Economic risk is associated primarily with delays in deployment or policy execution, not with the stringency of security requirements themselves.

A good example of Cybersecurity considerations in the US space ecosystem is given by the NASA budgetary reports [374], where cybersecurity activities are described as embedded within engineering, safety, mission services, and infrastructure modernisation accounts, rather than isolated as standalone cybersecurity programmes. NASA's Safety, Security, and Mission Services budget, amounting to approximately USD 446.5 million annually from FY-2026 onward, explicitly integrates cybersecurity into mission resilience, system protection, and technical authority functions.

In the United States, cybersecurity costs are largely internalised within defence and government space programmes, where mission assurance is non-negotiable. The primary economic concern expressed by industry is inefficiency rather than cost increases [443]. US private-sector actors call for clearer, more space-specific baselines and better-aligned incentives, particularly for commercial operators and legacy systems.

From a market perspective, this embedded approach means that cybersecurity demand is driven primarily by government procurement and mission requirements, and not by regulatory compliance obligations. While market studies estimate U.S. space cybersecurity spending at USD 1.1–1.2 billion in the mid-2020s [263], these figures reflect investment tied to defence and government-led programmes rather than responses to new regulatory mandates.

From an external economic perspective, U.S. authorities explicitly frame the EU Space Act as a potential source of trade distortion and duplicative compliance costs for U.S. space companies operating in the European market. Official U.S. reactions [511] express concern that the proposed cybersecurity and resilience requirements could function as non-tariff barriers, particularly if equivalence and mutual recognition mechanisms are not clearly defined. U.S. authorities argue that size-based and prescriptive regulatory obligations risk disproportionately affecting U.S. operators, especially large constellation providers, by increasing compliance costs and constraining investment decisions without demonstrable security gains.

In this context, U.S. economic concerns focus less on the absolute cost of cybersecurity measures and more on their extraterritorial effects, in-

cluding the risk of fragmented regulatory regimes, reduced interoperability, and weakened transatlantic supply chains. The preferred U.S. approach emphasises regulatory alignment, outcome-based requirements, and mutual recognition of existing cybersecurity assessments, to preserve market access and avoid duplicative compliance burdens for firms active across jurisdictions.

Table 35: Space Cybersecurity from the economic point of view of China, the EU and the US

Actor	Economic framing	Perceived burden	Market effect
China	Security as an industrial driver	Low political salience	Protected domestic expansion
EU	Security as quantified regulatory cost	Actively contested	Regulated market growth
US	Security as an internalised mission cost	Fragmentation-driven	Incentive and alignment focus

8.11 Divergent Models of Space Cybersecurity

Taken together, the political, technological, and economic dimensions form three distinct models of space cybersecurity. China's model is state-centric and sovereignty-driven. Cybersecurity, information control, and industrial policy are tightly integrated, and regulation serves both security and market-shaping functions: China emphases controllability, domestic capacity, and alignment with national strategic objectives.

The European Union's model is both regulatory and pluralistic. Space cybersecurity is embedded within a broader project of market integration and sustainability, implemented through shared authority, standardisation, and negotiated requirements with the industry. Security objectives coexist with explicit concern for competitiveness and proportionality.

The United States follows a mission-assurance model. Security narratives coexist with decentralised implementation and reliance on procurement and industry dialogue. Cybersecurity is treated as an operational necessity shaped by threat environments and system constraints rather than as a uniform regulatory domain.

These models reflect deeper differences in how states organise authority, manage technological risk, and structure markets. With space systems now central to economic and military power, these differences will increasingly shape cooperation, competition, and conflict in the space and cyber domains.

8.12 From Discourse to Practice

This paper's corpus analysis, along with the discussion surrounding space cybersecurity, illustrates the distinct paths of political discourse and strategic doctrine for the US, China, and the EU. These varying approaches to articulating space and its securitization have led to tangible operational choices, investment decisions, and strategic actions. This section aims to translate the analyzed discourse into specific actions and decisions that underlie it. The analysis conducted here connects the most frequently observed clusters and themes from our study to the operational capabilities developed by these three actors.

8.13 United States - From Discourse to Practice

The US framed space as a contested warfighting domain, driving a robust push for military space superiority (Macro-Theme 8: Geopolitical Positioning & Strategic Image). This framing has materialized in concrete capabilities that reflect U.S. doctrine and discourse. In line with the macro-theme of Space Infrastructure and Capability Building (Theme 4) – specifically cluster 4.3: Space Surveillance & Resilience – the U.S. expanded its space surveillance networks and built more resilient constellations. A key development was the Space Fence S-band radar system, which achieved initial operational capability in 2020 and is capable of tracking tens of thousands of objects in low Earth orbit [268]. Space Fence, along with a suite of optical telescopes and on-orbit inspector satellites like the GSSAP (Geosynchronous Space Situational Awareness Program, with six satellites by 2022), provides near-real-time awareness

of spacecraft maneuvers, enabling the U.S. to rapidly detect or attribute hostile acts in orbit [101].

To improve resilience under attack, the Pentagon radically shifted its satellite architectures. Rather than relying on a few large GEO satellites the U.S. is deploying proliferated constellations of smaller satellites in LEO on a rapid spiral development cycle. The recently created Space Development Agency (SDA) began fielding the National Defense Space Architecture (NDSA) with hundreds of satellites arranged in multiple layers with initial Tranche 0 launches in 2022–2023 and a plan for new tranches every 2 years [567]. This distributed approach, enabled by commercial mass production and frequent launch, inherently complicates enemy targeting. Even if some nodes are lost, the network can continue to function, ensuring continuity of service. The U.S. has also leveraged commercial mega-constellations for redundancy, partnering with SpaceX's Starlink network to support military communications (notably seen in Ukraine's connectivity) [9]. These investments in Space Domain Awareness and resilient constellations reflect the U.S. warfighting paradigm, translating into capabilities (Theme 4, Satellite Systems & Resilience) that secure space assets against interference.

Consistent with treating space as a key enabler of terrestrial warfighting, the U.S. heavily modernized and expanded its satellite constellations for intelligence, navigation, and communications (Macro-Theme 4, cluster 4.1: Satellite Systems and Applications). Between 2020 and 2026, the U.S. launched next-generation GPS III navigation satellites, enhancing positioning and timing services with higher accuracy and stronger anti-jam signals. The follow-on GPS IIIF program was funded to ensure continued global coverage and to add features like laser links and regional military uplinks for even greater resilience [267]. The aging SBIRS/DSP missile-warning satellites in GEO are being succeeded by the Next-Generation OPIR constellation, featuring advanced infrared sensors, while the SDA Tracking Layer in LEO adds dozens of sensors able to detect dimmer targets such as hypersonic glide vehicles [162]. For imagery intelligence, the National Reconnaissance Office (NRO) orbited new high-resolution optical and radar imaging satellites, and began ex-

perimenting with commercial imagery for tactical use [271]. Secure communications were bolstered via new military satellites like WGS-11+ (Wideband Global SATCOM) and AEHF-6 (Advanced Extremely High Frequency satellite) [30]. These efforts align with both Theme 4 (Capability Building) and Theme 5 (Military Modernization), and demonstrate how U.S. discourse about assured space support and dominance (captured in cluster 5.1: Space Superiority Doctrine) led to tangible programs strengthening U.S. C4ISR and PNT capabilities.

To sustain its space capabilities, the U.S. focused on assured and responsive launch. This falls under Space Infrastructure (Theme 4) and also reflects Commercialization and Industry (Theme 6), given the prominent role of private launch providers. The U.S. maintained heavy-lift launch capacity for the largest national-security payloads – for example, SpaceX Falcon Heavy flew several missions for DoD [540].

Because the U.S. perceives space dominance as critical to deterring adversaries, it pursued a range of counterspace capabilities for both offense and defense; a development guided by Macro-Theme 5: Military Modernization and Civil–Military Integration, particularly cluster 5.3: Counterspace Systems. U.S. officials have condemned destructive antisatellite (ASAT) testing, the U.S. declared a unilateral moratorium on debris-causing ASAT intercepts in 2022 [488], yet the Pentagon has developed non-kinetic offensive tools aimed at neutralizing enemy space assets if necessary without creating orbital debris. By 2025, the U.S. Space Force had at least one acknowledged operational counterspace weapon: the Counter Communications System (CCS) [340], a ground-based mobile jammer that targets adversary satellite communications. A major enhancement effort codenamed Meadowlands delivered a next-generation CCS jammer in 2025, offering multi-frequency jamming (covering S-band and X-band satcom links) in a much more compact, mobile package [365]. Multiple Meadowlands units are being tested and integrated, providing the U.S. with a flexible electronic attack option to dazzle enemy satellites without physical destruction. U.S. officials have even begun to openly acknowledge work on offensive space control weapons, signaling an intent to be able to disable or degrade hostile

satellites in wartime through reversible means (jamming, dazzling, cyber effects) rather than kinetic attacks.

On the defensive side, the U.S. also fielded measures to protect its own satellites. Many national-security satellites were equipped with improved maneuver capabilities and onboard threat detectors. Some, like the latest Syracuse comm satellites shared with France, carry optical cameras to identify nearby objects [434]. The U.S. operates on-orbit inspection satellites (the GSSAP spacecraft in GEO) to monitor potentially threatening approaches [87], and has tested the secretive X-37B spaceplane on six missions, carrying experiments that could include deploying small satellites, testing autonomous rendezvous, or other advanced technologies [248]. Cyber defense of space systems has likewise been a priority. Given that cyber-attacks could cripple satellite operations without any launch, Space Force works closely with U.S. Cyber Command and industry to harden satellite control networks and ground stations (for instance, through the Space Information Sharing and Analysis Center, Space-ISAC, which shares threat intelligence among government and commercial satellite operators).

All these efforts stem from Washington's consensus that control of space is vital to national security, a consensus prompting high-tech projects and organizational changes on an unprecedented scale. The U.S. approach shows framing, materialisation, and institutionalisation: a forceful doctrinal vision of space control (Theme 8 and Theme 5) led to concrete new technologies and units oriented around space superiority.

8.14 European Union: from discourse to practice

Our analysis demonstrated how the European Union's framing of space security has historically differed from the U.S.'s, emphasizing space as critical infrastructure to be protected and a domain to be kept peaceful, while more recently also moving toward a stronger security role in light of rising threats. Europe conceives of space assets as essential enablers of the economy and society, implicating the need for sovereignty and

resilience.

Europe on one hand, aims to preserve space as a global commons through diplomacy and norms (consistent with EU's multilateral, non-weaponisation ethos), and on the other, hardening Europe's space infrastructure and services against aggression. The EU's conceptual focus on resilience and autonomy steers it to develop capabilities that secure access to essential space services for Europeans, rather than offensive space weapons. Key EU initiatives from 2020 reflect this primarily defensive, dual-use approach. This aligns with Macro-Theme 4: Space Infrastructure & Capability and Macro-Theme 3: National Development/Tech Advancement, as well as Europe's strong discourse on Macro-Theme 7: Space Governance & Standards. Each of these themes is evident as the EU translates its discourse into concrete programs.

Regarding the development of dual-use constellations, the EU has recently invested heavily in its flagship space programs and upgraded their security features. The EU's Galileo satellite navigation system reached Full Operational Capability in the early 2020s, providing highly accurate PNT to over 2 billion global users. On top of its civilian applications, Galileo offers a Public Regulated Service (PRS) [510], an encrypted, jam-resistant signal reserved for government and military users. The PRS is seen as a pillar of European military autonomy, guaranteeing that European forces have sovereign PNT access even if GPS is denied. Similarly, the Copernicus Earth observation program delivers high-resolution imagery and a wealth of environmental data. Originally civilian, Copernicus data has increasingly been used for security missions, for example, maritime surveillance in the Mediterranean and mapping crisis zones, showing the dual-use value of Europe's EO assets [52].

The third major pillar, IRIS² is designed to provide secure, encrypted broadband communications for EU institutions, member state governments, and potentially troops; essentially a European GovSatCom system for civil protection, diplomatic communications, and military use. The IRIS² program was approved in 2022 with a budget of €2.4 billion, explicitly to reduce reliance on non-EU satellite operators.

These programs show the EU's preference for dual-use capabilities,

systems that strengthen the economy and civilian services while also equipping Europe with strategic security tools. The role of the EU Satellite Centre (SatCen) is a clear example of how this dual-use strategy is made operational. The Agency fuses imagery from both commercial sources and member-states' military satellites to produce geospatial intelligence for EU missions and policymakers [414]. By building out autonomous capacities, the EU reduces its dependence on foreign (often U.S.) assets and strengthens its decision-making autonomy during crise. This corresponds to Theme 3: National Technological Advancement (Europe seeking independent technological capabilities) and is mapped to thematic cluster 5.2 (Civil–Military Integration), as the EU deliberately designs civilian systems with secured military-grade components.

The EU's view of space infrastructure as essential services, translates in a particular focus on Space Situational Awareness (SSA) to safeguard satellites from collisions, interference, or attacks. This falls under Macro-Theme 7: Space Governance, Law & Standards, specifically cluster 7.4: Debris Mitigation and Space-Traffic Management. In the 2010s the EU launched a Space Surveillance and Tracking (SST) support framework, which federated sensors from multiple member states (radars, telescopes, laser-ranging stations) to provide collision avoidance warnings and debris monitoring for European satellites. This capability evolved further in recent times toward a more comprehensive Space Domain Awareness approach, also monitoring operational satellites and potential threats (e.g. uncooperative approaches or hostile maneuvers in orbit) [228]. In practice, this means encouraging countries that have relevant sensors (for example, France's GRAVES bi-static radar [411], and Germany's TIRA tracking radar [325]) to share real-time data and jointly maintain a catalog of objects and activities in key orbits.

On the cybersecurity side, the EU arguably operates one of the most regulated environments globally. Through instruments such as NIS2, the CER Directive, the Cybersecurity Act, and upcoming proposals including the EU Space Act and the Digital Networks Act, European space operators are increasingly required to meet defined cybersecurity baselines, adopt recognised standards, and comply with tighter oversight and re-

porting duties. However, the key question for this section is not to map the regulatory landscape in detail, but to understand what these rules produce operationally: which concrete capabilities and technologies are actually implemented as a result of this regulatory push.

Since 2022, the European External Action Service (EEAS) has operated a 24/7 Space Threat Response Architecture (STRA) team (under the EU's Special Envoy for Space) and has held annual exercises (e.g. STRA-22 in May 2022) to simulate how the EU would respond to an attack on a European satellite. These simulations involve coordinating diplomatic responses, activating mutual defense clauses, and possibly attributing the attack publicly. Indeed, the EU's strategy now openly states that if a serious space attack occurs, it could trigger the EU's mutual defense mechanisms (Article 42.7 TEU) or collective retaliation in other domains.

Strategic autonomy in space also requires independent European access to orbit. Europe recently grappled with challenges in its launch sector the retirement of Ariane 5 in 2023, delays in the next-gen Ariane 6 heavy launcher (first flight slipped to 2024), and the sudden loss of access to Russian Soyuz rockets after 2022 [326], which underscored the security implications of launch dependence.

The EU response was to double down on supporting a diversified European launcher family, aligning with Macro-Theme 6: Commercialisation and Industry (and cluster 6.1, Indigenous Launch Capability). The Ariane 6 (with two variants targeting 10 ton and 21 ton to GTO) and the upgraded Vega-C light/medium launcher (up to 2.3 ton to LEO) are central to ensuring Europe can launch its large satellites (like Galileo replacements or government missions) without foreign reliance. The EU and national agencies are also stimulating "responsive launch" options, including supporting a nascent ecosystem of European small launch startups. Germany, for instance, has fostered companies like Isar Aerospace and Rocket Factory Augsburg developing micro-launchers (500 kg to 1 ton class) capable of quick deployment of small satellites [399]. The European Commission has provided seed funding and prizes (via Horizon Europe and CASSINI space entrepreneurship programs) to several launcher startups and conducted competitive launch service procure-

ments to give them opportunities. The logic is that in a crisis, Europe may need the ability to rapidly reconstitute satellite capacity or launch replacement satellites on short notice, something only possible if a responsive launch industry exists domestically. Though Europe's launch cadence still does not match the high tempo of U.S. or Chinese operations, these measures show a clear intent to close critical gaps. The EU is also supporting its broader industrial base (e.g., via the European Chips Act, seeking to ensure secure supply of chips for satellites) to satellite manufacturing capacity, to minimize strategic dependencies that could undermine security.

8.15 China: From Discourse to Practice

China's approach to space security is rooted in its portrayal of space as a strategic frontier vital to national rejuvenation, technological advancement, and military modernization. Guided by this outlook, China rapidly expanded both its civilian space infrastructure and its military/dual-use space arsenal. China recently completed long-planned constellations and leap ahead in developing counterspace weapons, all under the organizational umbrella of a reformed military space apparatus. In line with Macro-Theme 3: National Development & Technological Advancement and Macro-Theme 5: Military Modernization/Civil–Military Fusion, Chinese discourse directly translated into ambitious programs to rival U.S. capabilities.

In the early 2020s, China established indigenous, global space systems, reflecting Theme 4: Space Infrastructure & Capability Building and the drive for self-reliance. In June 2020, China completed the deployment of the BeiDou-3 Navigation Satellite System [244], becoming the third entity (after the U.S. GPS and Russian GLONASS) with a full global GNSS constellation. BeiDou-3 consists of 30 operational satellites (24 in MEO 21,500 km orbits, 3 in inclined GEO, 3 in GEO), offers an encrypted military/navigation service for the PLA (with higher-precision and anti-jam features). At the same time, China built out a dense network of intelligence, surveillance, and reconnaissance (ISR) satellites, and by

early 2025, counted over 1,000 operational satellites in orbit (a more than 500% increase since 2015) [459] and by end of 2025, over 1,300 satellites [37]. Crucially, more than 510 of these ere PLA-operated or dual-use ISR satellites equipped with optical imaging, synthetic aperture radar (SAR) [459], electronic intelligence (ELINT), and radio-frequency (RF) signal-geolocation payloads. This gives the PLA near-real-time surveillance of targets, while the constellation of Yaogan reconnaissance satellites (electro-optical and SAR satellites) guarantee frequent revisit in areas of interest, (South China Sea or Western Pacific) and track foreign naval deployments [156].

China's communication satellite fleet also grew and modernized, with new constellations like Tianlian relay satellites (in GEO) to support its crewed space station and provide continuous comms for other missions, and a variety of military comsats (Fenghuo and Shentong) [485] dedicated to PLA command-and-control networks. Notably, responding to the global trend of LEO broadband mega-constellations, China announced plans for its own large-scale constellations. The flagship is "Guowang" (National Network) [161], a state-backed project unveiled in 2021 to deploy 12,992 LEO satellites by 2030 to provide worldwide internet and IoT connectivity. By late 2025, China had launched the first batches of Guowang test satellites; over 200 experimental broadband satellites were in orbit by 2025. In addition, a second mega-constellation, called "Qianfan" ("Thousand Sails"), is in development by a Chinese commercial consortium [166]. Beijing's framing of space, as both an economic and strategic domain, translates into massive investment in orbital infrastructure across all sectors: navigation, Earth observation, communications, and science. This gives China increasing self-reliance in space services and also the capacity to support power projection, such as the PLA forces operating abroad can use Chinese SATCOM and ISR systems. China's on-orbit assets demonstrate how technological development and national security are linked (Theme 3 and 5).

