2nd Edition
Published Q1 2024

CyberInflight

SPACE CYBERSECURITY

Market Intelligence Report

www.cyberinflight.com

CyberInflight
Space Cybersecurity Market Intel. partner

ABOUT US

A unique player in Space Cybersecurity Market Intelligence

Independent company, employee owned

Founded in 2019 and headquartered in Toulouse, France

Specialized in the Space market

Member of:

SPACE ISAC

1st French member of the Space ISAC
Chair member of the Supply Chain Working Group (SCWG)

Founding member of:

#EUSpaceISAC

EUSPA

Consulting
Market Intelligence
Competitive analysis
Due Diligence
OSINT researches
Space ISAC member (US and EU)
Part of operational security teams on EU projects (ex. EGNOS v3)

OUR ACTIVITIES

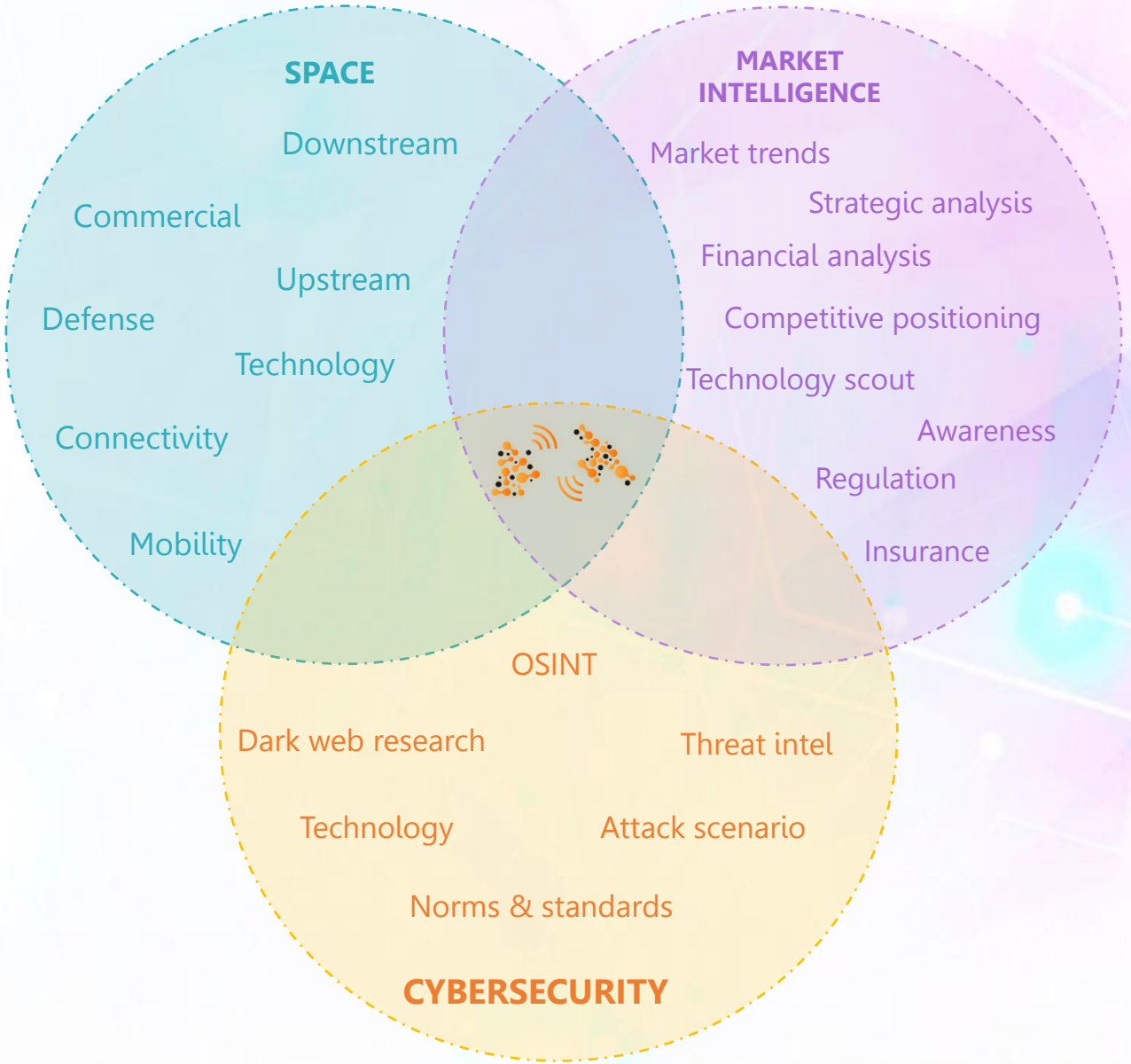
Provides **Aerospace Cybersecurity Intelligence** through different forms

- Strategic research resources
- Aerospace Cybersecurity Awareness Training
- Ad-hoc consulting and advisory missions
- Constant market monitoring (market watch)

Our customers:

- **Space agencies**
- **Institutions**
- **Aerospace industry leaders**
- **European & International stakeholders**

