

1<sup>st</sup> Edition

Published: April 2023



# SPACE CYBERSECURITY

Market Intelligence Report Presentation



Confidential

# A strategic report on Space Cybersecurity



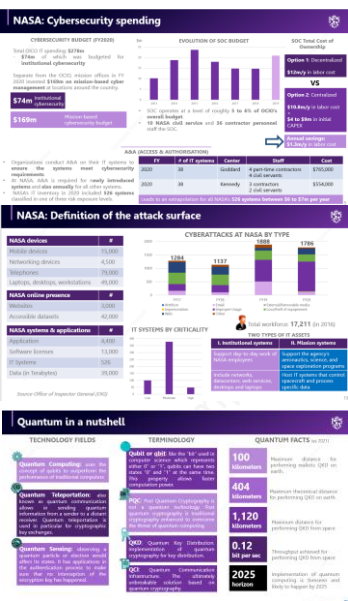
## OUR MAIN STRATEGIC REPORT

### Space Cybersecurity Market Intelligence report

- Strategic approach
- Interview campaign (~30 interviewees from the entire value chain)
- Market outlook
- Sector trends and dynamics
- Strategic analysis and forecast
- Stakeholders' profile
- Regulatory landscape
- Threat intelligence



Released in April 2023 : CyberInflight strategic report is a **unique resource on the space cybersecurity domain** consolidating all necessary information to better comprehend the market and make insightful decision making. CyberInflight is proud to be at the forefront of this domain and one of the **only market intelligence company** to have consolidated such amount of information in a single document.



