international journal of critical infrastructure protection 51 (2025) 100805

Contents lists available at ScienceDirect

International Journal of Critical Infrastructure Protection

journal homepage: www.elsevier.com/locate/ijcip

Developing security metrics for space systems: A study considering the NIST Cybersecurity Framework 2.0 and the NIS2

Francesco Casaril *, Letterio Galletta

IMT School for Advanced Studies Lucca, Lucca, Italy

ARTICLE INFO

Keywords:
Satellite cybersecurity
Space law
Security metrics
NIST CSF 2.0
Cybersecurity governance

ABSTRACT

Space-based assets are essential for critical societal functions across sectors like energy, transportation, communication, agriculture, and government. As these services become more integrated into daily life and reliance on cyber–physical systems grows, the interconnectivity and commercialization of space assets increases the attack surface and cybersecurity risks. Recent incidents affecting space infrastructure underscore the urgent need for robust cybersecurity measures. Legislators in the EU and other countries are addressing cyber risks to space and ground assets by developing minimum protection requirements. To support these measures, this paper evaluates whether existing security metrics in the literature cover all NIST functions, categories, and subcategories in the Cybersecurity Framework 2.0 (CSF 2.0). This framework provides a strong foundation for industry sectors and can serve as a baseline to ensure compliance with directives like NIS2. Our analysis reveals imbalances in academic discourse, with certain CSF 2.0 functions underrepresented. Then, we propose new metrics to address unaddressed NIST categories and adapt existing metrics to better suit the space domain. Considering practical challenges in implementing and monitoring these metrics, we propose a tool to facilitate their calculation and visualize security status. We also present a case study resembling real-world space infrastructure that demonstrates our tool's applicability and the value of the designed metrics. Our research has managerial implications, supporting managers, CIOs, and CISOs in making informed decisions, helping companies understand their security levels, and complying with existing and forthcoming space sector regulations. We advocate 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.

1. Introduction

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 [1]. 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,

* Corresponding author.
E-mail addresses: francesco.casaril@imtlucca.it (F. Casaril), letterio.galletta@imtlucca.it (L. Galletta).

https://doi.org/10.1016/j.ijcip.2025.100805
Received 8 January 2025; Received in revised form 19 August 2025; Accepted 28 September 2025
Available online 3 October 2025

has been an area that has received little attention [2]. Previous research has mainly focused on creating new metrics for specific sectors and addressing particular security challenges with new methodologies [3]. 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 [4], 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 that reflects the cybersecurity principles defined in the NIS2. Moreover, this paper 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 paper 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 paper 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 Tables 4, 5, 6, and online [5]. 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 [5]. 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 paper, we proceed as follows. Section 2 clarifies the context and the motivation behind our research. In Section 3, we discuss the relevant literature and compare it with the present paper. Section 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 5, we present our methodology to collect all the relevant security metrics from the literature. Section 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 7 and 8, we present our online tool and our case study, respectively, to show the practicality of the proposed and selected metrics. Finally, Section 9 draws some conclusions and discusses future lines of investigation.

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 [6].

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 [7]. 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 [8]. 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 [9].

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 [10]. As a result, governments started enacting policy measures to increase cybersecurity among all relevant parties [11]. These measures are usually in the form of best practices, technical guidelines, or threat reports. However, when compared to security 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 paper, 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 [12].

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 [4], 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.

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. [13] 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 [14] 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 cyberattacks experienced by participating entities).

Only a few researchers have conducted in-depth studies to develop security metrics for specific sectors. Gori et al. [15], 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. [16] 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. [17] 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 [18] 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 paper leverages the new NIST CSF 2.0 to advance our understanding of cybersecurity metrics for space systems. In addition, this paper 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, this paper highlights 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.

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 [19]. Similarly, CSF 2.0 can be considered a solid baseline for the NIS2 [17], because it reflects many of its principles.

4.1. The NIST CSF 2.0

The NIST CSF version 2.0, released in April 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

Table 1
Examples of NIST CSF 2.0 functions with the corresponding category and 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

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 [20] and the US National Cyber Strategy [21].

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 1 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.

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 gray 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.

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 [22]. Issued in January 2023, the directive mandates that EU Member States identify critical entities in specified sectors by July 17, 2026. These entities will 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 Europe'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.

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 connection 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.

Table 2
Dissimilarities between NIST CSF 2.0 and NIS2 directive.

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.

The NIS2 Directive, which came into effect on December 14, 2022, establishes measures to achieve a high common level of cybersecurity across the Union, replacing the initial EU-wide legislation on cybersecurity. The NIS2 broadens its scope by including a wider range of critical entities and sectors, now encompassing space. The directive also aims to enhance cybersecurity risk management requirements for companies and streamline incident reporting obligations.

