

2nd Edition

Published Q1 2024



SPACE CYBERSECURITY

Market Intelligence Report





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:



1st

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

Founding member of:

#EUSpaceISAC



ABOUT US



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 (Asia/PACific, Europe, Middle East/North Africa and North America)
Contract database
Updated on June 1st 2023
- Estimation of space cybersecurity budgets from 2018 to 2020
Space cyber Economy database
Updated on May 2023

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

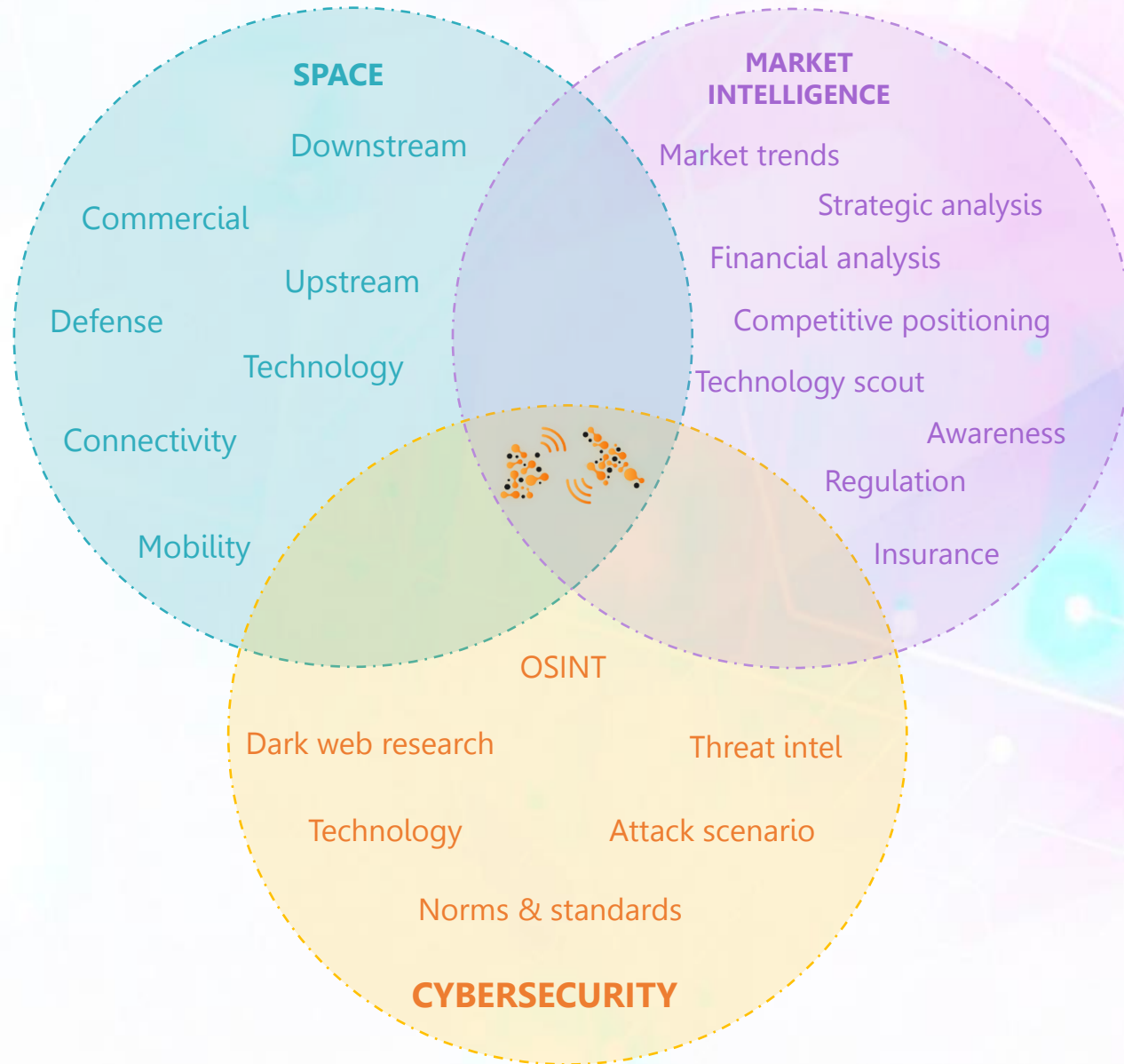


Aerospace
industry
leaders



European &
International
stakeholders

Our vision



A strategic report on Space Cybersecurity

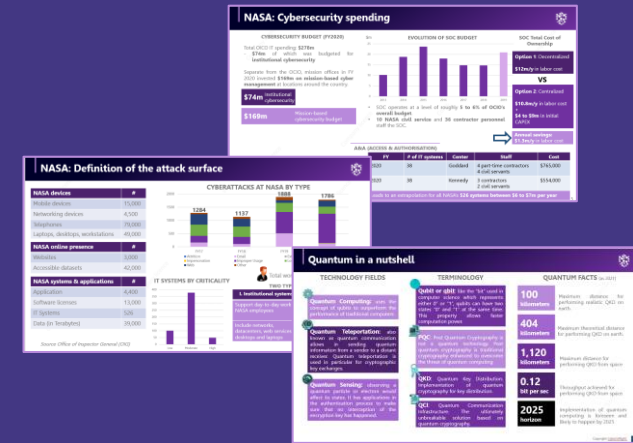


OUR STRATEGIC REPORTS



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)