155 Pages

8 chapters

30 Interviews conducted

Database of 130 cyberattacks

Database of 44 Space-cybersecurity contracts

Database of 265 Space-cybersecurity stakeholders

# Research Report's Table of content



Executive Summary	1	Examples of regional space threat players	40	Space Overlay and NIST SP 800-53 Rev. 5	76	Space Software & Operating System (2/4)	115
Acronym Table	2	<b>CHAPTER III. SPACE CYBERSECURITY STAKEHOLDERS</b>	<b>41</b>	Space Overlay overview	77	Space Software & Operating System (3/4)	116
Acronym Table	3			NIST 8323 overview	78	Space Software & Operating System (4/4)	117
Table of content	4	Introduction & Methodology	42	NIST 8270 overview	79	Quantum in a nutshell	118
<b>CHAPTER I. INTRODUCTION</b>	<b>5</b>	List of universities involved in space cybersecurity	43	ECSS (European Cooperation for Space Standardization) & BSI (Federal Office for Information Security)	80	Quantum technologies (1/2)	119
Introduction to the space economy	6	List of institutions involved in space cybersecurity – Europe region	44	CCSDS: Introduction	81	Quantum technologies (2/2)	120
The booming economy of space data	7	List of institutions involved in space cybersecurity – North America region	45	CCSDS: SEA-SEC	82	Quantum security (1/2)	121
More assets in space: a broader attack surface	8	List of institutions involved in space cybersecurity – APAC region & others	46	NIST 8401 overview	83	Quantum security (2/2)	122
Observed trends in the space sector	9	List of corporate actors involved in space cybersecurity – by number of employees	47	CNSSP-12 & SPD-5	84	Quantum supremacy (1/3)	123
New Space and Innovation	10	List of corporate actors involved in space cybersecurity – by number of employees	48	Tallin Manual 2.0 & Budapest convention	85	Quantum supremacy (2/3)	124
Cybersecurity principles	11	Corporate space cybersecurity actors (1/3)	49	NIS v2	86	Quantum supremacy (3/3)	125
Cybersecurity principles for space systems	12	Corporate space cybersecurity actors (2/3)	50	IA-PRE	87	Quantum projects	126
Increasing recognition of space cybersecurity	13	Corporate space cybersecurity actors (3/3)	51	HSN & Space Policy	88	<b>CHAPTER VII. CASE STUDIES</b>	<b>127</b>
Lack of skilled workforce : a major challenge	14	The soar of Space Forces	52	Recognizing Space as a “Critical Infrastructure”	89	Cybersecurity at NASA (1/5)	128
The global cybersecurity market	15	Space ISAC: a keystone for information sharing	53	Common Criteria & Other guidance	90	NASA: Definition of the attack surface (2/5)	129
Viasat : a turning point in space cybersecurity	16	Space ISAC overview	54	Introduction to EXPORT-CONTROL	91	NASA: General & Cybersecurity spending (3/5)	130
Evolution of cyberattacks against the space sector	17	Innovative space-cyber actors	55	EU and US EXPORT-CONTROL	92	NASA: SOC cybersecurity spending (4/5)	131
A new battlefield (1/2)	18	GSaaS Ground Segment/Station as a Service	56	US EXPORT-CONTROL overview	93	NASA: OIG Recommendations (5/5)	132
A new battlefield (2/2)	19	Company profile: Leaf Space	57	Takeaways on Export-Control from a satellite manufacturer	94	Starlink: an efficient DevSecOps approach	133