To deploy so many satellites, China scaled up its launch capabilities, Theme 4 (Infrastructure) and 3 (Development). Over 2020–2025, China's launch rate surged to rival, and in some years exceed, that of the United

States. In 2021 and 2022, China led the world with 55+ launches each year [385], and in 2025 it hit a record 70 launches (carrying 319 payloads to orbit that year alone [157]. This demonstrate a new industrial capacity that only a decade before was a fraction of this size. The Long March rocket family remains the main carrier, but ongoing upgrades produced newer models like the Long March 5B [425] (25 ton LEO capacity, used for space station modules) and the Long March 7A [94] (mid-class launcher). A series of commercial-spinoff launch firms have also emerged under Beijing's military-civil fusion policies. Companies such as CASC's Expace, CASIC's Kuaizhou series, and startups like iSpace, LandSpace, Galactic Energy [454], developed light launch vehicles (carrying a few hundred kilograms) to ensure China can launch satellites on demand and into diverse orbits, reducing reliance on any single launch system. China also made advancements in reusable launch technology; in September 2022, Chinese firm CAS Space performed a successful vertical takeoff & landing test of a rocket stage, and another startup, LandSpace, flew its Zhuque-2 methane-fueled rocket in Dec 2022 (the first methane orbital rocket launch attempt globally, though reaching orbit was missed).

Nowhere is China's rise as a space power more evident, and to rivals, more concerning, than in its development of a broad counterspace arsenal. The PLA has invested for over two decades in a spectrum of anti-satellite (ASAT) weapons, to deter or complicate U.S. intervention in regional conflicts. China has already demonstrated direct-ascent kinetic kill ASAT technology [559], and recently refined its SC-19 missile system and fielded it as an operational DA-ASAT for LEO targets [559]. The U.S. Defense Intelligence Agency publicly assessed that China probably intends to field ASAT weapons able to reach geosynchronous orbit, and that recent ASAT tests indicate China may already have a basic capability against higher-orbit satellites [426]. PLA is likely developing the means to threaten strategic GEO assets such as missile-warning or communication satellites.

Alongside missiles, China has deployed or tested several co-orbital anti-satellite techniques. Shijian-21 (SJ-21) [507], a space debris removal test satellite launched in 2021, in January 2022, rendezvoused with a

derelict Chinese satellite (Compass G2) and successfully towed it out to a graveyard orbit. This technology could be used offensively to approach an enemy satellite and push it off course or disable it. Multiple Chinese Shijian and Tongxin Jishu Shiyan (TJS) satellites in GEO have exhibited unusual maneuvers, including large orbital relocations and close approaches to other satellites, which Western analysts interpret as practice for co-orbital ASAT tactics [546][551].

China is also advancing directed-energy counterspace capabilities. It operates several ground-based laser systems for blinding imaging satellites, and to saturate or damage optical sensors (a Beijing astro-observatory was identified by U.S. sources as a PLA laser site) [465]. China also maintains extensive electronic warfare and cyber tools targeting space systems, and uses routinely GPS and SATCOM jammers in training exercises, including jammers aimed to jam the U.S. Protected Extremely High Frequency (EHF) satellites [566].

As a result of recent investments and technological developments, China has integrated space far more deeply into its military posture. The capabilities described in this section align with China's doctrine of "systems confrontation" or "systems destruction warfare," [487] which seeks to disable an adversary's networked C4ISR systems at the outset of conflict through coordinated space, cyber, and electronic attacks.

Beyond its military applications Chinese official discourse links space to national prestige, economic development, and diplomatic influence. BeiDou and satellite services are promoted abroad through Belt and Road–related cooperation, and has positioned itself as a provider of space-based public goods in the Asia–Pacific region. The CCP treats space as a source of national pride and as a critical enabler of future warfare, Macro-Theme 8 (Geopolitical Image) and 5 (Strategic Military Development), highlighting the fusion of strategic competition and military pragmatism.

8.16 Conclusions: Comparative Insights

The United States, the European Union, and China have all significantly expanded their space security toolkits, but tailored to different ends and

under different governance logics. The U.S. military-first space posture aims at deterring or winning a high-tech conflict, invests in dominance, offensive, and defensive military space forces.

The EU is in the process of strengthening its ability to withstand space threats and keep the domain safe and accessible, focusing on stability, sovereignty, and rule of law, and invested in autonomous infrastructure, system robustness, and diplomacy instead of weapons.

China rapidly constructed a space power apparatus, with civil and military elements, and the clear intent to secure its rise, challenge U.S. superiority, and protect its strategic interests.

These brief enumerations and description of capabilities do not pretend to encompass the whole space ecosystem of these actors, bu to illustrate capabilities developed and how they are used.

Each actor's discourse frequencies (themes and clusters) align with these outcomes: the U.S. discourse was rich in Military Modernization and Strategic Posture themes (Themes 5 and 8, together 34% of U.S. content), mirrored by its warfighting-oriented buildup; the EU discourse was dominated by Governance/Standards and Infrastructure themes (Themes 7 and 4, over 56% of EU content), and by its focus on regulation and resilience; China's discourse was balanced between Infrastructure, Development, and Geopolitical themes (Themes 4, 3, 1, together 66% of content), corresponding to its pursuit of both advanced systems and status.

This difference in emphasis is not accidental. Each actor operates within a distinct strategic culture that shapes how it defines space security in the first place.

The United States operates within a strategic culture that privileges military primacy and freedom of action. Space security is defined as a military problem requiring technological superiority and rapid response. This explains why U.S. discourse emphasises military modernisation, not because the U.S. is uniquely militaristic, but because its strategic narrative frames space as a contested domain.

China operates within a strategic culture anchored in historical memory and technological aspiration. Space security is defined as essen-

tial to reclaiming China's position as a leading power and undoing historical wrongs. This explains why Chinese discourse balances infrastructure, development, and geopolitical positioning—space is the arena where China demonstrates its legitimacy as a great power.

The European Union operates within a strategic culture focused on rules and negotiated harmonisation. Space security is defined as a regulatory coordination problem, not a military one. This explains why EU discourse emphasises governance and standards—because the EU's institutional logic solves problems through framework-building and norm-setting.

These are not policy choices between alternatives. They are expressions of deeper strategic cultures. And because strategic cultures are rooted in history, institutions, and identity, they are extraordinarily difficult to change.

The language each actor uses in official documents correlates directly with resource allocation, institutional structure, and concrete policy choices. When the U.S. emphasises military themes, it invests in military space capabilities and procurement. When the EU emphasises governance and standards, it builds regulatory frameworks and coordinates across member states. When China emphasises infrastructure and geopolitics, it invests in dual-use systems and positions itself as a legitimate space power.

The implication is that future space governance will not converge. The three actors are not moving toward shared frameworks or a common understanding. They are instead consolidating incompatible positions. The U.S. treats space as a military domain where advantage must be preserved. The EU treats it as a regulatory domain where rules must be harmonised. China treats it as a domain where state capacity must be demonstrated and protected.

This divergence means that international agreements on space arms control are unlikely to succeed, because the three parties disagree fundamentally on what constitutes legitimate state activity. It means that global standards for space cybersecurity will remain contested, with each actor embedding its own governance logic into technical requirements. It means that commercial space supply chains will fragment, as countries

prioritise technological sovereignty.

The practical implication is that space governance conflicts will intensify, and as space systems become more critical to military operations, economic activity, and civilian infrastructure, the stakes of governance disputes will increase. Each actor will invest more heavily in capabilities aligned with its governance model.

The focus on space cybersecurity illustrates this, with all three actors identifying it as critical, but with different approaches. China's insistence on state control of satellite connectivity conflicts with the U.S. model of commercial integration and the EU model of market-based resilience. There is no technical solution to this political problem. No standard can bridge these differences because the differences are not about technology but about authority and control.

Chapter 9

Conclusions and Future Work

9.1 Conclusions

This thesis answers a simple question: is the space domain adequately secured against cyber threats, and do the policies designed to protect it reflect the reality on the ground? The chapters respond negatively but provide a clear map of what needs to change and a set of tools to begin implementing it.

The attack surface of the space sector is large, exposed, and exploitable, as is that of many other critical infrastructure sectors. Still, space represents a single point of failure if compared to other sectors. T he reconnaissance analysis conducted through the Risk Exposure Framework found that a significant number of space organizations, including those operating dual-use and critical infrastructure, carry Internet-facing assets with known, unpatched vulnerabilities that are actively targeted. The Viasat attack demonstrated that a single intrusion into the user segment of a satellite communication network can produce cascading consequences with kinetic and humanitarian effects well beyond the intended target. Ground segment and user terminal security must be treated with the same urgency as spacecraft security, and basic hygiene measures such as

patching, network segmentation, encryption, and access control remain inconsistently applied across the sector.

Existing governance frameworks are not keeping pace with the threat landscape. The comparative analysis of space cybersecurity policies across several countries and jurisdictions reveals a fragmented picture in which requirements are often vague, compliance is difficult to verify, and enforcement is weak or absent. The EU has a strong baseline, through NIS2, the CER Directive, ESA standards, and the forthcoming European Space Law, but there is a wide gap between regulatory ambition and operational reality. No jurisdiction currently provides organizations with a clear, standardized methodology for demonstrating compliance with cybersecurity requirements. The compliance assessment tool developed in this thesis, which maps CIS Controls to the expected requirements of European Space Law, is a direct attempt to fill that gap before the legislation is enacted.

Without concrete indicators of security posture, neither organizations nor regulators can assess whether investments in cybersecurity are producing outcomes. The mapping of existing security metrics to the NIST CSF 2.0 reveals systematic coverage gaps, particularly in the Respond and Recover functions, capabilities most relevant to operational resilience. The seven new metrics proposed for the space sector, tested against a realistic satellite network architecture, show that meaningful measurement is achievable even in a domain as technically complex as space.

In this complex scenario, China, the United States, and the European Union do not merely disagree on policy details; they also operate from different governance philosophies, threat models, and assumptions about the relationship among state authority, commercial actors, and security. These divergences constrain the prospects for international cooperation and carry direct implications for European space security strategy. The EU's regulatory approach has real influence. Still, it will need stronger enforcement capacity and greater technical specificity if it is to produce security outcomes rather than compliance and an additional layer of bureaucratic complexity for companies.

The space domain is increasingly critical, increasingly threatened, and

insufficiently protected. The tools to improve this situation exist: empirical risk assessment, measurable security metrics, compliance frameworks, and a clearer-eyed understanding of geopolitical constraints. What remains is the institutional capacity and the political will, to use them.

9.2 Future work

This thesis presents a systematic attempt to map the cybersecurity of the space domain from both technical and policy perspectives. Precisely because it is a first map, it leaves significant territory unexplored.

The geopolitical and technological context has shifted considerably, even over the course of this research. Active conflicts in Europe, the Middle East, and Latin America have rendered space infrastructure a contested operational environment, with satellite communications and Earth observation systems documented roles in military operations. At the same time, the rapid diffusion of AI tools, automation, and autonomous agents altered both the offensive and defensive sides of cybersecurity in ways that were not fully foreseeable at the outset of this work. Future research will need to account explicitly for both dynamics.

On the technical side, the Risk Exposure Framework developed in this thesis operates as a point-in-time snapshot of an organization's exposed attack surface. A natural and important extension would be to automate and continuously update this scanning process, moving from periodic assessments to near-real-time monitoring. Future work could integrate automated exploit generation and controlled exploitation testing of identified CVEs, transforming REF from a risk assessment tool into a full adversarial simulation capability. This would bring the framework closer to what red teams do in practice, but at a scale and repeatability that manual testing cannot achieve. Additionally, the current framework focuses exclusively on the ground segment and Internet-facing infrastructure. Extending the analysis to onboard spacecraft systems, despite their more isolated and proprietary nature, remains an open and technically demanding challenge that the field has not yet addressed in a systematic way.

On the policy side, the frameworks and compliance tools proposed in this thesis anticipate legislation, particularly the European Space Law, that was still under development at the time of writing. A critical next step will be to evaluate whether these instruments hold up once the legislation is finalized, whether the mapping of CIS Controls to regulatory requirements remains accurate, and whether the tools prove useful to practitioners navigating real compliance processes. Beyond validation, future research could extend the governance comparison to actors currently absent from the analysis, including Russia, India, and the Gulf states, each of which is developing a significant space industrial base with distinct regulatory assumptions. Finally, the question of whether policy frameworks, once adopted, actually produce measurable improvements in organizational security posture remains largely unanswered in the literature. Studies tracking the security metrics of space organizations before and after regulatory interventions would provide the kind of empirical grounding that policy evaluation in this domain currently lacks.

Appendix A

Appendix Title

A.1 Macro Themes Overview

Table 36: Macro-Themes Overview

Macro-Theme No. & Title	Definition / Inclusion Criteria	Typical Indicators / Keywords	Illustrative Example (from Corpus)
1 International-ism and Global Governance	References to multilateral cooperation, international law, diplomacy, and the governance of outer space as a global commons.	international cooperation, UN, multilateralism, global governance, norms, treaties, collaboration, transparency	*"The EU will promote responsible behaviour in space through multilateral dialogue."* [129]
2 Peaceful Development and Normative Framing	Language stressing peace, restraint, sustainability, or moral principles guiding space activity.	peaceful use, stability, restraint, non-weaponisation, sustainability, responsible behaviour	*"China always adheres to the peaceful use of outer space."* [480]
3- National Development and Technological Advancement	Discussion of innovation, R&D, national rejuvenation, industrial or scientific progress through space activities.	innovation, frontier science, R&D, technology, modernization, talent, industrial upgrading	*"The Space Act will foster innovation and competitiveness of European industry."* [193]
4 Space Infrastructure and Capability Building	Material capabilities: satellites, launchers, ground systems, communications, navigation, resilience.	satellites, GNSS, EO, launch, TT&C, infrastructure, redundancy, resilience	*"The U.S. will field resilient architectures to ensure assured access to space."* [512]
5 Military Modernisation and Civil–Military Integration	References to military reform, joint operations, dual-use technology, or defence-industrial mobilisation.	PLA, defence, military modernisation, dual-use, integration, strategic deterrence	*"China will accelerate military–civil fusion in space technology."* [480]
6 Commercialisation and Industry	Mentions of private sector involvement, markets, entrepreneurship, industrial policy, or competition.	commercial, industry, market, PPP, innovation, competitiveness, new space	*"The Executive Order will enable competition in the commercial space industry."* [220]

7 Space Governance, Law and Standards	Legal and regulatory frameworks, oversight, technical standards, STM, liability, compliance.	regulation, legislation, standards, licensing, oversight, debris, STM	*"Regulation 2023/588 establishes rules for secure connectivity and governance."* [204]
8 Geopolitical Positioning and Strategic Image	Discourses linking space policy to prestige, global leadership, national identity, or geopolitical competition.	great-power, leadership, image, prestige, competition, multipolarity	*"Space achievements demonstrate China's rejuvenation as a great power."* [480]

Table 36: Macro-Themes Overview

A.2 Clusters

Table 37: Order Clusters — Macro-Themes and Sub-Clusters

Code	Cluster Label	Definition / Inclusion Criteria	Typical Indicators / Keywords	Illustrative Example (from Corpus)
Macro-Theme 1 — Internationalism and Global Governance				
1.1	International Cooperation (bilateral / multilateral)	Cooperative programmes, bilateral agreements, joint missions, participation in multilateral fora.	cooperation, partnership, joint mission, exchange, coordination	*"ESA and NASA will deepen transatlantic cooperation."*
1.2	Multilateral Governance and Treaties	References to UN treaties, COPUOS, global norms, or arms-control initiatives.	UN, Outer Space Treaty, PPWT, international law	*"Support for the UN framework on long-term sustainability."*
1.3	Global Leadership and Stability	Claims of leadership in maintaining global stability or norms.	leadership, stability, order, predictability	*"The U.S. will lead global efforts for a safe and sustainable space domain."*
Macro-Theme 2 — Peaceful Development and Normative Framing				
2.1	Peaceful Purpose and Peace Operations	Peaceful use, humanitarian assistance, disaster management.	peaceful, humanitarian, rescue, disaster response	*"Copernicus data support humanitarian aid operations."*
2.2	Disarmament and Arms Control	Calls for preventing an arms race in outer space.	disarmament, non-proliferation, no first use, arms control	*"Oppose weaponisation of outer space."*
2.3	Anti-Weaponisation and Demilitarisation	Explicit rejection of weapons in orbit or tests.	demilitarisation, non-weaponisation, restraint	*"The EU supports a ban on debris-creating ASAT tests."*
2.4	Non-Alignment and Restraint Norms	Advocacy of self-restraint, non-aggression, neutrality.	restraint, neutrality, minimal force	*"China advocates a defensive national defence policy."*
Macro-Theme 3 — National Development and Technological Advancement				
3.1	Economic Development and National Rejuvenation	Linking space to economic growth or national revival.	economic growth, rejuvenation, prosperity	*"Space contributes to building a modern socialist country."*

Continued on next page

Table 37 continued from previous page

Cluster Code	Cluster Label	Definition / Inclusion Criteria	Typical Indicators / Keywords	Illustrative Example (from Corpus)
3.2	Innovation, R&D and Frontier Science	Research, innovation, frontier exploration, new technologies.	innovation, R&D, frontier, breakthrough	*"Promoting cutting-edge technologies for exploration."*
3.3	Indigenous Capability and Self-Reliance	National autonomy in technology and supply chains.	self-reliance, domestic capability, autonomy	*"Developing autonomous European launch access."*
3.4	Technology Demonstration and Diffusion	Application of tech in civilian sectors.	technology transfer, diffusion, application	*"Space data used for climate monitoring and agriculture."*
3.5	State-Led Planning and Policy Support	Industrial or strategic planning instruments.	policy plan, roadmap, 5-year plan, coordination	*"The 14th Five-Year Plan defines priorities for space."*
Macro-Theme 4 — Space Infrastructure and Capability Building				
4.1	Satellite Systems and Applications	Communication, EO, navigation, or scientific satellites.	GNSS, EO, SatCom, constellation	*"Deployment of the BeiDou navigation system."*
4.2	Ground and Control Infrastructure	Ground stations, TT&C, command networks.	TT&C, control centre, ground station	*"EU SSA network for autonomous tracking."*
4.3	Deep-Space Exploration and Utilisation	Lunar, Martian, or asteroid missions; resource utilisation.	lunar, deep space, interplanetary, resource	*"Artemis III will return astronauts to the Moon."*
4.4	Human Spaceflight and Platforms	Crewed missions, stations, life-support, EVA.	crewed, space station, astronauts	*"Operation of Tiangong space station."*
4.5	Launch and Propulsion Systems	Launch vehicles, propulsion R&D, reusability.	launcher, propulsion, Long March, Vega	*"Testing reusable launcher prototypes."*
4.6	Cross-Cutting Capability and Resilience	Redundancy, robustness, secure connectivity.	resilience, redundancy, secure links	*"Fielding resilient architectures to ensure assured access."*
4.7	Space Combat and Weaponisation	Military use of space or counter-space capability.	counter-space, ASAT, defence space operations	*"PLA Aerospace Force conducts counter-space drills."*
Macro-Theme 5 — Military Modernisation and Civil–Military Integration				
5.1	Military Modernisation and Reform	Structural reform, new services, doctrine change.	reform, modernisation, restructuring	*"Establishment of the U.S. Space Force."*
5.2	Civil–Military Integration and Dual-Use Coordination	Integration of civilian and military resources.	dual-use, integration, synergy	*"Promoting civil–military integration in space R&D."*
5.3	Doctrine, Deterrence and Strategic Posture	Strategic doctrines, deterrence concepts.	deterrence, strategy, warfighting	*"Deterring aggression in, from, and to space."*
5.4	Resourcing and Buildup	Budgets, defence spending, resource allocation.	investment, funding, procurement	*"Increase defence spending for space resilience."*
Macro-Theme 6 — Commercialisation and Industry				
6.1	Market Development and Commercial Expansion	Private sector participation, new space markets.	market, competition, entrepreneurship	*"Support for start-ups through ESA BICs."*