Executive Summary	1	Case 1: Eavesdropping Athena-Fidus communications	40	List of corporate actors involved in space cybersecurity – APAC region	83	NIST overview of applicable guidance to space value chain	131
Acronym Table	3	Case 2: ROSAT satellite attack allegations	41	List of corporate actors involved in space cybersecurity – CIS region	84	Space Overlay and NIST SP 800-53 Rev. 5	132
Table of content	5	Case 3: Interfering with US satellites (Landsat-7, Terra EOS)	42	List of corporate actors involved in space cybersecurity – MEA & LATAM regions	85	Space overlay overview	133
CHAPTER I. INTRODUCTION	7	Case 4: Jamming satellite signals	43	Corporate space cybersecurity actors	86	NISTIR 8323 overview	134
Introduction to the space economy	8	Case 5: Intrusion of IT systems	44	The soar of Space Forces	89	NISTIR 8270 overview	135
Observed trends in the space sector	9	Case 6: Takeover and spoofing	45	Space Delta 6 (known as Cyber Delta or DEL6)	90	NISTIR 8401 overview	136
New Space and innovation	10	Case 7: Software bugs	46	Space Delta 7 (DEL 7)	91	CCSDS: Introduction	137
Main positioning and navigation services overview	11	Case 8: Supply chain compromise	47	Space ISAC: a keystone for information sharing	92	CCSDS: SEA-SEC	138
Main connectivity technologies overview	12	Case 9: NASA cybersecurity breach	48	US Space ISAC overview	94	ECSS (European Cooperation for Space Standardization) & BSI (Federal Office for Information Security)	139
The booming economy of space data	13	Case 10: South Korean satellite network attack	49	EU Space ISAC overview	95	Tallinn Manual 2.0 & Budapest Convention	141
Cybersecurity principles	14	Case 11: NewSat cyberattack	51	Mapping of corporate actors	98	NIS v2	142
The global cybersecurity market	15	Case 12: Starlink under attack	52	Mapping of institutional actors	99	IA-PRE	143
Cybersecurity principles for space systems	16	Tobol System	56	Mapping of academic actors	100	HSN & Space policy	144
Increasing recognition of space cybersecurity	17	Case 13: DDoS cyberattack and the space domain	62	CHAPTER IV. SPACE CYBERSECURITY ECONOMY	101	CNSSP-12 & SPD-5	145
More assets in space: a broader attack surface	18	Case 14: Centre Planeta	63	Introduction, methodology & market value estimation	102	Recognizing Space as a “Critical Infrastructure”	146
Evolution of cyberattacks against the space sector	19	Miscellaneous: NASA incident list	64	Space Cybersecurity market value	103	Common criteria & Other Guidance	148
Viasat: a turning point in space cybersecurity	20	Overview of the recent Viasat/KA-SAT cyberattack	65	Forecast of IT and cybersecurity budget	104	LOS – Law on Space Operations	149
Overview of the threat landscape	21	Demystifying cyberattacks in space	68	The space cybersecurity debt	105	METI – Cybersecurity Guidelines	150
Lack of skilled workforce: a major challenge	22	Geopolitics and Space: the growth of cyber threats	69	Different market visions	107	Australia Space Strategy	151
A new battlefield	23	GNSS/GPS and cyberattacks	70	Forecast from 2023 to 2033	108	Russian approach to standards in the space industry	152
CHAPTER II. THREAT INTEL. & CYBERATTACKS EXAMPLES	25	Space-cyber warfare	72	Systemic cost forecast from 2023 to 2033	109	European Union Space Strategy for Security and Defense	153
Introduction	26	The media aspect	73	Overview of significant space cybersecurity contracts	110	EU Space Law	154
Overview of cyberattacks on space ecosystem	27	Examples of regional space threat players	74	European Space Cybersecurity Ecosystem	111	SPARTA: Space Attack Research & Tactics	158
Space cyberattack landscape	28	CHAPTER III. SPACE CYBERSECURITY STAKEHOLDERS	75	Italian Space Cybersecurity Ecosystem	112	Analytics	159
2023 Space cyberattack landscape: types of cyberattacks	30	Introduction & Methodology	76	French Space & Cybersecurity Ecosystems	113	SPARTA v1.4 and v1,5 – Recent updates	159
Space cyberattack landscape (1977-2023)	31	List of universities involved in space cybersecurity	77	NASA Budget FY2024	114	Space SHIELD framework	160
Space cyberattack landscape: targeted segment	32	List of institutions involved in space cybersecurity – Europe region	78	NASA Future Actions	116	US: new strategies, new policies, new frameworks	161
Space cyberattack landscape: approach by countries	33	List of institutions involved in space cybersecurity – North America region	79	NASA Cybersecurity Progress	117	Introduction to EXPORT-CONTROL	163
Space cyberattack landscape: regional approach	35	List of institutions involved in space cybersecurity – APAC, CIS regions & others	80	NASA Cybersecurity Initiatives	118	EU and US EXPORT-CONTROL	164
2023 space cyberattacks landscape: motivation	37	List of corporate actors involved in space cybersecurity – North America region	81	NASA’s Pathway to Zero Trust	119	US EXPORT-CONTROL overview	165
2023 space cyberattack landscape: cyberattack credibility level	38	List of corporate actors involved in space cybersecurity – Europe region	82	Space Agencies Budget around the world	120	Takeaways on EXPORT-CONTROL from a satellite manufacturer	166
In-Orbit Eavesdropping	39			Cybersecurity talent shortage	122	CMMC: Introduction	167
				Colorado Space Cybersecurity Ecosystem	125	CMMC: CMMC levels and domains	168
				CHAPTER V. REGULATORY LANDSCAPE	128	CMMC: rollout phases	169
				Executive Summary	129		
				Most relevant guidance for cyber-space stakeholders	130		