<b>CHAPTER II. THREAT INTEL. &amp; CYBERATTACKS EXAMPLES</b>	<b>20</b>	Company profile: CGI	58	CMMC: Introduction	95	Russia: a master in Electronic Warfare	134
Introduction	21	Company profile: RHEA-GROUP	59	CMMC: CMMC Levels and Domains	96	China: Space Cyber activities	135
Overview of cyberattacks on space ecosystem	22	Mapping of corporate actors	60	CMMC: Processes and Practices	97	US Space Force (USSF) cybersecurity approach (1/2)	136
Case 1: Eavesdropping Athena-Fidus communications	23	Mapping of institutional actors	61	CMMC: Rollout phases	98	US Space Force (USSF) cybersecurity approach (2/2)	137
Case 2: ROSAT satellite attack allegations	24	Mapping of academic database	62	<b>CHAPTER VI. TECHNOLOGY</b>	99	The cybersecurity of rocket launchers	138
Case 3: Interfering with US satellites (Landsat-7, Terra EOS)	25	<b>CHAPTER IV. SPACE CYBERSECURITY ECONOMY</b>	<b>63</b>	Executive Summary	100	U.S. Defense Industrial Base (1/2)	139
Case 4: Jamming satellite signals	26	Overview of the cybersecurity budget evolution	64	A word on Satellite Platforms (1/2)	101	U.S. Defense Industrial Base (2/2)	140
Case 5: Intrusion of IT systems	27	Estimated budget evolution (global/IT/cyber)	65	A word on Satellite Platforms (2/2)	102	DIBs around the world	141
Case 6: Takeover and spoofing	28	The concept of “cybersecurity debt”	66	SWaP (Size, Weight and Power) (1/2)	103	<b>CHAPTER VIII. MISCELLANEOUS / CONTRACTS</b>	<b>142</b>
Case 7: Software bugs	29	Heterogenous cybersecurity investment levels	67	SWaP (Size, Weight and Power) (2/2)	104	Space conferences dedicated to space cybersecurity	143
Case 8: Supply chain compromise	30	Forecast of Cybersecurity budget	68	The evolution of hardware technology in space (1/3)	105	Overview of space cybersecurity conferences	144
Case 9: NASA cybersecurity breach	31	Forecast of budget evolution (global/IT/cyber)	69	The evolution of hardware technology in space (2/3)	106	Overview of the CYSAT conference 2022 (2nd edition)	145
Miscellaneous: NASA incident list	32	Forecast of the cybersecurity debt	70	The evolution of hardware technology in space (3/3)	107	Cyber-insurance: Introduction (1/2)	146
Overview of the recent Viasat/KA-SAT cyberattack (1/3)	33	Overview of significant space cybersecurity contracts	71	Other cybersecurity technologies for space systems	108	Cyber-insurance: Introduction (2/2)	147
Overview of the recent Viasat/KA-SAT cyberattack (2/3)	34	<b>CHAPTER V. REGULATORY LANDSCAPE</b>	<b>72</b>	Cryptography tradeoff for space applications	109	Cyber & Space insurance	148
Overview of the recent Viasat/KA-SAT case (3/3)	35	Executive summary	73	Ground segment security – Introduction	110	Cyber-insurance: Chronology of cyber-insurance	149
Demystifying cyberattacks in space	36	Most relevant guidance for cyber-space stakeholders	74	Ground segment security – Overview	111	Cyber-insurance: Defining the cyber-risk	150
Geopolitics and Space: the growth of cyber threats	37	NIST overview of applicable guidance to space value chain	75	Ground Segment Security – Example of cyberattacks	112	Cyber-insurance: Stakeholders and their influence	151
Space-cyber warfare	38			Cloud security in space	113	Cyber-Insurance: conventional VS specific cyber-contract	152
The media aspect	39			Space Software & Operating System (1/4)	114		