Our vision

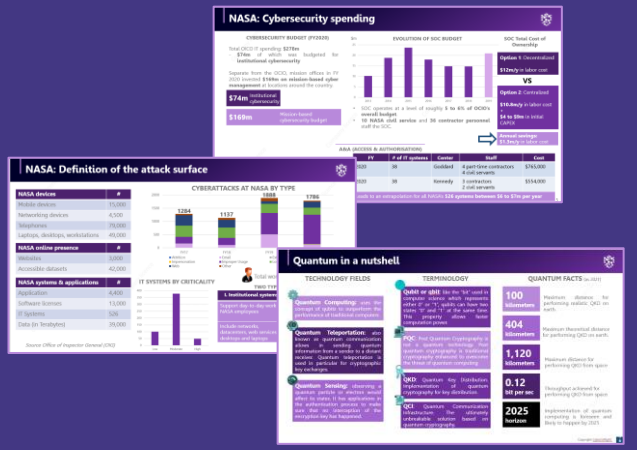

SPACE
Downstream
Commercial
Upstream
Defense
Technology
Connectivity
Mobility
MARKET INTELLIGENCE
Market trends
Strategic analysis
Financial analysis
Competitive positioning
Technology scout
Awareness
Regulation
Insurance
OSINT
Dark web research
Threat intel
Technology
Attack scenario
Norms & standards
CYBERSECURITY

A strategic report on Space Cybersecurity

OUR STRATEGIC REPORTS

Space Cybersecurity Market Intelligence report

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



First Edition released in April 2023: CyberInflight first 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 companies** to have consolidated such an amount of information in a single document.

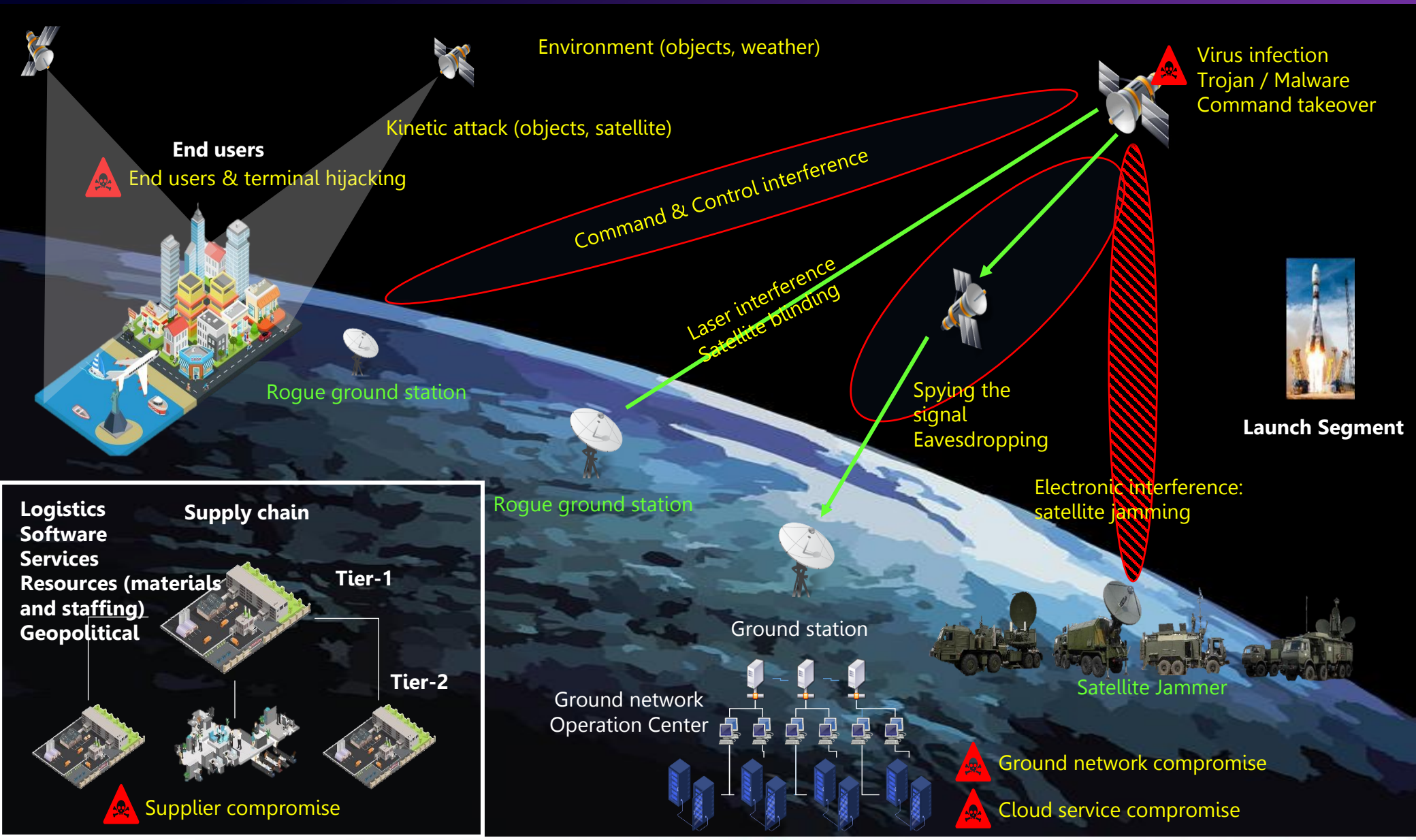
Second Edition released in April 2024: CyberInflight intends to publish an annual update of its strategic on Space Cybersecurity Market Intelligence report, in order to remain up-to-date and provide the latest consolidated information for a better understanding of the market.

