

4<sup>th</sup> Edition  
2026



# SPACE CYBERSECURITY

Market Intelligence Report



# Table of content (1/3)



|                                                             |           |                                                                                                  |    |                                                                                                |     |                                                                            |            |
|-------------------------------------------------------------|-----------|--------------------------------------------------------------------------------------------------|----|------------------------------------------------------------------------------------------------|-----|----------------------------------------------------------------------------|------------|
| Executive Summary                                           | 1         | Cyber-threat intelligence in the space domain                                                    | 38 | Satellite constellations: Starlink under attack                                                | 72  | Cyber-threats and the supply chain - Software supply chain threat overview | 129        |
| Acronym Table                                               | 3         | Geopolitics and space - The rise in cyberattacks                                                 | 39 | Cyber-threats targeting ISL Links                                                              | 78  | Case of a satellite suffering a supply chain attack                        | 130        |
| Table of contents                                           | 6         | Threat intelligence in the space domain - Overview of cyberattacks on the space domain           | 40 | Simulating the threat                                                                          | 79  | Threat landscape and the network segment                                   | 131        |
| <b>CHAPTER I. INTRODUCTION</b>                              | <b>9</b>  | Space cyber-threat landscape                                                                     | 41 | NASA's open-source CryptoLib vulnerabilities                                                   | 80  | Intrusion of IT systems                                                    | 132        |
| Introduction to the space economy                           | 10        | 2025 Space cyber-threat landscape - Attacker' motivation                                         | 52 | Threat landscape and the end-user segment - SFX2100 CVE                                        | 83  | NASA incident list                                                         | 133        |
| An overall rise in the governments' space budget since 2022 | 11        | 2026 Space cyber-threat landscape - Credibility level                                            | 53 | Starlink terminal vulnerability                                                                | 84  | OpenC3 COSMOS                                                              | 134        |
| Observed trends in the space sector                         | 13        | Critical Vulnerability Exposure                                                                  | 54 | Threat lanscape and the signal segment - Overview                                              | 85  | gr-satellites v5.8.0 vulnerability assessment by VisionSpace               | 136        |
| Sovereignty stakes in space                                 | 16        | DoS attacks against the space domain                                                             | 55 | Threat landscape, electronic warfare, and the signal segment                                   | 86  | YAMCS vulnerabilities                                                      | 137        |
| Main positioning and navigation services overview           | 18        | Threat landscape and the ground segment - Key statistics                                         | 56 | In-orbit eavesdropping                                                                         | 88  | South Korean satellite network under attack                                | 138        |
| The booming economy of space data                           | 19        | NewSat cyberattack - 2013                                                                        | 57 | Eavesdropping on Athena-Fidus communications                                                   | 89  | Overview of the Viasat/KA-SAT cyberattack                                  | 140        |
| Main connectivity technologies overview                     | 20        | Overview of cyber-threats on the launch base - Launch operations stakeholders' overview          | 59 | GNSS Interferences                                                                             | 90  | Centre Planeta under attack                                                | 143        |
| Cybersecurity principles                                    | 22        | Overview of cyber-threats on the launch base - Launch base facilities and responsibilities       | 61 | Space electronic warfare                                                                       | 93  | Software failures                                                          | 144        |
| The global cybersecurity market                             | 23        | The launch segment - General threat overview                                                     | 62 | Tobol System: 14Ts227                                                                          | 94  | Space-cyber warfare and modern conflicts                                   | 146        |
| Cybersecurity principles for space systems                  | 24        | Overview of cyber-threats on the launch base - Launch site threat vectors overview               | 63 | Russian Space Electronic Warfare                                                               | 100 | Threat evolution: space-to-ground                                          | 148        |
| Increasing recognition of space cybersecurity               | 25        | Overview of cyberattacks on launch systems - Liftoff and stage separation phases threat overview | 64 | China Space Electronic Warfare                                                                 | 101 | Sindoor operation and the space cyber domain                               | 150        |
| More assets in space: a broader attack surface              | 26        | Neutralizing launch systems                                                                      | 65 | The USSF and Electromagnetic Warfare                                                           | 104 | Midnight Hammer operation and the space-cyber domain                       | 151        |
| Evolution of cyberattacks against the space sector          | 27        | Threat landscape and the space segment                                                           | 66 | Counter Communication System: US Space Force                                                   | 110 | UAE's space domain under attack - 2026                                     | 152        |
| The Viasat attack - A turning point in space cybersecurity  | 28        | ROSAT satellite attack allegations                                                               | 67 | The merger of cyber and electronic warfare                                                     | 118 | Russian cyber and electronic warfare landscape                             | 153        |
| Overview of the threat landscape                            | 29        | Interfering with U.S. satellites (Landsat-7, Terra EOS)                                          | 68 | GNSS/GPS and cyberattacks                                                                      | 121 | Chinese cyber and electronic warfare landscape                             | 154        |
| Hybrid threats against the space sector                     | 30        | SPOT-7                                                                                           | 69 | The rise of electronic warfare - SAR increased targeting                                       | 123 | U.S. cyber and electronic warfare landscape                                | 155        |
| A new battlefield                                           | 31        | Sich-2-30                                                                                        | 71 | The use of electromagnetic warfare against Starlink links                                      | 124 | Space-cyber warfare - Demystifying cyberattacks in space                   | 156        |
| Normalizing space and cyber military operations             | 32        |                                                                                                  |    | Threat landscape and the supply chain - Key statistics                                         | 125 | Space-cyber warfare - The media aspect                                     | 157        |
| Rise of active defense in the space domain                  | 33        |                                                                                                  |    | Cyber-threats and the supply chain                                                             | 126 | <b>CHAPTER III. SPACE CYBERSECURITY STAKEHOLDERS</b>                       | <b>158</b> |
| Lack of skilled workforce: a major challenge                | 34        |                                                                                                  |    | Cyber-threats through the supply chain - Cyber-threats targeting FPGA through the supply chain | 127 | Introduction & Methodology                                                 | 159        |
| <b>CHAPTER II. SPACE CYBER-THREAT INTELLIGENCE</b>          | <b>35</b> |                                                                                                  |    | Supply chain compromise                                                                        | 128 | Space cybersecurity stakeholders – List of corporate actors by regions     | 160        |
| Introduction – Executive Summary                            | 36        |                                                                                                  |    |                                                                                                |     |                                                                            |            |
| Analyzing the threat intel environment                      | 37        |                                                                                                  |    |                                                                                                |     |                                                                            |            |