# Overview of cyberattacks on space ecosystem (excerpt)

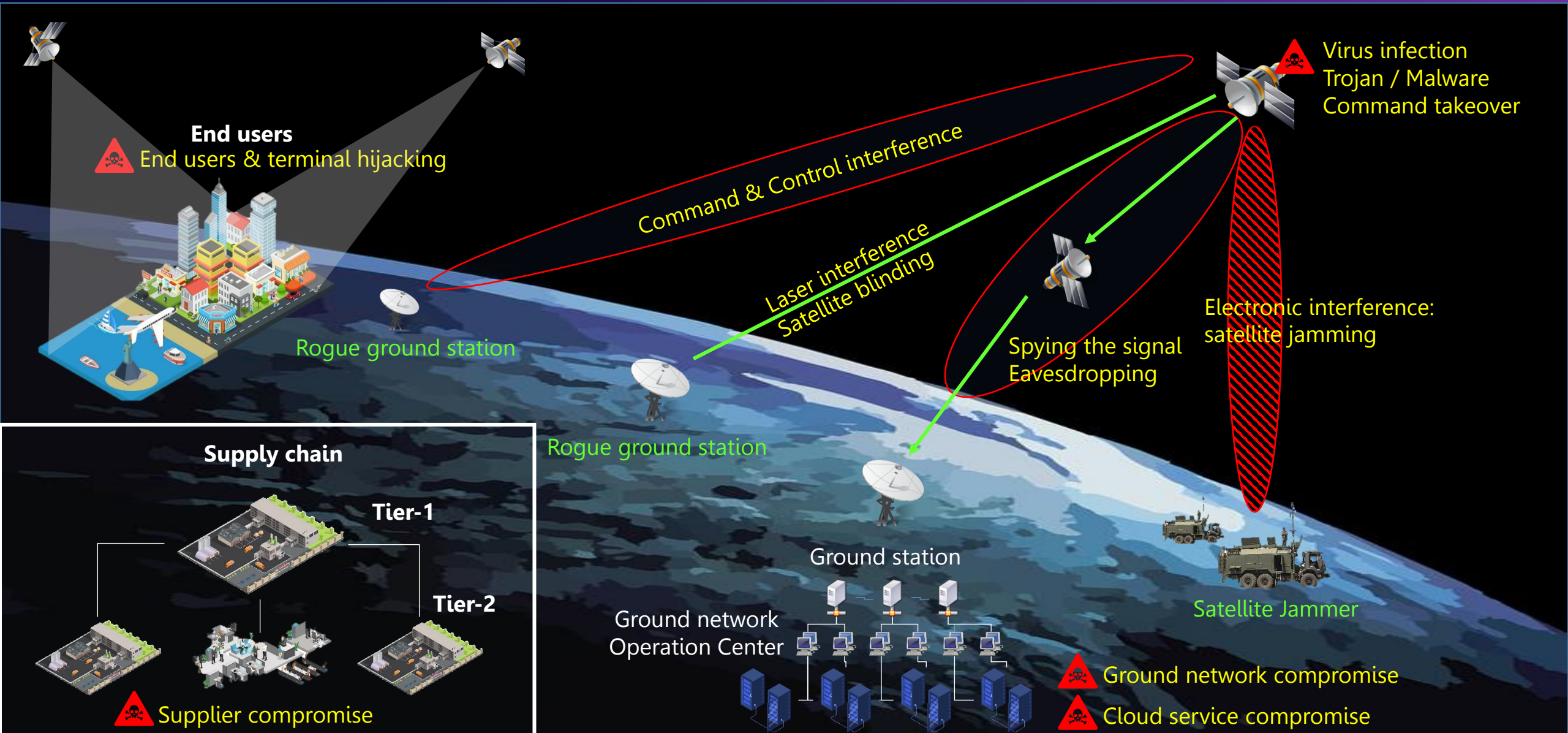
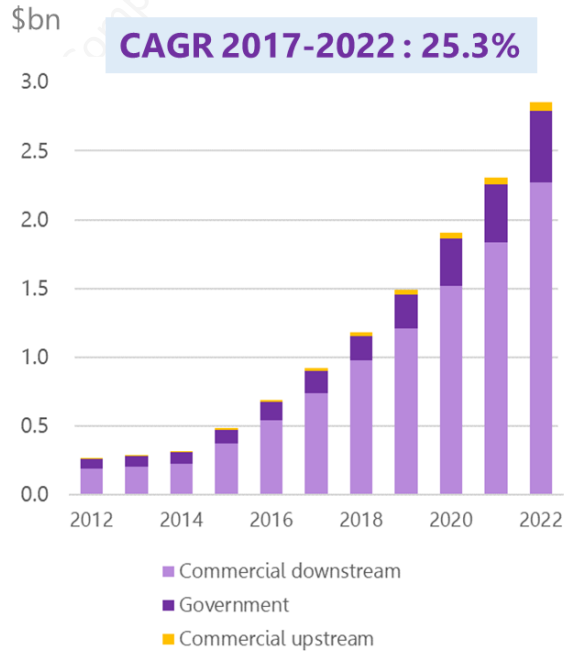




