



This activity is carried out with the support of the European Space Agency (ESA) under the ARTES 4S programme. The views expressed in this publication can in no way be taken to reflect the official opinion of the European Space Agency.

Cybersecurity MAKERSPACE Impacts of new cyber regulations on SATCOM ecosystem

White Paper



Table of Content

I. MISSION'S CONTEXT AND SCOPE	3
A. CYBERSECURITY CHALLENGES	4
B. PROLIFERATION AND LACK OF HARMONIZATION OF STANDARDS	4
C. RISING GEOPOLITICAL TENSIONS AND DUAL-USE OF SATCOM INFRASTRUCTURE	5
II. MISSION KEY TAKEAWAYS	6
A. CYBERSECURITY FRAMEWORKS APPLICABLE TO SATCOM OVERVIEW	6
B. MOST SATCOM-OPERATIONAL FRAMEWORKS' MAIN STRENGTHS, CHALLENGES, AND ONGOING EFFORTS	9
1. MAIN STRENGTHS OF THE MOST SATCOM-OPERATIONAL FRAMEWORKS	9
2. ONGOING EFFORTS MADE BY POLICYMAKERS	10
3. MAIN CHALLENGES FACED BY POLICYMAKERS	10
C. LESSONS LEARNT AND TAKEAWAYS FROM OTHER VERTICALS	12
D. GEOGRAPHICAL FOCUS TAKEAWAYS	13
E. FRAMEWORKS ROADMAP ENABLERS	14
F. OVERALL KEY TAKEAWAYS OF THE MISSION	15
1. MAIN TAKEAWAYS REGARDING POLICYMAKERS	15
2. MAIN TAKEAWAYS REGARDING THE INDUSTRY	20
3. MAIN RECOMMENDATIONS FOR EU AND NATIONAL POLICYMAKERS	21

Table of Figures

Figure 1: Factsheet regarding the mission	3
Figure 2: Number of cybersecurity frameworks published or in progress by country and region of origin	6
Figure 3: Key figures of the mission	7
Figure 4: Key enablers for framework adoption	15

Table of Tables

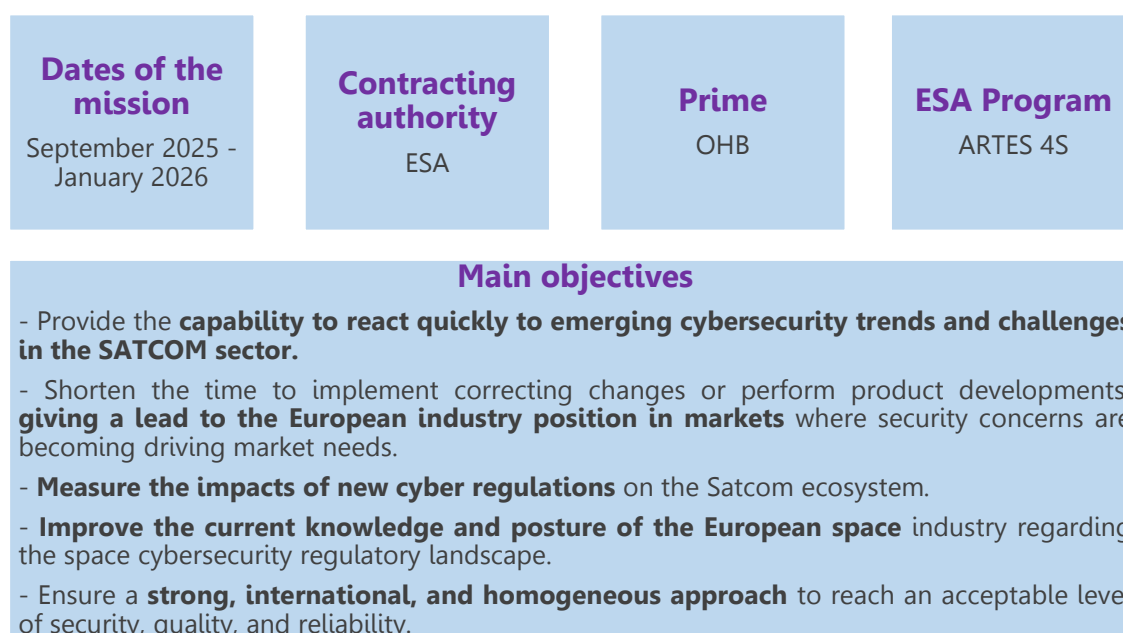
Table 1: Abbreviations table	2
Table 2: Most relevant cybersecurity frameworks applicable to SATCOM	7
Table 3: Most relevant Geographical Focus cybersecurity frameworks applicable to SATCOM	13
Table 4: Table of references	25

Table 1: Abbreviations table

ARTES 4S	Advanced Research in Telecommunications Systems (ARTES) Space Systems for Safety and Security (4S)
AFR	Africa
AI	Artificial Intelligence
APAC	Asia-Pacific
BSI	Bundesamt für Sicherheit in der Informationstechnik (German Federal Office for Information Security)
CNES	Centre National d'Études Spatiales (French Space Agency)
COMSATCOM	Commercial Satellite Communications
CNSS	Committee on National Security Systems (U.S.)
CIS	Commonwealth of Independent States
CCSDS	Consultative Committee for Space Data Systems
CER	Critical Entities Resilience
CRA	Critical Resilience Act
CMMC v2	Cybersecurity Maturity Model Certification v2
CAC	Cyberspace Administration of China
DLR	Deutsches Zentrum für Luft- und Raumfahrt (German Aerospace Center)
EUSA	EU Space Act
EU	Europe
ECSS	European Cooperation for Space Standardization
ESA	European Space Agency
ENISA	European Union Agency for Cybersecurity
GF	'Geographical Focus' (<i>CyberInflight terminology, in the context of this study</i>)
GOVSATCOM	Governmental Satellite Communications
IEEE	Institute of Electrical and Electronics Engineers
ISR	Intelligence, surveillance, and reconnaissance
ISO	International Standard Organization
JAXA	Japan Aerospace Exploration Agency
MILSATCOM	Military Satellite Communications
METI	Ministry of Economy, Trade and Industry (Japan)
MBSE	Model-Based Systems Engineering
NASA	National Aeronautics and Space Administration (U.S.)
NCSC	National Cyber Security Center (South Korea)
NIST	National Institute of Standards and Technology (U.S.)

NIS2	Network and Information Security 2
NA	North America
PSARB	Pakistan Space Activities Regulatory Board
PQC	Post-quantum Cryptography
SATCOM	Satellite Communications
SME	Small and Medium-sized Enterprise
SPACE-SHIELD	Space Attacks and Countermeasures Engineering Shield
SPARTA	Space Attack Research and Tactic Analysis
SPD-5	Space Policy Directive 5 (U.S.)
UKSA	UK Space Agency
WRG	German Space Act

Figure 1: Factsheet regarding the mission



I. MISSION'S CONTEXT AND SCOPE

SATCOM (SATellite COMmunications) corresponds to missions involving satellites that provide beyond-line-of-sight communications and networking services (including data relay and amplification of data, messaging, video, and voice signals) to and from various points on and around Earth. **The SATCOM ecosystem has grown considerably since the late 1990s and early 2000s** and corresponds to a structured network of actors, technologies, infrastructures, standards, and services involved in designing, operating, and using SATCOM. It encompasses satellites (in geostationary, medium, or low earth orbits), ground stations, user terminals, interconnection networks, and communication protocols. It covers a **wide range of actors, including operators, manufacturers, service providers, civilian and military institutions, and regulatory authorities**. SATCOM encompasses various operations and concepts to fulfill a mission. For example, some of the main concepts related to the SATCOM ecosystem are **COMSATCOM** (i.e., SATCOM capacity and service provided on the global open market, for commercial purposes, generally with a degree of 'on-demand' access), **GOVSATCOM** (i.e., communication services specifically tailored to meet the needs of governmental entities), and **MILSATCOM** (i.e., highly protected and guaranteed SATCOM, generally provided by military systems). **Security requirements can differ between those concepts**, depending on their

needs and means. For example, GOVSATCOM and MILSATCOM usually have more stringent security requirements than COMSATCOM.

Overall, today, SATCOM has become crucial across several areas, such as military communications and intelligence, surveillance, and reconnaissance (ISR). Countries or regions with advanced satellite capabilities can leverage SATCOM for **defense and deterrence, making it a strategic target for attackers**. Nations that influence satellite infrastructure can also gain economic leverage, shaping global trade, internet access, and digital sovereignty. States worldwide are increasingly willing to **reinforce their strategic autonomy and industrial positioning when accessing or developing SATCOM, notably through programs such as IRIS² in Europe**. Moreover, such programs are a strategic tool of soft power that can enhance geopolitical influence.

As it grows, the SATCOM ecosystem faces an increasing array of challenges.

A. CYBERSECURITY CHALLENGES

First, cybersecurity challenges are becoming increasingly pressing as the number of threats against which the SATCOM ecosystem must protect itself grows. The SATCOM infrastructure faces cybersecurity gaps due to inadequate or poor security standards for satellite systems, making it vulnerable to cyberattacks and a high-value target for state and non-state actors. Recently, significant regulatory efforts have been made to develop a number of frameworks, though there is **not yet a global, common, and efficient approach to regulating the cybersecurity of SATCOM systems**. The SATCOM ecosystem remains fragmented and needs a strong, global, and homogeneous approach to ensure an acceptable level of security, quality, and reliability.