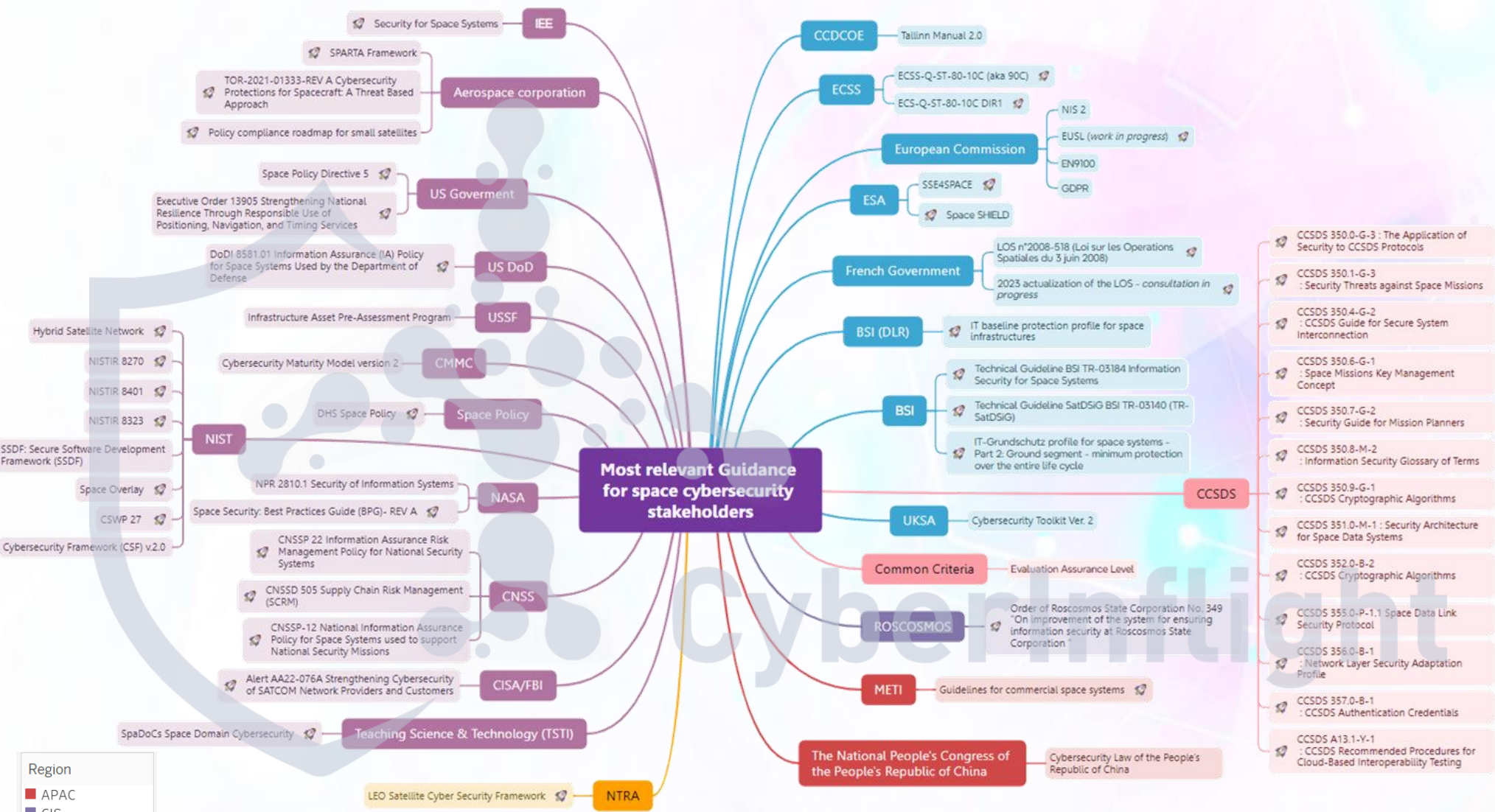
Table of content (2/2)