310 Pages	**8** chapters	**30** Interviews conducted	Database of **348** cyberattacks	Database of **200** Space-cybersecurity contracts	Database of **488** Space-cybersecurity stakeholders

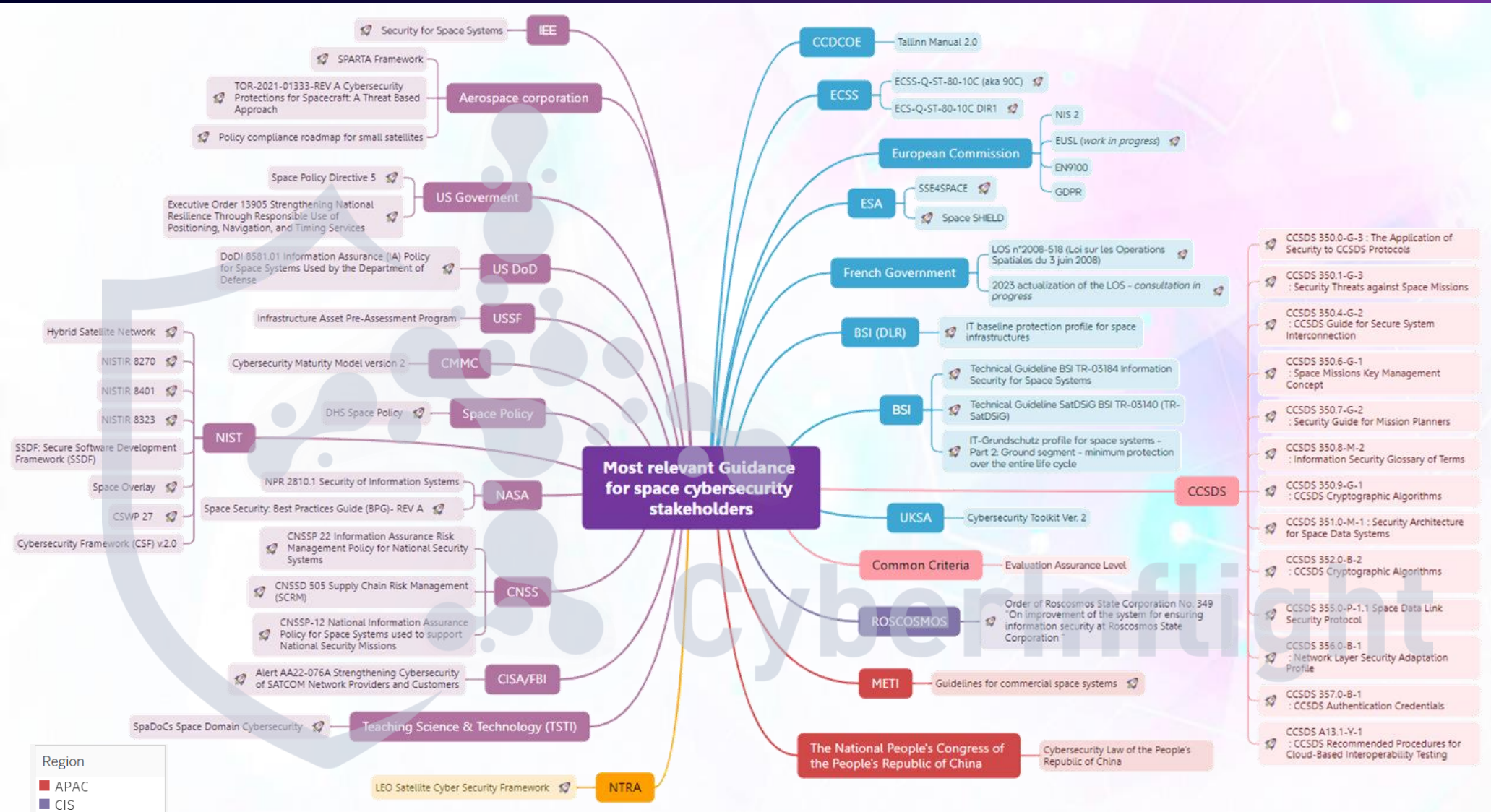
Table of content (1/2)

Table of content (2/2)