Continued on next page

Table 37 continued from previous page

Cluster Code	Cluster Label	Definition / Inclusion Criteria	Typical Indicators / Keywords	Illustrative Example (from Corpus)
6.2	Technology Diffusion and Value-Chain Integration	Integration of space tech in value chains.	supply chain, integration, industrial ecosystem	*"Promoting end-to-end industrial integration."*
6.3	Export Controls and International Trade	Regulation of exports or international market access.	export control, trade, technology transfer	*"Compliance with international export-control regimes."*
6.4	Indigenous Self-Reliance and Supply-Chain Security	Domestic production, supply-chain resilience.	localisation, sovereignty, autonomy	*"Ensuring EU sovereignty over critical space assets."*
Macro-Theme 7 — Space Governance, Law and Standards				
7.1	Legal Frameworks and Treaties	National or international legal regimes.	law, treaty, convention, ratification	*"Ratification of the Registration Convention."*
7.2	National Regulations and Oversight	National laws, licensing, oversight mechanisms.	regulation, licence, oversight	*"Licensing of private launch operators."*
7.3	Technical and Safety Standards	Standards, quality, certification.	standardisation, ISO, interoperability	*"Adoption of common standards for satellite design."*
7.4	Debris Mitigation and Space-Traffic Management	Debris control, STM, post-mission disposal.	debris, STM, disposal, mitigation	*"EU approach for space-traffic management."*
7.5	Transparency and Confidence-Building Measures (CBMs)	Data sharing, notification, openness.	transparency, CBM, data exchange	*"Advance transparency through open data policies."*
Macro-Theme 8 — Geopolitical Positioning and Strategic Image				
8.1	National Prestige and Image-Building	Nation-branding, pride, symbolic success.	prestige, pride, achievement	*"A symbol of national rejuvenation and pride."*
8.2	Responsible Great-Power Leadership	Leadership tied to responsibility and ethics.	responsible power, leadership, stewardship	*"U.S. leadership will ensure a secure space environment."*
8.3	Historical Narrative and Memory	References to past achievements or legacy.	history, heritage, memory	*"Celebrating 60 years of human spaceflight."*
8.4	Strategic Competition and Regional Focus	Rivalry, strategic competition, regional security.	competition, rivalry, Asia-Pacific, alliance	*"China faces strategic competition in the Asia-Pacific."*

A.3 Sentiment Coding Scheme

Sentiment Label	Definition / Interpretive Rule	Discursive Markers / Typical Expressions	Illustrative Example (from Corpus)
Conciliatory	Texts promoting cooperation, partnership, peace, or shared benefit.	cooperate, partnership, mutual, peaceful, shared future	*"Outer space should serve the common interests of humankind."* (China 2021)
Cautious	Balanced tone acknowledging challenges or uncertainty; prudent, technical, or conditional phrasing.	ensure safety, take measures, safeguard, manage risk	*"Member States shall take appropriate measures to ensure resilience."* (EU 2023)
Neutral	Descriptive or factual statements without evaluative tone.	provides, launches, includes, establishes	*"The EU Space Programme integrates Galileo and Copernicus."*
Assertive	Confident, leadership-oriented language expressing national or institutional strength or initiative.	lead, enhance, strengthen, accelerate	*"The United States will lead in the exploration and utilisation of outer space."*
Combative	Confrontational or competitive stance; references to defence, deterrence, or opposition.	oppose, deter, defend, counter, combat	*"The PLA Aerospace Force will defend national interests in outer space."*

Table 38: Sentiment Coding Scheme: Tone Analysis Categories

References

[1] 118th Congress (2023–2024). *Satellite Cybersecurity Act*. Tech. rep. 2023. URL: https://www.congress.gov/bill/118th-congress/senate-bill/1425.

[2] Federal Ministry for Economic Affairs (BMWK) and Climate Action. *The German Federal Government's Space Strategy*. Tech. rep. BMWK, 2023. URL: https://www.bmwi.de/Redaktion/EN/Publikationen/Technologie/the-german-federal-governments-space-strategy.pdf?__blob=publi.

[3] Consultative Committee for Space Data Systems (CCSDS). *Space Data Link Security Protocol (CCSDS 355.0-B-2)*. Tech. rep. CCSDS, 2022. URL: https://public.ccsds.org/Pubs/355x0b2.pdf.

[4] {CCSDS}. *Unified Space DATA link Protocol (USLP)*. Tech. rep. CCSDS, 2024. URL: https://public.ccsds.org/Pubs/732x1b3e1.pdf.

[5] {Kritikalität: Von der BSI-KritisV zur NIS2-Richtlinie}. "Vogel, V". In: *International Cybersecurity Law Review* (2023).

[6] 2023. "Wannafly: An approach to satellite ransomware." In: *2023. Falco, Gregory, Rajiv Thummala, and Arpit Kubadia. s.l. : IEEE 9th International Conference on Space Mission Challenges for Information Technology (SMC-IT)*. 2023.

[7] UK Parliament POSTNOTE 654). *Defence of Space-Based Assets (Technical Report No*. Tech. rep. 2024. URL: https://post.parliament.uk/research-briefings/post-pn-0654/.

[8] et . al. A. M. S. N. Amarasinghe. "' AI Based Cyber Threats and Vulnerability Detection, Prevention and Prediction System '". In: *International Conference on Advancements in Computing (ICAC), pp. 363–368 , doi : 10.1109/ICAC49085.2019.9103372* (2019).

[9] Joscha Abels. "Private infrastructure in geopolitical conflicts: The case of Starlink and the war in Ukraine". In: *European Journal of International Relations* 30.4 (2024), pp. 842–866.

[10] AI Act. *AI Act, Para 2, Annex III*.

[11] Department of Homeland Security Cybersecurity Agency and Infrastructure Security. *Budget Overview Fiscal Year 2024 Congressional Justification*. Tech. rep. US Government - CISA, 2024. URL: https://www.dhs.gov/sites/default/files/2023-03/CYBERSECURITY%20AND%20INFRASTRUCTURE%20S.

[12] National Security Agency. *Cybersecurity Advisory: Protecting VSAT Communications*. Tech. rep. U/OO/106122-22 — PP-22-0085. Version 1. National Security Agency, Jan. 2022.

[13] UK Space Agency. *Cyber Security Toolkit*. 2021. URL: https://www.gov.uk/government/publications/cyber-security-toolkit.

[14] *L. Sánchez, M. Vasile, and E. Minisci, ' AI to support decision making in collision risk assessment ' (2019) 70th International Astronautical Congress*. 2019.

[15] *A. Bécue, I. Praça, and J. Gama, ' Artificial intelligence, cyber- threats and Industry 4.0: challenges and opportunities ' (2021) Artif . Intell. Rev., vol. 54, no. 5, pp. 3849–3886, doi : 10.1007/s10462-020-09942-2*. 2021.

[16] *Art. 2(3), see note 29*.

[17] *Art. 2(6), see note 29*.

[18] *Art. 6(1), see note 29*.

[19] *Art. 6(2), see note 29*.

[20] *Art. 6(3), see note 29*.

[21] *Art. 6(5), see note 29*.

[22] *Art. 6(8), see note 29*.

[23] *Art. 7, se e note 29*.

[24] *Art. 9 (10), see note 29*.

[25] *Ibid*.

[26] *Recital 55, see note 6*.

[27] *See note 29*.

[28] *See note 9*.

[29] *An undertaking is any entity engaged in an economic activity, regardless of its legal status or the way it is financed*.

[30] Air and Space Forces. *Backdoor to Attack Satellites: CSO Highlights Ground Networks*. Accessed on 07 2023. 2023. URL: https://www.airandspaceforces.com/backdoor-to-attack-satellites-cso-highlights-ground-networks/.

[31] Airbus. *Airbus reports Full-Year (FY) 2024 results*. Accessed: 2025-03-30. Airbus. Feb. 2025. URL: https://www.airbus.com/en/newsroom/press-releases/2025-02-airbus-reports-full-year-fy-2024-results.

[32] Saleh AlDaajeh et al. "The role of national cybersecurity strategies on the improvement of cybersecurity education". In: *Computers & Security* 119 (2022), p. 102754.

[33] Faozi A Almaqtari et al. "The mediating effect of IT governance between corporate governance mechanisms, business continuity, and transparency & disclosure: An empirical study of Covid-19 Pandemic in Jordan". In: *Information Security Journal: A Global Perspective* 32.1 (2023), pp. 39–57.

[34] Izzat Alsmadi et al. "Vulnerability assessment of industrial systems using Shodan". In: *Cluster Computing* 25.3 (2022), pp. 1563–1573.

[35] Bruno Amable. "Institutional complementarities in the dynamic comparative analysis of capitalism". In: *Journal of institutional economics* 12.1 (2016), pp. 79–103.

[36] We Have an Anomaly: America Is Missing a Space Systems Critical Infrastructure Sector. *Ellsworth, J.* 2023.

[37] Joseph C Anselmo. ""Hide and Seek in Orbit: China Expands Military Space Capabilities."" In: *Aviation Week, Space Technology* (2025). URL: https://aviationweek.com/space/budget-policy-regulation/hide-seek-orbit-china-expands-military-space-capabilities.

[38] Vaibhav Anu. "Information security governance metrics: a survey and taxonomy". In: *Information Security Journal: A Global Perspective* 31.4 (2022), pp. 466–478.

[39] Apache Software Foundation. *CVE-2023-25690*. National Vulnerability Database (NVD). 2023. URL: %7Bhttps://nvd.nist.gov/vuln/detail/CVE-2023-25690%7D.

[40] Abouzar Arabsorkhi and Fariba Ghaffari. "Security metrics: principles and security assessment methods". In: *2018 9th International Symposium on Telecommunications (IST)*. IEEE. 2018, pp. 305–310.

[41] Aletéia Patrícia Favacho de Araújo, Paulo Franklin von Paumgartten, and Augusto César de Carvalho Fonseca. "Maturity analysis of information access control in an organization". In: *2013 8th Iberian Conference on Information Systems and Technologies (CISTI)*. IEEE. 2013, pp. 1–6.

[42] Josep Maria Perdigues Armengol et al. "Quantum communications at ESA: Towards a space experiment on the ISS". In: *Acta Astronautica* 63.1-4 (2008), pp. 165–178.

[43] Cyber defense of space assets. *Hutchins, R.*, 2016.

[44] The UK Civil Aviation Authority and European Air Services Liberalisation. "Humphreys, B.," in: *Journal of Transport Economics and Policy* (1996).

[45] Civil Aviation Authority. *Guidance on Cyber Security Strategies for Applicants and Licensees*. Tech. rep. 2023. URL: https://www.caa.co.uk/publication/pid/11990.

[46] Benjamin Aziz, Ali Malik, and Jeyong Jung. "Check your blind spot: a new cyber-security metric for measuring incident response readiness". In: *Risk Assessment and Risk-Driven Quality Assurance: 4th International Workshop, RISK 2016, Held in Conjunction with ICTSS 2016, Graz, Austria, October 18, 2016, Revised Selected Papers 4*. Springer. 2017, pp. 19–33.

[47] Michael Bartock et al. *Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services*. NISTIR NISTIR 8323. Superseded By: NISTIR 8323 Rev. 1 (01/31/2023). National Institute of Standards and Technology (NIST), Feb. 2021. URL: https://doi.org/10.6028/NIST.IR.8323.

[48] Michel Benaroch. "Cybersecurity risk in IT outsourcing—Challenges and emerging realities". In: *Information systems outsourcing: The era of digital transformation* (2020), pp. 313–334.

[49] Roberto C. Benitez. "Cyber Vulnerabilities in Satellite Communication Networks". MA thesis. Utica College, Jan. 2021.

[50] MM Bennett et al. "Improving satellite monitoring of armed conflicts". In: *Earth's Future* 10.9 (2022), e2022EF002904.

[51] Jahshan Bhatti and Todd E Humphreys. "Hostile control of ships via false GPS signals: Demonstration and detection". In: *NAVIGATION: Journal of the Institute of Navigation* 64.1 (2017), pp. 51–66.

[52] Rareș-Cristian Bișag and Dragoș Ilinca. "Enhancing Security Through Earth Observation: The Role of Copernicus in Monitoring Emerging Threats". In: *Land Forces Academy Review* 30.2 (2025), pp. 321–332.

[53] Einar Bjorgo and Olivier Senegas. "Operational applications of space technologies in international humanitarian emergency response". In: *Information Systems for Emergency Management* 16 (2009), pp. 279–301.

[54] BleepingComputer. *Hackers leak passwords for 500,000 Fortinet VPN accounts*. Accessed on 07 2023. 2021. URL: https://www.bleepingcomputer.com/news/security/hackers-leak-passwords-for-500-000-fortinet-vpn-accounts/.

[55] Bloomberg. *Bloomberg.com, ' What Kamala Harris Means for the Future of AI Policy ' Jul. 25, 2024* , 2024. URL: https://www.bloomberg.com/news/newsletters/2024-07-25/what-kamalaharris-means-for-the-future-of-ai-policy.

[56] Deborah J Bodeau et al. “Cyber resiliency metrics catalog”. In: *The MITRE Corporation, Bedford, MA* (2018).

[57] IT-Grundschutz-Profil für das Bodensegment von Satelliten. *undesamt für Sicherheit in der Informationstechnik*. Tech. rep. ESA, 2024. URL: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Profil_Bodensegment-Satellit.pdf?_.

[58] Sébastien Bonnart et al. “Chapter 3 Cybersecurity Threats to Space: From Conception to the Aftermaths”. In: Leiden, The Netherlands: Brill — Nijhoff, 2023, pp. 39–101. ISBN: 9789004527270. DOI: 10.1163/9789004527270_004. URL: https://brill.com/view/book/9789004527270/BP000004.xml.

[59] Harold Booth, Doug Rike, and Gregory A Witte. *The national vulnerability database (nvd): Overview*. 2013. URL: https://nvd.nist.gov/.

[60] Salvatore Borgia, Francesco Topputob, and Stefano Zaneroc. “HACK: a Holistic modeling Approach for Cubesat cyberattacKs”. In: *Aerospace Science and Engineering: III Aerospace PhD-Days* 33 (2023), p. 281.

[61] Emanuele Borgonovo and Elmar Plischke. “Sensitivity analysis: A review of recent advances”. In: *European Journal of Operational Research* 248.3 (2016), pp. 869–887.

[62] Nicolò Boschetti, Nathaniel G Gordon, and Gregory Falco. “Space Cybersecurity Lessons Learned from The ViaSat Cyberattack”. In: *ASCEND 2022*. 2022, p. 4380.

[63] Wayne Boyer and Miles McQueen. “Ideal based cyber security technical metrics for control systems”. In: *Critical Information Infrastructures Security: Second International Workshop, CRITIS 2007, Málaga, Spain, October 3-5, 2007. Revised Papers 2*. Springer. 2008, pp. 246–260.

[64] Matthea Brandenburg and Sarah Lieberman. “Critical spaces: European and US institutions for outer space”. In: *Astropolitics* 20.1 (2022), pp. 93–111.

[65] P. Breda. *P. Breda , et. al. ‘ An extended review on cyber vulnerabilities of AI technologies in space applications: Technological challenges and international governance of AI ’ (2023) J. Space Saf. Eng., vol. 10, no. 4, pp. 447–458 , doi : 10.1016/j.jsse.2023.08.003*. 2023.

[66] Broad Band Forum. *TR-069 CPE WAN Management Protocol*. Accessed on 07 2023. 2020. URL: https://www.broadband-forum.org/download/TR-069_Amendment-2.pdf.

[67] W Krag Brotby and Gary Hinson. *Pragmatic security metrics: applying metametrics to information security*. CRC Press, 2016.

[68] BryceTech. *2024 Q2 Launch and Satellite Trends*. 2024. URL: https://brycetech.com/reports.

[69] William Burke-White and Benjamin Gwyn Williams. *Geopolitical ambitions and rule contestations in space governance*. Tech. rep. CIGI Papers, 2025.

[70] George W Bush. "Executive order on critical infrastructure protection". In: *Proceedings of the 12th annual conference on Computers, freedom and privacy*. 2002, pp. 1–10.

[71] A. Calcara. *A. Calcara and G. Tricco, ' Outer Limits? Economic Security and the European Space Sector" (2024) CSDS Policy Brief*. 2024. URL: https://csds.vub.be/publication/outer-limits-economicsecurity-and-the-european-space-sector/.

[72] David Calcutt and Laurie Tetley. *Satellite communications: principles and applications*. Butterworth-Heinemann, 1994.

[73] Space Capital. *Space Investment Quarterly — Q1 2024*. 2024. URL: https://www.spacecapital.com/space-investment-quarterly.

[74] Maurantonio Caprolu et al. "Vessels cybersecurity: Issues, challenges, and the road ahead". In: *IEEE Communications Magazine* 58.6 (2020), pp. 90–96.

[75] Antonio Carlo and Kim Obergfaell. "Cyber attacks on critical infrastructures and satellite communications." In: *International Journal of Critical Infrastructure Protection* (2024).

[76] Antonio Carlo et al. "The importance of cybersecurity frameworks to regulate emergent AI technologies for space applications". In: *Journal of Space Safety Engineering* (2023).

[77] Francesco Casaril and Letterio Galletta. "Assessing the Attack Surface of Space Organizations: A Data-Driven Analysis". In: *Under Review* 0.0 (2025).

[78] Francesco Casaril and Letterio Galletta. *Assessing the Attack Surface of Space Organizations: A Data-Driven Analysis (Supplementary Material)*. https://github.com/Fracas20/REF-Risk-Exposure-Framework. 2025.

[79] Francesco Casaril and Letterio Galletta. "Developing Security Metrics for Space Systems: A Study Considering the NIST Cybersecurity Framework 2.0 and the NIS2". In: *Under Review* 0.0 (2025).

[80] Francesco Casaril and Letterio Galletta. *Developing Security Metrics for Space Systems: A Study Considering the NIST Cybersecurity Framework 2.0 and the NIS2 (Online Supplementary Material)*. https://sites.google.com/view/spacemetrics/home-page. 2025.

[81] Francesco Casaril and Letterio Galletta. "Securing SatCom user segment: A study on cybersecurity challenges in view of IRIS". In: *Comput. Secur.* 140 (2024), p. 103799. DOI: 10.1016/J.COSE.2024.103799. URL: https://doi.org/10.1016/j.cose.2024.103799.

[82] Francesco Casaril and Letterio Galletta. "Space cybersecurity governance: assessing policies and frameworks in view of the future European space legislation". In: *J. Cybersecur.* 11.1 (2025). DOI: 10.1093/CYBSEC/TYAF013. URL: https://doi.org/10.1093/cybsec/tyaf013.

[83] Francesco Casaril and Giovanni Tricco. "Space Infrastructure as Critical Infrastructure: Rights Beyond Earth in the Digital Age". In: *Technology and Regulation* In Press.0 (2026).

[84] H Cavusoglu. "HC and Jun Zhang". In: *Economics of security patch management. In workshop on the Economics of Information Security, Cambridge, UK*. 2006.

[85] CEN–CENELEC. *Position Paper on Standardisation and the EU Space Act, 2023*. Tech. rep. CEN–CENELEC, 2023. URL: https://www.cencenelec.eu/media/CEN-CENELEC/News/Brief%20News/2025/cen-and-cenelec-position-paper-on-eu-space-act.pdf.

[86] *CEOS Supporting Hurricane Matthew Recovery in Southwest Haiti — The 1st Recovery Observatory Triggered*. 2016. URL: https://ceos.org/home-2/ceos-supporting-hurricane-matthew-recovery-in-southwest-haiti-the-1st-recovery-observatory-triggered/.

[87] Michael B Cerny et al. "Countering Co-Orbital ASATs: Warning Zones in GEO as a Lawful Trigger for Self-Defense". In: *Study Report, May* (2020).

[88] *CFR 13636 - Executive Order 13636 of 02 12, 2013. Improving Critical Infrastructure Cybersecurity*. Federal Register. Vol. 78, No. 33, 02 19, 2013. 2013.

[89] Yi Cheng et al. "Metrics of security". In: *Cyber defense and situational awareness* (2014), pp. 263–295.

[90] Elizabeth Chew et al. *Guide for Developing Performance Metrics for Information Security*. Tech. rep. National Institute of Standards and Technology, 2006.

[91] Elizabeth Chew et al. *Performance Measurement Guide for Information Security*. Tech. rep. U.S. Department of Commerce. Gaithersburg, MD: National Institute of Standards and Technology, July 2008. URL: https://www.nist.gov/document-13265.