Fig 3.

### ESTIMATED EVOLUTION OF GLOBAL CYBERSECURITY BUDGET

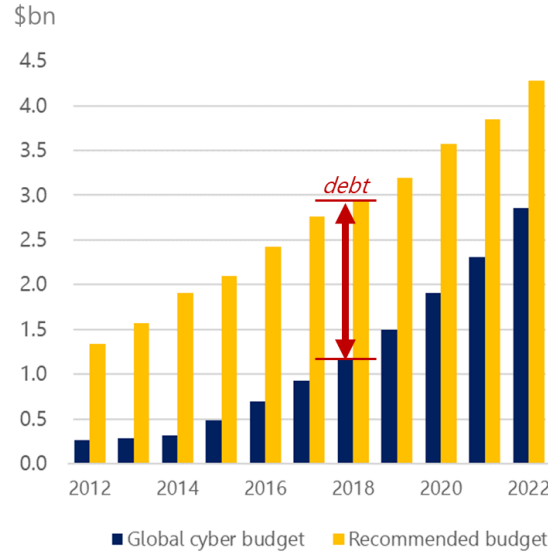


Space cybersecurity market seems to follow an outstanding **CAGR of 25% in the last 5 years**

(Source CyberInflight, see full Space Cybersecurity report)

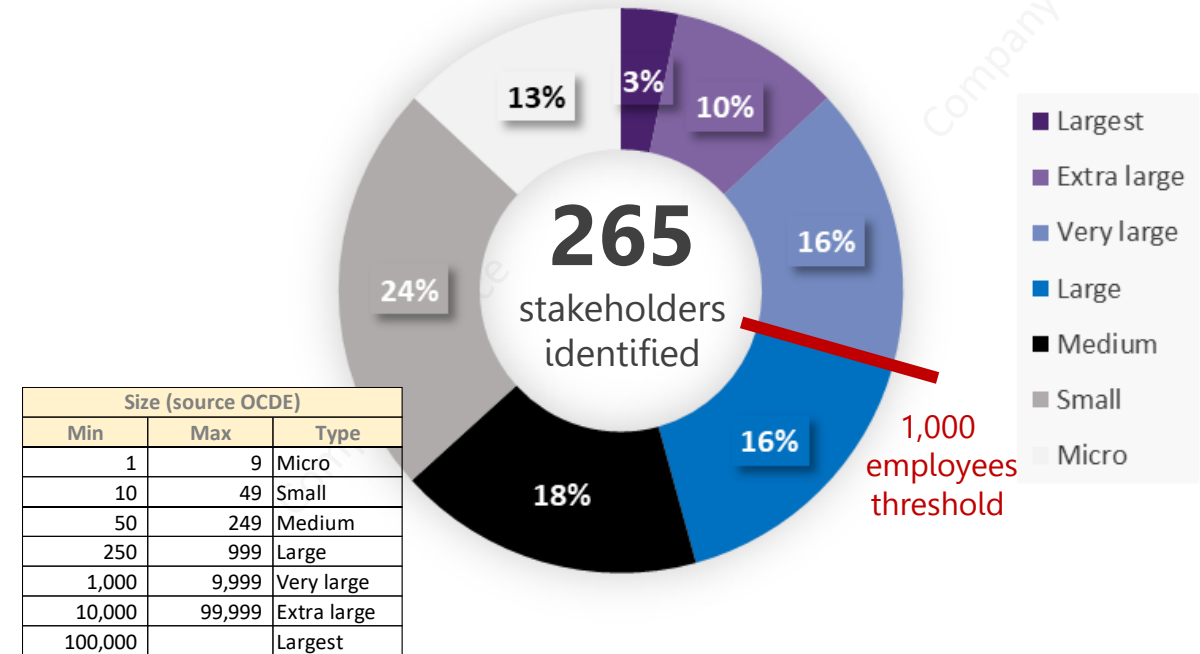
Fig. 4

### ESTIMATED RECOMMENDED VERSUS ACTUAL CYBERSECURITY BUDGET



Space cybersecurity market seems to **accumulate a technical debt every year**

### SPACE CYBERSECURITY STAKEHOLDERS



### SPACE CYBER STAKEHOLDERS MARKET TRENDS

- **Fragmented** but limited market (70% of companies are <1,000)
- Legacy stakeholders **shifting toward space cybersecurity**
- More **new entrants with innovative and expected space/cyber solutions**
- Growing **competition**
- Growing **tension** on cybersecurity staff (and salaries)
- Increasing business **opportunities**

# Most relevant guidance for cyber-space stakeholders *(excerpt)*



## CCSDS



<b>CCSDS 350.0-G-3</b>	The Application of Security to CCSDS Protocols
<b>CCSDS 350.1-G-2</b>	Security Threats against Space Missions
<b>CCSDS 350.4-G-2</b>	CCSDS Guide for Secure System Interconnection
<b>CCSDS 350.6-G-1</b>	Space Missions Key Management Concept
<b>CCSDS 350.7-G-2</b>	Security Guide for Mission Planners
<b>CCSDS 350.8-M-2</b>	Information Security Glossary of Terms
<b>CCSDS 350.9-G-1</b>	CCSDS Cryptographic Algorithms
<b>CCSDS 351.0-M-1</b>	Security Architecture for Space Data Systems
<b>CCSDS 352.0-B-2</b>	CCSDS Cryptographic Algorithms
<b>CCSDS 356.0-B-1</b>	Network Layer Security Adaptation Profile
<b>CCSDS 357.0-B-1</b>	CCSDS Authentication Credentials
<b>CCSDS A13.1-Y-1</b>	CCSDS Recommended Procedures for Cloud-Based Interoperability Testing