Overview of cyberattacks on space ecosystem



Most relevant guidance for cyber-space stakeholders



Technology Executive Summary *(excerpt)*

The ever-increased demand for higher performance

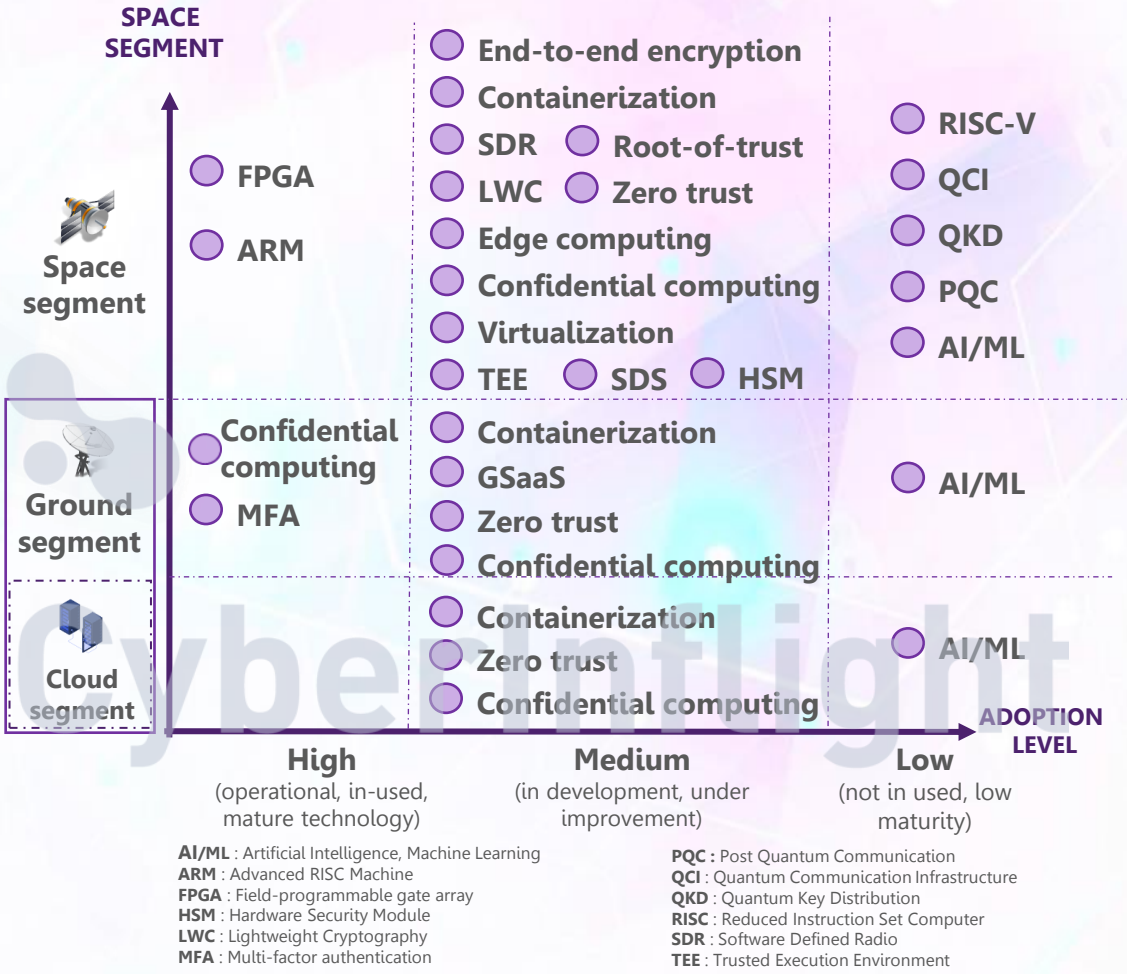
The increasing demand for data and reliance on space applications drives the need to process more data on board and transmit it to the ground. **New technologies are being developed to achieve higher performance, increased throughput, and secure communications**. This involves **improving existing technologies** (RISC, ARM, FPGA), **creating or adapting new ones for space applications** (lightweight cryptography, confidential computing, containerization, quantum), and **shifting to new business models** (such as GSaaS and as-a-service models in general). Overcoming these challenges is essential not only to meet the growing demand for space data but also to ensure the reliable security of these services in the face of an expanding threat landscape.

Incorporating more technologies into spacecraft means **meeting existing and future operational and environmental limitations.** This necessitates increased performance, power, weight, or size (known as the SWaP tradeoff). The **growing popularity of COTS products** has led to the adoption of technologies commonly used in traditional IT applications, such as containerization (virtualization, Kubernetes, Docker). Trust is established at various levels, from hardware (root-of-trust) to software (like LWC or confidential computing). The ground segment is also undergoing significant changes, shifting towards cloud-based systems.

Quantum foresight

As we reach higher levels of maturity, **future technologies like quantum computing, artificial intelligence, and machine learning may be considered as disruptive forces.** Quantum technology is currently in active development, and there is a **strong interest from industry in national and regional projects.** Cybersecurity technologies are evolving to meet current and future requirements, driven mainly by the rapid evolution and increasing interest in space within 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

An ever-growing threat landscape

Assumptions & known biases for this analysis :

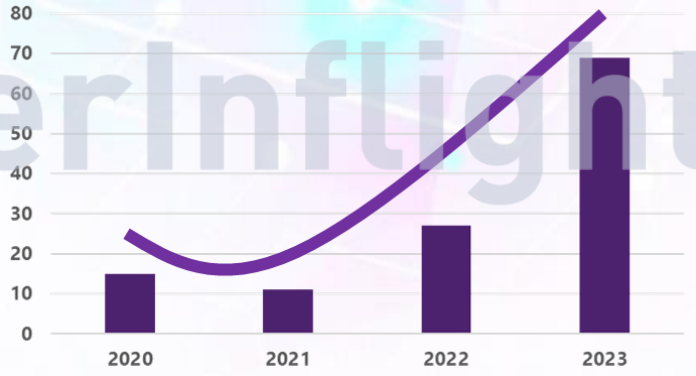
- **Observation bias**: The more we look, the more we find pieces of information.
- **Recency effect**: We tend to observe and remember more recent events.
- **Media exaggeration**: We challenge the way media cover information.
- **Definition of a cyberattack**: How you define a cyberattack defines how you count them (e.g., DDoS is always considered as "noise" among other attacks).
- **Inertia of identification**: Cyberattacks can be discovered or publicly mentioned years after the actual time of the attack. Our database is being regularly revised.