[92] Pier Giorgio Chiara. "The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements: An introduction". In: *International Cybersecurity Law Review* 3.2 (2022), pp. 255–272.

[93] Cyberspace Administration of China (CAC). *cac.gov.cn*. Tech. rep. Cyberspace Administration of China (CAC), Administrative Measures for Terminal Devices Directly Connecting to Satellite Services (Draft for Public Comment), 2024. URL: https://www.cac.gov.cn.

[94] China in Space. *China Concludes Global Launches in 2023*. Accessed 2026. 2023. URL: https://china-in-space.com/p/china-concludes-global-launches-in.

[95] Paolo Chini, Giovanni Giambene, and Sastri Kota. "A survey on mobile satellite systems". In: *International Journal of Satellite Communications and Networking* 28.1 (2010), pp. 29–57.

[96] F.J. Cilluffo. *and Cardash, S., .* 2023. URL: https://spacenews.com/time-to-designate-space-systems-as-critical-infrastructure/.

[97] *CIS Controls Measures and Metrics for Version 7*. https://www.uio.no/studier/emner/matnat/ifi/IN2120/h18/docs/cis-controls-measures-and-metrics-v7.pdf. Accessed: 2024-09-29. Center for Internet Security, 2018.

[98] CISA. *Resilient Positioning, Navigation, and Timing (PNT) Conformance Framework, Version 2.0*. Tech. rep. Department of Homeland Security (DHS) and CISA, May 2022. URL: https://www.dhs.gov/sites/default/files/2022-05/22_0531_st_resilient_pnt_conformance_framework_v2.0.pdf.

[99] 2021 CISA. *FY 2021*. Tech. rep. CISA, 2021. URL: https://www.cisa.gov/sites/default/files/2023-01/Section_9002_NDAA_Report_FINAL_508c.pdf.

[100] Zachary A Collier et al. "Security metrics in industrial control systems". In: *Cyber-security of SCADA and other industrial control systems* (2016), pp. 167–185.

[101] John M Colombi et al. "Multi-objective parallel optimization of geosynchronous space situational awareness architectures". In: *Journal of Spacecraft and Rockets* 55.6 (2018), pp. 1453–1465.

[102] EU Commission et al. "Recommendation 2003/361/EC". In: *Official Journal L* 124 (2003).

[103] European Commission. *Commission Work Programme 2024*. Tech. rep. 2024. URL: https://commission.europa.eu/strategy-and-policy/strategy-documents/commission-work-programme/commission-work-programme-2024_en.

[104] European Commission. *EU Space Strategy for Security and Defence*. Tech. rep. European Commission, 2023. URL: https://defence-industry-space.ec.europa.eu/eu-space/eu-space-strategy-security-and-defence_en.

[105] European Commission. *European Commission , ' White Paper on Artificial Intelligence: A European approach to excellence and trust ' (2020)*. Tech. rep. European Commission, 2020.

[106] European Commission. *Proposal for a Regulation of the European Parliament and of the Council on the safety, resilience and sustainability of space activities in the Union*. COM(2025) 335 final; 2025/0335 (COD). Accessed 12 July 2025. Brussels, June 2025. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0335.

[107] European Commission. *Proposal for a Regulation on the safety, resilience and sustainability of space activities in the Union (EU Space Act)*. Accessed 2025-09-27. 2025. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0335.

[108] Common Vulnerabilities and Exposures (CVE). *CVE-2018-13379*. Accessed on 07 2023. 2018. URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13379.

[109] McKinsey & Company. *The Commercial Space Age Is Here: How Companies Can Make the Most of It*. 2023. URL: https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/space-the-1-point-8-trillion-dollar-opportunity-for-global-economic-growth.

[110] *12th Edition, The Comsys VSAT Report, VSAT Statistics*. Accessed on 07 2023. 2010. URL: https://www.comsys.co.uk/wvr_stat.htm.

[111] Comtech. *10-Q Quarterly Report - 2024 Q1*. Access the quarterly report via the U.S. Securities and Exchange Commission (SEC) at https://s3.amazonaws.com/sec.irpass.cc/2718/0000023197-23-000070.htm. Accessed on: Insert Accessed Date. 2023.

[112] Comtech. *Comtech EF Data - Satellite Modems*. Accessed on 07 2023. 2023. URL: https://www.comtechefdata.com/products/satellite-modems.

[113] Congressional Budget Office. *Congressional Budget Office Cost Estimate*. https://www.cbo.gov/publication/59203. Accessed on: June, 2023. 2023.

[114] ConnexionFrance. *Thousands in France lose internet in suspected Russian cyberattack*. Accessed on 07 2023. 2022. URL: https://www.connexionfrance.com/article/French-news/Thousands-in-France-lose-internet-in-suspected-Russian-cyberattack.

[115] David A. Cooper et al. *NIST Special Publication 800-208: Recommendation for Stateful Hash-Based Signature Schemes*. NIST Special Publication 800-208. Computer Security Division, Information Technology Laboratory, Oct. 2020. URL: https://doi.org/10.6028/NIST.SP.800-208.

[116] *Copernicus Emergency Management Service — Statistics*. 2024. URL: https://mapping.emergency.copernicus.eu/stats/.

[117] *Copernicus Programme Overview*. 2023. URL: https://www.copernicus.eu/en.

[118] L Corcoran and M Jenkins. *RFC 9206 Commercial National Security Algorithm (CNSA) Suite Cryptography for Internet Protocol Security (IPsec)*. Accessed on 07 2023. 2022. URL: https://datatracker.ietf.org/doc/rfc9206/.

[119] Aerospace Corporation. *Resilience for Space Systems: Concepts, Tools and Approaches*. 2017.

[120] Ricardo Correia et al. "User terminal segments for low-Earth orbit satellite constellations: Commercial systems and innovative research ideas". In: *IEEE Microwave Magazine* 23.10 (2022), pp. 47–58.

[121] Rory Coulter et al. "Data-driven cyber security in perspective—Intelligent traffic analysis". In: *IEEE transactions on cybernetics* 50.7 (2019), pp. 3081–3093.

[122] White House / National Security Council. *Space System Cybersecurity: Industry Perspectives, 2023*. Tech. rep. White House / National Security Council, 2023. URL: https://bidenwhitehouse.archives.gov/wp-content/uploads/2025/01/Space-System-Cybersecurity-Industry-Perspectives-Report.pdf.

[123] *A Strategic Compass for Security and Defence*. Accessed on 07 2023. 2022. URL: https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/.

[124] Council of the European Union. *A Strategic Compass for Security and Defence*. Tech. rep. Council of the European Union, 2022.

[125] Council of the European Union. *Council Conclusions on an EU Approach to Space Traffic Management*. Tech. rep. Council of the European Union, 2022.

[126] Council of the European Union. *Council Conclusions on Copernicus 2035*. Tech. rep. Council of the European Union, 2022.

[127] Council of the European Union. *Council Conclusions on Key Principles for the Global Space Economy*. Tech. rep. Council of the European Union, 2020.

[128] Council of the European Union. *Council Conclusions on Space as an Enabler*. Tech. rep. Council of the European Union, May 2019.

[129] Council of the European Union. *Council Conclusions on the EU Space Strategy for Security and Defence*. Tech. rep. Council of the European Union, 2023.

[130] Council of the European Union. *EU Shapes its Future Space Policy Programme*. Tech. rep. Council of the European Union, 2019.

[131] Edward Criscuolo, Keith Hogie, and Ron Parise. "Transport protocols and applications for Internet use in space". In: *2001 IEEE Aerospace Conference Proceedings (Cat. No. 01TH8542)*. Vol. 2. IEEE. 2001, pp. 2–951.

[132] CrowdStrike. *CrowdStrike 2024 Global Threat Report*. 2024. URL: https://go.crowdstrike.com/global-threat-report-2024.html?utm_campaign=brand%5C&utm_content=crwd-brand-eur-bnlx-en-psp-x-.

[133] Z Cui and Yunfei Xu. "Impact simulation of Starlink satellites on astronomical observation using worldwide telescope". In: *Astronomy and Computing* 41 (2022), p. 100652.

[134] Zero Science Lab. *ZSL-2016-5359*. Available online at https://www.zeroscience.mk/en/vulnerabilities/ZSL-2016-5359.php. Accessed on 07 2023. 2016.

[135] Ruben Santamarta. *CVE-2013-6035*. Available online at https://www.cvedetails.com/cve/CVE-2013-6035/. Accessed on 07 2023. 2013.

[136] ModZero. *CVE-2020-11549*. Accessed on 07 2023. 2020. URL: https://www.cvedetails.com/cve/CVE-2020-11549/.

[137] Zero Science Lab. *CVE-2023-22971*. Available online at https://nvd.nist.gov/vuln/detail/CVE-2023-22971. Accessed on 07 2023. 2023.

[138] NIST. *CVE-2020-15778*. NIST. National Vulnerability Database (NVD). 2020. URL: https://nvd.nist.gov/vuln/detail/CVE-2020-15778.

[139] NIST. *CVE-2022-31813*. National Vulnerability Database. 2022. URL: https://nvd.nist.gov/vuln/detail/CVE-2022-31813.

[140] Industrial Cyber. *Lab Dookhtegan cyberattack on Iranian oil tankers traced to supply chain compromise of Fanava's infrastructure*. Accessed 2025-09-27. 2025. URL: https://industrialcyber.co/supply-chain-security/lab-dookhtegan-cyberattack-on-iranian-oil-tankers-traced-to-supply-chain-compromise-of-fanavas-infrastructure/.

[141] Cyber Risk Institute. *Profile v2 Guidebook*. Tech. rep. Accessed: 2025-06-07. Cyber Risk Institute, 2024. URL: https://cyberriskinstitute.org/wp-content/uploads/2024/04/Final-CRI-Profile-v2-Guidebook-Public-2024-04-03.pdf.

[142] Cyber Security Division, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry. *The Cyber/Physical Security Framework*. Version 1.0. Apr. 2019.

[143] Waking up to a new threat: Cyber threats and space. "Transactions of the Japan Society for Aeronautical and Space Sciences". In: *Aerospace Technology Japan* (2014).

[144] Space cybersecurity lessons learned from the viasat cyberattack. "Boschetti, N., Gordon, N.G". In: *ASCEND*. 2022.

[145] Cyberinflight. *Threat Intelligence Report – Space Sector*. Tech. rep. Accessed: 2025-03-30. Cyberinflight, 2022. URL: https://www.cyberinflight.com/.

[146] cyberinflight. *Space Cybersecurity Market Intelligence Report*. 2024. URL: https://www.cyberinflight.com/?page_id=1764.

[147] CyberPeace Institute. *Case Study: Viasat Attack*. Accessed 2025-09-27. 2022. URL: https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat.

[148] European Union Agency for Cybersecurity (ENISA). *5G Security Controls Matrix*. Tech. rep. Publication date: May 24, 2023. European Union Agency for Cybersecurity, May 2023. URL: https://www.enisa.europa.eu/publications/5g-security-controls-matrix.

[149] European Union Agency for Cybersecurity (ENISA). *PETs Controls Matrix – A Systematic Approach for Assessing Online and Mobile Privacy Tools*. Tech. rep. Publication date: December 20, 2016. Heraklion, Greece: European Union Agency for Cybersecurity, Dec. 2016. URL: https://www.enisa.europa.eu/publications/pets-controls-matrix/pets-controls-matrix-a-systematic-approach-for-assessing-online-and-mobile-privacy-tools.

[150] European Union Agency for Cybersecurity (ENISA). *Space Threat Landscape*. Tech. rep. Accessed: 2025-03-30. ENISA, 2024. URL: https://www.enisa.europa.eu/publications/space-threat-landscape.

[151] Cybersecurity and Infrastructure Security Agency (CISA). *Recommendations to Space System Operators for Improving Cybersecurity*. June 2024. URL: https://www.cisa.gov/sites/default/files/2024-06/Recommendations%20to%20Space%20System%20Operators%20for%20Improving%20Cybersecurity%20(508).pdf.

[152] Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI). *Joint Cybersecurity Advisory: Russian State-Sponsored Cyber Operations Targeting Satellite Communications*. Tech. rep. Accessed 2026. Cybersecurity, Infrastructure Security Agency, and Federal Bureau of Investigation, Mar. 2022. URL: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a.

[153] U.S Cybersecurity Strategy. *Department of Energy*. Tech. rep. U.S. Department of Energy, 2024. URL: https://www.energy.gov/cio/articles/doe-cybersecuritystrategy-2024.

[154] Cydome. *Second Wave of Cyberattacks on Iranian-Linked Vessels: Technical Analysis*. Accessed 2025-09-27. 2025. URL: https://www.cydome.io/blog/second-wave-iranian-vessels-cyberattack.

[155] Cynthia Brumfield. *Incident response lessons learned from the Russian attack on Viasat*. https://www.csoonline.com/article/649714/incident-response-lessons-learned-from-the-russian-attack-on-viasat.html. Accessed on: 10/12/2023. 2023.

[156] J Michael Dahm. "China C4ISR and counter-intervention". In: *China's Evolving Counter Intervention Capabilities and Implications for the US and Indo-Pacific Allies and Partners: Hearing before the US-China Economic and Security Review Commission (USCC)* (2024), p. 19.

[157] China Daily. *China to Enhance Space Governance and Promote International Cooperation*. 2025. URL: https://www.chinadaily.com.cn/a/202511/30/WS692c6eeaa310d6866eb2c21c.html.

[158] Artjoms Daskevics and Anastasija Nikiforova. "ShoBeVODSDT: Shodan and Binary Edge based vulnerable open data sources detection tool or what Internet of Things Search Engines know about you". In: *2021 second international conference on intelligent data science technologies and applications (IDSTA)*. IEEE. 2021, pp. 38–45.

[159] Gaurav Dave et al. "Cyber security challenges in aviation communication, navigation, and surveillance". In: *Computers & Security* 112 (2022), p. 102516.

[160] Rossouw De Bruin and Sebastiaan H von Solms. "Modelling cyber security governance maturity". In: *2015 IEEE International Symposium on Technology and Society (ISTAS)*. IEEE. 2015, pp. 1–8.

[161] Riccardo De Gaudenzi. "Satellite networks: Past present and future challenges-part 2: Broadband systems". In: *IEEE Aerospace and Electronic Systems Magazine* (2025).

[162] Marie Villarreal Dean. "US Space-Based Nuclear Command and Control: A Guide". In: *CSIS, January* 13 (2023).

[163] James Debruin. "Control systems for mobile satcom antennas". In: *IEEE Control Systems Magazine* 28.1 (2008), pp. 86–101.

[164] European Commission DG DEFIS. *EUSL Baseline*. 2024. URL: https://defence-industry-space.ec.europa.eu/document/download/43bfe8d3-032a-430f-b7fd-55753284d6c6_en?filename=Policy%20Options.pdf%5C&prefLang=el.

[165] Francisco Del Canto Viterale. “Global governance of the space system: A multilevel governance analysis”. In: *Systems* 12.9 (2024), p. 318.

[166] Michal Delkowski. “Evaluating the Strategic Intent and Competitive Dynamics of China’s Satellite Communications Constellations”. PhD thesis. Massachusetts Institute of Technology, 2025.

[167] Advancing Spacecraft Security Through Anomaly Detection. “Wiatrek, N., Burnett, K., Lin, S”. In: *2024 IEEE 6th International Conference on Trust*. 2024.

[168] Anastasia Dimakopoulou and Konstantinos Rantos. “Comprehensive Analysis of Maritime Cybersecurity Landscape Based on the NIST CSF v2. 0”. In: *Journal of Marine Science and Engineering* 12.6 (2024), p. 919.

[169] *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)*. 2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

[170] *Directive (EU) 2022/2557 on the resilience of critical entities (CER Directive)*. 2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2557/oj.

[171] US Space Force Personnel Role Distinctions. *Yonekura, e., Dinicola, s.e., Mann, s., Atkinson, k.* 2024.

[172] A. Donner, M. Berioli, and M. Werner. “MPLS-Based Satellite Constellation Networks”. In: *IEEE Journal on Selected Areas in Communications* 22.3 (2004), pp. 438–448.

[173] Audrey Dorofee et al. “Incident management capability metrics version 0.1”. In: *Retrieved April* 22 (2007), p. 2009.

[174] Zakir Durumeric et al. “A search engine backed by Internet-wide scanning”. In: *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security*. 2015, pp. 542–553.

[175] EARSC. *EARSC Position on the EU Space Law – New Rules for Safe, Resilient, and Sustainable Space Activities*. https://earsc-portal.eu/display/EOwiki/Policy+Observatory?preview=/131531853/173342985/090166e5041a1b9d.pdf. Accessed on: 14/12/2023. 2023.

[176] EASA. *Safety Information Bulletin: Increased probability of GNSS problems near conflict zones*. Accessed 2025-09-27. 2024. URL: https://www.easa.europa.eu/.

[177] The Economist. *The Economist, ‘ Using AI to speed up the processing of space images ’ Jun. 13, 2019* , 2019. URL: https://www.economist.com/science-and-technology/2019/06/13/using-ai-tospeed-up-the-processing-of-space-images.

[178] ENERCON. *Over 95% of WECs back online following disruption to satellite communication*. Accessed on 07 2023. 2022. URL: https://www.enercon.de/en/news/news-detail/cc_news/show/News/over-95-per-cent-of-wecs-back-online-following-disruption-to-satellite-communication/.

[179] Department for Energy Security, Net Zero, and Energy & Industrial Strategy Department for Business. *Civil Nuclear Cyber Security Strategy*. Tech. rep. Department for Business, Energy & Industrial Strategy, 2022. URL: https://www.gov.uk/government/publications/civilnuclear-cyber-security-strategy-2022.

[180] Simon Yusuf Enoch et al. "A systematic evaluation of cybersecurity metrics for dynamic networks". In: *Computer Networks* 144 (2018), pp. 216–229.

[181] Simon Yusuf Enoch et al. "Composite metrics for network security analysis". In: *arXiv preprint arXiv:2007.03486* (2020).

[182] Johan Eriksson and Giampiero Giacomello. "Cyberspace in space: fragmentation, vulnerability, and uncertainty". In: *Cyber Security Politics*. Routledge, 2022, pp. 95–108.

[183] ERR News. *GPS Disruption Has Affected 123,000 Flights in the Baltic Region*. Accessed 18 October 2025. July 2025. URL: https://news.err.ee/1609792437/gps-disruption-has-affected-123-000-flights-in-the-baltic-region.

[184] ESA. *' Artificial intelligence behind 21st Century spaceflight ' ESA*. URL: https://www.esa.int/Enabling_Support/Operations/Artificial_intelligence_behind_21st_Century_spaceflight.

[185] ESA. *QSVP - QUANTUM SECURITY VERIFICATION PLATFORM*. Tech. rep. ESA, 2024. URL: https://esastar-publication-ext.sso.esa.int/ESATenderActions/details/90340.

[186] ETSI. *Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM) services and architectures; Functional architecture for IP interworking with BSM networks*. Tech. rep. TS 102 292. Version V1.1.1. European Telecommunications Standards Institute (ETSI), Feb. 2004.

[187] Euroconsult. *New Historic High for Government Space Spending, Mostly Driven by Defense Expenditures*. Accessed October 2024. Riyadh, 2022. URL: https://www.euroconsult-ec.com/press-release/new-historic-high-for-government-space-spending-mostly-driven-by-defense-expenditures.

[188] EUROCONTROL. "Radio Frequency Interference to Satellite Navigation — A Growing Threat". In: *EUROCONTROL Think Papers* 9 (2019). Accessed: 2025-09-02. URL: https://www.eurocontrol.int/publication/eurocontrol-think-paper-9-radio-frequency-interference-satellite-navigation-active.

[189] 2024 Europe Economics - EU Space Act: Cost Impact Assessment - London. *Available at:* tech. rep. 2024. URL: https://www.progressivepolicy.org/wp-content/uploads/2025/12/Final-Report-EU-Space-Act-Cost-Impact-A.