In our analysis, we have considered not only the NIS2 itself but also the Implementing Regulation [4] document. This document outlines the technical and methodological requirements of cybersecurity risk-management measures and specifies the cases in which an incident is considered 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, 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 2 clarifies the key structural and legal differences between the NIST CSF 2.0 and NIS2, Table 3 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.

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

Table 3
NIS2 and NIST CSF 2.0 similarities.

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.

statement: "*the policy on the security of network and information systems shall: […] lay down roles and responsibilities [4]*". 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 entities shall establish and maintain an appropriate risk management framework to identify and address the risks posed to the security of network and information systems. [4]*". 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 [4]*".

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 [4].*" 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 [4].*"

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*" [4]. 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*" [4].

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" [4].* 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*" [4].

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*" [4]. 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.

Table 3 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 3, 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.

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 [28], the NIST SP 800-55 performance measurement guide [1], ISACA's Guideline G41 on Return on Security Investment [69], and the PRAGMATIC approach by W. Krag Brotby [26].

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

Table 4
Cybersecurity metrics aligned with NIST CSF subcategories (First Part)

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) [23,24]
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 [25]
Govern	GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders	• Security policy management maturity [26] • % critical assets/functions with cost of compromise estimated [26]
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 [26]
Govern	GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated	• % critical assets/functions with documented risk mitigation plan [26]
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 [26]
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 [26]
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 [1] • Return on Security Investment [27]
Govern	GV.RR-04: Cybersecurity is included in human resources practices	• % BU heads with implemented operational procedures aligned with controls [28] • % new employees completing security awareness training [29]
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 [23]
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 [25]
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 [30] • Proportion of information assets not (correctly) classified [26] • Information asset management maturity [26]
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 [31] • Number of unpatched vulnerabilities [32] • Number of historically exploited vulnerability [32] • Weakest-Adversary [33] • k-Zero Day Safety [34]
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 [14]

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 5
Cybersecurity metrics aligned with NIST CSF subcategories (Second Part)

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) [35] • Probability of vulnerability exploited [36]
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 [28] • Attack Shortest Path [37]
Identify	ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated	• Risk Assessment Coverage [38]
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 [25] • Number of important operations with documented and tested security procedures [25]
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 [39]
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 [28] • Number of access rights authorized, revoked, reset, or changed [40] • Number and type of suspected and actual access violations [40]
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 [29]
Protect	PR.AA-03: Users, services, and hardware are authenticated	• Percentage of business units that have proven their identification and authentication mechanisms [40] • Minimum Password Strength [41]
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 [28] • Number of customer consultations with security teams [28] • Number of security team consultations by business units [28]
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 [40]
Protect	PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected	• Restriction of Number of Executable Components [42] • Data transmission exposure [43] • Percentage of assets with antivirus and antispyware software [28]
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 [28]
Protect	PR.PS-01: Configuration management practices are established and applied	• Rogue Change Days [44] • Mean Cost to Mitigate Vulnerabilities [31] • Patch Policy Compliance [31] • Mean Time to Patch [45] • Mean Cost to Patch [46] • Percentage of Configuration Compliance [47]
Protect	PR.PS-02: Software is maintained, replaced, and removed commensurate with risk	• % of critical assets/functions residing on compliant systems [28]

Table 7, but an extensive sample of validated metrics, and the whole set of metrics analyzed are available on the online supplementary material [5].

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

Table 6
Cybersecurity metrics aligned with NIST CSF subcategories (Third Part)

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 [28]
Protect	PR.IR-01: Networks and environments are protected from unauthorized logical access and usage	• Penetration resistance [32]
Protect	PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	• Attack Resistance Metric [48] • Mean Time to Complete Changes [49]
Protect	PR.IR-04: Adequate resource capacity to ensure availability is maintained	• Host uptime/downtime [50] • Network Resilience [51]
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 [52]
Detect	DE.CM-01: The network is monitored to detect potential cybersecurity events	• Information access control maturity [53] • Viruses and Spyware Detected in Email Messages, websites, user files (number [#], percent [%]) [28] • Percentage of business-critical systems under active monitoring [28] • Vulnerability scanner coverage (#, %, frequency) [28] • Encounter rate [32] • Network Compromise Percentage (NCP) [54] • Attack surface [55] • Intrusion Detection Capability [56]
Detect	DE.CM-02: The physical environment is monitored to find potentially adverse events	• Percentage of critical assets/functions reviewed for physical security risks [28] • Mean-Time-To-Incident-Discovery [57]
Detect	DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events	• Administrator and operator logs [52] • Number of corrective actions [52]
Detect	DE.AE-02: Potentially adverse events are analyzed to better understand associated activities	• Attack Impact [58] • Number of detected incidents [52]
Detect	DE.AE-02: Potentially adverse events are analyzed to better understand associated activities	• Attack Cost [59] • Cost metric [60]
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 [61] • Time per incident [62]
Respond	RS.AN-08: An incident's magnitude is estimated and validated	• Mean Cost of Incidents [63]

(*continued on next page*)

- *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.