Evolution of the threat landscape:

- **Significant growth rate in the last years** despite potential biases
- Peaks in cyberattacks are **strongly linked to geopolitical events** (2014: annexation of Crimea, 2022: start of the war in Ukraine)
- **Evolution in the type of attacks** observed (jamming, spoofing, IA-powered, in-orbit eavesdropping, etc.)
- **A total of 357 cyberattacks against space systems have been identified to date (until July 2024).** 35 already identified in 2024 (considering in-orbit eavesdropping)

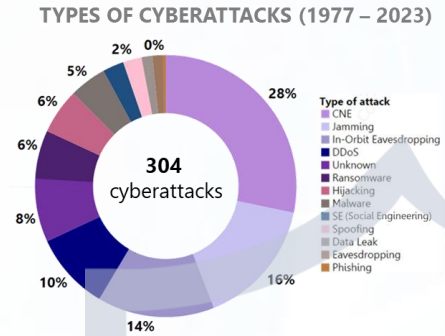
EVOLUTION OF THE NUMBER OF CYBERATTACKS (1977 – 2023)

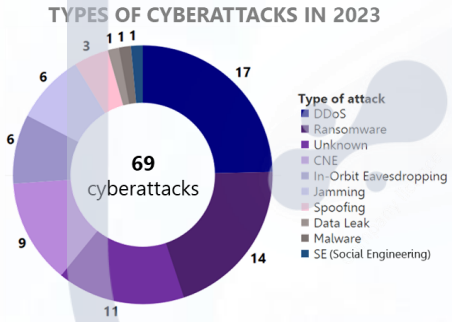
EVOLUTION OF THE NUMBER OF CYBERATTACKS ON THE SPACE DOMAIN (2020 – 2023)