# Table of content (2/3)



|                                                              |     |                                                                                |     |                                                                                        |     |                                                                   |     |
|--------------------------------------------------------------|-----|--------------------------------------------------------------------------------|-----|----------------------------------------------------------------------------------------|-----|-------------------------------------------------------------------|-----|
| Corporate space cybersecurity actors                         | 165 | Overview of significant space cybersecurity contracts                          | 199 | ESA frameworks: Space SHIELD & SSE4Space                                               | 262 | Overview of Space Security technologies                           | 293 |
| Space cybersecurity stakeholders - Institutions by regions   | 169 | Italian Space Cybersecurity Ecosystem                                          | 202 | Frameworks increasingly addressing resilience in an EW context - SPARTA & Space SHIELD | 263 | Overview of Technology Program and their TRL (ESA GSTP 2026-2028) | 294 |
| Space cybersecurity stakeholders - Academics                 | 172 | French Space and Cybersecurity Ecosystems                                      | 203 | Initiatives from ENISA, ANSSI & BSI                                                    | 264 | Overview of Technology Program and their TRL (ESA GSTP 2022-2025) | 295 |
| The soar of Space Forces                                     | 173 | NASA Budget FY2025                                                             | 204 | ECSS (European Cooperation for Space Standardization)                                  | 265 | Overview of Digital technologies for space resilience             | 296 |
| Delta 6                                                      | 175 | NASA cybersecurity initiatives                                                 | 206 | CMMC: Introduction                                                                     | 266 | The gateway to the space cybersecurity market                     | 297 |
| Delta 7                                                      | 176 | <b>Space Agencies Budget around the world</b>                                  | 207 | CMMC version 2.0                                                                       | 267 | Cybersecurity onboard space-assets                                | 298 |
| Space ISAC: a keystone for information sharing               | 177 | NASA's Pathway to Zero Trust                                                   | 209 | CMMC: CMMC levels and Domains                                                          | 268 | In-Orbit detection and reaction as a rising market                | 300 |
| Emerging trends of Information Sharing Associations          | 179 | Colorado Springs Space Cybersecurity Ecosystem                                 | 210 | CMMC: Rollout phases                                                                   | 269 | Dive into a space detection product's features                    | 301 |
| Regional dynamics of space cybersecurity information sharing | 180 | Talent Shortage                                                                | 213 | CNSSP-12 & SPD-5                                                                       | 270 | Protect & Detect players' overview                                | 303 |
| Space ISAC Overview                                          | 181 | <b>CHAPTER V. FRAMEWORKS' LANDSCAPE</b>                                        | 215 | IA-PRE                                                                                 | 271 | Chinese vision of Onboard Security                                | 304 |
| EU Space ISAC Overview                                       | 182 | Executive Summary                                                              | 216 | Space ISAC and NASA initiatives                                                        | 272 | Mission categorization                                            | 306 |
| Innovative space-cyber actors                                | 183 | Key enablers for frameworks adoption                                           | 219 | HSN & Space Policy                                                                     | 273 | Key Electromagnetic Warfare events in space                       | 307 |
| GSaaS Ground Segment/Station as a Service                    | 184 | Takeaways                                                                      | 223 | NIST overview of applicable guidance to space value chain                              | 274 | Overview of jamming offensive and defensive techniques            | 309 |
| Space Cybersecurity Corporate Landscape                      | 185 | A consolidation of the space ecosystems worldwide                              | 227 | Space Overlay and NIST 800-53 Rev. 5                                                   | 275 | Overview of spoofing and its impacts                              | 310 |