B. PROLIFERATION AND LACK OF HARMONIZATION OF STANDARDS

European SATCOM stakeholders and policymakers are witnessing the **development and influence, in particular from the United States, of a set of institutional initiatives that lay the groundwork** for future regulatory work (such as NIST profiles, SPARTA, and other directives emerging from the SPD-5 directive). Influencing or controlling cybersecurity frameworks can help nations or players gain a lead in global governance, technology, and security, demonstrating a strong commitment to sovereignty. Moreover, with several cyber frameworks applicable or relevant to the SATCOM ecosystem, nation-states that actively influence or control them indirectly influence the SATCOM ecosystem and market. Many States, for instance, aim to come out on top in the cybersecurity frameworks competition, resulting in a **proliferation of frameworks and a perceived disparity** that makes it harder for the SATCOM ecosystem to navigate them. This **lack of harmonization in standards** is often criticized, as it can complicate interoperability among players and hinder international cooperation, slowing innovation and limiting the number and reach of projects.

Europe, with a strong history and experience in information security and space, seems to be **moving toward more specific and oriented guidance for space stakeholders**. However, these efforts remain misunderstood or unknown in the field of SATCOM, and a greater understanding of cybersecurity frameworks in the SATCOM domain is needed.

C. RISING GEOPOLITICAL TENSIONS AND DUAL-USE OF SATCOM INFRASTRUCTURE

The SATCOM infrastructure, critical and strategic to sovereignty and autonomy, is inherently subject to geopolitical tensions, with players sometimes facing restrictions on market access and limits on technology transfer.

Moreover, **SATCOM services and infrastructure are often dual-use by nature** (i.e., applicable to both civilian and military users), as they are used for civilian (e.g., internet or navigation) and military (e.g., ISR, military communications, missile guidance) purposes. Following the same logic, many dual-use applications are covered by the current cybersecurity SATCOM-related frameworks, which can add complexity and **blur the line between civilian and military targets**. Indeed, even if a satellite is commercially owned, its integration into military command systems or its direct support of combat operations can make it a lawful target for enemy attacks, according to international legal frameworks such as the Geneva Conventions of 1949 or the Hague Conventions of 1899 and 1907, provided the attack complies with principles of distinction and proportionality.

Moreover, depending on the sensitivity of the information exchanged, cybersecurity standards for the SATCOM infrastructure may differ. However, because cybersecurity standards are often theoretically applicable to civil and military projects, there is a **risk of inadequate standards that result in security that does not meet actual needs**.

Cybersecurity MAKERSPACE, therefore, aims to support several objectives:

- Provide the **capability to react quickly to emerging cybersecurity trends and challenges in the SATCOM sector**.
- Shorten the time to implement correcting changes or perform product developments, **giving a lead to the European industry position in markets** where security concerns are becoming driving market needs.
- **Measure the impacts of new cyber regulations** on the Satcom ecosystem.
- **Improve the current knowledge and posture of the European space industry** regarding the space cybersecurity regulatory landscape.
- Ensure a **strong, international, and homogeneous approach** to reach an acceptable level of security, quality, and reliability.

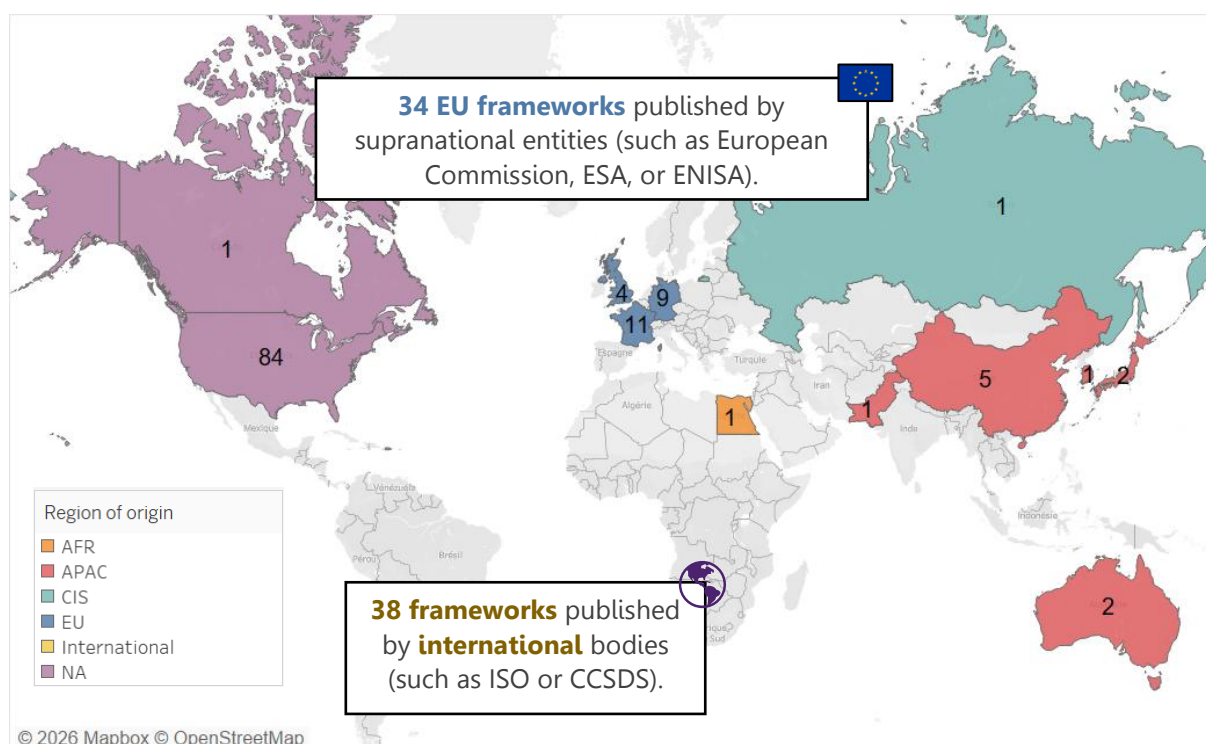
II. MISSION KEY TAKEAWAYS

A. CYBERSECURITY FRAMEWORKS APPLICABLE TO SATCOM OVERVIEW

*For this mission, a framework is defined as any cybersecurity-related document, such as Regulations, Law, Act, Directive, Standard, and Guide, that can be centered around requirements or best practices. Based on those cybersecurity generic frameworks, the study enabled a **deeper analysis of those impacting the space domain as a whole or the SATCOM domain specifically.***

194 cybersecurity frameworks issued by **72 different framework issuers worldwide** have been identified for this mission. **11 issuers stand out as the most active (NIST, NASA, CCSDS, U.S. Government, European Commission, BSI / DLR, and ECSS).** Moreover, a strong **American influence in the most relevant frameworks for the SATCOM ecosystem**, especially with the NIST as the most active framework issuer by far, can be observed. A shortlist of the main frameworks identified is included below (Tables 2 and 3).

Figure 2: Number of cybersecurity frameworks published or in progress by country and region of origin



Reading grid: For each relevant country, the number of frameworks published or in progress is displayed. If a framework is issued or to be issued by a supranational or international body, it is not included in the numbers on the map and is therefore included in the added text boxes.