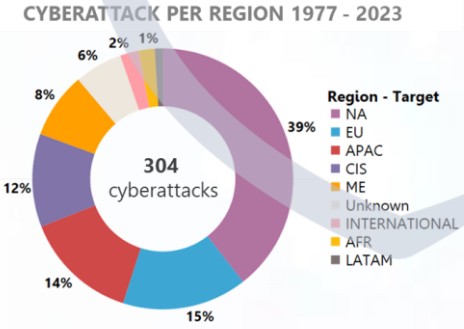


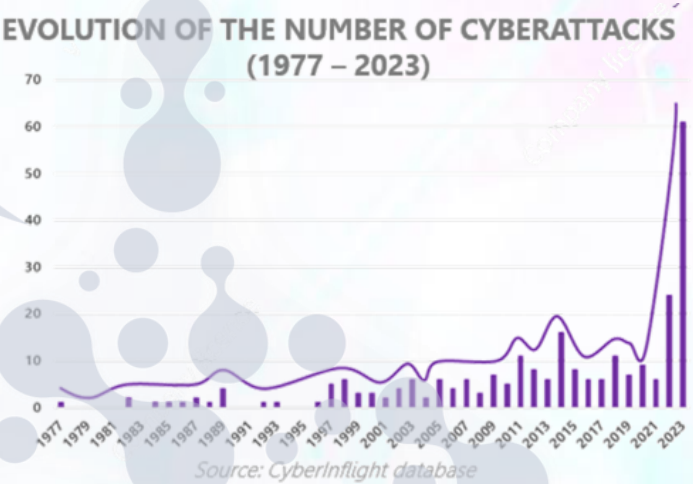
Source: CyberInflight database

Threat landscape indicators

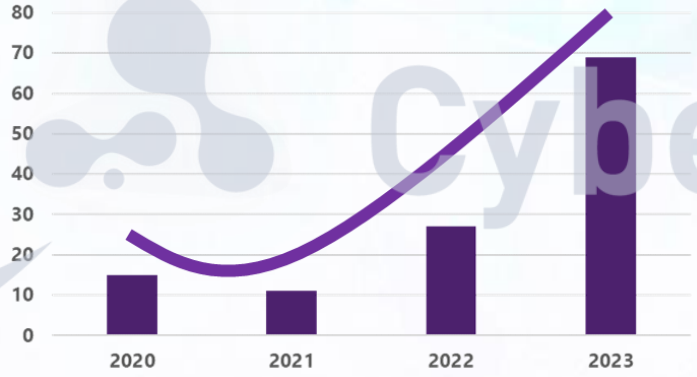




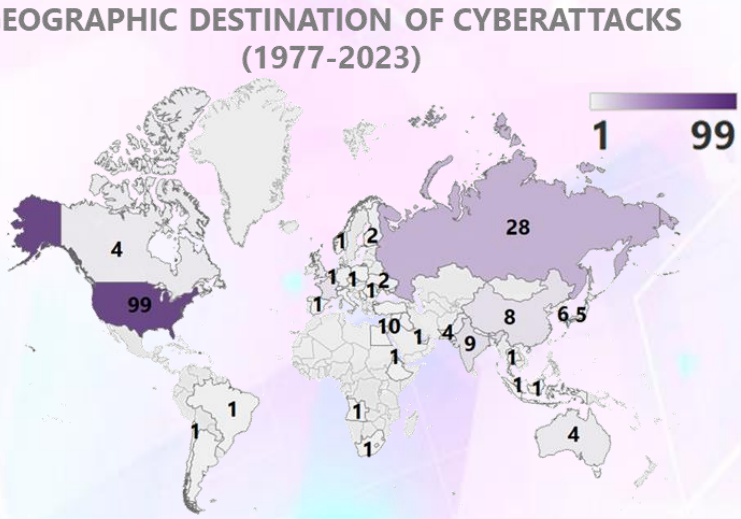


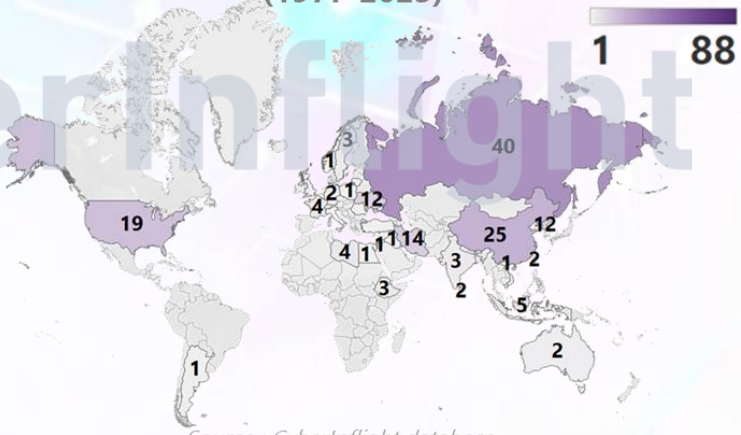


Source: CyberInflight database



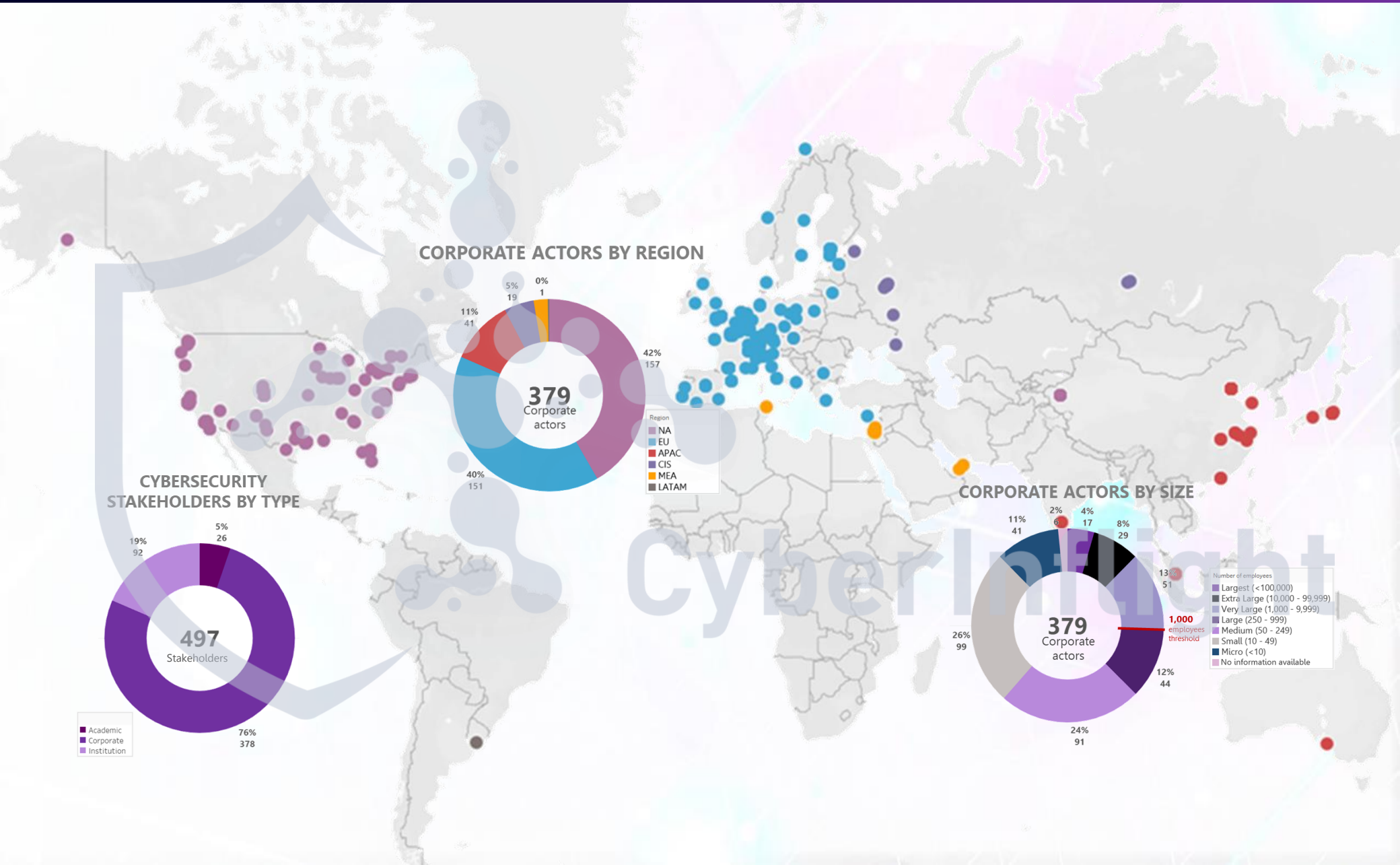
Source: CyberInflight database





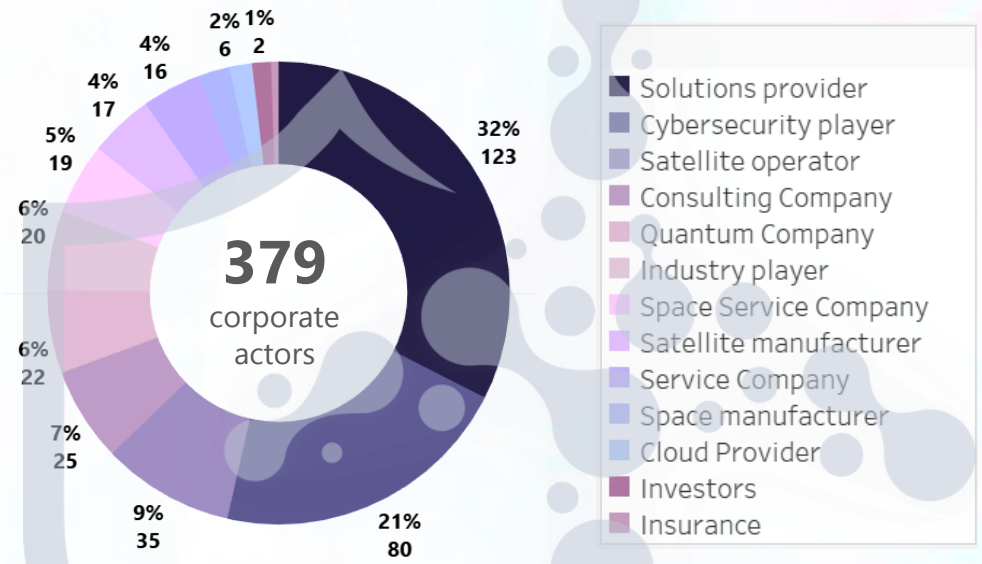
Source : CyberInflight database

Overview of the ecosystem

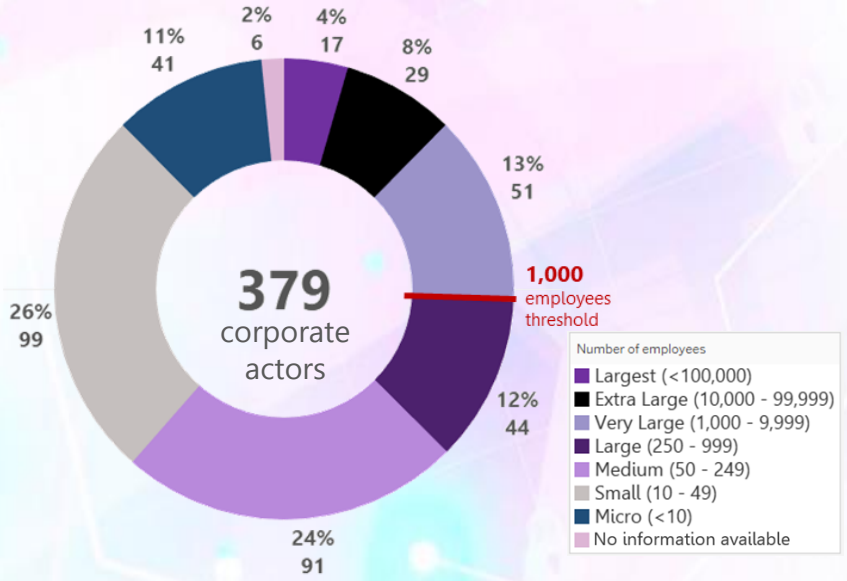


Overview of the corporate ecosystem

CORPORATE ACTORS BY ACTIVITY



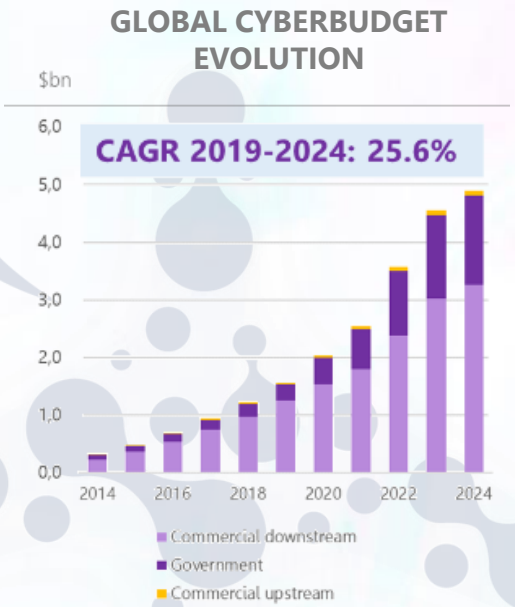
CORPORATE ACTORS BY SIZE