| Space Cybersecurity Institutional Landscape                  | 187 | Harmonizing the frameworks landscape                                           | 231 | Space Overlay overview                                                                 | 276 | Introduction to Cyber-Electronic Warfare                          | 311 |
| Space Cybersecurity Academic Landscape                       | 188 | Lessons learned from other market verticals – Aviation and Maritime ecosystems | 232 | NIST IR 8323 overview                                                                  | 277 | Recommended cybersecurity practices for space stakeholders        | 314 |
| <b>CHAPTER IV. SPACE CYBERSECURITY ECONOMY</b>               | 189 | Recognizing Space as a "Critical Infrastructure"                               | 235 | NIST IR 8270 overview                                                                  | 278 | Overview of mitigations techniques                                | 315 |
| Introduction, methodology & market value estimation          | 190 | Most relevant guidance for cyber-space stakeholders                            | 237 | NIST IR 8401 overview                                                                  | 279 | Set of countermeasures proposed by SPARTA (Aerospace Corporation) | 316 |
| Space cybersecurity market value                             | 191 | NIS2 Directive                                                                 | 238 | Introduction to EXPORT-CONTROL                                                         | 280 | TinyML-Driven models for spacecraft                               | 318 |
| Forecast of space cybersecurity budget                       | 192 | FSOA - French Space Operation Act                                              | 240 | EU and U.S. EXPORT-CONTROL                                                             | 281 | EU space security programs                                        | 320 |
| Average costs of cybersecurity                               | 193 | European Union's approach to Space Security                                    | 242 | U.S. EXPORT-CONTROL overview                                                           | 282 | The cybersecurity tradeoff                                        | 324 |
| Costs of cyberattacks against the space domain               | 194 | EU Space Act                                                                   | 243 | Takeways on Export-Control from a satellite manufacturer                               | 283 | A word on Satellite Platforms                                     | 327 |
| Forecast and geopolitical context                            | 195 | Executive orders 14412 & 14413                                                 | 247 | Common criteria & Other guidance                                                       | 284 | The evolution of hardware technology in space                     | 329 |
| Examples of cybersecurity budget split                       | 196 | Executive order 14144                                                          | 248 | CCSDS: Introduction                                                                    | 285 | Other cybersecurity technologies for space systems                | 332 |
| Observed cybersecurity budget                                | 197 | CNES Cybersecurity hygiene guides                                              | 250 | CCSDS: SEA-SEC                                                                         | 286 | Cryptography tradeoff for space applications                      | 333 |
| A momentum for the space cybersecurity economy               | 198 | BSI IT –Grundschutz for Space Systems                                          | 251 | Tallin Manual 2.0 & Budapest Convention                                                | 287 | Ground Segment security                                           | 334 |
|                                                              |     | Space cybersecurity regulations in the APAC region                             | 253 | <b>CHAPTER VI. TECHNOLOGY</b>                                                          | 288 | Cloud Security in space                                           | 337 |
|                                                              |     | Space cybersecurity regulations approaches in the CIS and MENA regions         | 258 | Executive summary                                                                      | 289 |                                                                   |     |
|                                                              |     | SPARTA : Space Attack Research & Tactics Analytics                             | 259 | Recent key technology space cybersecurity milestones (2024-2026)                       | 290 |                                                                   |     |
|                                                              |     |                                                                                |     | Key space-cyber technological milestones                                               | 291 |                                                                   |     |