[190] European Commission. *Commission Implementing Regulation (EU) C(2024) 7151 final of 17.10.2024: Laying Down Rules for the Application of Directive (EU) 2022/2555 Regarding Cybersecurity Risk-Management Measures*. Accessed: 2024-10-17. Oct. 2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=pi_com%3AC%282024%297151.

[191] European Commission. *EU Space Strategy for Security and Defence – White Paper*. Accessed: 2025-04-23. 2023. URL: https://defence-industry-space.ec.europa.eu/eu-space/eu-space-strategy-security-and-defence_en.

[192] European Commission. *Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020*. COM(2022) 454 final. Accessed on 07 2023. 2022. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739259/EPRS_BRI(2022)739259_EN.pdf.

[193] European Commission. *Proposal for a Regulation on the Safety, Resilience and Sustainability of Space Activities (EU Space Act)*. Tech. rep. European Commission, 2025.

[194] European Commission. *Targeted Consultation on EU Space Law*. https://defence-industry-space.ec.europa.eu/consultations-0/targeted-consultation-eu-space-law. Accessed on: Insert Accessed Date. 2023.

[195] European Commission and High Representative of the Union for Foreign Affairs and Security Policy. *An EU Approach for Space Traffic Management*. Tech. rep. European Commission, 2022.

[196] Impact Assessment Report Accompanying the Proposal for a Regulation on Space Activities in the Union (EU Space Act) SWD(2024) 335 final Parts I–II Brussels 2024 European Commission. *Available at:* tech. rep. European Commission, 2024. URL: https://defence-industry-space.ec.europa.eu/eu-space-act_en.

[197] European External Action Service. *Strategic Compass for Security and Defence*. Accessed: 2025-04-23. 2022. URL: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en.

[198] European Parliament. *European Parliament Resolution on an EU Approach to Space Traffic Management*. Tech. rep. European Parliament, 2022.

[199] European Repository of Cyber Incidents (EuRepoC). *Cyber Incident Data Framework (2000–2025)*. https://eurepoc.eu/. Accessed: 2025-03-30. 2025.

[200] European Telecommunications Standards Institute (ETSI). *ETSI TR 103 866 V1.1.1 (2023-02), Cyber Security (CYBER); Implementation of the Revised Network and Information Security (NIS2) Directive applying Critical Security Controls*. Tech. rep. 103 866 V1.1.1. Version 1.1.1. Available at: https://www.etsi.org/deliver/etsi_tr/103800_103899/103866/01.01.01_60/tr_103866v010101p.pdf. European Telecommunications Standards Institute (ETSI), Feb. 2023.

[201] European Union. *Charter of Fundamental Rights of the European Union*. Official Journal of the European Union. OJ C 326/391, Articles 2, 3, 6, 11, 35, 37 and 38. 2012. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT.

[202] European Union. *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC*. OJ L 333, 27.12.2022, p. 164–198. Dec. 27, 2022. URL: http://data.europa.eu/eli/dir/2022/2557/oj.

[203] European Union. *Regulation (EU) 2023/588 Establishing the Union Secure Connectivity Programme (IRIS2)*. Tech. rep. Regulation (EU) 2023/588. European Union, 2023.

[204] European Union. *Regulation (EU) 2023/588 of the European Parliament and of the Council of 15 March 2023 Establishing the Union Secure Connectivity Programme 2023–2027*. Official Journal of the European Union. OJ L 79/1. 2023. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32023R0588 (visited on 06/29/2025).

[205] European Union Agency for Cybersecurity. *European Repository of Cyber Incidents*. Tech. rep. ENISA, 2024. URL: https://www.enisa.europa.eu/topics/csirt-cert-services/cyber-incidents.

[206] European Union Agency for Cybersecurity (ENISA). *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*. Tech. rep. Accessed: 2025-06-07. Heraklion, Greece: ENISA, 2017. URL: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity.

[207] European Union Agency for Cybersecurity (ENISA). *Cybersecurity for SMEs - Challenges and Recommendations*. Tech. rep. European Union Agency for Cybersecurity, July 2021. URL: https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes.

[208] European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2022*. Tech. rep. ENISA, Nov. 2022. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

[209] European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2024*. Tech. rep. Accessed: 2025-03-30. ENISA, 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

[210] European Union Agency for Cybersecurity (ENISA). *Minimum Security Measures for Operators of Essential Services*. Accessed: 2024-11-01. 2024. URL: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/minimum-security-measures-for-operators-of-essentials-services.

[211] European Union Agency for Cybersecurity (ENISA). *NIS Investments Report 2023*. https://www.enisa.europa.eu/publications/nis-investments-2023. Accessed on: Insert Accessed Date. Nov. 2023.

[212] European Union Agency for Cybersecurity (ENISA). *Space Threat Landscape*. Tech. rep. Accessed 2026. European Union Agency for Cybersecurity, 2025. URL: https://www.enisa.europa.eu/publications/space-threat-landscape.

[213] European Union Agency for the Space Programme. *EUSPA Industry Directory*. https://www.euspa.europa.eu/opportunities/fundamental-elements/industry-directory. Accessed: 2025-03-13. 2025.

[214] European Union Agency for the Space Programme (EUSPA). *Galileo to be the first GNSS to offer authentication service worldwide with launch of OSNMA*. June 2025. URL: https://www.euspa.europa.eu/pressroom/press-releases/galileo-be-first-gnss-offer-authentication-service-worldwide-launch-osnma.

[215] European Union Aviation Safety Agency (EASA). *EASA updates Safety Information Bulletin on GNSS jamming/spoofing*. July 2024. URL: https://www.easa.europa.eu/en/newsroom-and-events/news/easa-updates-safety-information-bulletin-global-navigation-satellite.

[216] EUSPA. *CALL FOR EXPRESSIONS OF INTEREST: EU SPACE INFORMATION SHARING AND ANALYSIS CENTRE (EU SPACE ISAC)*. https://www.euspa.europa.eu/opportunities/isac. Version: 1.5, Date: 19/09/2023, Accessed on: Date. 2023.

[217] Eutelsat. *Reference Document - Universal Registration Document*. Access the document via Eutelsat at https://www.eutelsat.com/files/EUTELSAT_BAT%2020-10_UK.pdf. Accessed on: Insert Accessed Date.

[218] Eutelsat. *Satellite Operator Eutelsat Calls for International Response to Persistent Jamming*. 2011. URL: https://www.eutelsat.com/news/compress/en/2011/pdf/PR%207611%20Iran.pdf.

[219] Executive Office of the President. *Executive Order 14144 of January 16, 2025: Strengthening and Promoting Innovation in the Nation's Cybersecurity*. Federal Register, 90 FR 6755–6771. Signed by President Joseph R. Biden Jr.; published January 17, 2025. Jan. 2025. URL: https://www.federalregister.gov/documents/2025/01/17/2025-01470/strengthening-and-promoting-innovation-in-the-nations-cybersecurity (visited on 05/30/2025).

[220] Executive Office of the President of the United States. *Executive Order: Enabling Competition in the Commercial Space Industry*. Tech. rep. The White House, 2025.

[221] Executive Office of the President of the United States. *National Space Policy of the United States of America*. Tech. rep. Accessed 2026. The White House, 2020. URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/12/National-Space-Policy.pdf.

[222] Executive Office of the President of the United States. *Space Policy Directive-4: Establishment of the United States Space Force*. Tech. rep. Accessed 2026. The White House, 2019. URL: https://trumpwhitehouse.archives.gov/presidential-actions/space-policy-directive-4-establishment-united-states-space-force/.

[223] Executive Office of the President of the United States. *Space Policy Directive-5: Cybersecurity Principles for Space Systems*. Tech. rep. Accessed 2026. The White House, 2020. URL: https://www.cisa.gov/resources-tools/resources/space-policy-directive-5.

[224] Norman Fairclough. *Analysing Discourse: Textual Analysis for Social Research*. London: Routledge, 2003.

[225] et al Falco Gregory. "An international technical standard for commercial space system cybersecurity-a call to action." In: *ASCEND*. 2022.

[226] et al Falco Gregory. "Minimum Requirements for Space System Cybersecurity-Ensuring Cyber Access to Space." In: 2024.

[227] Gregory Falco. "The vacuum of space cyber security". In: *2018 AIAA SPACE and Astronautics Forum and Exposition*. 2018, p. 5275.

[228] Pascal Faucher, Regina Peldszus, and Amélie Gravier. “Operational space surveillance and tracking in Europe”. In: *Journal of Space Safety Engineering* 7.3 (2020), pp. 420–425.

[229] FBI-CISA. *APT Actors Exploit Vulnerabilities to Gain Initial Access for Future Attacks*. Accessed on 07 2023. 2021. URL: https://www.ic3.gov/Media/News/2021/210402.pdf.

[230] Federal Communications Commission. *Notice of Apparent Liability for Forfeiture: Gary P. Bojczak*. Tech. rep. FCC 13-106. FCC, Aug. 2013. URL: https://transition.fcc.gov/eb/Orders/2013/FCC-13-106A1.html.

[231] Michael Felux et al. “Impacts of global navigation satellite system jamming on aviation”. In: *NAVIGATION: Journal of the Institute of Navigation* 71.3 (2024).

[232] Tiago M Fernández-Caramés and Paula Fraga-Lamas. “Teaching and learning iot cybersecurity and vulnerability assessment with shodan through practical use cases”. In: *Sensors* 20.11 (2020), p. 3048.

[233] Patrick E Finch, Donald V Sullivan, and William D Ivancic. “An evaluation of Protocol Enhancing Proxies and modern file transport protocols for geostationary satellite communication”. In: *2012 IEEE Aerospace Conference*. IEEE. 2012, pp. 1–8.

[234] John A Fitch III and Lance J Hoffman. “A shortest path network security model”. In: *Computers & Security* 12.2 (1993), pp. 169–189.

[235] Matthew Fleming and Eric Goldstein. “Metrics for measuring the efficacy of critical-infrastructure-centric cybersecurity information sharing efforts”. In: *Available at SSRN 2201033* (2012).

[236] Forrester Consulting. *The Total Economic Impact™ of Cisco Duo: Cost Savings and Business Benefits Enabled by Duo*. Tech. rep. Commissioned by Cisco. Forrester Consulting, Feb. 2023. URL: https://resources.duo.com/explore/assets/the-tei-of-cisco-duo-2.

[237] Fortinet. *Malicious Actor Discloses FortiGate SSL-VPN Credentials*. Accessed on 07 2023. 2021. URL: https://www.fortinet.com/blog/psirt-blogs/malicious-actor-discloses-fortigate-ssl-vpn-credentials.

[238] Carla P Freeman. “The impact of US-China strategic competition on the idea of space as a “global commons””. In: *Frontiers in Space Technologies* 6 (2025), p. 1664300.

[239] S. G. Freeman. *S. G. Freeman, et. al. ‘ Attack Surface of Wind Energy Technologies in the United States (2024) Idaho National Laboratory (INL), Idaho Falls, ID (United States), INL/RPT-24-76133-Rev000 , doi : 10.2172/2297403*. 2024.

[240] Jason Fritz. "Satellite hacking: A guide for the perplexed". In: *Culture Mandala* 10.1 (2013), p. 5906.

[241] Frontiers Economics. *Assessing the Economic Impact of EU Initiatives on Cybersecurity*. https://www.frontier-economics.com/media/izyk5rgz/assessing-the-economic-cost-of-eu-initiatives-on-cybersecurity.pdf. Accessed on: 10/12/2023. 2023.

[242] *FY 2024 CIO FISMA Metrics, Version 1.0*. https://www.cisa.gov/sites/default/files/2023-12/FY24_FISMA_CIO_Metrics_v1.0_FINAL_1.pdf. Accessed: 2024-09-29. Federal Information Security Modernization Act (FISMA) Chief Information Officer Metrics, Dec. 2023.

[243] M. P. Gallaher. *M. P. Gallaher et al. ' Economic benefits of the Global Positioning System (GPS) ' (2019) RTI International*. 2019. URL: https://www.rti.org/publication/economic-benefitsglobal-positioning-system-gps.

[244] Weiguang Gao et al. "High-precision services of BeiDou navigation satellite system (BDS): Current state, achievements, and future directions". In: *Satellite Navigation* 5.1 (2024), p. 20.

[245] Joseph Gedeon. *For the First Time, U.S. Government Lets Hackers Break into Satellite in Space*. https://www.politico.com/news/2023/08/11/def-con-hackers-space-force-00110919. Accessed on: 10/12/2023. 2023.

[246] Béla Genge and Călin Enăchescu. "ShoVAT: Shodan-based vulnerability assessment tool for Internet-facing services". In: *Security and communication networks* 9.15 (2016), pp. 2696–2714.

[247] A.A.D. George et al. "Onboard Processing with Hybrid and Reconfigurable Computing on Small Satellites". In: *NSF SHREC*. 2018. URL: https://www.nsf-shrec.org/....

[248] Subrata Ghoshroy. "The X-37B: Backdoor weaponization of space?" In: *Bulletin of the Atomic Scientists* 71.3 (2015), pp. 19–29.

[249] Gilat Satellite Networks. *Gilat Presents Fourth Quarter and Full Year 2023 Results*. Accessed: 2025-03-30. Gilat Satellite Networks, Mar. 2024. URL: https://www.gilat.com/pressreleases/gilat-presents-fourth-quarter-and-full-year-2023-results/#:~:text=Adi%20Sfadia%2C%20Gilat's%20CEO%2C%20commented,up%2044%25%20over%20last%20year..

[250] Sait Murat Giray. "Anatomy of unmanned aerial vehicle hijacking with signal spoofing". In: *2013 6th International Conference on Recent Advances in Space Technologies (RAST)*. IEEE. 2013, pp. 795–800.

[251] Andrey B Gladyshev et al. "Electronic Jamming of the System of Subscriber Terminals of the Starlink Satellite Communication System". In: *Journal of Siberian Federal University. Engineering & Technologies* 16.7 (2023), pp. 789–796.

[252] GMV. *Annual Report 2023*. Tech. rep. Accessed: 2025-03-30. GMV, July 2024. URL: https://www.gmv.com/sites/default/files/content/file/2024/07/31/114/annual_report_2023_3.pdf.

[253] D. Goldman. *D. Goldman, ' Notice of Ex Parte Presentation, Mitigation of Orbital Debris in the New Space Age, WT Docket No. 18-313 ' May 23, 2024*. 2024. URL: https://www.fcc.gov/ecfs/document/10523697220317/1.

[254] J. Goodwill. *Current Technology in Space: Briefing on Rad-Hard Compute Constraints*. Tech. rep. NASA, 2024. URL: https://ntrs.nasa.gov/api/citations/20240001139/downloads/Current%20Technology%20in%20Space%20v4%20Briefing.pdf/.

[255] Rajeev Gopal, Channasandra Ravishankar, and Xiaoling Huang. "Smart network connectivity for hybrid space and terrestrial connectivity". In: *39th International Communications Satellite Systems Conference (ICSSC 2022)*. Vol. 2022. IET. 2022, pp. 84–90.

[256] Giacomo Gori et al. "A Systematic Analysis of Security Metrics for Industrial Cyber–Physical Systems". In: *Electronics* 13.7 (2024), p. 1208.

[257] Sri Nikhil G Gourisetti et al. *Cybersecurity Risk Assessment Framework for Externally Exposed Energy Delivery Systems*. Tech. rep. Pacific Northwest National Lab.(PNNL), Richland, WA (United States), 2021.

[258] Australian Government. *"Voluntary AI Safety Standard." Australian Government Department of Industry, Science and Resources, The%20Voluntary%20AI&text=The st%20do*. 2010. URL: https://www.industry.gov.au/publications/voluntary-aisafetystandard#:~:text=About%20the%20standard,-.

[259] Australian Government. *Australian Government, Department of Industry, Science and Resources, ' Safe and Responsible AI in Australia Consultation: Australian Government's Interim Response ' (2024)*. 2024. URL: https://consult.industry.gov.au/supporting-responsible-ai.

[260] UK Government. *National Risk Register: 2023*. Tech. rep. 2023. URL: https://assets.publishing.service.gov.uk/media/64ca1dfe19f5622669f3c1/2023_NATIONAL_RISK_REGISTER_NRR.pdf.

[261] United States Government. *Executive Order 14028: Improving the Nation's Cybersecurity*. Tech. rep. US Government, 2023. URL: https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/information-technology-category/it-security/executive-order-14028.

[262] T. Graham. *T. Graham and K. Thangavel , ' Artificial Intelligence in Space: An Analysis of Responsible AI Principles for the Space Domain ' (2023) 74 th International Astronautical Congress*. 2023.

[263] Grand View Research. *U.S. Space Cybersecurity Market Size, Share & Trends Analysis Report*. Tech. rep. Accessed 2026. Grand View Research, 2024. URL: https://www.grandviewresearch.com/industry-analysis/us-space-cybersecurity-market-report.

[264] CIC Security Working Group. *Incident Cost Analysis and Modeling Project*. University of Michigan, 1998.

[265] Guofei Gu et al. "Measuring intrusion detection capability: An information-theoretic approach". In: *Proceedings of the 2006 ACM Symposium on Information, computer and communications security*. 2006, pp. 90–101.

[266] Device Security Guidance. *UK National Security Center*. Tech. rep. NCSC, 2021. URL: https://www.ncsc.gov.uk/collection/device-security-guidance.

[267] Ranwa Haddad et al. "GPS modernization and beyond". In: *2020 IEEE/ION Position, Location and Navigation Symposium (PLANS)*. 2020, pp. 399–406.

[268] Joseph A. Haimerl and Gregory P. Fonder. "Space fence system overview." In: *Proceedings of the Advanced Maui Optical and Space Surveillance Technology Conference*. 2015.

[269] Kemal Hajdarevic and Pat Allen. "A new method for the identification of proactive information security management system metrics". In: *2013 36th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. IEEE. 2013, pp. 1121–1126.

[270] Peter A Hall and David Soskice. "Varieties of capitalism and institutional change: A response to three critics". In: *Comparative European Politics* 1.2 (2003), pp. 241–250.

[271] Todd Harrison, Kaitlyn Johnson, and Thomas G Roberts. *Space threat assessment 2019*. Center for Strategic & International Studies., 2019.

[272] Charles Harry, Ido Sivan-Sevilla, and Mark McDermott. "Measuring the size and severity of the integrated cyber attack surface across US county governments". In: *Journal of Cybersecurity* 11.1 (2025), tyae032.

[273] John Heidemann et al. *Exploring visible internet hosts through census and survey*. Tech. rep. Technical Report ISI-TR-2007-640, USC/Information Sciences Institute, 2007.

[274] Jeff Heissler et al. "A performance analysis on the application of commercial standards for IP SATCOM modems". In: *MILCOM 2005-2005 IEEE Military Communications Conference*. IEEE. 2005, pp. 787–793.

[275] Debra S Herrmann. *Complete guide to security and privacy metrics: measuring regulatory compliance, operational resilience, and ROI*. Auerbach Publications, 2007.

[276] Senate Committee on Homeland Security and Governmental Affairs. *S. 1425, Satellite Cybersecurity Act*. June 2023. URL: https://www.cbo.gov/publication/59203.

[277] Jin Bum Hong. "Scalable and adaptable security modelling and analysis." In: (2015).

[278] Alex Horton, Sergii Korolchuk, and Eva Dou. "Russia's Illicit Procurement Networks and Its Advance in Ukraine". In: *The Washington Post* (Oct. 2024). Accessed 19 October 2025. URL: https://www.washingtonpost.com/world/2024/10/12/starlink-russia-ukraine-elon-musk/.

[279] House of Commons Defence Committee. *Defence Space: through Adversity to the Stars?* Accessed 5 May 2024. London, 2022. URL: https://committees.parliament.uk/publications/30320/documents/175331/default/.

[280] Henry Howland. "CVSS: Ubiquitous and Broken". In: *Digital Threats* 4.1 (Feb. 2022). DOI: 10.1145/3491263. URL: https://doi.org/10.1145/3491263.