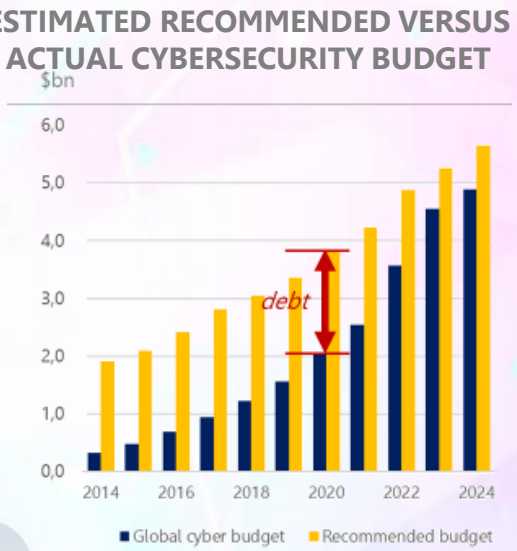


A competitive space cybersecurity market

- An increasing number of stakeholders are demonstrating **space-cybersecurity initiatives** (from 189 at YE2022 to 379 at YE2023). **Pure cybersecurity players** enter the space market, and **more space companies** tend to cybersecure their operations.
- **Increasing dual-use** (civil/defense) for stakeholders of space cybersecurity contracts.
- More **sovereignty considerations** for contractual agreements.
- **More implication and maturity of the supply chain** through the pressure of buyers or dedicated programs (IA-PRE, CMMC, future EUSL, etc.)