Figure 3: Key figures of the mission

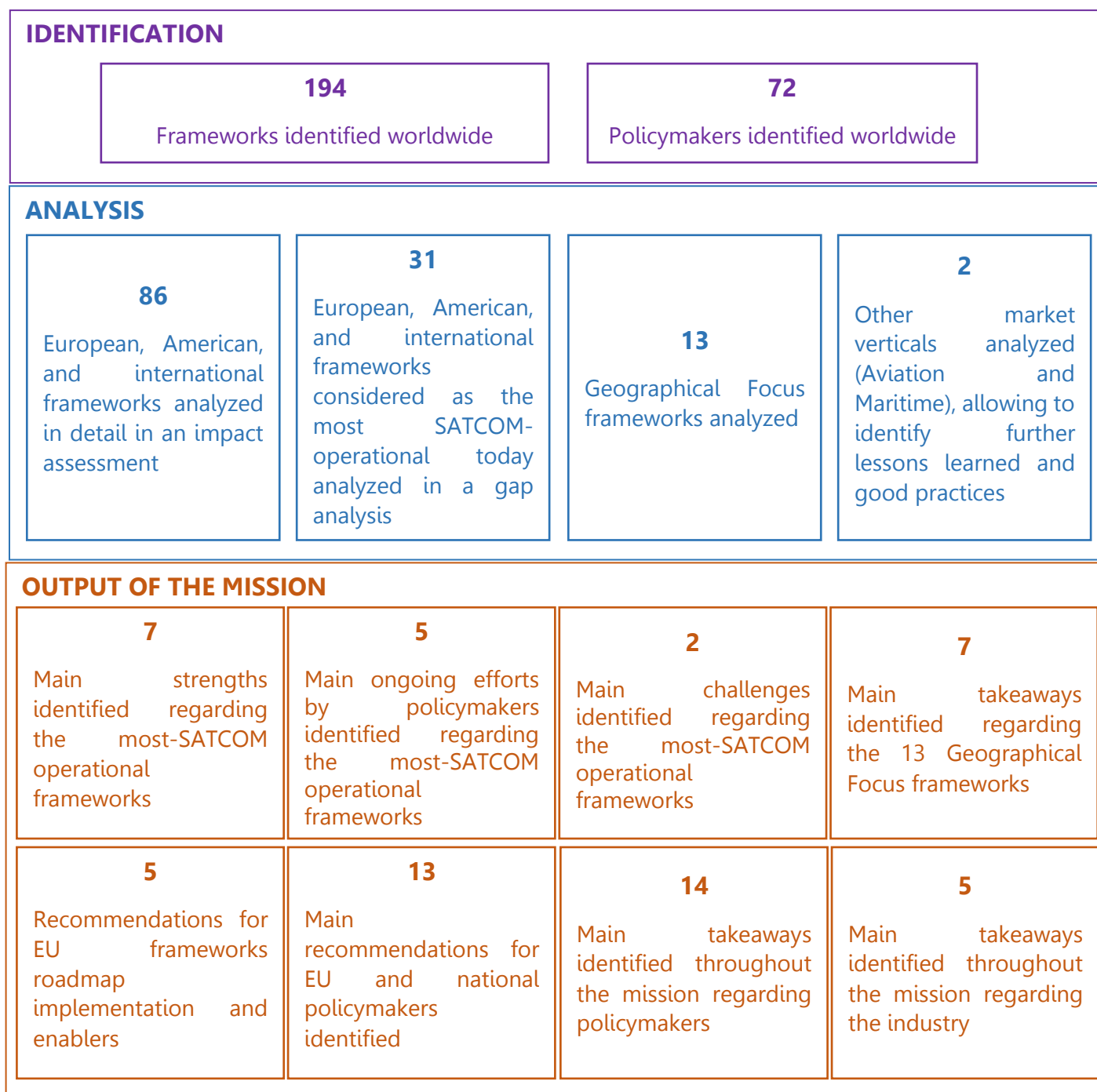


Table 2: Most relevant cybersecurity frameworks applicable to SATCOM

(Non-exhaustive list as of March 2026, alphabetical order excluding Geographical Focus)

Framework Issuer	Framework Title	Release date	Country of origin	Region of origin
Aerospace Corporation	SPARTA Framework	2022	US	NA
BSI	IT-Grundschutz Profile for Space Systems - Part 2: Ground segment – minimum protection over the entire life cycle	2024	Germany	EU

Framework Issuer	Framework Title	Release date	Country of origin	Region of origin
BSI (DLR)	IT-Grundschutz Profile for Space Infrastructures – Minimum Protection for Satellites Covering their Entire Life Cycle	2022	Germany	EU
BSI (DLR)	Technical Guideline BSI TR-03184 Information Security for Space Systems Part 1	2023	Germany	EU
BSI (DLR)	Technical Guideline BSI TR-03184 Information Security for Space Systems Part 2	2025	Germany	EU
CCSDS	CCSDS 355.0-B-2 Space Data Link Security Protocol	2021	International	International
CCSDS	CCSDS 350.5-G-2 – SPACE DATA LINK SECURITY PROTOCOL—EXTENDED PROCEDURES—SUMMARY OF CONCEPT AND RATIONALE	2024	International	International
CCSDS	CCSDS 355.1-B-1 – SPACE DATA LINK SECURITY PROTOCOL — EXTENDED PROCEDURES	2020	International	International
CMMC v2	Cybersecurity Maturity Model version 2	2019	US	NA
CNES	Orbital System Cybersecurity Hygiene Guide (Guide d'Hygiène Cybersécurité des Systèmes Orbitaux)	2025	France	EU
CNSS (and NASA)	CNSSP-12	2007	US	NA
ECSS	ECSS-E-ST-80C: Space engineering – Security in space systems lifecycles	2024		EU
ECSS	ECSS-Q-ST-80C Software Product Assurance	2024		EU
ESA	Space Attacks and Countermeasures Engineering Shield (SPACE-SHIELD)	2023		EU
ESA	SSE4SPACE	To be released		EU
European Commission	NIS 2 measures for a high common level of cybersecurity across the Union	2023		EU
European Commission	EU Space Act	To be released		EU
European Commission	EU Space Strategy for Security and Defence	2022		EU
French Government	“Arrêté du 8 septembre 2017” (Decree establishing security rules and reporting procedures for critical information systems and security incidents relating to the critical sub-sector of “Space” activities)	2017	France	EU
German Government	“Eckpunkte der Bundesregierung für ein Weltraumgesetz (WRG)” (Key Issues Paper for a Future German Space Act - For a stronger space industry)	To be released	Germany	EU
IEEE	Minimum Requirements for Space System Cybersecurity - Ensuring Cyber Access to Space	2024	International	International
ISO sub committee 14	ISO/TS 20517:2024 Space systems - Cybersecurity management requirements and recommendations	2024	International	International
ISO sub committee 14	ISO14300-1 “Structuring a project”	2011	International	International
ISO sub committee 14	ISO14300-2 “Product Assurance”	2011	International	International
ISO sub committee 14	ISO10795 “Vocabulary”	2019	International	International
ISO sub committee 14	ISO17666 “Risk management”	2025	International	International
ISO sub committee 14	ISO 18676:2024 “Requirements and guidelines for the management of systems engineering”	2024	International	International
NASA	Space Security Best Practices Guide BPG REV B	2024	US	NA
NIST	NISTIR 8441: Cybersecurity Framework Profile for Hybrid Satellite Networks	2023	US	NA
NIST	NISTIR 8270: Introduction to Cybersecurity for Commercial Satellite Operations	2023	US	NA
NIST	NISTIR 8401: Satellite Ground Segment: Applying the Cybersecurity Framework to Satellite Command and Control	2022	US	NA
NIST	Cybersecurity Framework (CSF) v.2.0	2024	US	NA
U.S. GOV	Space Policy Directive 5	2020	US	NA

Framework Issuer	Framework Title	Release date	Country of origin	Region of origin
UKSA	Cybersecurity Toolkit Ver. 2	2020	UK	EU
UKSA	National Space Strategy	2019	UK	EU

B. MOST SATCOM-OPERATIONAL FRAMEWORKS' MAIN STRENGTHS, CHALLENGES, AND ONGOING EFFORTS

86 cybersecurity European, American, and international frameworks were analyzed in detail, as part of an impact assessment. Based on this impact assessment, 31 cybersecurity frameworks were selected as the most SATCOM-operational and relevant to SATCOM today. For those 31 frameworks, a gap analysis was conducted, **identifying several strengths, ongoing efforts by policymakers, and challenges in the most SATCOM-operational frameworks.**

1. MAIN STRENGTHS OF THE MOST SATCOM-OPERATIONAL FRAMEWORKS

Overall, one of the main strengths of the most SATCOM-operational frameworks is their **applicability and actionability** for SATCOM stakeholders.

*APPLICABLE CASE: A growing number of frameworks aim to allow users to **tailor them to a specific context, based on the actual SATCOM players' needs and operational constraints.** The EU Space Act, for instance, leverages the concept of proportionality, while BSI and NIST aim to develop mission-oriented, actionable "profile" frameworks that can be adapted to each mission's security needs.*

Most SATCOM-operational frameworks are **mainly published by framework issuers widely recognized as legitimate**, which allows them to be generally accepted by the industry.

*APPLICABLE CASE: Several institutions such as **NIST, in the U.S., or ENISA in Europe are seen as a reference** for cybersecurity frameworks.*

Moreover, most SATCOM-operational frameworks **are overall collaborative and open to feedback**, demonstrating a **willingness to incorporate the space industry into the policy and regulatory landscape.**

*APPLICABLE CASE: The **CNES Hygiene Guides and the EUSA are collaborative and open to feedback from the industry.***

The maturity of the most SATCOM-operational frameworks is also a strength, as they are **sufficiently mature to be widely used across the SATCOM ecosystem.**

*APPLICABLE CASE: **NIST frameworks are overall mature enough** to be used by the SATCOM ecosystem, as NISTIR 8441, NISTIR 8270, and NISTIR 8401, for instance, were published in 2022 and 2023, allowing the ecosystem access to final versions of the documents.*

2. ONGOING EFFORTS MADE BY POLICYMAKERS

5 principal ongoing efforts by policymakers were identified.

First, to avoid overlaps with other frameworks, a **strong emphasis is placed on clearly defining each framework's scope**. This shows **policymakers' willingness to enable a clear understanding of the framework's approach and objectives**.

*APPLICABLE CASE: This is an essential ongoing effort by policymakers, notably in **Europe with NIS2 and EUSA**, as they recognize that the SATCOM ecosystem needs to understand the overall framework's approach and objectives to adopt it.*

Moreover, overall, the most SATCOM-operational frameworks **aim to leverage existing best practices**, notably risk management methodologies, **thereby complementing the current and in-progress frameworks landscape and serving as harmonization initiatives**.

*APPLICABLE CASE: This is an ongoing work for **SSE4SPACE**, as **ESA aims to facilitate interoperability between frameworks** and improve the operational aspects of implementing and maintaining them. **SSE4SPACE notably aims to provide a coherent, comprehensive, and end-to-end approach to security**.*

An **emphasis is also placed on clearly defining the authorities responsible for enforcing the framework**, especially when it is binding by law (issued by a competent authority and whose application directly produces legal effects, thereby legally binding on the parties concerned, even without their explicit consent). Policymakers are indeed mostly aware of the importance of clearly defined roles and responsibilities for the SATCOM ecosystem to have a clear, holistic vision of the frameworks landscape.

Another trend is that most SATCOM-operational frameworks **have also recently begun to consider geopolitical-related topics**. This factor is expected to gain increasing emphasis, reflecting a growing desire for greater sovereignty and resilience in the space domain.

Prospective and future technological trends are also increasingly emphasized in the regulatory landscape (such as Artificial Intelligence and quantum and post-quantum cryptography), as policymakers seek to anticipate trends and be proactive rather than reactive. Overall, the frameworks' issuers tend to develop frameworks that can **structure concepts over time, anticipate technological and organizational changes, and maintain their relevance in constantly evolving contexts**. This is the case with **NIS2**, for instance, which addresses Artificial Intelligence.