CMMC version 2.0	170	CHAPTER VII. CASE STUDIES	214	China's Cyber Defensive Capabilities	252	Cyber-insurance: chronology	295
CHAPTER VI. TECHNOLOGY	171	Executive Summary	215	US Space Force (USSF) cybersecurity approach	216	Cyber-insurance: defining the cyber-risk	296
Executive Summary	172	Cybersecurity at NASA	217	The cybersecurity of rocket launchers	218	Cyber-insurance: stakeholders and their influence	297
A word on Satellite Platforms	173	NASA: Definition of the attack surface	218	US Defense Industrial Base	219	Cyber-insurance: conventional VS specific cyber-contract	298
SWaP (Size, Weight and Power)	175	NASA: General & Cybersecurity spending	219	DIBs around the world	220	APPENDIX – LIST OF CORPORATE ACTORS	299
The evolution of hardware technology in space: ARM & RISC architecture	177	NASA: SOC cybersecurity spending	221	AsterX	221		
The evolution of hardware technology in space: FPGA (Field Programmable Gate Array)	178	NASA: OIG recommendations	222	AsterX 2024	222		
The evolution of hardware technology in space: SDR (Software Defined Radio) & SDS (Software Defined Satellite)	179	Starlink: an efficient DevSecOps approach	222	OPS-SAT on-orbit satellite hacking demonstration	223		
Other cybersecurity technologies for space systems: Lightweight cryptography (LWC) and hardware security module (HSM)	180	Russian Space Cybersecurity Landscape	223	Hack-A-Sat 4	223		
Cryptography tradeoff for space applications	181	Introduction	223	RETEX from Hack-A-Sat 4: HaS-4	224		
Ground Segment security: Introduction	182	List of Acronyms	224	The future of cyber warfare: Several new trends and types of cyberattacks	225		
Ground Segment security: Overview	183	Roscosmos Information Security - Zarya NTC	225	Thunderlight and the future of cyber warfare	226		
Ground Segment security: Examples of cyberattacks	184	Zarya NTC and the Russian Space Industry	226	Introduction to Thunderlight	227		
Cloud Security in space	185	SOPKA-Roscosmos	227	Impact estimation and security costs estimation studies	227		
Space Software & Operating Systems	186	GoSOPKA System	228	Reasons for running this simulation	228		
Quantum in a nutshell	190	Russian Information Security Regulation Landscape	228	Direct and indirect impacts estimation study	229		
Quantum technologies	191	Russian Space Cybersecurity Sector Trends	229	Security costs implementation estimation study	230		
Quantum Security	194	Russian Space Cybersecurity Mapping	230	Initial security costs estimation study	231		
Building up quantum projects	196	Russian Electronic Warfare Industry Landscape	231	Impacts estimation and security measures estimation studies	232		
Quantum supremacy: Europe	197	Chinese Space cybersecurity landscape	232	Comparison	233		
Quantum supremacy: China	198	Introduction (1/2)	233	CHAPTER VIII. MISCELLANEOUS	234		
Quantum supremacy: USA	199	List of Acronyms	234	Introduction: Defining the cyber risk score	235		
European Quantum projects	200	Introduction (2/2)	235	Company profile: GSaaS company	236		
National Quantum strategies in Europe	202	The West and China: two different visions of the world	236	Company profile: Space service company	237		
EU Space Security Programs	205	Chinese State cybersecurity and space stakeholders	237	Company profile: Cybersecurity player	238		
EU Space Security Programs: IRIS ² (Infrastructure for Resilience, Interconnectivity and Security by satellite)	206	Chinese space cybersecurity stakeholders	238	Rise of Space Cybersecurity in South Korea	239		
EU Space Security Programs: EGNOS (European Geostationary Navigation Overlay Service)	207	Chinese cybersecurity and space industries evolution	239	Space cybersecurity conferences	240		
SpiderOak and Space Cybersecurity	208	China: A Global Space Cybersecurity Player	240	Space cybersecurity conference maps	241		
SpiderOak Dynamic Trust Platform: To Secure Application Development within Space Organizations	209	Chinese Strengths and Weaknesses	241	Overview of the 2022 CYSAT conference (2 nd edition)	242		
SAIC/SDA: Secure Satellite Software Factory	210	BeiDou Navigation Satellite System	242	Overview of the 2023 CYSAT conference (3 rd edition)	243		
ARCA Satcom – To secure satellite communications	211	China's Cyber Offensive Capabilities	243	Cyber-insurance: introduction	244		
Cyber-range and satellite systems	213		244	Cyber and space insurance	245		
			245	Satellite insurance	246		



Most relevant guidance for cyber-space stakeholders



- Region
- APAC
 - CIS
 - EU
 - International
 - LATAM
 - MEA
 - NA



Technology Executive Summary (excerpt)