## NIST



**NIST SP 800-53 Rev. 5**  
Security and Privacy Controls for Information Systems and Organizations

**NIST SP 800-161**  
Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

**SPACE PLATFORM OVERLAY**

**NIST 8270**  
Introduction to Cybersecurity for Commercial Satellite Operations

**NIST 8401**  
Satellite Ground Segment

**NIST 8323**  
Foundational PNT Profile

**METI**  
Guidelines for commercial space systems

**BSI**  
IT baseline protection profile for space infrastructures

**ECSS**  
ECSS-Q-ST-90C

## Miscellaneous



**Tallin Manual**

**Memorandum on SPD-5**



**CNSSP-12**  
National information assurance policy for space systems used to support national security missions



**NIS v2**  
**EN9100**  
**GDPR**  
Etc.



**Space Specific**

**Generic**

**CMMC**

**IA-PRE**

**CC EAL**

**AS/EN9100**

# Technology Executive Summary *(excerpt)*



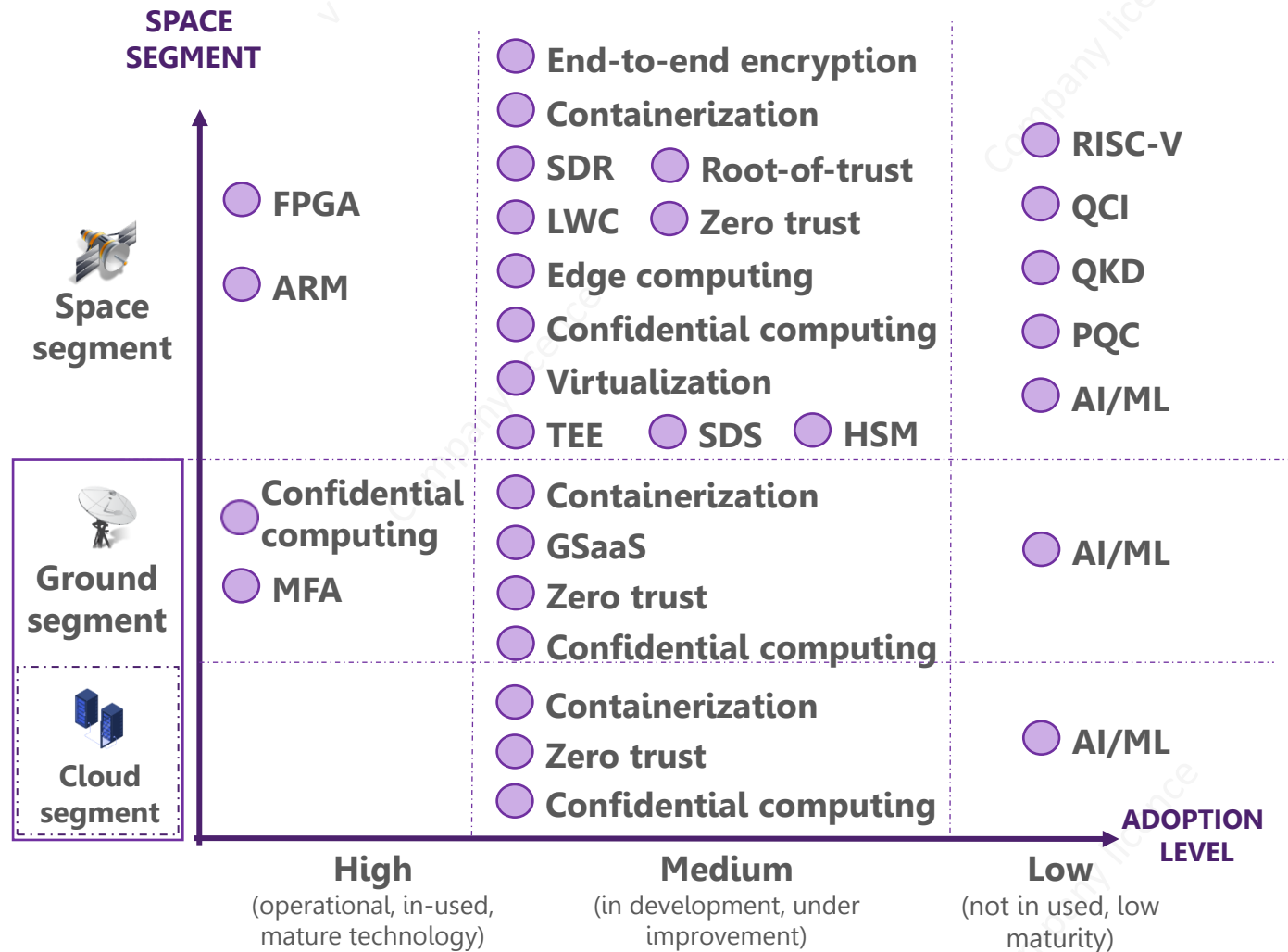
The **ever-increasing demand for data** and the growing dependency on space applications is pushing the need for processing more data on board and to send them to the ground. A new set of technologies is being developed allowing for higher performance, increased throughput, and secure communications. The **improvement of existing technologies** (RISC, ARM, FPGA), the **creation or the adaption of new ones to space applications** (lightweight cryptography, confidential computing, containerization, quantum) **the shift to new business models** (such as GSaaS, and as-a-service models in general) are a set of new challenges to be overcome not only to meet the growing demand for space data but also to reliably secure these services in front of an expanding threat landscape.