3. MAIN CHALLENGES FACED BY POLICYMAKERS

Policymakers face 2 primary challenges.

First, it is to find the **right balance and trade-off between the need for industry competitiveness and the costs of implementing a framework**. Indeed, **those factors can often be overlooked**. The implementation cost of a framework (including human, time, and financial resources) should be considered to ease its adoption by a SATCOM player. Adopting a framework should include estimating effort, costs, and other factors that could directly impact the company's decisions.

A few frameworks, such as the EU Space Act draft, are considering the impact and cost aspects, but these considerations remain limited. Implementing frameworks can entail both costs and benefits, and understanding these factors can help facilitate their adoption. Moreover, indicators such as ease of implementation and ease of handling the framework are often overlooked. To simplify the adoption process, the framework **should also provide relevant guidance (based on technical guides, toolbox, etc.) to improve the overall understandability**. It is the BSI's willingness, for instance, as highlighted by the releases of the IT-Grundschutz technical guidelines. Finding an **equilibrium between guidance and a clear, concise methodology** is also necessary for the SATCOM industry to better understand the approach to a framework and be willing and able to use it.

Reducing the implementation cost and keeping in mind the need for competitiveness of the industry also go hand in hand with the **ability for a framework to tackle the specific needs of a space mission, notably through a Risk Analysis approach and security adapted to the right need**, as emphasized in frameworks such as BSI's IT-Grundschutz, or CNES' Cybersecurity Hygiene Guide.

Overall, **policymakers today strongly emphasize approaches to bring greater understandability, adaptability, and guidance for the ecosystem**. This suggests a growing **willingness to increasingly take industry's competitiveness into account** and to foster a more dynamic, stable, high-trust, technologically advanced, and globally competitive ecosystem, notably by addressing the needs for security, autonomy, sovereignty, and resilience among SATCOM players and missions.

*APPLICABLE CASE: EUSA is based on an implementation cost study and aims to **strengthen the industry**, notably through concepts of **proportionality** (therefore reducing implementation costs).*

Moreover, **maintaining frameworks represents another challenge, since revisions and updates of SATCOM operational frameworks are often complex**. Indeed, maintaining a framework over time requires a structured and continuous process to ensure that existing frameworks evolve in line with changes in the ecosystem, emerging threats, and technological advancements. This can be hindered by short or medium-term objectives that sometimes conflict with the long-term need for resilience. **Therefore, maintaining cybersecurity frameworks may sometimes be seen as an overlooked priority**. More broadly, the challenge can be attributed to several factors, including the lack of long-term strategic leadership, constraints in terms of time and human resources, instability in development roadmaps, and the accelerating pace of technological and market evolution.

The complexity of maintaining a framework is also true within an organization that can dedicate the necessary resources to its implementation but struggles to sustain them over time. **A framework must consider the human dimension of its maintainability within an organization**. Its readability, adaptability to different user profiles, alignment with evolving working models, and facilitation of knowledge transfer are critical determinants of its long-term adoption and longevity.

A causal link can be observed between those 2 challenges: **a lack, for policymakers, to maintain the frameworks leads to a lack of ability to retain the frameworks at the organizational level.** Indeed, frameworks built and maintained over time avoid becoming outdated as the industry's needs and constraints constantly evolve. Thus, these frameworks can continue to be adopted across the ecosystem, as they remain relevant and responsive to the industry's evolving operational and governance needs. Over time, well-maintained frameworks tend to become shared points of reference, reducing the costs associated with replacing obsolete frameworks, facilitating knowledge transfer, supporting organizational maturity, and ultimately contributing to long-term value creation and governance stability.

*APPLICABLE CASE: **Aerospace Corporation plans to provide regular updates to the SPARTA framework** (every 4 months on average), which is already at version v3.1 (first publication in 2022).*

C. LESSONS LEARNT AND TAKEAWAYS FROM OTHER VERTICALS

Other market verticals (notably Aviation and Maritime) have been analyzed as part of this mission, and lessons can be learned from those, notably that concerns about the framework's landscape maturity exist across various verticals.

On the **aviation market**, one can observe maturity and awareness efforts over the past few years, notably thanks to several institutions that have been working on the **consolidation of a fragmented regulatory landscape**. Indeed, the **aviation ecosystem is ruled by a framework's arsenal** that is moving toward a more consistent approach regarding cybersecurity. International bodies, such as ICAO and IATA, have begun developing a global cybersecurity strategy in the early 2020s to guide national and local initiatives. In 2025, the aviation ecosystem has strengthened its cybersecurity by adopting the European Part-IS regulation, which establishes a unified framework for risk management, security integration from the design phase, and enhanced collaboration among airlines, airports, manufacturers, and authorities. Despite the ongoing efforts, the regulatory landscape **remains fragmented, and similar stakes and challenges to those in the space sector** can be observed, including the rise of cyberattacks, a larger attack surface, and an evolving threat landscape. **Fears of overlapping frameworks are also observed between Part-IS, the NIS2 directive, the Cyber Resilience Act (CRA)**, and other national and international standards, sometimes making compliance activities more complex for industry players.

Regarding the **maritime market**, it is considered more mature than other verticals in **adopting cyber frameworks**. The 1st cybersecurity-related guidance for ports and operators was published in 2017. Today, the maritime ecosystem has reached a **relatively high level of maturity and may be less targeted by APT groups than the space industry**. Moreover, ENISA has strongly supported the maritime industry through various publications and the management of the EU Maritime ISAC. Therefore, the maritime ecosystem appears ahead of the aviation and space ecosystems in adopting cybersecurity frameworks. However, similar challenges to those observed in Space or Aviation exist, such as limited budget, support, and resources.

Overall, **the space regulatory landscape is considered a bit less mature than in Aviation and Maritime**, as the initial phase of consolidation is still underway, with a growing number

of frameworks being issued, and the need for consistency and to limit overlaps between frameworks.

D. GEOGRAPHICAL FOCUS TAKEAWAYS

Of the 194 frameworks identified, **13 have been published by policymakers who have only recently begun to position themselves on the development of space or security frameworks** (therefore mostly coming from the Asia-Pacific or African regions). These frameworks are referred to in this study as "Geographical Focus (GF)" and are presented below.

Table 3: Most relevant Geographical Focus cybersecurity frameworks applicable to SATCOM

(Non-exhaustive list as of March 2026, alphabetical order)

Framework Issuer	Framework Title	Release date	Country of origin	Region of origin
Chinese Ministry of National Defense	New Military Strategy White Paper	2015	China	APAC
Chinese Ministry of National Defense	Five-year Cybersecurity plan	2015	China	APAC
CyberOps	Australian Space Cyber Framework	To be released	Australia	APAC
Cyberspace Administration of China (CAC)	National Cybersecurity Strategy	2016	China	APAC
Japanese National Cybersecurity Office	Cybersecurity Strategy	2025	Japan	APAC
METI (and Jaxa)	Guidelines for commercial space systems (v1.1)	2022	Japan	APAC
NTRA	LEO Satellite Cyber Security Framework	2022	Egypt	AFR
Pakistan Space Activities Regulatory Board (PSARB)	Pakistan Space Activities Rules 2024	2024	Pakistan	APAC
Parliament of Australia	Cyber Security Legislative Package 2024	2024	Australia	APAC
People's Republic of China State Council	Decree No. 147: Computer Information System Security Protection Regulations of the People's Republic of China	1994	China	APAC
Roscosmos	Order of Roscosmos State Corporation No. 349 "On improvement of the system for ensuring information security at Roscosmos State Corporation"	2020	Russia	CIS
South Korea National Cyber Security Center (NCSC)	Space Systems Cybersecurity Guidelines v1.0	2025	South Korea	APAC
The National People's Congress of the People's Republic of China	Cybersecurity Law of the People's Republic of China	2017	China	APAC

Those 13 GF frameworks have been assessed in detail, as part of the mission, allowing to **identify main trends**. Overall, GF framework issuers tend to address gaps in their current national legislation and mandate minimum cybersecurity standards across all sectors, **drawing on lessons from countries with more advanced cybersecurity strategies**.

APPLICABLE CASE: *Australian frameworks are intended to address gaps in current legislation and mandate minimum cybersecurity standards across all sectors, such as the Australian Defense ecosystem. Their frameworks are therefore not restricted to the SATCOM domain. By learning from what other countries have been doing over the past decades, Australia aims to draw lessons and develop an adaptable legislative framework that addresses modern challenges by focusing on basic cybersecurity recommendations across all sectors.*

GF framework issuers also aim to **develop an adaptable legislative framework** that addresses modern challenges by focusing on governance and more operational aspects.

*APPLICABLE CASE: **The South Korean NCSC was developed in reaction to a significant cyberattack** targeting South Korean SATCOM systems and infrastructures in the early 2020s.*

The GF frameworks also tend to leverage existing foreign frameworks, notably the NIST ones. This allows foreign nations to have a quicker maturity progression. The objective is to **simplify the use of GF frameworks by leveraging existing industry frameworks**, enabling strong complementarity and interoperability.