The ever-increased demand for higher performance

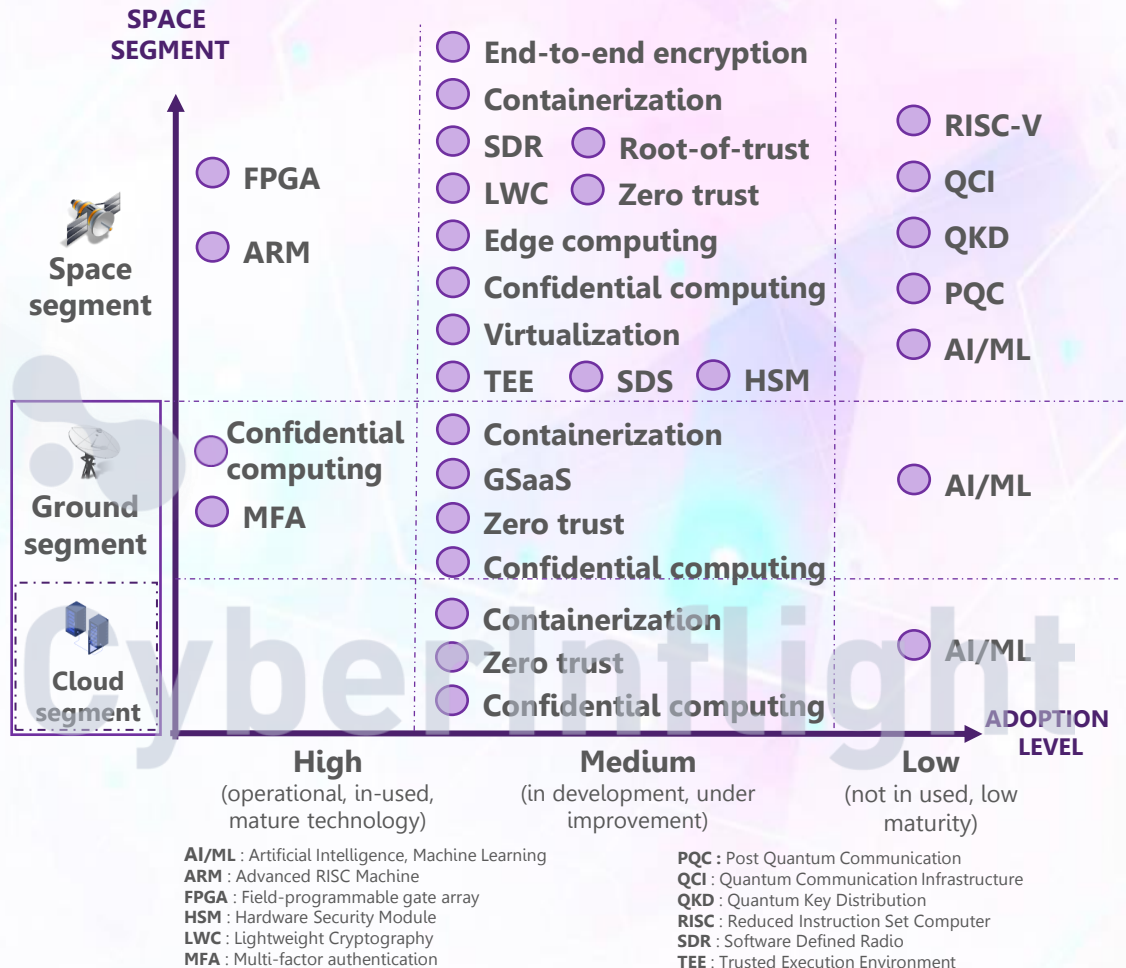
The increasing demand for data and reliance on space applications drives the need to process more data on board and transmit it to the ground. **New technologies are being developed to achieve higher performance, increased throughput, and secure communications.** This involves **improving existing technologies** (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



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.

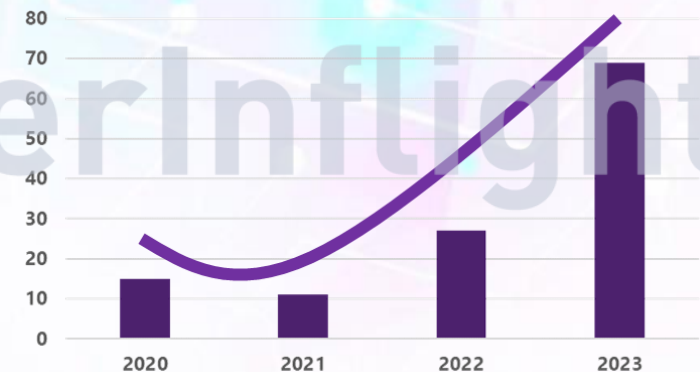
Evolution of the threat landscape:

- **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)

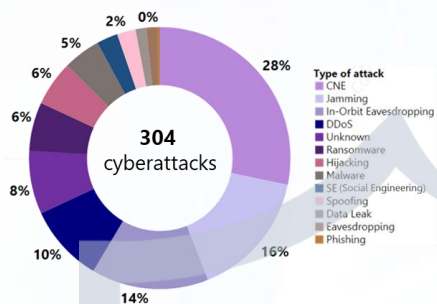


Source: CyberInflight database

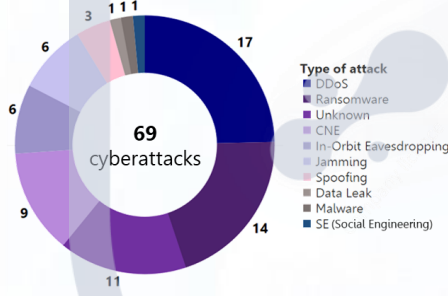
Threat landscape indicators



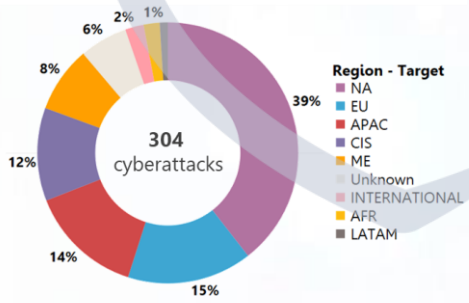
TYPES OF CYBERATTACKS (1977 – 2023)