Table 6 (*continued*).

CSF function	Subcategory	Metric
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) [28] • Median time to initially respond to the reporter [64] • Mean blind spot metric [65]
Respond	RS.MI-01: Incidents are contained	• Mean-Time to Mitigate Vulnerabilities [66]
Recover	RC.RP-02: Recovery actions are selected, scoped, prioritized, and performed	• Mean Time between Security Incidents [61]
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) [67] • Incidents Cleanup Cost (By business unit) [28] • Mean Incident Recovery Cost [68]

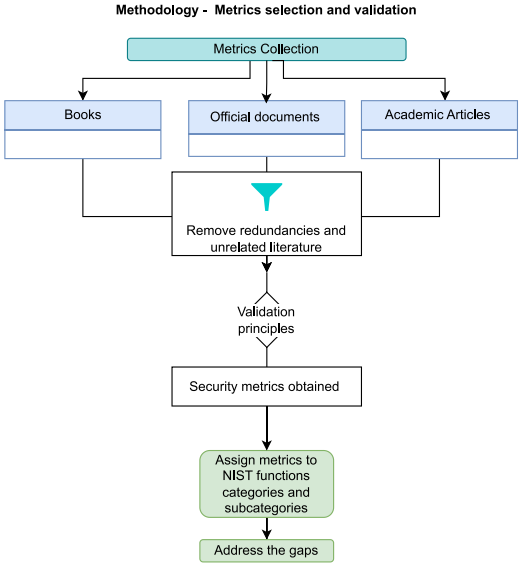

Fig. 1. Metric selection methodology.

- *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 [70] 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 5.2 and 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 (Fig. 1) 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 indexed 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.

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 [28]. 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 labor spend [28]. 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 [28].

The PRAGMATIC method [26], 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 normalized score that sits beside Predictive, Relevant, Actionable and the other criteria mentioned by Brotby and Hinson [26]. 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 annualized 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 [26]. 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 [26].

Taken together, the two approaches operationalize 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, annualize 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 8.1, while discussing the metrics we used in our case study.

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 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. Finally, 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.

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 Fig. 1, 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* [71]: 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)* [64]: 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.[26]*: A comprehensive bibliographic resource that details more than 150 metrics, offering a pragmatic approach to quantifying and managing security risks.
- *Security Metrics* [28] 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* [47]: 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* [72]: 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 Catalog [45]*: 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 [73]: 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 [74]: 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 areas where gaps or limitations in coverage exist.

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 informative 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 subcategories.

Tables 4, 5 and 6 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 4 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 [26].

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

6.1. 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 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 [75].

Developed by the European Cooperation for Space Standardization, the ECSS-E-ST-80C [76] 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 [77] (software product assurance) and ECSS–E-ST-40C [78] (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.

6.2. 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 7, we provide some examples of the validation procedure and reasoning behind the selection of the metrics reported in Tables 4, 5 and 6. 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 5 we discuss their application in Table 7. 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. 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 toward 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 7 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, detection, 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.

Table 7
Risk mitigation metrics for critical assets/functions.

Metric	Ref.	CO	Q	AD	A	CR	CSF	IV	CE
Percentage of critical assets/functions with documented risk mitigation plan	[26]	✓	✓	✓	✓	✓	✓	✓	✓
Network Compromise Percentage (NCP)	[54]	✓	✓	✓	✓	✓	✓	✓	✓
Number of Attacks	[28]	✓	✓	✓	✗	✗	✗	✓	✓
Number of active user IDs assigned to only one person.	[28]	✓	✓	✓	✗	✗	✗	✓	✓

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 [5]. 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 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.

6.3. 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.

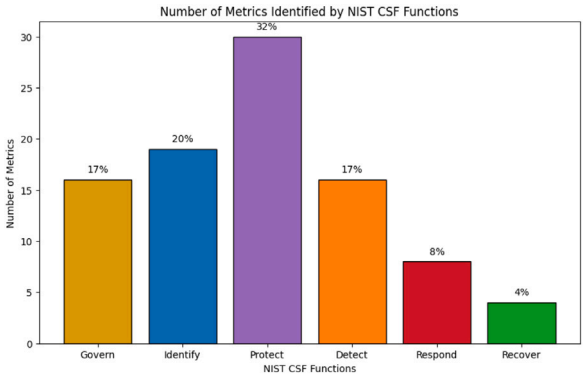

Fig. 2. Distribution of metrics per each NIST CSF function.