[281] Hughes. *Hughes - Mobile Satellite Terminals*. Accessed on 07 2023. 2023. URL: https://www.hughes.com/what-we-offer/satellite-ground-systems/mobile-satellite-terminals.

[282] Todd E Humphreys et al. "Assessing the spoofing threat: Development of a portable GPS civilian spoofer". In: *Proceedings of the 21st International technical meeting of the satellite division of the institute of navigation (ION GNSS 2008)*. 2008, pp. 2314–2325.

[283] Ana Hurova. "Earth Observation for the Protection of Human Rights during the Armed Aggression." In: *Advanced Space Law* 9 (2022).

[284] Ryan Hutchins. "Cyber defense of space assets". In: *Tufts School of Engineering: Medford, MA, USA* (2016), pp. 1–18.

[285] iDirect. *iDirect - 9350 Satellite Modem*. Accessed on 07 2023. 2023. URL: https://www.idirect.net/products/9350-satellite-modem/.

[286] IEEE. *A. Nanjangud, P. C. Blacker, S. Bandyopadhyay, and Y. Gao, ' Robotics and AI-Enabled On-Orbit Operations With Future Generation of Small Satellites ' (2018) Proc. IEEE, vol. 106, no. 3, pp. 429–439 , doi : 10.1109/JPROC.2018.2794829*. 2018.

[287] IEEE. *G. Furano et al., ' Towards the use of artificial intelligence on the edge in space systems: Challenges and O pportunities ' (2020) IEEE Aerosp . Electron. Syst. Mag., vol. 35, no. 12, pp. 44–56*. 2020.

[288] IEEE. *G. Furano, A. Tavoularis, and M. Rovatti, ' AI in space: applications examples and challenges ' (2020) IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), pp. 1–6 , doi : 10.1109/DFT50435.2020.9250908*. 2020.

[289] IEEE. *X. X. Zhu et al., ' Deep Learning in Remote Sensing: A Comprehensive Review and List of Resources ' (2017) IEEE Geosci. Remote Sens. Mag., vol. 5, no. 4, pp. 8–36, doi : 10.1109/MGRS.2017.2762307*. 2017.

[290] Vasilis Ieropoulos. "The impact of GPS interference in the Middle East." In: 2024.

[291] *Improving Starlink's Latency*. 2024. URL: https://www.starlink.com/public-files/StarlinkLatency.pdf.

[292] Department of Industry. *Department of Industry Science and Resources, ' Australia's AI Ethics Principles — Australia's Artificial Intelligence Ethics Framework*. URL: https://www.industry.gov.au/node/91877.

[293] A security metric for assessing the security level of critical infrastructures. "Tortorelli, A., Fiaschetti, A., Giuseppi, A., Suraci, V., Germanà, R". In: (2020).

[294] Joint Task Force Transformation Initiative. *Guide for Conducting Risk Assessments (NIST Special Publication 800-30 Revision 1)*. Tech. rep. NIST SP 800-30 Rev. 1. Gaithersburg, MD: National Institute of Standards and Technology, Sept. 2012. DOI: 10.6028/NIST.SP.800-30r1. URL: https://doi.org/10.6028/NIST.SP.800-30r1.

[295] NASA Office of Inspector General. *Cybersecurity Management and Oversight at the Jet Propulsion Laboratory*. 2019. URL: https://oig.nasa.gov/docs/IG-19-022.pdf.

[296] Huajin Securities Research Institute. *Satellite Internet Security Industry Report, 2023*. Tech. rep. Huajin, 2023. URL: https://pdf.dfcfw.com/pdf/H3_AP202312201614589701_1.pdf.

[297] *International Charter "Space and Major Disasters" Annual Report 2023*. 2023. URL: https://disasterscharter.org.

[298] International Civil Aviation Organization. *Resolution A41-8: Protection of Radio Navigation Satellite Service (RNSS) Signals Used for Safety-of-Life Applications*. 41st Session of the ICAO Assembly, Montréal. para. 3. 2022. URL: https://www.icao.int/sites/default/files/Meetings/a41/Documents/WP/wp_080_en.pdf.

[299] Iran International. *Hackers disrupt communications of Iranian tankers and cargo ships*. Accessed 2025-09-27. 2025. URL: https://www.iranintl.com/en/202509xxxx/hackers-disrupt-communications-iranian-tankers-cargo-ships.

[300] *ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*. Available at: https://www.iso.org/standard/64120.html. International Organization for Standardization, 2016.

[301] One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive. "Schmitz-Berndt, S". In: *International Cybersecurity Law Review* (2022).

[302] Article IV. *Article IV, ' Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, opened for signature 27 January 1967, 610 UNTS 8843 (entered into force 10 October 1967)*. Tech. rep. Article IV, 1967.

[303] William Ivancic et al. "Satellite communications using commercial protocols". In: *18th International Communications Satellite Systems Conference and Exhibit*. 2000, p. 1185.

[304] B. Jacobs. *B. Jacobs, ' A Comparative Study of EU and US Regulatory Approaches to Cybersecurity in Space ' (2024) Air Space Law, vol. 48, no. 4 /5,* 2024.

[305] Bas Jacobs. "A Comparative Study of EU and US Regulatory Approaches to Cybersecurity in Space". In: *Air and Space Law* 48.4/5 (2023).

[306] Bas Jacobs. "Understanding the EU's Competence to Harmonise Space Law Amid Publication Delays." In: *Air and Space Law* (2024).

[307] Wayne Jansen. *Directions in security metrics research*. Diane Publishing, 2010.

[308] Andrew Jaquith. *Security metrics*. Pearson Education, 2007.

[309] Nizar Jegham et al. "Performance of Voice over IP in DVB-RCS and iDirect satellite networks". In: *26th International Communications Satellite Systems Conference (ICSSC)*. 2008, pp. 1–11.

[310] Noor Ul Amin Jhanjhi et al. "The Rise of GPS Spoofing Attacks on Drones in the Russia-Ukraine War". In: *Authorea Preprints* (2025).

[311] Joan Johnson-Freese and Andrew S Erickson. "The emerging China–EU space partnership: a geotechnological balancer". In: *Space policy* 22.1 (2006), pp. 12–22.

[312] Alastair Iain Johnston. "Thinking about strategic culture". In: *International security* 19.4 (1995), pp. 32–64.

[313] Jack A Jones. "An Introduction to Factor Analysis of Information Risk (FAIR)." In: *Norwich University Journal of Information Assurance (NUJIA)* 2.1 (2006).

[314] Mouna Jouini and Latifa Ben Arfa Rabai. "Comparative study of information security risk assessment models for cloud computing systems". In: *Procedia Computer Science* 83 (2016), pp. 1084–1089.

[315] Paul Kyle KALLENDER. "Waking up to a new threat: Cyber threats and space". In: *Transactions of the Japan Society for Aeronautical and Space Sciences, Aerospace Technology Japan* 12.ists29 (2014), Tv_1–Tv_10.

[316] Chronis Kapalidis et al. "Cyber risk management in satellite systems". In: *Living in the Internet of Things (IoT 2019)*. IET, 2019, pp. 1–8. DOI: 10.1049/cp.2019.0139.

[317] Elliott D Kaplan and Christopher Hegarty. *Understanding GPS/GNSS: principles and applications*. Artech house, 2017.

[318] Georgios Kavallieratos and Sokratis Katsikas. "An exploratory analysis of the last frontier: A systematic literature review of cybersecurity in space". In: *International Journal of Critical Infrastructure Protection* (2023), p. 100640.

[319] C. B. Keating. *C. B. Keating, P. F. Katina, J. Sisti, J. C. Pyne, and A. V. Gheorghe, "Critical Space Infrastructure: Contributions of Complex System Governance ' (2020) Space Infrastructures: From Risk to Resilience Governance, IOS Press, pp. 60–87 , doi : 10.3233/NICSP200008*. 2020.

[320] Marjan Keramati and Fatemeh Sadat Halataei. "Innovative Cyber-Security Metrics for Intrusion Prevention". In: ().

[321] Omer F Keskin et al. "Cyber third-party risk management: A comparison of non-intrusive risk scoring reports". In: *Electronics* 10.10 (2021), p. 1168.

[322] Shah Khalid Khan et al. "Space cybersecurity challenges, mitigation techniques, anticipated readiness, and future directions". In: *International Journal of Critical Infrastructure Protection* 47 (2024), p. 100724.

[323] K. Khanna. *K. Khanna, B. K. Panigrahi, and A. Joshi, ' AI-based approach to identify compromised meters in data integrity attacks on smart grid ' (2018) IET Gener . Transm. Distrib., vol. 12, no. 5, pp. 1052–1066 , doi : 10.1049/iet-gtd.2017.0455*. 2018.

[324] James T Kitchen, David R Coogan, and Keeton H Christian. "The Evolution of Legal Risks Pertaining to Patch Management and Vulnerability Management". In: *Duq. L. Rev.* 59 (2021), p. 269.

[325] Jens Klare et al. "The future of radar space observation in Europe—Major upgrade of the tracking and imaging radar (TIRA)". In: *Remote Sensing* 16.22 (2024), p. 4197.

[326] Nina Klimburg-Witjes. “Shifting articulations of space and security: boundary work in European space policy making”. In: *European Security* 30.4 (2021), pp. 526–546.

[327] Larry Klosterboer. *Implementing ITIL configuration management*. Pearson Education, 2007.

[328] Oltjon Kodheli et al. “Satellite communications in the new space era: A survey and future challenges”. In: *IEEE Communications Surveys & Tutorials* 23.1 (2020), pp. 70–109.

[329] Michael Olorunfunmi Kolawole. *Satellite communication engineering*. CRC Press, 2017.

[330] Ville Korhonen. “Future after OpenVPN and IPsec”. Master’s Thesis. Tampere University, 2019.

[331] A. Koskina. *A. Koskina, ‘ The Use of AI Weapons in Outer Space: Regulatory Challenges ’ (2023) in Artificial Intelligence and Normative Challenges, vol. 59, A. Kornilakis, G. Nouskalis, V. Pergantis, and T. Tzimas, Eds., in Law, Governance and Technology Series, vol. 59 . , Cham: Springer International Publishing, pp. 237–254 , doi: 10.1007/978-3-031-41081-9_13*. Springer, 2023.

[332] Barbara Krumay, Edward WN Bernroider, and Roman Walser. “Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the NIST cybersecurity framework”. In: *Secure IT Systems: 23rd Nordic Conference, NordSec 2018, Oslo, Norway, November 28-30, 2018, Proceedings 23*. Springer. 2018, pp. 369–384.

[333] Linling Kuang et al. *Terrestrial-Satellite Communication Networks: Transceivers Design and Resource Allocation*. Springer, 2017.

[334] Hanno Langweg. “Software Security Metrics for Malware Resilience”. PhD thesis. Universitäts-und Landesbibliothek Bonn, 2008.

[335] Deborah Welch Larson. “Realism: Excavating a historical tradition”. In: *Routledge Handbook of Historical International Relations*. Routledge, 2021, pp. 71–79.

[336] Conrad C Lautenbacher. “The global earth observation system of systems: Science serving society”. In: *Space Policy* 22.1 (2006), pp. 8–11.

[337] The Space Industry Regulations 2021: Another Giant Leap? “Simmonds, A.,” in: (2021).

[338] Mai T Lee. “Feasibility and performance analyses of adapting Ethernet-based protocols in space-based networks”. In: *2011-MILCOM 2011 Military Communications Conference*. IEEE. 2011, pp. 1845–1852.

[339] David John Leversage and Eric James Byres. “Estimating a system’s mean time-to-compromise”. In: *IEEE Security & Privacy* 6.1 (2008), pp. 52–60.

[340] Jeffrey Lewis. *Weapons in Space?* 2019.

[341] Ruiguang Li et al. "A survey on cyberspace search engines". In: *Cyber Security: 17th China Annual Conference, CNCERT 2020, Beijing, China, August 12, 2020, Revised Selected Papers 17*. Springer Singapore. 2020, pp. 206–214.

[342] M. Lieu. *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*. Tech. rep. 2023.

[343] S. Lightman. *Applying the NIST CSF to the Satellite Ground Segment*. Tech. rep. NIST, 2022. URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=935449.

[344] S. Lightman et al. *Satellite Ground Segment: Applying the NIST Cybersecurity Framework*. Tech. rep. NIST IR 8401. National Institute of Standards and Technology, 2022. URL: https://csrc.nist.gov/pubs/ir/8401/final.

[345] Suzanne Lightman, Theresa Suloway, and Joseph Brule. *Satellite Ground Segment: Applying the Cybersecurity Framework to Satellite Command and Control*. NISTIR NISTIR 8401. National Institute of Standards and Technology (NIST), Dec. 2022. URL: https://doi.org/10.6028/NIST.IR.8401.

[346] Yang Liu et al. "Cloudy with a chance of breach: Forecasting cyber security incidents". In: *24th USENIX security symposium (USENIX Security 15)*. 2015, pp. 1009–1024.

[347] Ye Liu et al. "Research on Design and Implementation of an Intelligent Network Asset Search System Based on LLM Agent and FOFA". In: *Proceedings of the 2025 4th International Conference on Cyber Security, Artificial Intelligence and the Digital Economy*. 2025, pp. 483–488.

[348] liveeo.com. *' LiveEO raises €25 Million to leverage AI-powered satellite data for critical infrastructure and climate risk M anagement ', LiveEO*. URL: https://www.liveeo.com/article/liveeo-raises-eu25-million-to-leverage-ai-powered-satellite-data-for-critical-infrastructureand-climate-risk-management.

[349] Yang Lu and Li Da Xu. "Internet of Things (IoT) cybersecurity research: A review of current research topics". In: *IEEE Internet of Things Journal* 6.2 (2018), pp. 2103–2115.

[350] M. Madi. *M. Madi and O. Sokolova , ' Artificial Intelligence for Space: AI4SPACE: Trends, Applications, and Perspectives ' (2023) Boca Raton: CRC Press , doi : 10.1201/9781003366386*. 2023.

[351] P. Maguire. *P. Maguire, ' AI at the crossroads of cybersecurity, space and national security in the digital age ' Apr. 3, 2024, SpaceNews*. 2024. URL: https://spacenews.com/ai-crossroadscybersecurity-space-national-security-digital-age/.

[352] Logan O Mailloux. "Examination of security design principles from NIST SP 800-160." In: *2018 Annual IEEE International Systems Conference (SysCon)*. 2018.

[353] Yassine Maleh, Abdelkebir Sahid, and Mustapha Belaissaoui. "A maturity framework for cybersecurity governance in organizations". In: *EDPACS* 63.6 (2021), pp. 1–22.

[354] Pratyusa K Manadhata and Jeannette M Wing. "An attack surface metric". In: *IEEE Transactions on Software Engineering* 37.3 (2010), pp. 371–386.

[355] M. Manulis et al. "Cyber security in New Space: Analysis of threats, key enabling technologies and challenges". In: *International Journal of Information Security* 20 (2021), pp. 287–311. DOI: 10.1007/s10207-020-00503-w.

[356] et al Masson Louis. *Developing a CCSDS compliant platform to reliably secure current and future space data links.* 2024.

[357] John Matherly. "Complete guide to shodan". In: *Shodan, LLC (2016-02-25)* 1 (2015).

[358] Alana Maurushat and Kathy Nguyen. "The legal obligation to provide timely security patching and automatic updates". In: *International Cybersecurity Law Review* 3.2 (2022), pp. 437–465.

[359] James McCarthy et al. *Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN)*. US Department of Commerce, National Institute of Standards and Technology, 2023.

[360] Robert D McLaughlin Jr. *Leveraging an SNMP agent in terminal equipment for network monitoring of US Navy SATCOM*. Tech. rep. NAVAL POSTGRADUATE SCHOOL MONTEREY CA, 2011.

[361] Peter Mell, Tiffany Bergeron, David Henning, et al. "Creating a patch and vulnerability management program". In: *NIST Special Publication* 800 (2005), p. 40.

[362] The Law: Presidential memoranda, trump cards executive orders: Of patchwork quilts, and shell games. *Cooper, P.J.*, 2001.

[363] François Michel et al. "A first look at starlink performance". In: *Proceedings of the 22nd ACM Internet Measurement Conference*. 2022, pp. 130–136.

[364] R. Mikac. *R. Mikac, ' Protection of the EU's Critical Infrastructures: Results and Challenges ' (2023) Appl. Cybersecurity Amp Internet Gov., vol. 2, no. 1, pp. 1–25*. 2023.

[365] Claire Mills and Patrick Butchard. “The militarisation of space”. In: *House of Commons Library of UK Parliament* (2021).

[366] Shokoufeh Mirzaei and Dennis Wong. “The Optimization of Assurance Level for Space Flight Electronic Hardware”. In: *IISE Annual Conference. Proceedings*. Institute of Industrial and Systems Engineers (IISE). 2023, pp. 1–6.

[367] Monojit Mitra. *Satellite communication*. PHI Learning Pvt. Ltd., 2005.

[368] Anita Modi, Ievgeniia Kuzminykh, and Bogdan Ghita. “Data Driven Approaches to Cybersecurity Governance for Board Decision-Making–A Systematic Review”. In: *arXiv preprint arXiv:2311.17578* (2023).

[369] James Clay Moltz. *The politics of space security: strategic restraint and the pursuit of national interests*. Stanford University Press, 2019.

[370] R. Montasari. *Cyber threats and the security risks they pose to national security: an assessment of cybersecurity policy in the United Kingdom*. Berlin: Springer, 2023.

[371] Jean-Frédéric Morin and Eytan Tepper. “The empire strikes back: Comparing US and China’s structural power in outer space”. In: *Global Studies Quarterly* 3.4 (2023), ksad067.

[372] Ellen Nakashima. “Chinese Hackers Breach NOAA Satellite Systems”. In: *The Washington Post* (Nov. 2014). Accessed 18 October 2025. URL: https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-noaa-satellite-systems/2014/11/12/4e7a81d0-6a3d-11e4-a31c-77759fc1eacc_story.html.

[373] NASA. *B. Lal and K. Calvin, ‘ NASA’s Responsible AI Plan ’ NASA, Sep. 01, 2022*. 2022. URL: https://ntrs.nasa.gov/api/citations/20220013471/downloads/RAI%20Plan%20Sept%201%202022.pdf.

[374] NASA. *National Aeronautics and Space Administration (NASA) FY 2026 Budget Technical Supplement*. Tech. rep. NASA, 2025. URL: https://www.nasa.gov/fy-2026-budget-request/.

[375] NASA. *Small Spacecraft Technology State of the Art 2024*. Tech. rep. NASA, 2024. URL: https://www.nasa.gov/smallsat-institute/sst-soa/.

[376] NASA. *Space Security: Best Practices Guide (BPG)*. Tech. rep. NASA, 2023. URL: https://www.nasa.gov/general/nasa-issues-new-space-security-best-practices-guide/.

[377] National Institute of Standards and Technology. *FIPS 197: Federal Information Processing Standards Publication - Advanced Encryption Standard (AES)*. FIPS FIPS 197. Published November 26, 2001; Updated May 9, 2023. Gaithersburg, MD 20899-8900: Information Technology Laboratory, Nov. 2001. URL: https://doi.org/10.6028/NIST.FIPS.197-upd1.

[378] National Institute of Standards and Technology. *FIPS PUB 180-4: Federal Information Processing Standards Publication - Secure Hash Standard (SHS)*. FIPS FIPS PUB 180-4. Gaithersburg, MD 20899-8900: Information Technology Laboratory, Aug. 2015. URL: http://dx.doi.org/10.6028/NIST.FIPS.180-4.

[379] National Institute of Standards and Technology. *Guide for Cybersecurity Event Recovery*. Tech. rep. NIST SP 800-184. Accessed: 2025-06-07. Gaithersburg, MD: National Institute of Standards and Technology, 2016. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf.

[380] National Institute of Standards and Technology. *NIST SP 800-131A rev2*. Tech. rep. National Institute of Standards and Technology, 2019. URL: https://csrc.nist.gov/publications/detail/sp/800-131a/rev-2/final.