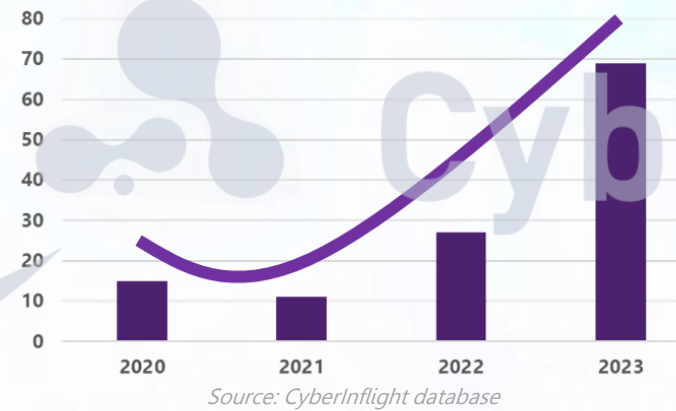
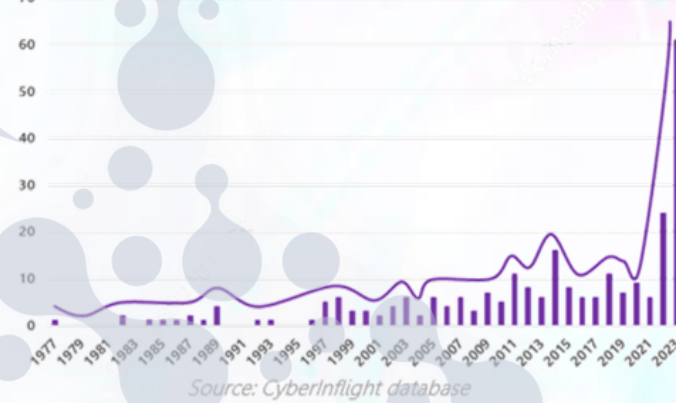
TYPES OF CYBERATTACKS IN 2023



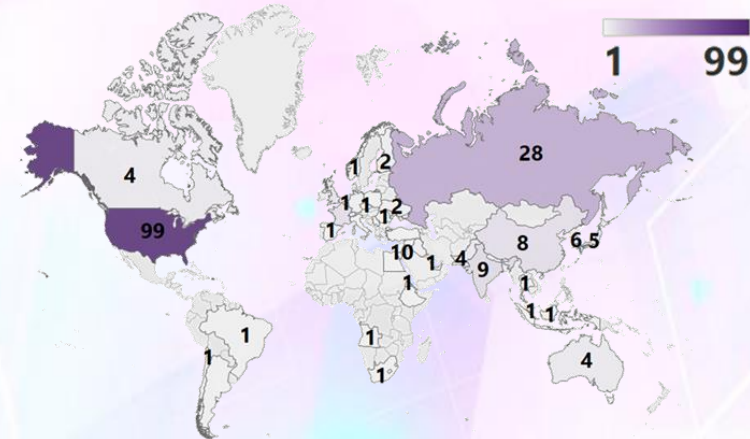
CYBERATTACK PER REGION 1977 - 2023



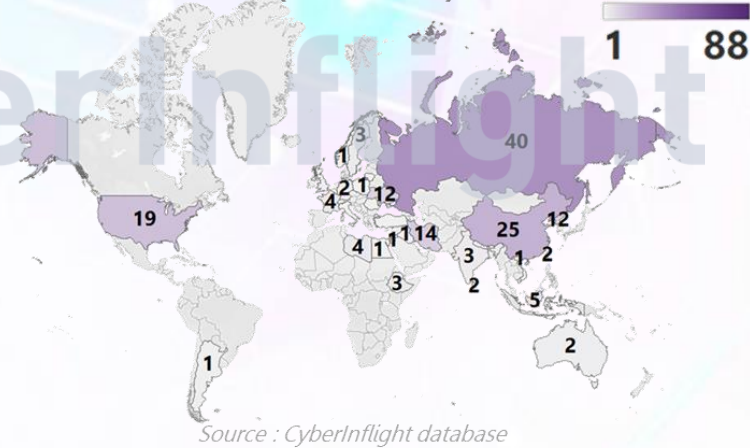
EVOLUTION OF THE NUMBER OF CYBERATTACKS (1977 – 2023)



GEOGRAPHIC DESTINATION OF CYBERATTACKS (1977-2023)



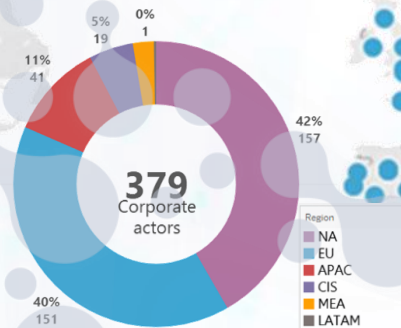
GEOGRAPHIC ORIGIN OF CYBERATTACKS (1977-2023)