*APPLICABLE CASE: With the **Japanese METI Cybersecurity Guidelines for Commercial Space Systems**, SATCOM operators working on programs involving both Japanese and international partners can adapt most NIST practices to meet their specific needs.*

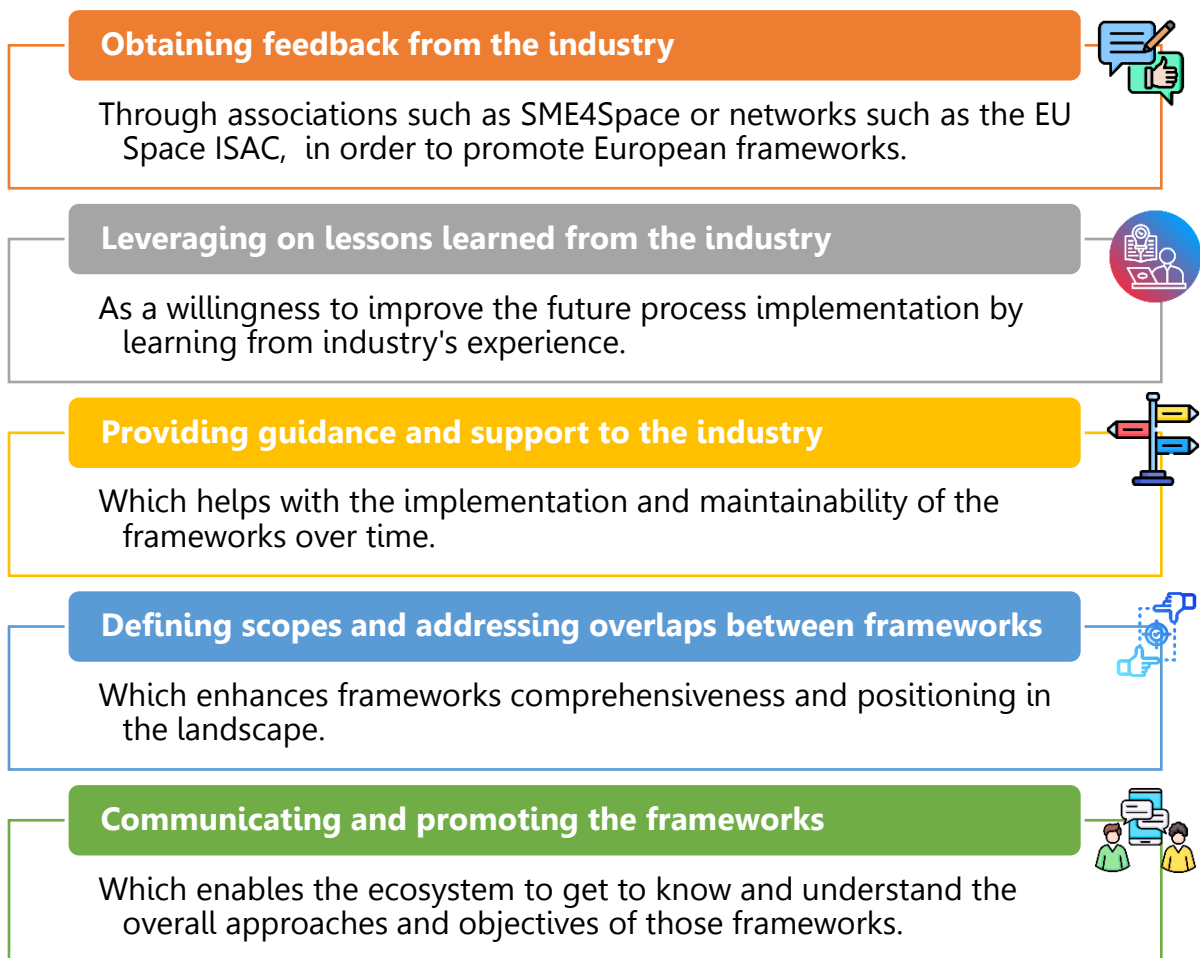
Overall, GF frameworks aim to develop a **comprehensive, step-by-step approach that builds on previous work**. There is a willingness to support the industry in compliance, provide guidelines, and allow for a comprehensive, step-by-step maturity progress.

*APPLICABLE CASE: **The Chinese Communist Party has been building its cybersecurity strategy since 1994, step by step**, with multi-year Cybersecurity plans, updates, and new frameworks that leverage existing work.*

E. FRAMEWORKS ROADMAP ENABLERS

Framework issuers should keep in mind a **set of potential recommendations to facilitate framework adoption**. These steps could be considered **enablers that increase the likelihood of the framework's acceptance within the SATCOM ecosystem**, particularly among new space players and SMEs. The main enablers are identified in the figure below:

Figure 4: Key enablers for framework adoption



F. OVERALL KEY TAKEAWAYS OF THE MISSION

1. MAIN TAKEAWAYS REGARDING POLICYMAKERS

14 main takeaways were identified regarding policymakers, whether European, American, or policymakers in general, and **5 takeaways were identified regarding the industry**.

- **Frameworks as a tool for states' influence, sovereignty, and autonomy**

Influencing or controlling cybersecurity frameworks enables nation-states to shape global governance, technological development, and security practices. Today, there is a **growing emergence of cybersecurity frameworks worldwide**, whether from traditional framework issuers such as the U.S. and Europe, or from nation-states that have only recently positioned themselves as framework issuers, such as China, Australia, South Korea, and Japan.

The EU institutions, for instance, emerged as a pole of influence in shaping the EU market through new frameworks, notably driven by **growing concerns about sovereignty and resilience**.

Overall, frameworks are seen and used as tools to achieve higher levels of sovereignty, autonomy, and resilience by orienting markets and shaping security culture, legal frameworks, and geopolitical power dynamics at the regional and international levels.

- **Governance as the main lever for space cybersecurity in Europe**

The European approach primarily focuses on establishing high-level, top-down strategies, thereby making governance the primary lever for space cybersecurity.

The EU, by emphasizing high-level strategies, aims to avoid regulatory fragmentation that would lead to a growing maturity gap between more advanced and less advanced Member States. For instance, the European directive **NIS2 directly shapes national frameworks by pushing nation-states to transpose the directive into their national laws**, with the aim of avoiding regulatory fragmentation, allowing each Member State to place greater emphasis on specific topics while retaining a degree of flexibility.

Governance is also strongly driven by a recent surge in interest in resilience and sovereignty. Notably, the **EU Space Act places strong emphasis on safeguarding European space assets and markets** against foreign cyber threats and external competitive pressures. This ambition is notably embodied in the proposed "*Single Market for space services*", a concept that has been contested by the United States, highlighting the geopolitical and economic power dynamics inherent in the design, promotion, and enforcement of regulatory frameworks.

- **A consolidation of the EU Member States' national ecosystems**

Within the European Union, member states are establishing cybersecurity frameworks and providing guidelines to their national ecosystems, with a strong emphasis on defense, security, and sovereignty—particularly in Western Europe, where there is a wide range of well-developed and well-positioned regulatory authorities on space and security issues, such as CNES, ANSSI, the BSI, the DLR, and the UKSA, for example, which play an active role in the regulatory landscape in the space sector.

An initial phase of consolidation of the national ecosystems, getting closer and working jointly on security and sovereignty topics in space, is also ongoing in Europe, for instance, between space and security agencies at the national level (as highlighted in the publication of frameworks jointly by the BSI and DLR, such as the IT-Grundschutz Profile for Space Infrastructures Part.1 or the Technical Guidelines associated).

- **A consolidation of the EU Member States' national ecosystems across countries**

Ecosystems are also getting closer across countries, as evidenced by ongoing discussions among the French, German, and Italian space ecosystems. This triad, France-Germany-Italy, is highlighted in the **BROMO project**, announced in October 2025, a strategic European initiative aimed at creating a European space giant by merging the space activities of Airbus, Thales, and Leonardo. This merger aims to strengthen Europe's technological sovereignty and competitiveness in the face of foreign competition, particularly from the United States and China.

- **A rise in budgets that leads to a need for structuration**

This willingness to keep consolidating national and European ecosystems is strongly highlighted in the **rise in budgets dedicated to space, space security, and cybersecurity.** Indeed, national institutions, along with their new strategies, have also been announcing a

surge in budgets. France, for instance, announced a €4.2bn increase (around 70%) to the military space budget for 2026–2030, raising the total to around €10.2bn over the period.

The strong rise in space budgets in Europe is also evident, with **ESA raising more than €22bn at the 2025 Ministerial Conference in November 2025 for the period 2026-2028, representing a 31% increase from the 2023-2025 period** (17% when corrected for inflation).

Within those space budgets, **the amount dedicated to security is also expected to grow**. For the 2026-2028 period, for instance, a **key focus is on secure and resilient communication networks, which gather about €2.1bn**, highlighting the importance of space-based communication security, resilience, and robustness.

Those rises in space and security budgets will contribute to the **need to structure the market and, indirectly, to regulate it as it is being structured**.

- **The American approach prioritizes operationality and space missions**

The U.S. approach to building cybersecurity frameworks also follows a top-down, strategic approach, with the Government likely to publish Executive Orders that then cascade across all U.S. institutional agencies (e.g., NASA, DoD) that must comply with the requirements.

Another characteristic of the U.S. approach is its **stronger focus on operational topics** and frameworks compared with those observed in Europe and other regions. Indeed, whereas in Europe the EU focuses more on developing governance frameworks, U.S. policymakers are already developing frameworks targeting a wider range of activities, such as risk assessment or security operations, highlighting that overall, **American policymakers have successfully moved beyond the initial baseline stage and are now focusing on the development of more operational frameworks**.

Moreover, **U.S. culture tends to prioritize mission, with a resilience-first, mission-oriented mindset**. In this mindset, security is considered efficient if a high level of resilience is also achieved.

- **A strong duality aspect in the U.S. frameworks**

American frameworks emphasize a strong focus on duality (i.e., applicability to both civilian and military domains). **The military, having strong operational needs, can push policymakers to emphasize operational security**. The space ecosystem, overall mature and closely linked to the defense space ecosystem, falls under the scope of operational frameworks targeting dual-use or defense applications (e.g., CMMC v2), leading to the development and widespread adoption of these frameworks in the U.S.