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. Fig. 2 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 (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 [79,80]

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 [81,82].

These gaps, highlighted in Fig. 2, 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. Fig. 3 presents the extent of metric coverage for the subcategories.

Such shortcomings, as those highlighted in Figs. 2 and 3 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

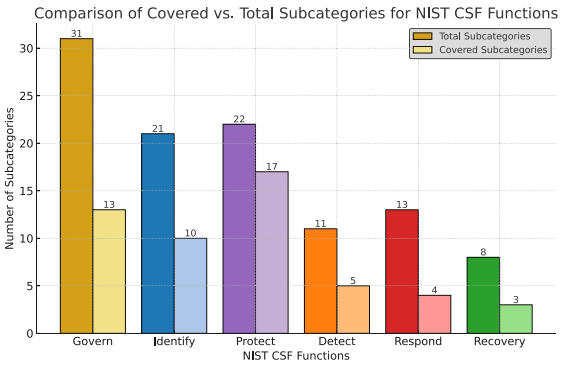

Fig. 3. Metrics identified over total number of NIST CSF subcategories.

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 inherently 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 [25,83]. 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, [71] 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 [84] 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® [85] 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.

6.4. 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.

6.5. 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 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.

The proposed metrics are summarized in Table 8, and we briefly comment on them below. Table 9 defines the abbreviation used in the metric formulas. Our metrics are designed to tackle specific risks

Table 8
Security metrics for space systems with related metrics updated.

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

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 formula 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 [86]. 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 management 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 [87]. Attackers leveraged a third-party network vulnerability, using an unsecured Raspberry Pi device to gain unauthorized access to

Table 9
Abbreviations used in metrics formulas.

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

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 [88]. 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 [43]. By monitoring jamming intensity, operators can respond quickly—like SpaceX did by updating Starlink systems [89]. By tracking the number of jamming attempts and their severity using a metric like 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 [90]. 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) [91], 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 [92], 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) [93] for space-grade components, monitoring the frequency with which telemetry, tracking, and command (TT&C) keys are rotated [94], 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. The domain relevance of the proposed metrics

Some of the metrics introduced in this paper 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 [95] 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 [95]. 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 [95]. 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 [95]. In some cases, commercial airlines and maritime operators reported navigation failures, while satellite operators detected interference affecting uplink/downlink channels [96]. 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 [95].

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 [8] 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 [95].

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 [95]. 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.

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 [5] 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 6.5. 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 functionalities, 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 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.

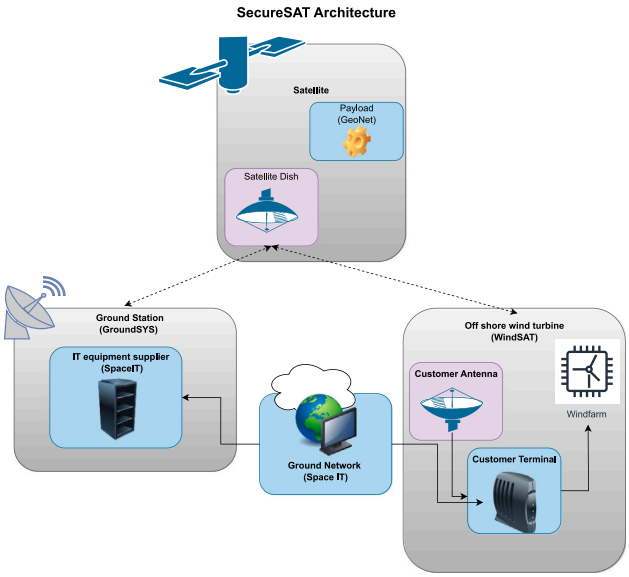

Fig. 4. SecureSAT architecture.

8. Case study: Security metrics into space system design

In this section, we present a case study to validate our metrics, defined in Fig. 4 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 [97]. 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 [98], where satellite communication 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 Fig. 4:

- *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 (GrounSys):* Manage secure communication channels between ground stations and the satellites.

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 10, 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 Signal 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

Table 10
CSF subcategories and their applicability to SecureSat.

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 assets and 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 continuity	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

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) [97], 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.

8.1. Cost-effectiveness of the metrics in the SecureSat case study

In line with the criteria defined in Section 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 interdependence 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 standards 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 firewall, 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 [99]. 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. Vulnerability 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 [26], 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.

9. Conclusions

Our research 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.