[381] National Institute of Standards and Technology. *NIST SP 800-56A rev3*. Tech. rep. National Institute of Standards and Technology, 2020. URL: https://csrc.nist.gov/publications/detail/sp/800-56a/rev-3/final.

[382] National Security Agency. *Network Infrastructure Security Guide*. Cybersecurity Technical Report U/OO/118623-22. PP-22-0293 Version 1.1. National Security Agency, June 2022.

[383] Committee on National Security Systems. *CNSSP 15 Use of Public Standards for Secure Information Sharing*. Tech. rep. Committee on National Security Systems, 2016. URL: https://nsarchive.gwu.edu/sites/default/files/documents/3521685/Document-08-Committee-on-National-Security.pdf.

[384] National Space Council. *United States Space Priorities Framework*. Tech. rep. Accessed 2026. The White House, 2021. URL: https://www.whitehouse.gov/wp-content/uploads/2021/12/United-States-Space-Priorities-Framework.pdf.

[385] Rubab Nawaz, Asma Bilal, and Maria Rehman. "United States-China space offensive: A dangerous competition". In: *Astropolitics* 20.1 (2022), pp. 27–42.

[386] Netlas. *Netlas.io – Search Engine for Internet Infrastructure*. Accessed: 2025-07-08. 2025. URL: https://netlas.io/.

[387] OECD. *' Explanatory memorandum on the updated OECD definition of an AI system ' OECD Artificial Intelligence Papers 8, Mar. 2024 , doi : 10.1787/623da898-en*. 2024.

[388] OECD. *The Space Economy in Figures: Unlocking the Potential of Space Data*. 2023. URL: https://www.oecd.org/sti/inno/space-economy.htm.

[389] ESA Security Office. *ESA Cyber Security Resilience Achievement*. 2023. URL: https://esamultimedia.esa.int/docs/corporate/ESA_Cyber_Security_Resilience_Achievement.pdf.

[390] Giorgio Olivero. *Asset Discovery Tools Supporting Cybersecurity Inventory*. Master Degree Thesis. Politecnico Di Torino, 2022.

[391] Boguslaw Olszewski. "Advanced persistent threats as a manifestation of states' military activity in cyber space". In: *Scientific Journal of the Military University of Land Forces* 50.3 (189 (2018), pp. 57–71.

[392] Luka Orešković and Sonja Grgić. "The New EU Space Regulation: One Small Step or One Giant Leap for the EU?." In: *Croatian yearbook of European law & policy* (2021).

[393] Scott et al. Pace. *The Global Positioning System: Assessing National Policies*. Rand Corporation, 1995.

[394] U. Pagallo. *U. Pagallo, E. Bassi, and M. Durante, ' The Normative Challenges of AI in Outer Space: Law, Ethics, and the Realignment of Terrestrial Standards ' (2023) Philos. Technol., vol. 36, no. 2, p. 2 3 , doi : 10.1007/s13347-023-00626-7*. 2023.

[395] Matthew J Page et al. "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews". In: *bmj* 372 (2021).

[396] Joseph Pamula et al. "A weakest-adversary security metric for network configuration security analysis". In: *Proceedings of the 2nd ACM workshop on Quality of protection*. 2006, pp. 31–38.

[397] Matteo Paone. "Aerospace clusters". In: *World's Best Practice and Future Perspectives. An Opportunity for South Australia* (2016).

[398] C.Y. Park et al. "Secure and Lightweight Firmware Over-the-Air Update for Constrained Devices". In: *Electronics* (2025).

[399] Soon-Young Park. "A Comparative Study of Some Country's Policy Directions to the Space Transportation in the New Space Era". In: *AIAA SCITECH 2024 Forum*. 2024, p. 2578.

[400] European Parliament. *Chapter I, article 3(1), Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and. (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). 2024*. Tech. rep. European Union, 2024. URL: http://data.europa.eu/eli/reg/2024/1689/oj/eng.

[401] European Parliament. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, vol. 119. 2016*. Tech. rep. European Parliament and of the Council, 2016. URL: http://data.europa.eu/eli/reg/2016/679/oj/eng.

[402] European Parliament. *Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU*. Tech. rep. European Parliament and of the Council, 2021.

[403] Manisha Parmar and Andy Miles. "Cyber Security Frameworks (CSFs): An Assessment Between the NIST CSF v2. 0 and EU Standards". In: *2024 Security for Space Systems (3S)*. IEEE. 2024, pp. 1–7.

[404] James Pavur. "Securing new space: on satellite cyber-security". PhD thesis. University of Oxford, 2021.

[405] James Pavur and Ivan Martinovic. "Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight". In: *Journal of Cybersecurity* 8.1 (2022), tyac008.

[406] Walter Peeters. "Cyberattacks on Satellites: An Underestimated Political Threat". In: *LSE IDEAS* (2022). URL: https://www.lse.ac.uk/ideas/projects/space-policy/publications/Cyberattacks-on-Satellites.

[407] J. Pelkmans. *J. Pelkmans and A. Renda, ' Does EU Regulation Hinder or Stimulate Innovation? ' Nov. 19, 2014, Rochester, NY: 2528409*. Tech. rep. J. Pelkmans, 2014. URL: https://papers.ssrn.com/abstract=2528409.

[408] Marcus Pendleton, Richard Garcia-Lebron, and Shouhuai Xu. "A survey on security metrics". In: *arXiv preprint arXiv:1601.05792* (2016).

[409] Manuel Perez-Ruiz and Shrini K Upadhyaya. "GNSS in precision agricultural operations". In: *New approach of indoor and outdoor localization systems* (2012), 3e26.

[410] *Pléiades Neo — 30 cm Very High Resolution Imagery*. 2023. URL: https://space-solutions.airbus.com/imagery/our-optical-and-radar-satellite-imagery/pleiades-neo/.

[411] Angelo Podda et al. "Exploitation of bi-static radar architectures for LEO Space Debris surveying and tracking: The BIRALES/BlRALET project". In: *2020 IEEE Radar Conference (RadarConf20)*. IEEE. 2020, pp. 1–6.

[412] Clemence Poirier. *Cyber Operations against Space Infrastructure*. Tech. rep. Zurich: Center for Security Studies (CSS), ETH Zurich, 2025. URL: https://css.ethz.ch/en/services/digital-library/articles/article.html.

[413] Germany's Cybersecurity Policy. *Brzostek, A.*, 2022.

[414] Jan Pomés López. "The dual use, civil and military, of the European Union space programmes: The link between the European Space Policy (ESP) and the Common Security and Defence Policy (CSDP)". In: *EU and the Mediterranean in light of the global EU security strategy: future challenges in neighbourhood, security and defence policies* (2022), pp. 163–179.

[415] Jakub Pražák. "Space cyber threats and need for enhanced resilience of space assets". In: *European Conference on Cyber Warfare and Security*. Academic Conferences International Limited. 2021, pp. 542–XIV.

[416] Oxford University Press. *A. Bradford, ' The Brussels Effect: How the European Union Rules the World ' (2020) Oxford University Press*. Oxford University Press, 2020.

[417] Mark L. Psiaki and Todd E. Humphreys. "GNSS Spoofing and Detection". In: *Proceedings of the IEEE* 104.6 (2016), pp. 1258–1270. DOI: 10.1109/JPROC.2016.2526658.

[418] C. Pursiainen. *C. Pursiainen and E. Kytömaa , ' From European critical infrastructure protection to the resilience of European critical entities: what does it mean? ' (2023) Sustain. Resilient Infrastruct., vol. 8, no. sup1, pp. 85–101 , doi : 10.1080/23789689.2022.2128562*. 2023.

[419] *Market perspectives of Ground Segment as a Service (GSaaS)*. Accessed on 07 2023. 2020. URL: https://www.pwc.fr/fr/assets/files/pdf/2020/11/en-france-pwc-space-practice-research-paper-gsaas.pdf.

[420] Da Qi. "The Changing Legal Landscape for Network Security under the PRC Cybersecurity Law". In: *Competition L. Int'l* 13 (2017), p. 55.

[421] Zhicheng Qu et al. "LEO satellite constellation for Internet of Things". In: *IEEE access* 5 (2017), pp. 18391–18401.

[422] Alex Ramos et al. "Model-based quantitative network security metrics: A survey". In: *IEEE Communications Surveys & Tutorials* 19.4 (2017), pp. 2704–2734.

[423] Gregory C Rasner. *Cybersecurity and third-party risk: Third party threat hunting*. John Wiley & Sons, 2021.

[424] Kaushik Ray and William Selvamurthy. "Starlink's Role in Ukraine". In: *Journal of Defence Studies* 17.1 (2023), pp. 25–44.

[425] European Space Agency – Reentry. *Long March 5B Re-entry*. URL: https://www.reentry.esoc.esa.int/home/blog/long-march-5b-reentry.

[426] Camille Reeves and Cortney Weinbaum. "China, Russia, and the United States in Low Earth Orbit". In: (2025).

[427] Jingjing Ren et al. "Information exposure from consumer iot devices: A multidimensional, network-informed measurement approach". In: *Proceedings of the Internet Measurement Conference*. 2019, pp. 267–279.

[428] Reuters. *European countries report GPS jamming, hacked satellite TV broadcasts*. Reports submitted to ITU regarding malicious interference with satellite systems. 2024. URL: https://www.reuters.com/technology/european-countries-report-gps-jamming-hacked-satellite-tv-broadcasts-2024-06-17/.

[429] Reuters. *Exclusive: U.S. spy agency probes sabotage of satellite internet during Russian cyberattack*. Accessed on 07 2023. 2022. URL: https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/.

[430] Reuters. *Exclusive: Western intelligence agencies investigating satellite internet outage*. Coverage of KA-SAT Viasat cyberattack linked to Russian military operations. 2022. URL: https://www.reuters.com/business/media-telecom/exclusive-western-intelligence-agencies-investigating-satellite-internet-outage-2022-03-30/.

[431] Reuters. "Two tankers collide near UAE's Khor Fakkan; fire reported". In: *Reuters* (June 2025). Accessed 2025-09-27. URL: https://www.reuters.com/.

[432] Reversemode. *VIASAT incident: from speculation to technical details*. Accessed on 07 2023. 2022. URL: https://www.reversemode.com/2022/03/viasat-incident-from-speculation-to.html.

[433] Jean-Marc Rickli and Federico Mantellassi. *The war in Ukraine: Reality check for emerging technologies and the future of warfare*. GCSP, Geneva Centre for Security Policy, 2024.

[434] Sebastian Samuele Rizzuto et al. "Object detection on space-based optical images leveraging machine learning techniques". In: *Neural Computing and Applications* 37.22 (2025), pp. 17153–17177.

[435] Arpan Roy, Dong Seong Kim, and Kishor S Trivedi. "Attack countermeasure trees (ACT): towards unifying the constructs of attack and defense trees". In: *Security and communication networks* 5.8 (2012), pp. 929–943.

[436] Sacra. *SpaceX: Company Financials and Overview*. Accessed: 2025-03-30. Sacra, 2024. URL: https://sacra.com/c/spacex/#:~:text=The%20company%20achieved%20profitability%20in,total%20revenue%20of%20%2414.2B..

[437] Bader Al-Sada, Alireza Sadighian, and Gabriele Oligeri. "Mitre att&ck: State of the art and way forward". In: *ACM Computing Surveys* 57.1 (2024), pp. 1–37.

[438] Nasir Saeed et al. "Point-to-point communication in integrated satellite-aerial 6G networks: State-of-the-art and future challenges". In: *IEEE Open Journal of the Communications Society* 2 (2021), pp. 1505–1525.

[439] Johnny Saldana. *The Coding Manual for Qualitative Researchers*. SAGE Publications, 2021.

[440] Ruben Santamarta. *A wake-up call for SATCOM security.* Tech. rep. 2014.

[441] Ruben Santamarta. *Last Call for SATCOM Security*. Seattle, WA: IOActive, 2018.

[442] State-of-the-Art Authentication Measures in Satellite Communication Networks: A Comprehensive Analysis. *Suhaimi, N*. 2024.

[443] Satellite Industry Association. *Cybersecurity Best Practices and Industry Positions*. Tech. rep. Report and policy statements published 2022–2023. Accessed 2026. Satellite Industry Association, 2023. URL: https://sia.org/satellite-industry-association-reiterates-its-commitment-to-cybersecurity-and-best-practices/.

[444] Satellite Today. *Axiros, ViaSat to Produce First Deployment of TR-069 Protocol over a Satellite Network*. Accessed on 07 2023. 2013. URL: https://www.satellitetoday.com/telecom/2013/10/04/axiros-viasat-to-produce-first-deployment-of-tr-069-protocol-over-a-satellite-network/.

[445] Karen Scarfone, Tim Grance, and Kelly Masone. "Computer security incident handling guide". In: *NIST Special Publication* 800.61 (2008), p. 38.

[446] Christian Schaller. "Sabotage of Submarine Cables and Pipelines as a Use of Force and Armed Attack". In: *International Law Studies* 106.1 (2025), p. 8.

[447] Matthew Scholl and Theresa Suloway. *NISTIR 8270: Introduction to Cybersecurity for Commercial Satellite Operations (2nd Draft)*. Tech. rep. NISTIR 8270. National Institute of Standards and Technology (NIST), Feb. 2022.

[448] Margrit Schreier. *Qualitative Content Analysis in Practice*. SAGE Publications, 2012.

[449] Andrej Schreiner et al. "Risk assessment of distribution system: real case application of value at risk metrics". In: *CIRED 2009-20th International Conference and Exhibition on Electricity Distribution-Part 1*. IET. 2009, pp. 1–4.

[450] CCSDS Secretariat. *The Application of Security to CCSDS Protocols*. Tech. rep. CCSDS, 2019. URL: https://public.ccsds.org/Pubs/350x0g3.pdf.

[451] Secure World Foundation. *Global Counterspace Capabilities: An Open Source Assessment*. Tech. rep. Washington, DC: Secure World Foundation, 2024. URL: https://swfound.org/counterspace/.

[452] Federal Office for Information Security. *Technical Guidelines (BSI TR-03184)*. Tech. rep. 2023. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03184/BSI-TR-03184_part1.pdf?__blob=publicationFile%5C&v=2.

[453] Sejal Akre. *Satellite Communication Market Information by Product, Technology, End-Use, and Region-Forecast to 2025*. Accessed on 07 2023. 2022. URL: https://www.marketresearchfuture.com/reports/satellite-communication-market-8466.

[454] Lucie Sénéchal-Perrouault. "Chinese commercial space launchers: historical perspective; policy framework". In: *Space Policy* 66 (2023), p. 101572.

[455] SentinelLabs. *AcidRain: A Modem Wiper Rains Down on Europe*. Accessed 2025-09-27. Mar. 2022. URL: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/.

[456] Syed Muhammad Jamil Shah, Ammar Nasir, and Hafeez Ahmed. "A survey paper on security issues in satellite communication network infrastructure". In: *International Journal of Engineering Research and General Science* 2.6 (2014), pp. 887–900.

[457] V. Shah. *V. Shah, ' Next-Generation Space Exploration: AI-Enhanced Autonomous Navigation Systems ' (2024) J. Environ. Sci. Technol., vol. 3, no. 1, Art. no. 1*. 2024.

[458] S. Shahzad. *S. Shahzad, L. Qiao, and K. Joiner, ' Need for a Cyber Resilience Framework for Critical Space Infrastructure ' (2022) Int. Conf. Cyber Warf. Secur., vol. 17, no. 1, pp. 404–412 , doi : 10.34190/iccws.17.1.52*. 2022.

[459] Space Threat Assessment Fact Sheet. *National Security Space Association, 16 May 2025*. Tech. rep. Space Threat Assessment Fact Sheet, 2025. URL: https://nssaspace.org/wp-content/uploads/2025/05/20250516-S2-Space-Threat-Fact-Sheet-v8-RELEASE.pdf.

[460] Bundesamt für Sicherheit in der Informationstechnik (BSI). *IT-Grundschutz-Profil für Weltrauminfrastrukturen*. Tech. rep. Available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Profil_Weltrauminfrastrukturen.html. Bundesamt für Sicherheit in der Informationstechnik (BSI), June 2022.

[461] *Significant Security Deficiencies in NOAA's Information Systems Create Risks in Its National Critical Mission*. https://www.oig.doc.gov/OIGPublications/OIG-14-025-A.pdf. Final Report No. OIG-14-025-A, U.S. Department of Commerce, Office of Inspector General, Office of Audit and Evaluation. Accessed: 2024-09-29. National Oceanic and Atmospheric Administration, July 2014.

[462] Umesh Kumar Singh and Chanchala Joshi. "Comparative study of information security risk assessment frameworks". In: *International Journal of Computer Application* 2.8 (2018), pp. 2250–1797.

[463] Joshua Smailes et al. *Dishing Out DoS: How to Disable and Secure the Starlink User Terminal*. 2023. arXiv: 2303.00582 [cs.CR].

[464] Marshall Smith et al. "The artemis program: An overview of nasa's activities to return humans to the moon". In: *2020 IEEE aerospace conference*. IEEE. 2020, pp. 1–10.

[465] Henry Sokolski. "A China-US war in space: The after-action report". In: *Bulletin of the Atomic Scientists* 78.1 (2022), pp. 11–16.

[466] Wes Sonnenreich, Jason Albanese, and Bruce Stout. "Return on security investment (ROSI)-a practical quantitative model". In: *Journal of Research and practice in Information Technology* 38.1 (2006), pp. 45–56.

[467] Young European Enterprises Syndicate Space. *YEESS Position Paper on the EU Space Law*. https://www.yeess.eu/. Submitted as an attachment to the targeted and public consultation on the EU Space Law, Brussels, 28 November, 2023. Accessed on: Date.

[468] Resiliency in Space as a Combined Challenge for NATO. *Vasen, T.*, 2021.

[469] *Space Cybersecurity: Threats, Challenges, and Opportunities*. 2022. URL: https://www.esa.int.

[470] Space Industry Office, Manufacturing Industries Bureau, Ministry of Economy, Trade and Industry (METI). *Cybersecurity Guidelines for Commercial Space Systems*. Version 1.1. Mar. 2019.

[471] European Cooperation for Space Standardization. *ECSS-E-ST-80C: Space engineering – Security in space systems lifecycles*. https://ecss.nl/standard/ecss-e-st-80c-space-engineering-security-in-space-systems-lifecycles/. July 2024.

[472] European Cooperation for Space Standardization. *ECSS-Q-ST-80C Rev.2: Software product assurance*. https://ecss.nl/standard/ecss-q-st-80c-rev-2-software-product-assurance-30-april-2025/. Apr. 2025.

[473] European Cooperation for Space Standardization. *ECSS-E-ST-40C Rev.1: Space engineering – Software general requirements*. ESA-ESTEC, Noordwijk. Approved 30 April 2025; defines software engineering processes, verification, validation, and secure delivery requirements. Apr. 2025. URL: https://ecss.nl/standard/ecss-e-st-40c-rev-1-space-engineering-software-general-requirements/.

[474] SPACE SYSTEMS COMMAND. *Press Release: SSC CSCO reaches critical milestone for IA-Pre, roll-out begins today*. Press Release. Office of Public Affairs (SSC/PA), 483 N. Aviation Blvd., El Segundo, Calif. 90245-2808. SPACE SYSTEMS COMMAND, May 2022.

[475] J. M. Spring. *J. M. Spring, A. Galyardt, A. D. Householder, and N. VanHoudnos , ' On managing vulnerabilities in AI/ML S ystems ' (2021) Proceedings of the New Security Paradigms Workshop 2020 . New York, NY, USA : Association for Computing Machinery, pp. 111–126 , doi : 10.1145/3442167.3442177*. 2021.

[476] Vincent Sritapan et al. "Developing a metrics framework for the federal government in computer security incident response". In: *Communications of the IIMA* 11.3 (2011), p. 5.

[477] V.A. Stafford. *Zero trust architecture*. 2020.

[478] International Organization for Standardization and International Electrotechnical Commission. *ISO/IEC 27002:2022 Information technology — Security techniques — Code of practice for information security controls*. Accessed on 07 2023. 2022. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en.