- **A growing number of nation-states publishing cybersecurity frameworks**

The willingness to consolidate the space and SATCOM ecosystem is also evident in other regions of the world, not only in Europe and the U.S. CyberInflight identified 13 frameworks published or to be released in non-traditional countries, including Asia-Pacific (APAC), notably China, South Korea, Japan, Australia, and Pakistan; Africa, notably Egypt; and the Commonwealth of Independent States (CIS), notably Russia.

New frameworks emerging in those regions emphasize a strengthening approach to immediate security, as well as long-term resilience. The approach of those new entrants to regulatory issues is mainly focused on robustness and resilience in space, highlighting a trend towards structuring due to increased fragmentation at the international level.

They also highlight a **growing willingness for more sovereignty** with an emphasis on protecting assets, whether space or cyber, considered sovereign and strategic.

- **Binding frameworks are used as a tool for harmonization**

In Europe, over the past few years, the trend has been to issue non-binding documents focused on recommendations and good practices rather than requirements, notably to provide support and advice to new entrants. **Today, the EU is increasingly emphasizing a common approach among EU Member States, thereby increasingly using binding documents as a harmonization tool (NIS2, EUSA, CRA, for instance).**

This **rise in binding frameworks is also noticeable in the U.S.**, with frameworks such as CMMC v2, which is binding under conditions for defense subcontractors.

This suggests a shift in approach compared with past years, as more binding frameworks were published or announced worldwide in the last 5 years, between 2020 and 2025, than in the previous 3 decades, from 1990 to 2019. This change is notably attributed to policymakers who have been working to expand the application of the frameworks considered essential baselines for improving cybersecurity maturity and reducing cybersecurity gaps. This highlights that cybersecurity is increasingly considered a strategic and sovereign issue that must be addressed in the face of evolving cyber-threats and technologies, coherently and uniformly across the whole ecosystem.

This trend has also accompanied **the emergence of New Space, resulting in a growing number of market entrants, some of which possess limited resources and cybersecurity maturity**. This evolution has increased the need to reshape market structures and adapt security frameworks to the unique characteristics, capabilities, and operational requirements of the New Space ecosystem.

- **The difficulty of enforcing frameworks**

Enforcement of frameworks is considered a primary challenge for policymakers. Enforcement can be regarded as the moment the ecosystem adopts a framework that is implemented and technically maintained. Usually, enforcement implies requirements and the binding nature of the framework. It also means that policymakers request evidence (technical evidence that the system is complying with the security requirements). The concept of enforcement sometimes runs counter to a more pragmatic approach put in place by the industry: **ticking the compliance box by following a requirement, but with a very limited positive impact on security**.

Moreover, enforcing frameworks is complex because of **discrepancies in dialogue among the different enforcement stakeholders**. The multiplicity of stakeholders (framework issuer, regional framework enforcing authority, national framework enforcing authorities, industrials, etc.) makes it challenging to establish effective communication and dialogue that would enable all to fulfill and understand their responsibilities.

- **A growing third-party intervention when building frameworks**

Geopolitical and economic competition and the race for frameworks publication, recognition, and adoption lead to a growing intervention by third-party nation-states in national or regional frameworks-building processes. **The U.S. government, for instance, provided feedback on the EU Space Act draft**. Overall, the U.S. expressed concerns about measures in the proposed Act that would impose regulatory burdens on U.S. providers of space services to European

customers, as well as non-tariff barriers that would introduce challenges to collaboration and business with Europe. Overall, this illustrates how **frameworks are increasingly used and exploited as tools for power and influence**.

- **Resilience is seen as a triad**

Resilience can be referred to as a triad of 3 aspects: Technical, Governance, and Risk Analysis.

The Technical aspect represents Operational Security (OPSec), and the operational capacity to withstand, absorb, and adapt, thereby continuing to operate even during a crisis or an attack. Overall, security must be implemented with the mission's operational aspects in mind.

The Governance aspect operates at a more strategic level, with notably top-down strategies that orient and enable operational levels to meet their objectives.

Risk Analysis is the third element needed to achieve a high level of resilience. Indeed, the Risk Analysis enables a step-by-step approach to identify, monitor, and mitigate threats to missions or systems.

To achieve resilience, those 3 aspects need to be addressed. **A growing number of frameworks aim to present a comprehensive approach to resilience by addressing 3 aspects**, such as the CNES Cybersecurity Hygiene Guide for Orbital Systems. It is presented in categories, each addressing a precise topic; notably, the Governance category also addresses the Risk Analysis need, and the other categories allow for diving into more operational and technical good practices, thereby also addressing this aspect of resilience.

- **Seeking a better complementarity between security and resilience topics**

In those past years, the frameworks' landscape showed a strong focus on security, addressing notably short- or medium-term needs and constraints, and less on the overall mission and long-term resilience. **Immediate security has been prioritized over long-term resilience, with policymakers sometimes adopting a reactive rather than a proactive approach** when building frameworks.

A shift is operating, however, as there is a **growing tendency to take into account resilience topics today**, notably by putting emphasis, within frameworks, on future or prospective trends to allow the industry to anticipate and adapt to evolving threats and technologies, and also by emphasizing new subjects such as sovereignty and autonomy, seen as pillars for resilience. For instance, **SPARTA**, considered one of the most SATCOM-relevant frameworks notably in the context of Risk Analysis, increasingly emphasizes resilience.

This growing tendency and willingness to build more holistic and comprehensive frameworks are **visible in all regions and are expected to continue in the years to come**.

- **Defending against electromagnetic interference**

A main trend observed throughout the mission is a growing concern about the rise of electromagnetic interference worldwide, leading to an increasing number of cybersecurity frameworks that address this new typology of threat.

On the European side, this has gone hand in hand with a surge in jamming episodes, notably in Eastern Europe, since the beginning of the war in Ukraine in 2022. As such threats are notably growing, **the ecosystem is seeking ways to respond by addressing them through**

frameworks, leading to a step-by-step increase in maturity. Thus, the approach is mainly to **develop a comprehensive overview of threats that includes both cyber and electromagnetic topics.** For instance, in the CNES Cybersecurity Hygiene Guide for Orbital Systems, published in 2025, an entire category is dedicated to addressing electromagnetic interference, highlighting how cyber and electromagnetic interference are increasingly addressed together in Europe.

A growing maturity regarding those topics is also visible in the U.S., where the American ecosystem faces such threats (with GPS increasingly targeted by electromagnetic interference) and is adapting. The approach used when developing frameworks, however, differs from Europe, as the tendency in the U.S. is to build fewer bridges between cyber and electronic topics and instead develop frameworks targeting electromagnetic interference topics only.

2. MAIN TAKEAWAYS REGARDING THE INDUSTRY



- **Security is often addressed too late in space programs**

When to introduce security into space missions is a crucial question for industry players. Concepts such as "*Security-by-Design*" emphasize the need to address security in the early stages of development. However, some space actors tend to underestimate its importance or fail to account for it properly in the mission timeline. In the course of the project, it then sometimes happens that **cybersecurity is brought up, on delay, as a topic that needs to be addressed** (most of the time for certification or compliance reasons). As it was not taken into account at the beginning, it can lead to delays, and stakeholders sometimes cut it to the minimum to be compliant. In all cases, it can lead to **duplicate efforts, late design changes, and low agility in project management.**



- **Difficulty in sustaining frameworks over time**

Space players sometimes struggle to monitor requirements 'compliance throughout the project's lifecycle. It may be challenging to track requirements across an increasing number of frameworks. In some cases, space actors need to implement and maintain incompatible or overlapping standards, which leads to compliance uncertainties and issues. In such cases, **space actors often need to choose between standards, making compromises that can sometimes reduce mission security or efficiency.** Space actors sometimes face a contradiction: while being subject to more security standards, security is sometimes overlooked due to operational challenges arising from the implementation and maintenance of a framework over time. Overall, **the space industry needs greater rationalization of frameworks.** It also needs a **more comprehensive view of the frameworks landscape.**



- **Technical debt issue in legacy systems**

Technical debt in cybersecurity refers to the accumulated security risks and vulnerabilities resulting from deferred security measures, rushed implementations, or suboptimal decisions during software development and IT operations. **Legacy space systems were frequently designed in an era when cybersecurity requirements were minimal or nonexistent, resulting in lower levels of security and a substantial security debt that organizations must now remediate.**

In some cases, industry players are making a compromise between a costly, operationally complex security solution and leaving the systems unsecured. In such cases, **a trade-off is often necessary.**



- **A complex traceability process**

Within an industrial organization, **difficulty in retaining a framework's requirements or recommendations over time** can make it **challenging to establish an effective traceability process**. Overall, traceability involves defining security objectives, identifying risks, specifying requirements or good practices to mitigate those risks, and ensuring evidence is stored for compliance.

In space missions, sustaining a framework over time is difficult because of changes in human resources (with teams rotating), supply and value chain changes that sometimes require evolving security approaches, and the evolution of architectures, for instance. In the medium and long term, evidence management tends to get lost in separate documents, making proper traceability harder.

Sometimes, industry players struggle to meet the evidence requirement, particularly when cross-mission duplication occurs during framework implementation. For instance, **if a mission addresses different stakes, such as commercial or dual-use, the industry can face difficulties providing evidence that addresses the needs associated with all of them**.



- **Difficulty in understanding and achieving certification**

This difficulty with traceability and security, often addressed too late, also **complicates the certification process**. Indeed, if security is introduced too late and there is little or no evidence to support a certification demand, the **certification process tends to become complex and costly**. When traceability is incomplete, for instance, certification teams tend to be forced to reconstruct the entire risk analysis, rerun tests, or regenerate missing evidence.