Embedding more technologies within the spacecraft implies meeting current and future operational and environmental constraints. It requires additional performance, power, weight or size (the SWaP tradeoff). The **soar of COTS** has pushed the use of technologies which are well-used within traditional IT applications such as containerization (virtualization, Kubernetes, Docker). Trust is implemented at different level from hardware (root-of-trust) to software (LWC or confidential computing). The ground segment is also sustaining significant transformation - becoming more and more cloud-oriented.

**Future technologies such as quantum or artificial intelligence or machine learning may be seen as disruptors** when reaching a higher maturity level.

Cybersecurity technologies are evolving between current and future requirements mainly driven by the rapid evolution and growing interest for space by the cyber threat landscape.

SPACE CYBERSECURITY TECHNOLOGY EXAMPLES & THEIR MATURITY LEVEL



AI/ML : Artificial Intelligence, Machine Learning  
 ARM : Advanced RISC Machine  
 FPGA : Field-programmable gate array  
 HSM : Hardware Security Module  
 LWC : Lightweight Cryptography  
 MFA : Multi-factor authentication

PQC : Post Quantum Communication  
 QCI : Quantum Communication Infrastructure  
 QKD : Quantum Key Distribution  
 RISC : Reduced Instruction Set Computer  
 SDR : Software Defined Radio  
 TEE : Trusted Execution Environment



## 4 MAIN DATABASES

**173** cyberattacks reported publicly from 1977 to 2023

### **Cyberattack database**

*Updated on June 1<sup>st</sup> 2023*

**380** academic, corporate and institution actors of all size involved in the field of space cybersecurity

### **Actors database**

*Updated on June 1<sup>st</sup> 2023*

**85** contracts from five regions of the world (**AsiaPACific**, **EU**rope, **Meadle East/North Africa** and **North America**)

### **Contract database**

*Updated on June 1<sup>st</sup> 2023*

Estimation of space cybersecurity budgets from 2018 to 2020

### **Space cyber Economy database**

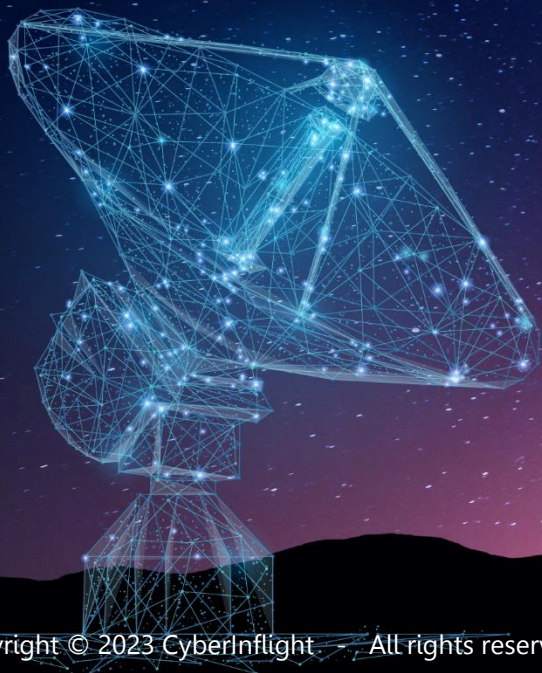
*Updated on May 2023*



**1<sup>st</sup> Edition**

Published: April 2023

Contact us at: [research@cyberinflight.com](mailto:research@cyberinflight.com)



### **Report summary**

- Market outlook
- Sector trends and dynamics
- Strategic analysis and forecast
- Stakeholders' profile
- Regulatory landscape
- Threat intelligence