1st Edition

Published: April 2023

CyberInflight

SPACE CYBERSECURITY

Market Intelligence Report Presentation

Confidential

www.cyberinflight.com

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

1st Edition
Published: April 2023

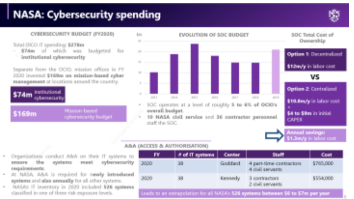
CyberInflight

SPACE CYBERSECURITY

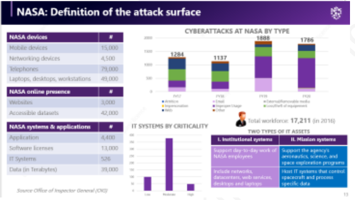
Market Intelligence Report

Copyright © 2023 CyberInflight - All rights reserved.

www.cyberinflight.com



NASA: Cybersecurity spending



NASA: Definition of the attack surface

Quantum in a nutshell

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

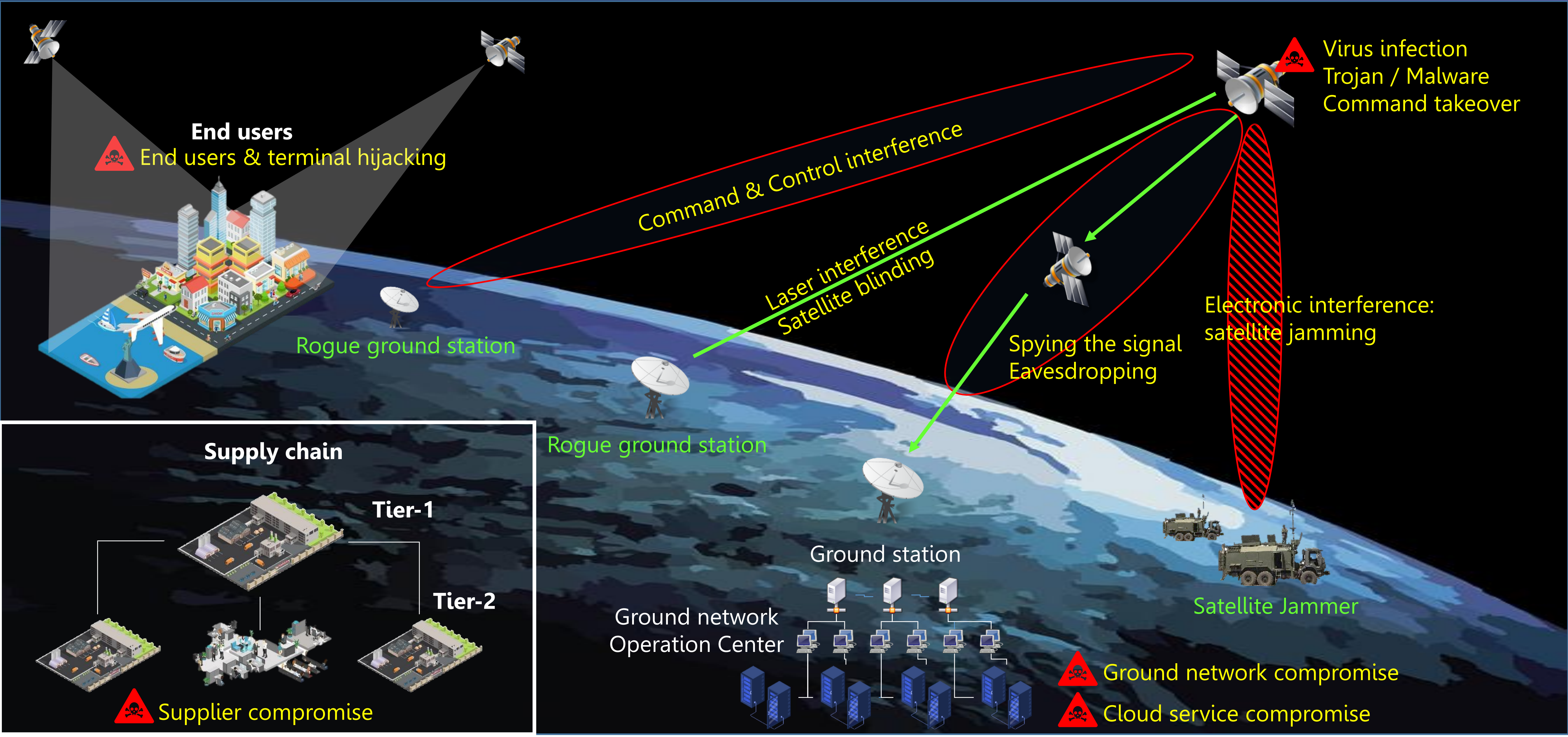
Database of **130** cyberattacks

Database of **44** Space-cybersecurity contracts

Database of **265** Space-cybersecurity stakeholders

Research Report’s Table of content

Overview of cyberattacks on space ecosystem *(excerpt)*



Market economics *(excerpt)*

Fig 3.
ESTIMATED EVOLUTION OF GLOBAL CYBERSECURITY BUDGET

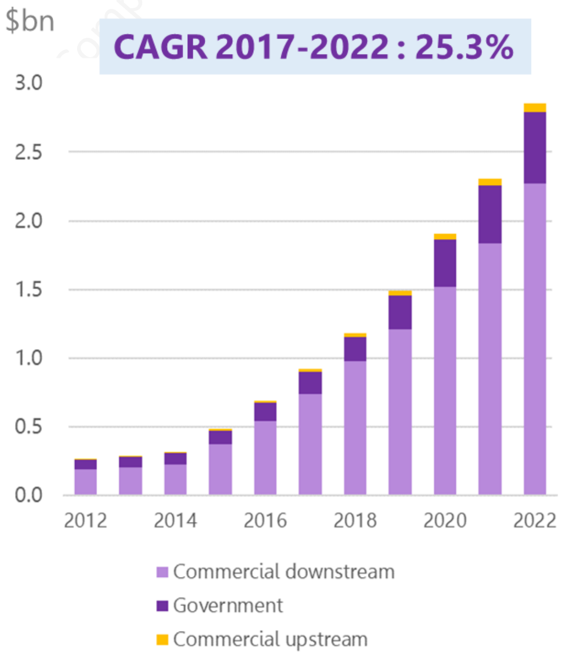
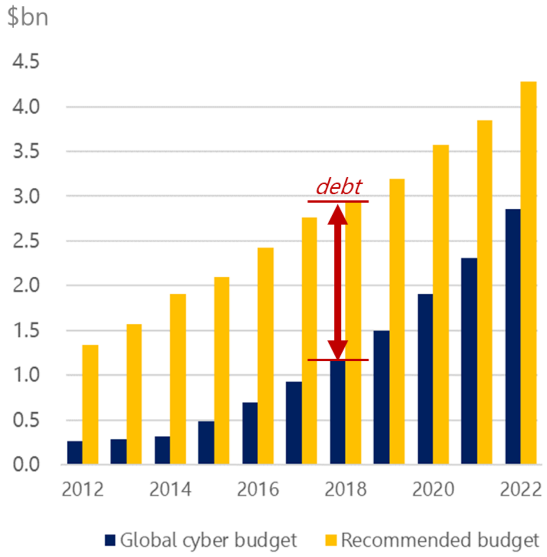
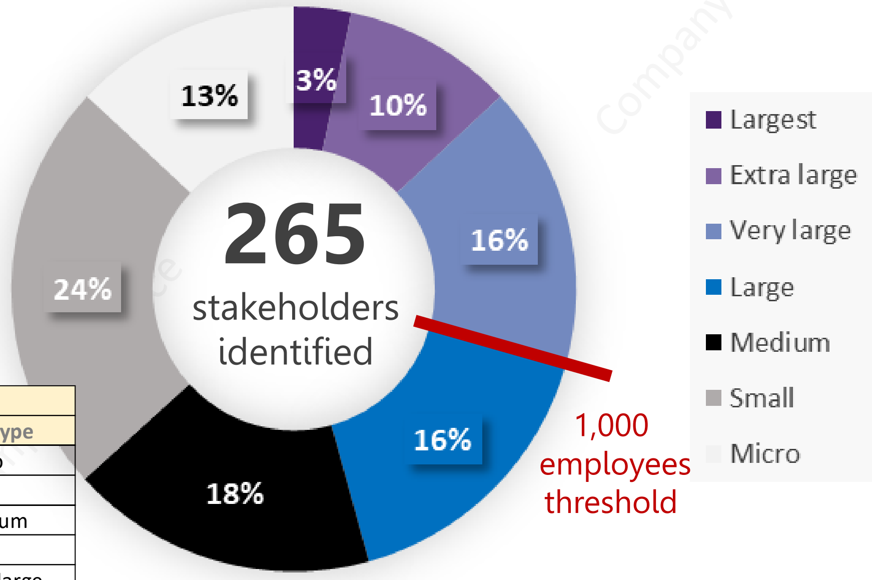