CRediT authorship contribution statement

Francesco Casaril: Writing – review & editing, Writing – original draft, Methodology, Investigation, Conceptualization. **Letterio Galletta:** Writing – review & editing, Writing – original draft, Supervision, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

We thank the anonymous reviewers for their careful and helpful comments and suggestions. This work was supported by the project "*SEcurity and RIghts in the CyberSpace*" (SERICS), PE0000014, funded by the European Union - NextGenerationEU under the National Recovery and Resilience Plan M4C2 I1.3., CUP: D67G22000340001.

Data availability

No data was used for the research described in the article.

References

[1] E. Chew, M. Swanson, K. Stine, N. Bartol, A. Brown, W. Robinson, Performance Measurement Guide for Information Security, Technical Report, National Institute of Standards and Technology, Gaithersburg, MD, 2008, URL: https://www.nist.gov/document-13265, U.S. Department of Commerce.

[2] D.S. Herrmann, Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI, Auerbach Publications, 2007.

[3] W. Jansen, Directions in Security Metrics Research, Diane Publishing, 2010.

[4] 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, 2024, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=pi_com%3AC%282024%297151. (Accessed 17 October 2024).

[5] F. Casaril, L. Galletta, Developing security metrics for space systems: A study considering the NIST cybersecurity framework 2.0 and the NIS2 (Online supplementary material), 2025, https://sites.google.com/view/spacemetrics/homepage.

[6] J. Pavur, Securing New Space: On Satellite Cyber-Security (Ph.D. thesis), University of Oxford, 2021.

[7] G. Kavallieratos, S. Katsikas, An exploratory analysis of the last frontier: A systematic literature review of cybersecurity in space, Int. J. Crit. Infrastruct. Prot. (2023) 100640.

[8] F. Casaril, L. Galletta, Securing SatCom user segment: A study on cybersecurity challenges in view of IRIS, Comput. Secur. 140 (2024) 103799, http://dx.doi.org/10.1016/J.COSE.2024.103799.

[9] L. Yu, J. Hao, J. Ma, Y. Sun, Y. Zhao, B. Luo, 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, ACM, New York, NY, USA, 2024, pp. 1–15, http://dx.doi.org/10.1145/3658644.3670390.

[10] T. Harrison, K. Johnson, T.G. Roberts, Space Threat Assessment 2019, Center for Strategic & International Studies, 2019.

[11] F. Casaril, L. Galletta, Space cybersecurity governance: assessing policies and frameworks in view of the future European space legislation, J. Cybersecur. 11 (1) (2025) http://dx.doi.org/10.1093/CYBSEC/TYAF013.

[12] E.U.A. for Cybersecurity (ENISA), Cybersecurity for SMEs - Challenges and Recommendations, Technical Report, European Union Agency for Cybersecurity, 2021.

[13] A. Tortorelli, A. Fiaschetti, A. Giuseppi, V. Suraci, R. Germanà, F.D. Priscoli, A security metric for assessing the security level of critical infrastructures, Int. J. Crit. Comput.-Based Syst. 10 (1) (2020) 74–94.

[14] M. Fleming, E. Goldstein, Metrics for measuring the efficacy of critical-infrastructure-centric cybersecurity information sharing efforts, 2012, Available at SSRN 2201033.

[15] G. Gori, L. Rinieri, A. Melis, A. Al Sadi, F. Callegati, M. Prandini, A systematic analysis of security metrics for industrial cyber–physical systems, Electronics 13 (7) (2024) 1208.

[16] B. Krumay, E.W. Bernroider, R. 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.

[17] M. Parmar, A. 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.

[18] A. Dimakopoulou, K. Rantos, Comprehensive analysis of maritime cybersecurity landscape based on the NIST CSF v2. 0, J. Mar. Sci. Eng. 12 (6) (2024) 919.

[19] European Union Agency for Cybersecurity (ENISA), Minimum security measures for operators of essential services, 2024, URL: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/minimum-security-measures-for-operators-of-essentials-services. (Accessed 01 November 2024).

[20] G.W. Bush, Executive order on critical infrastructure protection, in: Proceedings of the 12th Annual Conference on Computers, Freedom and Privacy, 2002, pp. 1–10.

[21] S. AlDaajeh, H. Saleous, S. Alrabaee, E. Barka, F. Breitinger, K.-K.R. Choo, The role of national cybersecurity strategies on the improvement of cybersecurity education, Comput. Secur. 119 (2022) 102754.

[22] 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, 2022, pp. 164–198, URL: http://data.europa.eu/eli/dir/2022/2557/oj, OJ L 333, 27.12.2022.