3. MAIN RECOMMENDATIONS FOR EU AND NATIONAL POLICYMAKERS

13 main recommendations for EU and national policymakers were identified, whether European, American, or policymakers in general.



- **Keep anticipating the future trends and technologies**

A wide variety of new technologies and topics are gaining momentum and already disrupting space missions and operations. They all come with cybersecurity opportunities and risks, and continually addressing them is a necessity in today's landscape of frameworks. Main trends highlight the **growing digitalization of space**, with the integration of digital technologies into all phases of the space mission. Those technologies include, for instance, quantum and post-quantum cryptography (PQC), Artificial intelligence (AI) onboard, Direct-to-device (D2D) constellations, and Inter-satellite optical (ISL) links, on-board IDS, over-the-air rekeying (OTAR) etc.

On the industry side, **greater emphasis is placed on those topics through research and development and standardization**. The industry, for instance, anticipates robust PQC with appropriate cryptographic algorithms and is pushing policymakers to address these issues through standardization. This is how NIST released 3 cryptographic algorithms in August 2025, driven by industry moving quickly on those topics. Therefore, standardization is usually driven by industrial needs. **Policymakers should remain aware of industrial needs and address them by updating standards and frameworks**.

Another recommendation is for **policymakers themselves to anticipate emerging technologies and issues**, enabling them to respond more quickly and efficiently to future industry needs. Staying aware of those topics is also necessary for the frameworks to remain relevant over time.



- **Being able to anticipate the evolving threat landscape**

The threat landscape is evolving rapidly, and anticipating its changes is key to ensuring that European and national cybersecurity frameworks remain relevant, valuable, and capable of regulating an increasingly challenged landscape. Therefore, European and national **policymakers cannot adopt only a reactive stance; they must anticipate changes in the cyber-threat landscape.**

This is achieved through a proactive understanding of threats, which requires strategic monitoring, information sharing between public and private actors, and the development of CTI capabilities. **The threat intelligence activities must become more structured, and information should flow more easily among all stakeholders.**



- **Keep addressing sovereignty and geopolitical-related topics**

Frameworks should aim to **tackle, anticipate, and understand the growing stakes that Nations face in the space sector**, as space has become profoundly linked to geopolitics, with growing tensions, and economics, with economic dependencies.

New frameworks are emerging in regions where policymakers started only recently to position themselves on the cyber and space topics, such as APAC or CIS, highlighting a **growing willingness for more sovereignty with an emphasis on protecting assets, whether space or cyber, considered sovereign and strategic.** This willingness is also evident in the U.S. and Europe, with a growing number of frameworks addressing these topics. A recommendation is to keep addressing those strategic topics to prevent Europe from lagging, as those stakes will keep growing in other regions of the world.



- **Keep looking to include robustness and resilience topics**

Frameworks should emphasize the need to address robustness and resilience to ensure they are as comprehensive as possible. There is a growing tendency to address resilience today, notably by emphasizing, within frameworks, future or prospective trends to enable the industry to anticipate and adapt to evolving threats and technologies, and by highlighting new subjects such as sovereignty and autonomy, seen as pillars of resilience. **Taking resilience into account involves addressing the triad of OPSec, governance, and risk analysis.** Therefore, to remain relevant and add value to the industry, European and national policymakers can ensure their future frameworks address those topics together. Overall, Europe shows a growing willingness to do so, as highlighted notably with the **NIS2 Directive.**



- **Improve the ability to do the maintenance of the frameworks**

Several recommendations can be implemented to improve the ability to maintain the frameworks and their supporting documents and sources. First, make sure to **structure the framework as soon as its first draft or release, keeping in mind its maintenance through a clear architecture.**

Another recommendation could be to **automate the framework building and updating as much as possible.** This also goes hand in hand with automating its basis documents. The EU Space Act, for instance, relies on an impact analysis as a basis document. Therefore, the initial

impact assessment should also be maintainable through automation (for instance, leveraging automated calculation formulas) and the transmission of knowledge between teams (clear processes for updating through versioning rules, date update rules, etc.).



- **Bring an added value to the industry**

For the frameworks to be widely adopted, the industry needs to see them as providing added value to the existing landscape. To do so, leveraging industry feedback, experience, and lessons learned is recommended. It can be done through networks such as the EU Space ISAC.

This goes hand in hand with **clearly defining the scope of the leading European frameworks to ensure there are no overlaps** and that each is seen as an essential building block within this landscape.

Another recommendation to bring real added value to the industry would be to **ensure the framework is widely accessible and that no practical barriers hinder its use**. In Europe, the ESA's SSE4PACE framework, if made more easily accessible to the ecosystem, could become widely adopted and useful for the SATCOM players.



- **Take into account the timeline differences between the EU and national levels**

The differences in timelines between the EU and national levels, notably when transposing EU Directives into national laws or complying with new EU frameworks, can sometimes create a rush among nation-states, leading to market distortions and uncertainty.

The EU can ensure it takes this structural timeline difference into account and adapts its processes accordingly. Recommendations regarding **adapting administrative processes and implementing an agile project method**. To follow the process, roles and responsibilities should also be clearly defined within a group at the European level, especially dedicated to monitoring EU deadlines (an interministerial permanent team, for instance), which would follow and practically support implementation at the national level.

Difficulties for Member States to meet EU deadlines, as seen with NIS2 transpositions, also highlight the **challenge of reaching consensus, especially when debating sovereign or critical issues**. To get a consensus, a holistic approach is also needed, notably by addressing the ecosystem as a whole.



- **Addressing the SATCOM ecosystem holistically**

One main recommendation to help reach a consensus when building or updating a framework would be to **address all stakeholders' concerns and real-life challenges, notably by taking into account challenges related to the securization of the supply chain**.

As seen in the aviation market, PART-IS is a framework that holistically addresses the aerospace ecosystem and covers a wide range of players, from minor to major. Similarly, framework development within the SATCOM and space ecosystems can benefit from an ecosystem-wide perspective. Considering the diversity of stakeholders involved enables the identification of common interests, cross-cutting challenges, and shared objectives, all of which are critical to building consensus.



- **Understand the need for competitiveness and strengthening of the industry**

There is a growing trend to **further take into account the industry's need for competitiveness** when policymakers write and enforce frameworks. **The EU Space Act, for instance, emphasizes proportionality** by scaling obligations to an operator's size, risk profile, and mission-criticality rather than applying a uniform set of requirements that could become a burden for some operators, notably smaller ones.

Strengthening the industry also involves understanding and accounting for the operational needs and challenges of industrials. The **emergence of mission-oriented, actionable "profile" frameworks (e.g., NASA's or BSI's) highlights a willingness from policymakers to move in that direction, and further help industrials implement a security tailored to the right need**. However, those needs and challenges are still too often overlooked, adding complexity to debates and the development of frameworks that aim to find a satisfying compromise for all stakeholders. The main risks identified with NIS2, for instance, concern the introduction of heavy requirements without space-specific tailoring, leading operators to struggle to adapt.

The main recommendation is to **simplify the frameworks landscape in Europe by harmonizing the initiatives and reducing their numbers**. The point is not only to reduce administrative and legal burdens, but mainly to allow the industry, European and extra-European, that seeks to implement and invest in Europe, to better understand the overall frameworks and approaches surrounding them. The SATCOM industry may face complexity in maintaining multiple frameworks, multiplying costs and effort. A Europe-wide cybersecurity framework, established to streamline processes and facilitate cooperation in the space domain among Member States, may be reassuring for the industry.

Another point is to **further ensure that the industry knows or can at least estimate the costs associated with implementing and retaining the frameworks over time**. The EU Space Act puts an Impact Assessment, which focuses notably on the anticipation of the implementation cost, at its core, but overall, usually very few frameworks leverage such a study, making it difficult for the industry to estimate the costs associated with it. Thus, keeping leverage on such a proactive document when building frameworks is necessary.



- **Helping the industry with the sustainability of the frameworks, over time, within the organization**

Overall, industry players struggle to monitor requirements throughout the project's lifecycle, to track requirements across a growing number of frameworks, with no standard tool, which complicates interoperability and follow-up over time.

To address those issues, **European and national frameworks should aim to provide a coherent, comprehensive, and end-to-end approach to security**, with a focus on improving the framework's reusability. The framework should also ensure traceability from objectives to risks, requirements, and evidence, and should help support compliance over time. Providing a set of tools, or at least methodologies, to build and address the frameworks' requirements is necessary (e.g., SSE4SPACE, SPARTA).

A key point is also to propose a **homogeneous tooling that could help ensure interoperability** between missions and frameworks (e.g., the SSE4Space tool, if made widely available, could help industrials develop a more homogeneous approach to Risk Assessment). Developing a framework based on **Model-Based Systems Engineering (MBSE)** can be helpful (e.g., SSE4Space is following this approach). Indeed, MBSE is an approach that favors the use of digital models rather than text documents as the primary means of information.



- **Avoid uncertainty for the industry**

There is a **strong need within the SATCOM ecosystem to understand the overall approach to a framework early in its development**, to anticipate and adapt, ensuring a smooth market transition and consolidation. Moreover, as observed, uncertainty surrounding one framework can lead to uncertainty about several others that aim to leverage it. For instance, uncertainty about the actual obligations under the EU Space Act is leading to growing uncertainty across the German market, as the WRG aims to follow EUSA guidance and is therefore awaiting its publication. Thus, in this situation, the German ecosystem faces a double uncertainty.

The main recommendation for policymakers to reduce uncertainty for the industry is to **provide clear guidance and information on the frameworks as early as possible**. One axis is therefore to **invest in growing communication between policymakers and the industry**, and to maintain a link to answer their questions and reassure them.