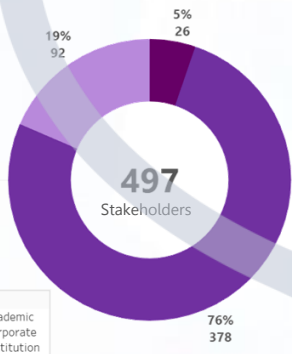
Overview of the ecosystem



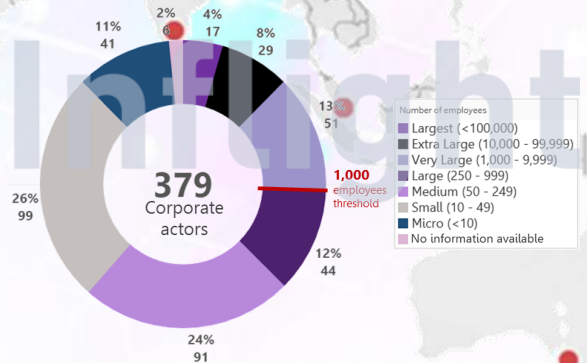
CORPORATE ACTORS BY REGION



CYBERSECURITY STAKEHOLDERS BY TYPE



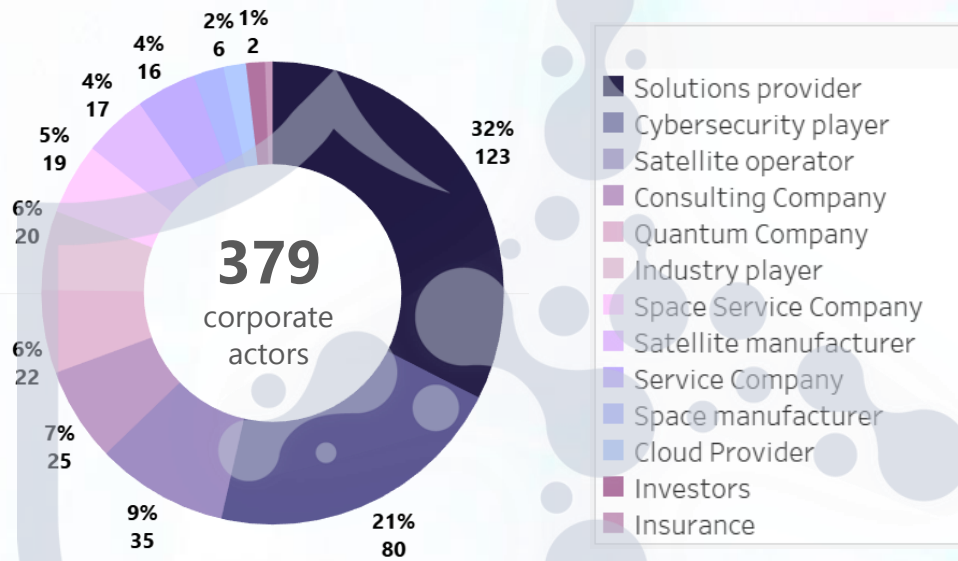
CORPORATE ACTORS BY SIZE



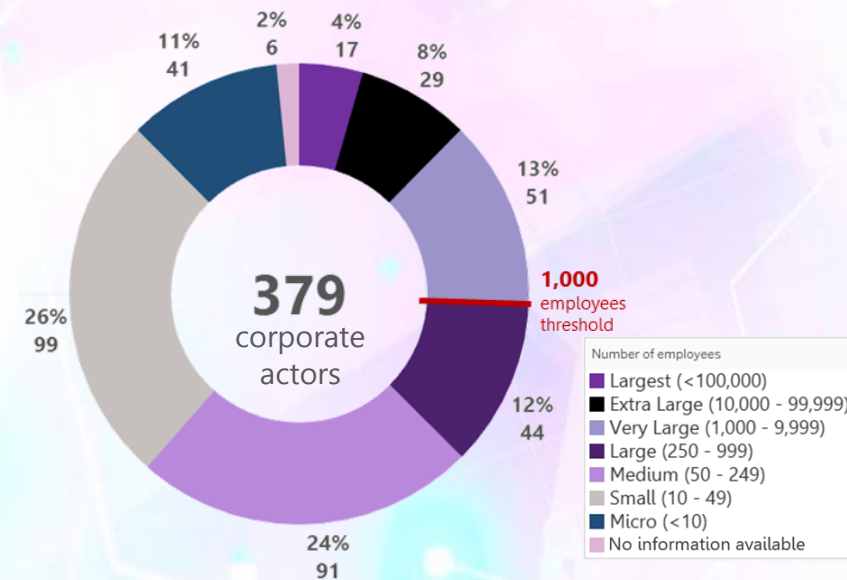
CyberInflight



CORPORATE ACTORS BY ACTIVITY

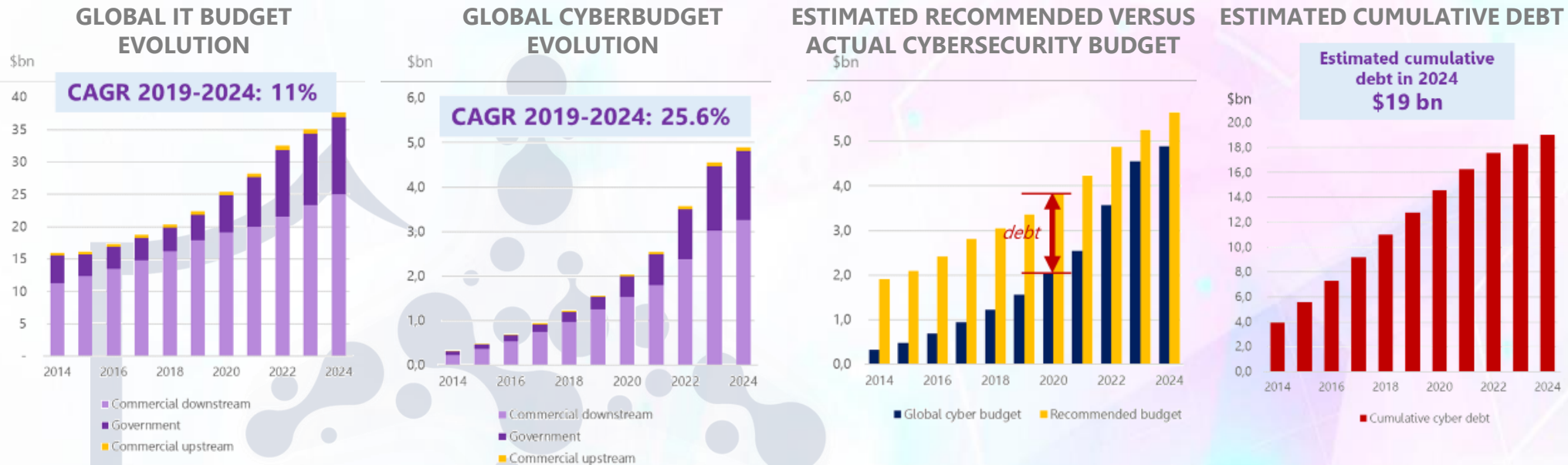


CORPORATE ACTORS BY SIZE



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.)



A globally positive market, though locally challenging:

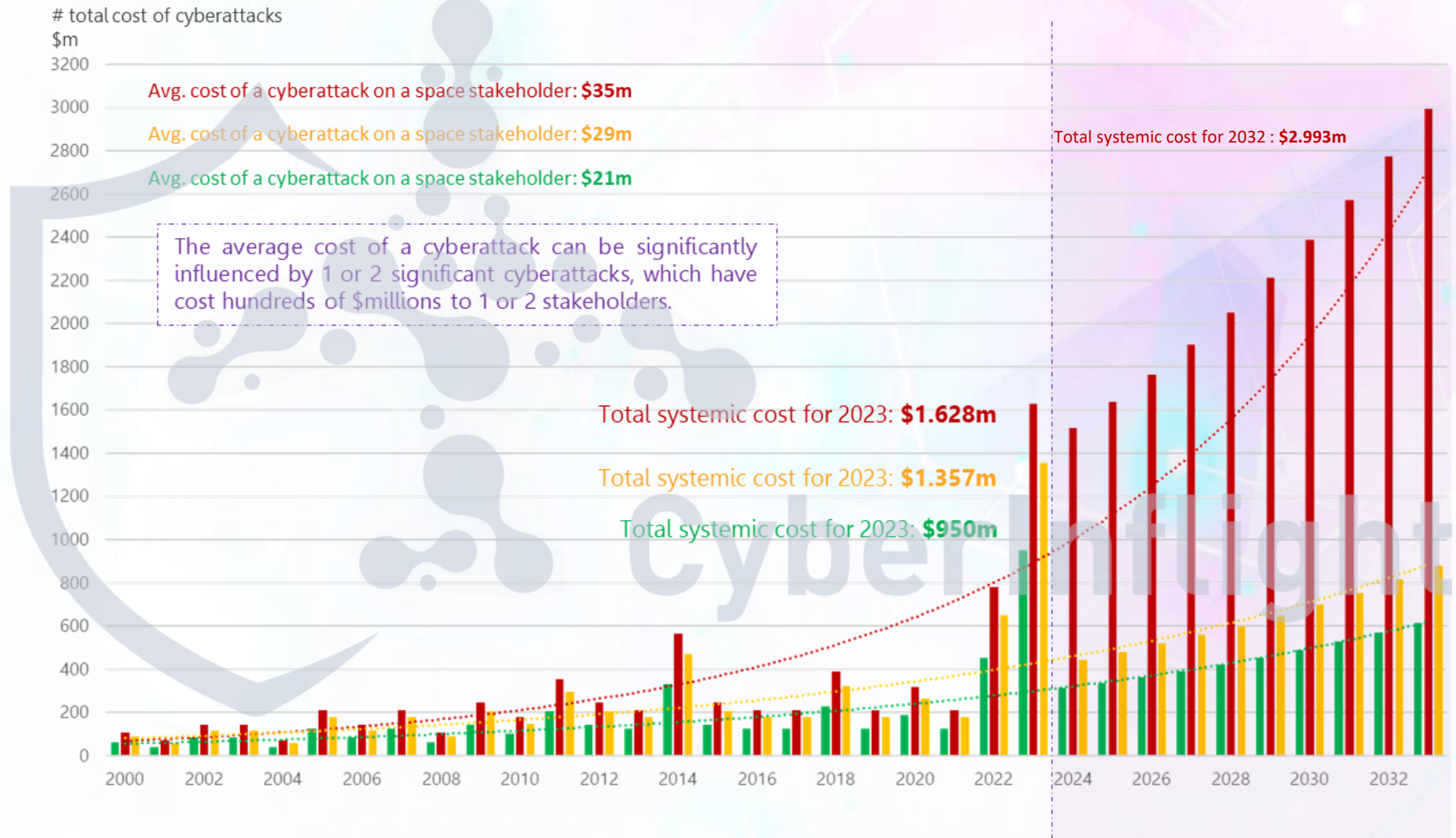
- A top-down approach allows for estimating the **overall space cybersecurity market value**.
- It is estimated that the space cybersecurity dedicated budget will be **close to \$5bn by YE2024**. Future major programs may significantly impact this budget (IRIS² ~€2.5m total)
- This global cybersecurity 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





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**P**acific, **E**Urope, **M**iddle **E**ast & **A**frica, **C**ommonwealth of Independent States 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