[23] R. De Bruin, S.H. von Solms, Modelling cyber security governance maturity, in: 2015 IEEE International Symposium on Technology and Society, ISTAS, IEEE, 2015, pp. 1–8.

[24] Y. Maleh, A. Sahid, M. Belaissaoui, A maturity framework for cybersecurity governance in organizations, EDPACS 63 (6) (2021) 1–22.

[25] V. Anu, Information security governance metrics: a survey and taxonomy, Inf. Secur. J.: A Glob. Perspect. 31 (4) (2022) 466–478.

[26] W.K. Brotby, G. Hinson, Pragmatic Security Metrics: Applying Metametrics to Information Security, CRC Press, 2016.

[27] W. Sonnenreich, J. Albanese, B. Stout, Return on security investment (ROSI)-a practical quantitative model, J. Res. Pr. Inf. Technol. 38 (1) (2006) 45–56.

[28] A. Jaquith, Security Metrics, Pearson Education, 2007.

[29] R.B. Vaughn, R. Henning, A. 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, pp. 10–pp.

[30] A. Arabsorkhi, F. Ghaffari, Security metrics: principles and security assessment methods, in: 2018 9th International Symposium on Telecommunications, IST, IEEE, 2018, pp. 305–310.

[31] P. Mell, T. Bergeron, D. Henning, et al., Creating a patch and vulnerability management program, NIST Spec. Publ. 800 (2005) 40.

[32] M. Pendleton, R. Garcia-Lebron, S. Xu, A survey on security metrics, 2016, arXiv preprint arXiv:1601.05792.

[33] J. Pamula, S. Jajodia, P. Ammann, V. Swarup, 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.

[34] L. Wang, S. Jajodia, A. Singhal, P. Cheng, S. Noel, K-zero day safety: A network security metric for measuring the risk of unknown vulnerabilities, IEEE Trans. Dependable Secur. Comput. 11 (1) (2013) 30–44.

[35] D.J. Leversage, E.J. Byres, Estimating a system's mean time-to-compromise, IEEE Secur. Priv. 6 (1) (2008) 52–60.

[36] H. Zhang, F. Lou, Y. Fu, Z. Tian, 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.

[37] J.A. Fitch III, L.J. Hoffman, A shortest path network security model, Comput. Secur. 12 (2) (1993) 169–189.

[38] A. Schreiner, G. Balzer, A. Precht, C. Schorn, 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.

[39] A. Ramos, M. Lazar, R. Holanda Filho, J.J. Rodrigues, Model-based quantitative network security metrics: A survey, IEEE Commun. Surv. Tutor. 19 (4) (2017) 2704–2734.

[40] F.A. Almaqtari, N.H. Farhan, A.T. Yahya, B.O.A. Al-Dalaien, M. Shamim, The mediating effect of IT governance between corporate governance mechanisms, business continuity, and transparency & disclosure: An empirical study of Covid-19 Pandemic in Jordan, Inf. Secur. J.: A Glob. Perspect. 32 (1) (2023) 39–57.

[41] M. Weir, S. Aggarwal, M. Collins, H. Stern, 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.

[42] H. Langweg, Software Security Metrics for Malware Resilience (Ph.D. thesis), Universitäts-und Landesbibliothek Bonn, 2008.

[43] J. Ren, D.J. Dubois, D. Choffnes, A.M. Mandalari, R. Kolcun, H. Haddadi, Information exposure from consumer iot devices: A multidimensional, network-informed measurement approach, in: Proceedings of the Internet Measurement Conference, 2019, pp. 267–279.