Space cybersecurity economy



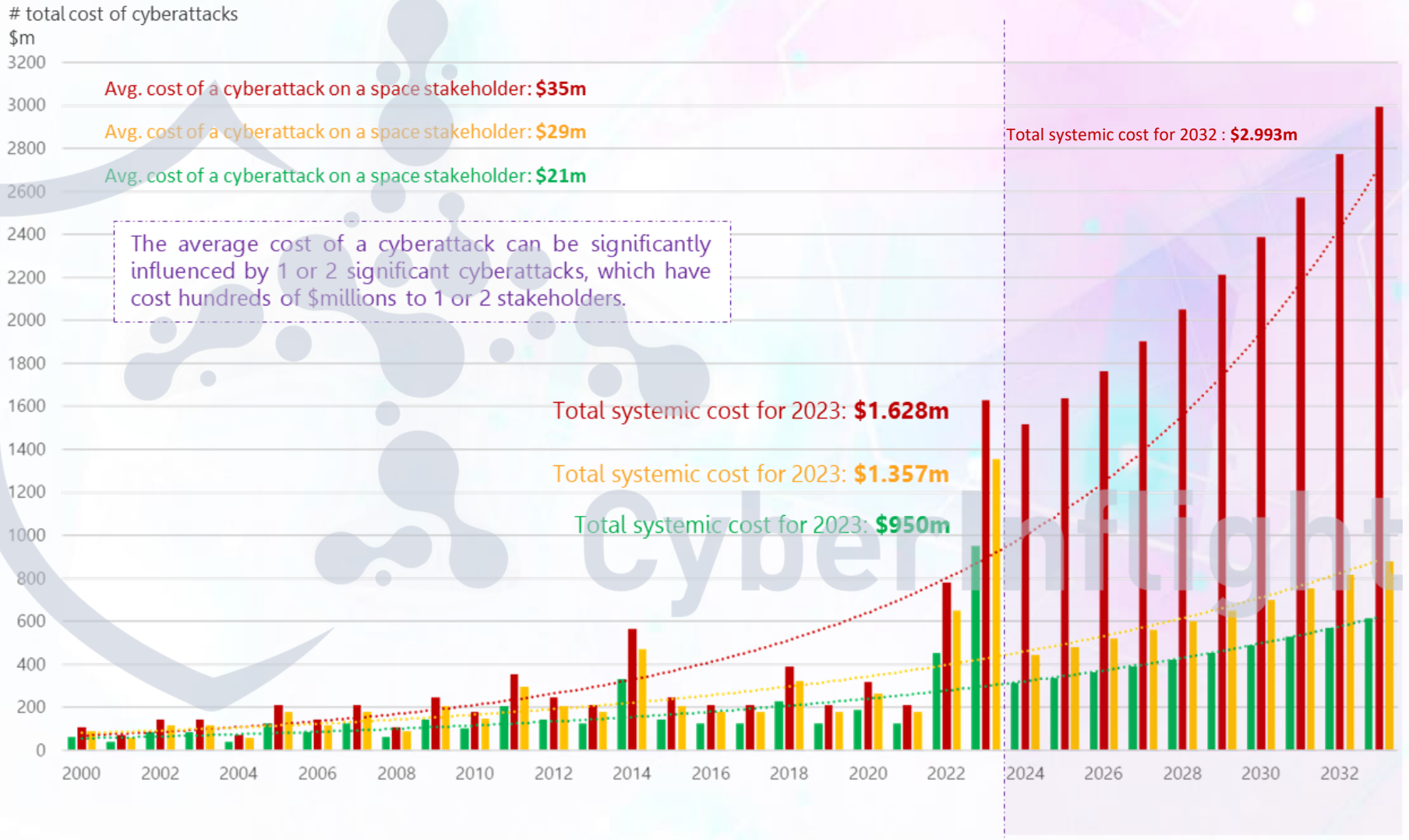


A globally positive market, though locally challenging:

- A top-down approach allows for estimating the **overall space cybersecurity market value**.
- It is estimated that the space cybersecurity dedicated budget will be **close to $5bn by YE2024.** Future major programs may significantly impact this budget (IRIS^2 ~€2.5m total)
- This global cybersecurity budget is, on average, still lagging behind average security agency's recommendations, triggering the **accumulation of cybersecurity debt.** This debt is forecasted to **peak by 2027**, and an **inflection point will occur from that point onward.**
- The **economic situation varies for the different types of actors** or in **other regions** of the world (competitive landscape, cyclical programs, EU vs US, among other factors).

Forecast of cyberattacks against the space sector
Systemic cost to the space industry from 2023 to 2033

3 SCENARIOS OF THE EVOLUTION OF CYBERATTACKS AGAINST THE SPACE DOMAIN



Space Cybersecurity Market Intelligence report supporting databases

5 MAIN DATABASES

357 cyberattacks reported publicly from 1977 to 2024

Cyberattack database
Updated on July 1, 2024

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

Space Cybersecurity actors database
Updated on July 1, 2024

229 contracts from five regions of the world (**A**sia**PAC**ific, **EU**rope, **Mid**dle **E**ast & **A**frica, **C**ommonwealth of **I**ndependent **S**tates and **N**orth **A**merica)

Contract database
Updated on July 1, 2024

116 regulations worldwide in the fields of space cybersecurity

Regulation database
Updated on July 1, 2024

Estimation of space cybersecurity budgets from 2015 to 2034

Space cyber Economy database
Updated on July 1, 2024


Contact us at contact@cyberinflight.com