Fig. 4
ESTIMATED RECOMMENDED VERSUS ACTUAL CYBERSECURITY BUDGET



SPACE CYBERSECURITY STAKEHOLDERS



Size (source OCDE)		
Min	Max	Type
1	9	Micro
10	49	Small
50	249	Medium
250	999	Large
1,000	9,999	Very large
10,000	99,999	Extra large
100,000		Largest

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

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

(Source CyberInflight, see full Space Cybersecurity report)

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

Consultative Committee for Space Data Systems

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

Federal Office for Information Security

BSI
IT baseline protection profile for space infrastructures

METI
Ministry of Economy, Trade and Industry

METI
Guidelines for commercial space systems

ECSS
ECSS-Q-ST-90C

Miscellaneous

CCDCOE

Tallin Manual

White House

Memorandum on SPD-5

CMMC

IA-PRE

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

CC EAL

AS/EN9100

European Commission

NIS v2
EN9100
GDPR
Etc.

Space Specific

Generic

Technology Executive Summary *(excerpt)*

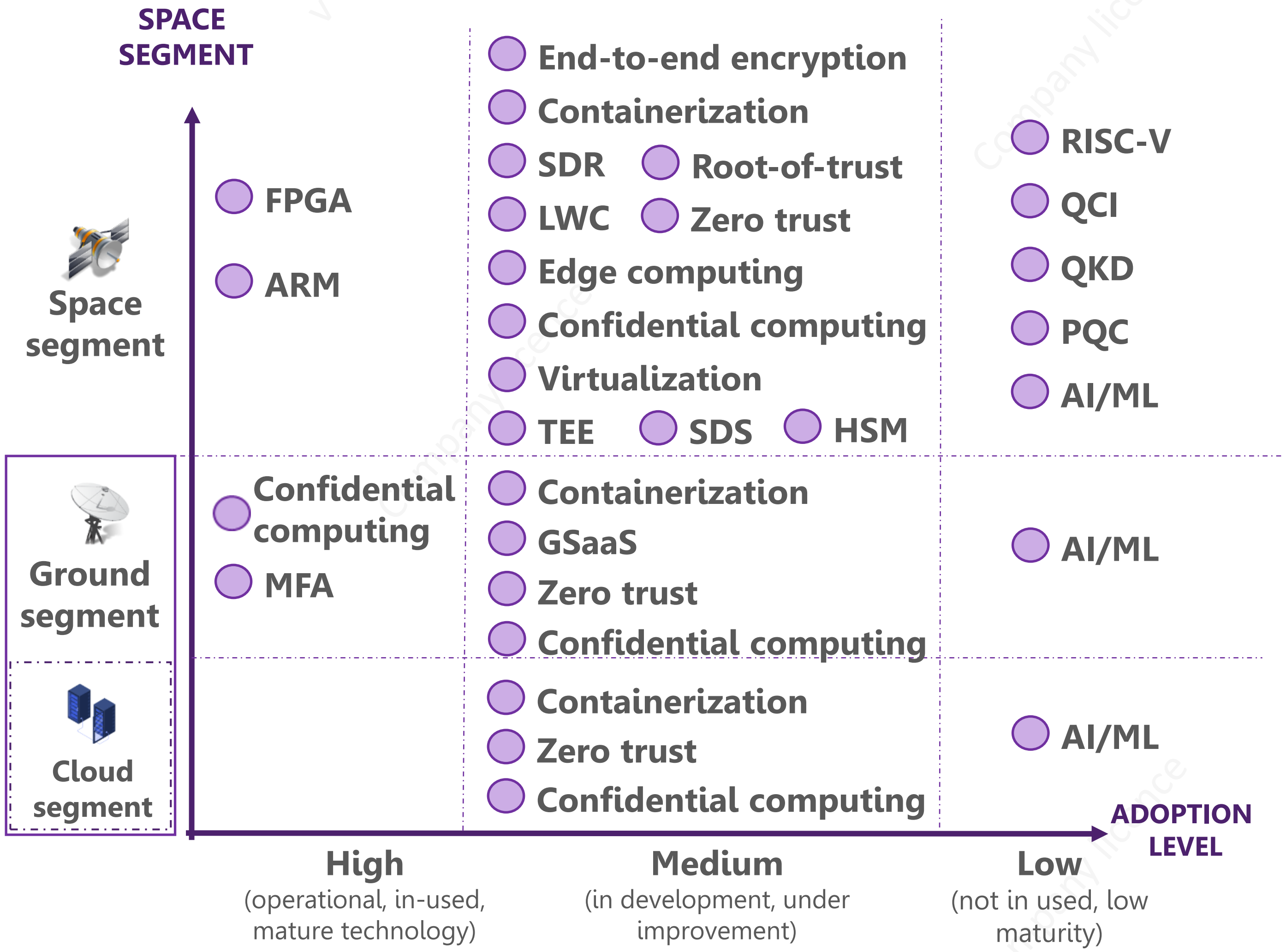
The **ever-increasing demand for data** and the growing dependency on space applications is pushing the need for processing more data on board and to send them to the ground. A new set of technologies is being developed allowing for higher performance, increased throughput, and secure communications. 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



	High (operational, in-used, mature technology)	Medium (in development, under improvement)	Low (not in used, low maturity)
Space segment	FPGA ARM	End-to-end encryption Containerization SDR Root-of-trust LWC Zero trust Edge computing Confidential computing Virtualization TEE SDS HSM	RISC-V QCI QKD PQC AI/ML
Ground segment	Confidential computing MFA	Containerization GSaaS Zero trust Confidential computing	AI/ML
Cloud segment		Containerization Zero trust Confidential computing	AI/ML

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

Space Cybersecurity Market Intelligence report supporting databases

4 MAIN DATABASES

173 cyberattacks reported publicly from 1977 to 2023

Cyberattack database
Updated on June 1st 2023

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

Actors database
Updated on June 1st 2023

85 contracts from five regions of the world (**A**sia**PAC**ific, **EU**rope, **M**eadle **E**ast/**N**orth **A**frica and **N**orth **A**merica)

Contract database
Updated on June 1st 2023

Estimation of space cybersecurity budgets from 2018 to 2020

Space cyber Economy database
Updated on May 2023

1st Edition

Published: April 2023

Contact us at: *research@cyberinflight.com*

Report summary

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

www.cyberinflight.com