[44] W. Boyer, M. 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.
[45] D.J. Bodeau, R.D. Graubart, R.M. McQuaid, J. Woodill, Cyber resiliency metrics, measures of effectiveness, and scoring, Enabling Syst. Eng. Program Manag. Sel. Most Useful. Assess. Methods (2018).
[46] H. Cavusoglu, HC and jun zhang, in: Economics of Security Patch Management. in Workshop on the Economics of Information Security, Cambridge, UK, 2006.
[47] E. Chew, A. Clay, J. Hash, N. Bartol, A. Brown, Guide for Developing Performance Metrics for Information Security, Technical Report, National Institute of Standards and Technology, 2006.
[48] L. Wang, A. Singhal, S. 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.
[49] L. Klosterboer, Implementing ITIL Configuration Management, Pearson Education, 2007.
[50] J. Heidemann, Y. Pradkin, R. Govindan, C. Papadopoulos, J. Bannister, Exploring Visible Internet Hosts Through Census and Survey, Technical Report ISI-TR-2007-640, USC/Information Sciences Institute, 2007.
[51] Y. Cheng, J. Deng, J. Li, S.A. DeLoach, A. Singhal, X. Ou, Metrics of security, Cyber Déf. Situat. Aware. (2014) 263–295.
[52] K. Hajdarevic, P. 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.
[53] A.P.F. de Araújo, P.F. von Paumgartten, A.C. 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.
[54] S.Y. Enoch, J.B. Hong, M. Ge, D.S. Kim, Composite metrics for network security analysis, 2020, arXiv preprint arXiv:2007.03486.
[55] P.K. Manadhata, J.M. Wing, An attack surface metric, IEEE Trans. Softw. Eng. 37 (3) (2010) 371–386.
[56] G. Gu, P. Fogla, D. Dagon, W. Lee, B. Skorić, 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.
[57] Z.A. Collier, M. Panwar, A.A. Ganin, A. Kott, I. Linkov, Security metrics in industrial control systems, Cyber-Security SCADA Other Ind. Control. Syst. (2016) 167–185.
[58] J.B. Hong, Scalable and adaptable security modelling and analysis., 2015.
[59] A. Roy, D.S. Kim, K.S. Trivedi, Attack countermeasure trees (ACT): towards unifying the constructs of attack and defense trees, Secur. Commun. Netw. 5 (8) (2012) 929–943.
[60] C. Strasburg, N. Stakhanova, S. Basu, J.S. Wong, 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.
[61] K. Scarfone, T. Grance, K. Masone, Computer security incident handling guide, NIST Spec. Publ. 800 (61) (2008) 38.
[62] V. Sritapan, W. Stewart, J. Zhu, C. Rohm Jr., Developing a metrics framework for the federal government in computer security incident response, Commun. IIMA 11 (3) (2011) 5.
[63] CIC Security Working Group, Incident Cost Analysis and Modeling Project, University of Michigan, 1998.
[64] FY 2024 CIO FISMA metrics, version 1.0, 2023, https://www.cisa.gov/sites/default/files/2023-12/FY24_FISMA_CIO_Metrics_v1.0_FINAL_1.pdf. (Accessed 29 September 2024).
[65] B. Aziz, A. Malik, J. 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.
[66] W. Wang, J. Chen, L. Yang, H. Zhang, Z. Wang, Understanding and predicting incident mitigation time, Inf. Softw. Technol. 155 (2023) 107119.
[67] M. Keramati, F.S. Halataei, Innovative Cyber-Security Metrics for Intrusion Prevention.
[68] A. Dorofee, G. Killcrece, R. Ruefle, M. Zajicek, Incident management capability metrics version 0.1, 2007, Retrieved 22 April 2009.
[69] S. Walker, Economics and the cyber challenge, Inf. Secur. Tech. Rep. 17 (1–2) (2012) 9–18.
[70] M.J. Page, J.E. McKenzie, P.M. Bossuyt, I. Boutron, T.C. Hoffmann, C.D. Mulrow, L. Shamseer, J.M. Tetzlaff, E.A. Akl, S.E. Brennan, et al., The PRISMA 2020 statement: an updated guideline for reporting systematic reviews, Bmj 372 (2021).
[71] CIS controls measures and metrics for version 7, 2018, https://www.uio.no/studier/emner/matnat/ifi/IN2120/h18/docs/cis-controls-measures-and-metrics-v7.pdf. (Accessed 29 September 2024).
[72] P. Trimintzios, Measurement frameworks and metrics for resilient networks and services: technical report, Eur. Netw. Inf. Secur. Agency 109 (2011).
[73] ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation, 2016, Available at: https://www.iso.org/standard/64120.html.
[74] K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, S. Lightman, A. Hahn, S. Saravia, A. Sherule, M. Thompson, Guide to Operational Technology (OT) Security, Technical Report NIST SP 800-82 Rev.3, National Institute of Standards and Technology, 2023, http://dx.doi.org/10.6028/NIST.SP.800-82r3.
[75] L. Vessels, K. Heffner, D. Johnson, Cybersecurity risk assessment for space systems, in: 2019 IEEE Space Computing Conference, SCC, IEEE, 2019, pp. 11–19.
[76] European Cooperation for Space Standardization, ECSS-E-ST-80C: Space engineering – Security in space systems lifecycles, 2024, https://ecss.nl/standard/ecss-e-st-80c-space-engineering-security-in-space-systems-lifecycles/.