[479] *Bugcrowd - SpaceX*. https://bugcrowd.com/spacex. Accessed on: 10/12/2023. 2023.

[480] State Council Information Office of the People's Republic of China. *China Defense White Papers, 1995–2019*. Tech. rep. Collection of official white papers published between 1995 and 2019. Accessed via Andrew S. Erickson. Beijing: State Council Information Office, 2019. URL: https://www.andrewerickson.com/2019/07/china-defense-white-papers-1995-2019-download-complete-set-read-highlights-here/.

[481] State Council Information Office of the People's Republic of China. *China's Space Program: A 2021 Perspective*. Tech. rep. Accessed 2026. Beijing: State Council Information Office, 2022. URL: https://english.www.gov.cn/archive/whitepaper/202201/28/content_WS61f35b3dc6d09c94e48a4.html.

[482] Keith Stouffer et al. *Guide to Operational Technology (OT) Security*. Tech. rep. NIST SP 800-82 Rev. 3. National Institute of Standards and Technology, Sept. 2023. DOI: 10.6028/NIST.SP.800-82r3. URL: https://doi.org/10.6028/NIST.SP.800-82r3.

[483] Chris Strasburg et al. "A framework for cost sensitive assessment of intrusion response selection". In: *2009 33rd Annual IEEE international computer software and applications conference*. Vol. 1. IEEE. 2009, pp. 355–360.

[484] Dimitrios Stroikos. "China and India as Rising Powers and the Militarisation of Space". In: *The Militarization of European Space Policy*. Routledge, 2023, pp. 170–188.

[485] Dimitrios Stroikos. "Still lost in space? Understanding China and India's anti-satellite tests through an eclectic approach". In: *Astropolitics* 21.2-3 (2023), pp. 179–205.

[486] R. Sun. *R. Sun, ' Global AI Regulation Tracker ' ,* tech. rep. R. Sun. URL: https://www.techieray.com/GlobalAIRegulationTracker.

[487] Robert Chandler Swallow. "Considering the cost of cyber warfare: advancing cyber warfare analytics to better assess tradeoffs in system destruction warfare". In: *The Journal of Defense Modeling and Simulation* 20.1 (2023), pp. 3–37.

[488] McKayla Swan. "Anti-satellite Tests: A Risk to The Security and Sustainability of Outer Space". In: *Liberty University Journal of Statesmanship & Public Policy* 3.1 (2022), p. 4.

[489] *Sweden Accuses Russia of Widespread GPS Jamming Over Baltic Sea*. Accessed 18 October 2025. Sept. 2025. URL: https://www.themoscowtimes.com/2025/09/04/sweden-accuses-russia-of-widespread-gps-jamming-over-baltic-sea-a90427.

[490] Makena Swope, Jack Watling, Clayton S. Dankwa, et al. *Space Threat Assessment 2025*. Center for Strategic and International Studies, 2025. URL: https://www.csis.org/analysis/space-threat-assessment-2025.

[491] M. Tarka, M. Blankstein, and P. Schottel. *Empowering boards: how the National Cyber Security Centre Board (United Kingdom) toolkit is transforming cyber security governance*. 2023, p. 110897.

[492] WebRAY Technology. *Threat Intelligence Report on Cyber Exposure in China's Aerospace and Satellite-Related Organisations, 2023*. WebRAY, 2023. URL: https://www.webray.com.cn.

[493] Techq. *Thousands of internet users go dark in Europe from 'cyberattack'*. Accessed on 07 2023. 2022. URL: https://techhq.com/2022/03/cyberattack-knocks-thousands-offline-in-europe/.

[494] Pietro Tedeschi, Savio Sciancalepore, and Roberto Di Pietro. "Satellite-based communications security: A survey of threats, solutions, and research challenges". In: *Computer Networks* (2022), p. 109246.

[495] Telespazio. *Company Profile*. Accessed: 2025-03-30. Telespazio, 2024. URL: https://www.telespazio.com/en/company/profile.

[496] K. Thangavel. *K. Thangavel, R. Sabatini, A. Gardi, K. Ranasinghe, P. Servidia, and D. Spiller, ' Artificial Intelligence for Trusted Autonomous Satellite Operations ' (2024) Prog . in Aero . Sci . 144, 100960*. 2024.

[497] The Aerospace Corporation. *The Aerospace Corporation*. Accessed: March 13, 2025. 2025. URL: https://aerospace.org/.

[498] *The Economic Impact on the UK of a Disruption to GNSS*. 2021. URL: https://londoneconomics.co.uk/blog/publication/the-economic-impact-on-the-uk-of-a-disruption-to-gnss/.

[499] *The Space Report 2023 Q2*. 2023. URL: https://www.thespacereport.org.

[500] P The White House Trump. *D*. 2022. URL: http://irp.fas.org/offdocs/nspm/spd-5-fs.pdf.

[501] Giovanni Tricco Thomas Graham and Francesco Casaril. "From Europe to Europa: Implications of the European AI Act for the Space Industry." In: *Under Review* 0.0 (2025).

[502] Rajiv Thummala and Gregory Falco. "Hacktivism Goes Orbital: Investigating NB65's Breach of ROSCOSMOS." In: 2024.

[503] Financial Times. "GPS interference raises risk of accidents in the Strait of Hormuz". In: *Financial Times* (2025). Accessed 2025-09-27. URL: https://www.ft.com/content/ac3c571f-2c4e-4c57-b582-21e2b27170f8.

[504] Andrea Tortorelli et al. "A security metric for assessing the security level of critical infrastructures". In: *International Journal of Critical Computer-Based Systems* 10.1 (2020), pp. 74–94.

[505] G. Tricco. *G. Tricco , et. al. ' The protection of AI-based space systems from a data-driven governance perspective ' (2025) Acta Astronautica*. 2025.

[506] Giovanni Tricco, Thomas Graham, and Francesco Casaril. "From Europe to Europa: Implications of the EU AI Act for the Space Industry". In: *AIRe – Journal of AI Law and Regulation* 3 (2025). Article 6. DOI: 10.21552/aire/2025/3/6. URL: https://aire.lexxion.eu/article/AIRE/2025/3/6.

[507] Markos Trichas and Matthew Mowthorpe. "Space and the New Frontier of Warfare". In: *The Co-evolution of Technology and Warfare*. Routledge, 2025, pp. 56–70.

[508] Panagiotis Trimintzios. "Measurement frameworks and metrics for resilient networks and services: technical report". In: *Eur. Netw. Inf. Secur. Agency* 109 (2011).

[509] Andrea Tundis, Wojciech Mazurczyk, and Max Mühlhäuser. "A review of network vulnerabilities scanning tools: Types, capabilities and functioning". In: *Proceedings of the 13th international conference on availability, reliability and security*. 2018, pp. 1–10.

[510] M Turner et al. "Galileo public regulated services (PRS) with limited key distribution". In: *Proceedings of the 28th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2015)*. 2015, pp. 3397–3404.

[511] U.S. Department of Commerce, Office of Space Commerce. *U.S. Government Provides Feedback on Draft EU Space Act*. Tech. rep. Accessed 2026. U.S. Department of Commerce, 2025. URL: https://space.commerce.gov/u-s-government-provides-feedback-on-draft-e-u-space-act/.

[512] U.S. Department of Defense. *Defense Space Strategy Summary*. Tech. rep. Accessed 2026. U.S. Department of Defense, 2020. URL: https://media.defense.gov/2020/Jun/17/2002317391/-1/-1/1/2020_DEFENSE_SPACE_STRATEGY_SUMMARY.PDF.

[513] U.S. Department of State. *A Strategic Framework for Space Diplomacy*. Tech. rep. Accessed 2026. U.S. Department of State, 2023. URL: https://www.state.gov/wp-content/uploads/2023/04/Strategic-Framework-for-Space-Diplomacy.pdf.

[514] U.S. Department of Transportation. *Complementary PNT Action Plan*. Mar. 2024. URL: https://www.transportation.gov/pnt/complementary-pnt-action-plan.

[515] U.S. Government Accountability Office. *Cybersecurity: NASA Needs to Fully Implement Risk Management*. Tech. rep. GAO-25-108138. Accessed 2026. U.S. Government Accountability Office, 2025. URL: https://www.gao.gov/products/gao-25-108138.

[516] U.S. Maritime Administration. *2017-005A Black Sea GPS Interference Advisory*. Accessed 2025-09-27. 2017. URL: https://www.maritime.dot.gov/msci/2017-005a-black-sea-gps-interference.

[517] UK Cabinet Office. *Public Summary of Sector Security and Resilience Plans*. Accessed 4 October 2024. London, 2018. URL: https://assets.publishing.service.gov.uk/media/5c8a7845ed915d5c1456006a/20190215_PublicSummaryOfSectorSecurityAndResiliencePlans2018.pdf.

[518] UK Cabinet Office. *Written Evidence from the Cabinet Ofice*. Accessed 5 May 2024. London, 2023. URL: https://committees.parliament.uk/writtenevidence/126643/html/cyber-resilience-of-the-UKs-Critical-National-Infrastructure-CNI.

[519] Innovation & Technology UK Department for Science. *Cyber risks of cloud computing in the ground segment of the space sector*. Tech. rep. Expert insights on risks in Ground Segment as a Service (GSaaS). UK Department for Science, Innovation and Technology (DSIT), Aug. 2025. URL: https://www.gov.uk/government/publications/cyber-risks-of-cloud-computing-in-the-ground-segment-of-the-space-sector.

[520] UK Department for Science, Innovation and Technology. *The Case for Space: Research and Analysis*. Accessed 5 October 2024. London, 2023. URL: https://www.gov.uk/government/publications/the-case-for-space.

[521] UK Government. *National Risk Register: 2023*. Accessed 5 April 2024. London, 2023. URL: https://assets.publishing.service.gov.uk/media/64ca1dfe19f5622669f3c1b1/2023_NATIONAL_RISK_REGISTER_NRR.pdf.

[522] *UK Space Agency Rural Connectivity Pilot Projects*. 2024. URL: https://www.gov.uk/government/news/uk-space-agency-funds-rural-connectivity-projects.

[523] 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*. 2025. URL: https://polish-presidency.consilium.europa.eu/en/programme/programme-of-the-presidency/.

[524] United Nations. *International Covenant on Economic, Social and Cultural Rights*. United Nations Treaty Series. Adopted 16 December 1966, entered into force 3 January 1976, 993 UNTS 3, Article 11. 1966. URL: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights.

[525] United States Delegation to the United Nations Committee on the Peaceful Uses of Outer Space. *Statement to the Scientific and Technical Sub-Committee*. United Nations Office for Outer Space Affairs. Statement delivered to COPUOS STSC. Feb. 2024. URL: https://www.unoosa.org/documents/pdf/copuos/2024/statements/6_UnitedStates.pdf.

[526] United States Space Force. *Space Capstone Publication: Spacepower*. Tech. rep. Accessed 2026. United States Space Force, 2020. URL: https://www.spaceforce.mil/Portals/2/Documents/Spacepower/Spacepower_Doctrine_Publication.pdf.

[527] United States creates the US space command and the US space force to strengthen military capabilities in space. "Galbraith, J.," in: (2020).

[528] Ovidiu Valea and Ciprian Oprişa. "Towards pentesting automation using the metasploit framework". In: *2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP)*. IEEE. 2020, pp. 171–178.

[529] E Van Breukelen. "Qualitative fault tree analysis applied as a design tool in a low cost satellite design: Method and lessons learned." In: 2006.

[530] V. Varadharajan et al. "Security Challenges when Space Merges with Cyberspace". In: *Computer Law & Security Review* (2024).

[531] C. Vasquez. *C. Vasquez, ' Satellite hack on eve of Ukraine war was a coordinated, multi-pronged assault, ' CyberScoop*. URL: https://cyberscoop.com/viasat-ka-sat-hack-black-hat/.

[532] Rayford B Vaughn, Ronda Henning, and Ambareen Siraj. "Information assurance measures and metrics-state of practice and proposed taxonomy". In: *36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of the*. IEEE. 2003, 10–pp.

[533] M. Veale. *M. Veale, K. Matus, and R. Gorwa, ' AI and Global Governance: Modalities, Rationales, Tensions ' Oct. 01, 2023, Rochester, NY: 4605727 , doi : 10.1146/annurev-lawsocsci-020223-040749*. 2023.

[534] M. Verma. *M. Verma, ' Edge Computing in Space Enhancing Data Processing and Communication for Space Missions ' (2024) Int. J. Trend Sci. Res. Dev., vol. 8, no. 1*. 2024.

[535] Ly Vessels, Kenneth Heffner, and Daniel Johnson. "Cybersecurity risk assessment for space systems". In: *2019 IEEE Space Computing Conference (SCC)*. IEEE. 2019, pp. 11–19.

[536] Viasat. *10-K Viasat Annual Report - May 22, 2023*. Access the annual report via Viasat Investor Relations at https://investors.viasat.com/sec-filings/sec-filing/10-k/0000950170-23-023444. Accessed on: 14/12/2023. 2023.

[537] Viasat. *KA-SAT Network Cyber Attack Overview*. Accessed 2025-09-27. Mar. 2022. URL: https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/.

[538] Viasat News Blog. *Ka-Sat Network Cyber Attack Overview*. Accessed on 07 2023. 2022. URL: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview.

[539] Viasat, Inc. *Viasat Annual Report FY24*. Tech. rep. Accessed: 2025-04-06. Viasat, Inc., 2024. URL: https://investors.viasat.com/static-files/5e5c4a86-4602-46ad-b17f-e2e2b8158d79.

[540] David Voelkel et al. "The STP-2 mission: rideshare lessons learned from the air force's first falcon heavy launch". In: (2020).

[541] Wireless Signal Injection Attacks on VSAT Satellite Modems. *Bisping, R., Willbold, J., Strohmeier, M.* 2024.

[542] VT. *GPS Disruption Has Affected 123,000 Flights in the Baltic Region*. 23 July 2025. Accessed 18 October 2025. 2025. URL: https://news.err.ee/1609792437/gps-disruption-has-affected-123-000-flights-in-the-baltic-region.

[543] On the capability of static code analysis to detect security vulnerabilities. "Goseva-Popstojanova, K". In: *Information and Software Technology* (2015).

[544] Karl Waedt et al. "Automatic assets identification for smart cities: Prerequisites for cybersecurity risk assessments". In: *2016 IEEE international smart cities conference (ISC2)*. IEEE. 2016, pp. 1–6.

[545] Simon Walker. "Economics and the cyber challenge". In: *Information Security Technical Report* 17.1-2 (2012), pp. 9–18.

[546] Howard Wang, Jackson Smith, and Cristina L. Garafola. *Chinese Military Views of Low Earth Orbit*. Tech. rep. Research report. RAND Corporation, 2025.

[547] Lingyu Wang, Anoop Singhal, and Sushil Jajodia. "Measuring the overall security of network configurations using attack graphs". In: *IFIP annual conference on data and applications security and privacy*. Springer. 2007, pp. 98–112.

[548] Lingyu Wang et al. "k-zero day safety: A network security metric for measuring the risk of unknown vulnerabilities". In: *IEEE Transactions on Dependable and Secure Computing* 11.1 (2013), pp. 30–44.

[549] Weijing Wang et al. "Understanding and predicting incident mitigation time". In: *Information and Software Technology* 155 (2023), p. 107119.

[550] Stephen Weatherill. "The Limits of Legislative Harmonization Ten Years after Tobacco Advertising: How the Court's Case Law has become a "Drafting Guide"." In: (2011).

[551] Brian Weeden. *Current and Future Trends in Chinese Counterspace Capabilities*. Tech. rep. 62. Institut français des relations internationales (IFRI), 2020, pp. 1–42.

[552] Brian Weeden and Victoria Samson. *Global counterspace capabilities: An open source assessment*. Secure World Foundation Washington, DC, 2018.

[553] Matt Weir et al. "Testing metrics for password creation policies by attacking large sets of revealed passwords". In: *Proceedings of the 17th ACM conference on Computer and communications security*. 2010, pp. 162–175.

[554] *The Open Security Controls Assessment Language (OSCAL): Schema and Metaschema*. en. 23. Proceedings of Balisage: The Markup Conference, Rockville, MD, July 2019, pp. 1–21. DOI: https://doi.org/10.4242/BalisageVol23.Piez01.

[555] *When Outer Space Falls into Conflict: Key ICRC Recommendations*. 2022. URL: https://www.icrc.org/en/document/when-outer-space-falls-conflict.

[556] Johannes Willbold et al. "Vsaster: Uncovering inherent security issues in current vsat system practices". In: *Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 2024, pp. 288–299.

[557] Ryan Williams et al. "Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach". In: *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*. IEEE. 2017, pp. 179–181.

[558] Jonathan Wilmot. "Using CCSDS standards to reduce mission costs." In: 2017.

[559] Tomasz Wójtowicz. "American, Russian, and Chinese anti-satellite Weapons: A Comparative Analysis." In: *Polish Political Science Review/Polski Przeglad Politologiczny* 13.2 (2025).

[560] World Economic Forum. *The Future of Space: Why Satellites Matter*. 2022. URL: https://www.weforum.org/stories/2024/04/space-economy-technology-invest-rocket-opportunity/.

[561] Zhijun Wu et al. "Spoofing and anti-spoofing technologies of global navigation satellite system: A survey". In: *IEEE Access* 8 (2020), pp. 165444–165496.

[562] Jeff Wysocarski et al. "Integrating COTS Routers Into Terminals for Future Protected SATCOM Systems With Dynamic Resource Allocation". In: *MILCOM 2007-IEEE Military Communications Conference*. IEEE. 2007, pp. 1–7.

[563] Space Y. *Position Paper on the EU Space Act and Downstream Space Services, 2023*. Tech. rep. Space Y, 2023. URL: https://spacey.eu.

[564] Anjali Yadav et al. “Internet From Space Anywhere and Anytime-Starlink”. In: *Available at SSRN 4160260* (2022).

[565] et al Yahia Olfa Ben. *Securing Satellite Link Segment: A Secure-by-Component Design*. 2024.

[566] Xiaocui Yang et al. “Propagation characteristics of modulated EHF signal in the wake region of plasma sheath”. In: *Aerospace* 9.4 (2022), p. 194.

[567] Emmi Yonekura et al. *Commercial Space Capabilities and Market Overview: The Relationship Between Commercial Space Developments and the US Department of Defense*. Tech. rep. RAND, 2022.

[568] Makena Young, Kaitlyn Johnson, and Clayton Swope. *Space Threat Assessment 2025*. Tech. rep. Accessed: 5 June 2025. Center for Strategic and International Studies (CSIS), Apr. 2025. URL: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-04/250425_Swope_Space_Threat.pdf?VersionId=orhySgjISemJLjhdQKKes2OVb35jwk

[569] Lingjing Yu et al. “A Comprehensive Analysis of Security Vulnerabilities and Attacks in Satellite Modems”. In: *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24)*. Salt Lake City, UT, USA: ACM, 2024, pp. 1–15. ISBN: 979-8-4007-0636-3. DOI: 10.1145/3658644.3670390.

[570] Lingjing Yu et al. “A Comprehensive Analysis of Security Vulnerabilities and Attacks in Satellite Modems”. In: *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24)*. Salt Lake City, UT, USA: ACM, 2024, p. 20. DOI: 10.1145/3658644.3670390.

[571] Yafeng Zhan et al. “Challenges and solutions for the satellite tracking, telemetry, and command system”. In: *IEEE Wireless Communications* 27.6 (2020), pp. 12–18.

[572] Yafeng Zhan et al. “Challenges and solutions for the satellite tracking, telemetry, and command system”. In: *IEEE Wireless Communications* 27.6 (2021), pp. 12–18.

[573] Hua Zhang et al. “A conditional probability computation method for vulnerability exploitation based on CVSS”. In: *2017 IEEE Second International Conference on Data Science in Cyberspace (DSC)*. IEEE. 2017, pp. 238–241.