- **EU policymakers should invest in diplomacy through frameworks worldwide**

European policymakers can strengthen their partnerships beyond Europe to structure cooperation networks in line with security and industrial interests. Space security can be a significant pillar of relations and can integrate regulatory issues into a joint approach. Such ties can be especially emphasized with emerging space powers that are increasingly developing space cybersecurity frameworks, **notably in the APAC region**, such as Australia, Japan, and South Korea.



- **Responsibilities at the national level should be clearly defined**

An increasing number of policymakers can also be observed, with more and more framework issuers (mainly national) positioning themselves on the frameworks landscape. Encouraging national initiatives can help foster the ecosystem's growing maturity. However, their multiplication can also complicate obtaining a clear overview of each entity's scope of action.

National authorities should clearly define the accountability and responsibilities of each policymaker (such as the Space Agency and the Security Agency). This definition can be challenging, but the discussion needs to be addressed if policymakers are willing to simplify the frameworks landscape. Overall, questions such as **which authority has the necessary expertise to build a cybersecurity framework for the space ecosystem** are the main ones to be addressed.

Overall, national authorities should also align their initiatives with the broader European areas of work to ensure greater harmonization of the frameworks landscape.

Table 4: Table of references

Reference	URL
Arrêté du 8 septembre 2017 (Decree establishing security rules and reporting procedures for critical information systems and security incidents relating to the critical sub-sector of "Space" activities), French government	https://www.legifrance.gouv.fr/loda/id/LEGISCTA000035580592
Australian Space Cyber Framework, CyberOps	https://www.cyberops.com.au/space-cyber-framework

CCSDS 350.5-G-2 – SPACE DATA LINK SECURITY PROTOCOL—EXTENDED PROCEDURES—SUMMARY OF CONCEPT AND RATIONALE, CCSDS	https://ccsds.org/Pubs/350x11g1e1.pdf
CCSDS 355.0-B-2 Space Data Link Security Protocol, CCSDS	https://public.ccsds.org/Pubs/355x0b2.pdf
CCSDS 355.1-B-1 – SPACE DATA LINK SECURITY PROTOCOL — EXTENDED PROCEDURES, CCSDS	https://ccsds.org/Pubs/355x1b1.pdf
CNSSP-12, CNSS (and NASA)	https://www.cnss.gov/CNSS/openDoc.cfm?a=NvLYGLBEZBZknFli%2FhhjnA%3D%3D&b=D99F81ADDAD55A5044E5A91258503FAB42BCBF0B65B142F2E823BBBE7D523C4DC53109905D890F6BE9084CF24A640635
Cyber Security Legislative Package 2024, Parliament of Australia	https://www.lexology.com/library/detail.aspx?g=75d7efa0-2a68-46fd-9167-237bd659f279
Cybersecurity Framework (CSF) v.2.0, NIST	https://www.nist.gov/cyberframework
Cybersecurity Law of the People's Republic of China, the National People's Congress of the People's Republic of China	https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ ; https://www.gov.cn/yaowen/liebiao/202510/content_7046194.htm
Cybersecurity Maturity Model version 2, CMMC v2	https://dodcio.defense.gov/cmmc/Resources-Documentation/
Cybersecurity Strategy, Japanese National Cybersecurity Office	https://www.cyber.go.jp/pdf/policy/kihon-s/cs_strategy2025.pdf ; https://www.cyber.go.jp/pdf/policy/kihon-s/cs_strategy2025_abstract_english.pdf
Cybersecurity Toolkit Ver. 2, UKSA	https://www.gov.uk/government/publications/cyber-security-toolkit
Decree No. 147: Computer Information System Security Protection Regulations of the People's Republic of China, People's Republic of China State Council	https://chinacopyrightandmedia.wordpress.com/1994/02/18/computer-information-system-security-protection-regulations-of-the-peoples-republic-of-china/
Eckpunkte der Bundesregierung für ein Weltraumgesetz (WRG) - (Key Issues Paper for a Future German Space Act - For a stronger space industry), German Government	https://www.bundeswirtschaftsministerium.de/Redaktion/EN/Downloads/E/eckpunkte-breg-weltraumgesetz_en.pdf?__blob=publicationFile&v=3
ECSS-E-ST-80C: Space engineering – Security in space systems lifecycles, ECSS	https://ecss.nl/wp-content/uploads/2024/07/ECSS-E-ST-80C(1July2024).pdf

ECSS-Q-ST-80C Software Product Assurance, ECSS	https://ecss.nl/standard/ecss-q-st-80c-rev-2-software-product-assurance-30-april-2025/
EU Space Act Factsheet, Proposal, and Impact Assessment (Implementation Cost study), European Commission	https://defence-industry-space.ec.europa.eu/eu-space-act_en .
EU Space ISAC	https://www.euspa.europa.eu/eu-space-programme/eu-space-and-security/eu-space-isac
EU Space Strategy for Security and Defence, European Commission	https://defence-industry-space.ec.europa.eu/eu-space/eu-space-strategy-security-and-defence_en
Guidelines for commercial space systems (ver 1.1), METI (and Jaxa)	https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_uchu_sangyo/pdf/20230331_1e.pdf
ISO 18676:2024 "Requirements and guidelines for the management of systems engineering", ISO sub committee 14	https://www.iso.org/fr/standard/87631.html
ISO/TS 20517:2024 Space systems - Cybersecurity management requirements and recommendations, ISO sub committee 14	https://www.iso.org/standard/86305.html?browse=tc
ISO10795 "Vocabulary", ISO sub committee 14	https://www.iso.org/fr/standard/72936.html
ISO14300-1 "Structuring a project" and ISO14300-2 "Product Assurance", ISO sub committee 14	https://www.iso.org/fr/standard/86543.html ; https://www.iso.org/fr/standard/86544.html
ISO17666 "Risk management", ISO sub committee 14	https://www.iso.org/fr/standard/89819.html
IT-Grundschatz Profile for Space Infrastructures – Minimum Protection for Satellites Covering their Entire Life Cycle, BSI (DLR)	https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschatz/profiles/Profile_Space-Infrastructures.pdf?__blob=publicationFile&v=2
IT-Grundschatz Profile for Space Systems - Part 2: Ground segment – minimum protection over the entire life cycle, BSI	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschatz/Hilfsmittel/Profile/Profil_Bodensegment-Satellit.pdf?__blob=publicationFile&v=5
LEO Satellite Cyber Security Framework, NTRA	https://www.egcert.eg/wp-content/uploads/2022/12/LEO-Satellite-Cyber-Security-Framework_V2.0.pdf
Minimum Requirements for Space System Cybersecurity - Ensuring Cyber Access to Space, IEEE	N/A

National Cybersecurity Strategy , Cyberspace Administration of China (CAC)	https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/
National Space Strategy , UKSA	https://www.gov.uk/government/publications/national-space-strategy/national-space-strategy
New Military Strategy White Paper, and Five-year Cybersecurity plan , Chinese Ministry of National Defense	https://news.usni.org/2015/05/26/document-chinas-military-strategy ; https://layersevensecurity.com/cybersecurity-targets-in-chinas-new-five-year-plan/
NIS 2 measures for a high common level of cybersecurity across the Union , European Commission	https://eur-lex.europa.eu/eli/dir/2022/2555
NISTIR 8270: Introduction to Cybersecurity for Commercial Satellite Operations , NIST	https://csrc.nist.gov/pubs/ir/8270/final
NISTIR 8401: Satellite Ground Segment: Applying the Cybersecurity Framework to Satellite Command and Control , NIST	https://csrc.nist.gov/pubs/ir/8401/final
NISTIR 8441: Cybersecurity Framework Profile for Hybrid Satellite Networks , NIST	https://csrc.nist.gov/pubs/ir/8441/final
Orbital System Cybersecurity Hygiene Guide (Guide d'Hygiène Cybersécurité des Systèmes Orbitaux) , CNES	https://cnes.fr/entreprises/centre-cyber-spatiale
Order of Roscosmos State Corporation No. 349 "On improvement of the system for ensuring information security at Roscosmos State Corporation" , Roscosmos	https://www.roscosmos.ru/media/files/2021/SEP/roskosmos_go-2020.pdf
Pakistan Space Activities Rules 2024 , Pakistan Space Activities Regulatory Board (PSARB)	https://www.parc.gov.pk/SitelImage/Misc/files/Page%20C%20%20012.pdf
SME4Space	https://www.sme4space.org/
Space Attacks and Countermeasures Engineering Shield (SPACE-SHIELD) , ESA	https://spaceshield.esa.int/
Space Policy Directive 5 , U.S. government	https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/
Space Security Best Practices Guide BPG REV B , NASA	https://swehb.nasa.gov/download/attachments/146540183/Space%20Security%20Best%20Practices%20Guide%20BPG%20REV%20B.pdf?version=1&modificationDate=1706014154000&api=v2

Space Systems Cybersecurity Guidelines V1.0 , South Korea NCSC	https://www.ncsc.go.kr:4018/main/cop/bbs/selectBoardArticle.do?bbsId=InstructionGuide_main&nttId=215638&menuNo=070000&subMenuNo=070300&thirdMenuNo=
SPARTA , Aerospace Corporation	https://sparta.aerospace.org/
SSE4SPACE , ESA	https://mb4se.esa.int/MB4SE_Home.html
Technical Guideline BSI TR-03184 Information Security for Space Systems Part 1 and Part 2 , BSI (DLR)	https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03184/BSI-TR-03184_part1.html ; https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03184/TR-03184_node.html