[77] European Cooperation for Space Standardization, ECSS-Q-ST-80C Rev.2: Software product assurance, 2025, https://ecss.nl/standard/ecss-q-st-80c-rev-2-software-product-assurance-30-april-2025/.
[78] European Cooperation for Space Standardization, ECSS-E-ST-40C Rev.1: Space engineering – Software general requirements, 2025, ESA-ESTEC, Noordwijk, URL: https://ecss.nl/standard/ecss-e-st-40c-rev-1-space-engineering-software-general-requirements/, engineering processes, verification, validation, and secure delivery requirements.
[79] S.Y. Enoch, M. Ge, J.B. Hong, H. Alzaid, D.S. Kim, A systematic evaluation of cybersecurity metrics for dynamic networks, Comput. Netw. 144 (2018) 216–229.
[80] National Institute of Standards and Technology, Guide for Cybersecurity Event Recovery, Technical Report NIST SP 800-184, National Institute of Standards and Technology, Gaithersburg, MD, 2016, URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf. (Accessed 07 June 2025).
[81] European Union Agency for Cybersecurity (ENISA), Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity, Technical Report, ENISA, Heraklion, Greece, 2017, URL: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity. (Accessed 07 June 2025).
[82] Cyber Risk Institute, Profile V2 Guidebook, Technical Report, Cyber Risk Institute, 2024, URL: https://cyberriskinstitute.org/wp-content/uploads/2024/04/Final-CRI-Profile-v2-Guidebook-Public-2024-04-03.pdf. (Accessed 07 June 2025).
[83] A. Modi, I. Kuzminykh, B. Ghita, Data driven approaches to cybersecurity governance for board decision-making–A systematic review, 2023, arXiv preprint arXiv:2311.17578.
[84] National Institute of Standards and Technology, Security and Privacy Controls for Information Systems and Organizations, NIST Special Pub-lication 800-53 Revision 5 Update 1, U.S. Department of Commerce, National Institute of Standards and Technology, 2024, Final version. URL: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.
[85] B. Al-Sada, A. Sadighian, G. Oligeri, Mitre att&ck: State of the art and way forward, ACM Comput. Surv. 57 (1) (2024) 1–37.
[86] S. Pace, et al., The Global Positioning System: Assessing National Policies, Rand Corporation, 1995.
[87] 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.
[88] 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.
[89] A.B. Gladyshev, A.N. Fomin, D.S. Ermolenko, S.V. Serebrinnikov, Electronic jamming of the system of subscriber terminals of the starlink satellite communication system, J. Sib. Fed. Univ. Eng. Technol. 16 (7) (2023) 789–796.
[90] J.M.P. Armengol, B. Furch, C.J. de Matos, O. Minster, L. Cacciapuoti, M. Pfennigbauer, M. Aspelmeyer, T. Jennewein, R. Ursin, T. Schmitt-Manderbach, et al., Quantum communications at ESA: Towards a space experiment on the ISS, Acta Astronaut. 63 (1–4) (2008) 165–178.
[91] Significant security deficiencies in noaa's information systems create risks in its national critical mission, 2014, Final Report No. OIG-14-025-A, U.S. Department of Commerce, Office of Inspector General, Office of Audit and Evaluation. https://www.oig.doc.gov/OIGPublications/OIG-14-025-A.pdf. (Accessed 29 September 2024).
[92] P.K. Kallender, Waking up to a new threat: Cyber threats and space, Trans. Jpn. Soc. Aeronaut. Space Sci. Aerosp. Technol. Jpn. 12 (ists29) (2014) Tv_1–Tv_10.
[93] S. Mirzaei, D. 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.
[94] Y. Zhan, P. Wan, C. Jiang, X. Pan, X. Chen, S. Guo, Challenges and solutions for the satellite tracking, telemetry, and command system, IEEE Wirel. Commun. 27 (6) (2021) 12–18.
[95] M. Swope, J. Watling, C.S. Dankwa, et al., Space threat assessment 2025, 2025, URL: https://www.csis.org/analysis/space-threat-assessment-2025.

[96] M. Felux, P. Fol, B. Figuet, M. Waltert, X. Olive, Impacts of global navigation satellite system jamming on aviation, NAVIGATION: J. Inst. Navig. 71 (3) (2024).
[97] J. McCarthy, J. McCarthy, D. Mamula, J. Brule, K. Meldorf, R. Jennings, J. Wiltberger, C. Thorpe, J. Dombrowski, O. Lattin, et al., Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN), US Department of Commerce, National Institute of Standards and Technology, 2023.
[98] N. Boschetti, N.G. Gordon, G. Falco, Space cybersecurity lessons learned from the viasat cyberattack, in: ASCEND 2022, 2022, p. 4380.
[99] Forrester Consulting, The Total Economic Impact™ of Cisco Duo: Cost Savings and Business Benefits Enabled by Duo, Technical Report, Forrester Consulting, 2023, Commissioned by Cisco. URL: https://resources.duo.com/explore/assets/the-tei-of-cisco-duo-2.