# Table of content (3/3)



|                                                                                                                                                           |            |                                                        |     |                                                  |            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|------------|--------------------------------------------------------|-----|--------------------------------------------------|------------|
| Space Software & Operating System                                                                                                                         | 338        | Russian Space Cybersecurity Landscape                  | 399 | OPS-SAT on-orbit satellite hacking demonstration | 457        |
| SAIC/SDA                                                                                                                                                  | 343        | Russian Information Security Regulation Landscape      | 408 | Hack-A-Sat 4                                     | 459        |
| Cyber-range and satellite systems                                                                                                                         | 344        | Russian Space Cybersecurity Sector Trends              | 410 | RETEX from Hack-A-Sat 4                          | 461        |
| ARCA Satcom – To secure satellite communications                                                                                                          | 345        | Russian Space Cybersecurity Mapping                    | 411 | The future of Cyber Warfare                      | 464        |
| SpiderOak and Space Cybersecurity                                                                                                                         | 347        | Russian Electronic Warfare Industry Landscape          | 412 | Thunderlight and the future of Cyber Warfare     | 465        |
| Quantum Executive Summary                                                                                                                                 | 349        | Chinese Space Cybersecurity Landscape                  | 415 | <b>CHAPTER VIII. MISCELLANEOUS</b>               | <b>473</b> |
| Quantum in a nutshell                                                                                                                                     | 351        | The West and China: two different visions of the world | 418 | Introduction: Defining the Cyber Risk Score      | 474        |
| Quantum technologies                                                                                                                                      | 352        | Chinese Cybersecurity and Space Stakeholders           | 419 | Company Profile - RKS                            | 475        |
| Quantum security                                                                                                                                          | 355        | Chinese Cybersecurity and Space Industries Evolution   | 429 | Company profile - Positive Technologies          | 476        |
| Building up quantum projects                                                                                                                              | 358        | China: A Global Space Cybersecurity Player             | 430 | Company profile - Shengbang Security             | 477        |
| NATO's Quantum Positioning                                                                                                                                | 361        | Chinese Strengths and Weaknesses                       | 431 | Regional ecosystem overview - South Korea        | 478        |
| Overview of the Chinese Quantum projects                                                                                                                  | 362        | BeiDou Navigation Satellite System                     | 432 | New space cybersecurity in the U.S.              | 479        |
| Overview of the American positioning on quantum and PQC                                                                                                   | 366        | China Cyber Offensive Capabilities                     | 433 | From drone to satellite cybersecurity            | 480        |
| Quantum projects in the U.S.                                                                                                                              | 369        | China Cyber Defensive Capabilities                     | 436 | Space Cybersecurity Conferences                  | 481        |
| European positioning on quantum and PQC                                                                                                                   | 370        | NATO and Space Cybersecurity                           | 437 | Space Cybersecurity Conferences Maps             | 484        |
| European Quantum Projects                                                                                                                                 | 371        | GNSS threats and security                              | 439 | Cyber-insurance - Introduction                   | 488        |
| National Quantum Strategies and Projects in Europe                                                                                                        | 377        | Galileo's cybersecurity                                | 440 | Cyber & Space insurance                          | 490        |
| <b>CHAPTER VII. CASE STUDIES</b>                                                                                                                          | <b>385</b> | GPS cybersecurity                                      | 441 | Satellite Insurance                              | 491        |
| Introduction                                                                                                                                              | 386        | US Space Force cybersecurity approach                  | 442 | Cyber insurance                                  | 492        |
| Evaluating leading powers' capabilities in space cybersecurity                                                                                            | 388        | Cybersecurity at NASA                                  | 444 | Appendix                                         | 496        |
| Examples of threat scenarios against the space domain – The Black Box approach                                                                            | 390        | NASA: Definition of the attack surface                 | 445 |                                                  |            |
| Examples of threat scenarios against the space domain - Fictional scenario for illustrating the convergence of cyber and electromagnetic threats in space | 391        | NASA: General & Cybersecurity spending                 | 446 |                                                  |            |
| Examples of threat scenarios against the space domain - Scenario of a drone intercepting a Wi-Fi network                                                  | 392        | NASA: SOC cybersecurity spending                       | 447 |                                                  |            |
| Examples of threat scenarios against the space domain - Takeaways                                                                                         | 393        | NASA: OIG recommendations                              | 448 |                                                  |            |
| Examples of threat scenarios against the space domain - Synthetic view of the space threats landscape                                                     | 394        | Starlink: an efficient DevSecOps approach              | 449 |                                                  |            |
|                                                                                                                                                           |            | Cobra Gold War exercise                                | 450 |                                                  |            |
|                                                                                                                                                           |            | AsterX                                                 | 451 |                                                  |            |
|                                                                                                                                                           |            | AsterX 2024                                            | 452 |                                                  |            |
|                                                                                                                                                           |            | U.S. Defense Industrial Base                           | 453 |                                                  |            |
|                                                                                                                                                           |            | DIBs around the world                                  | 455 |                                                  |            |
|                                                                                                                                                           |            | The cybersecurity of rocket launchers                  | 456 |                                                  |            |

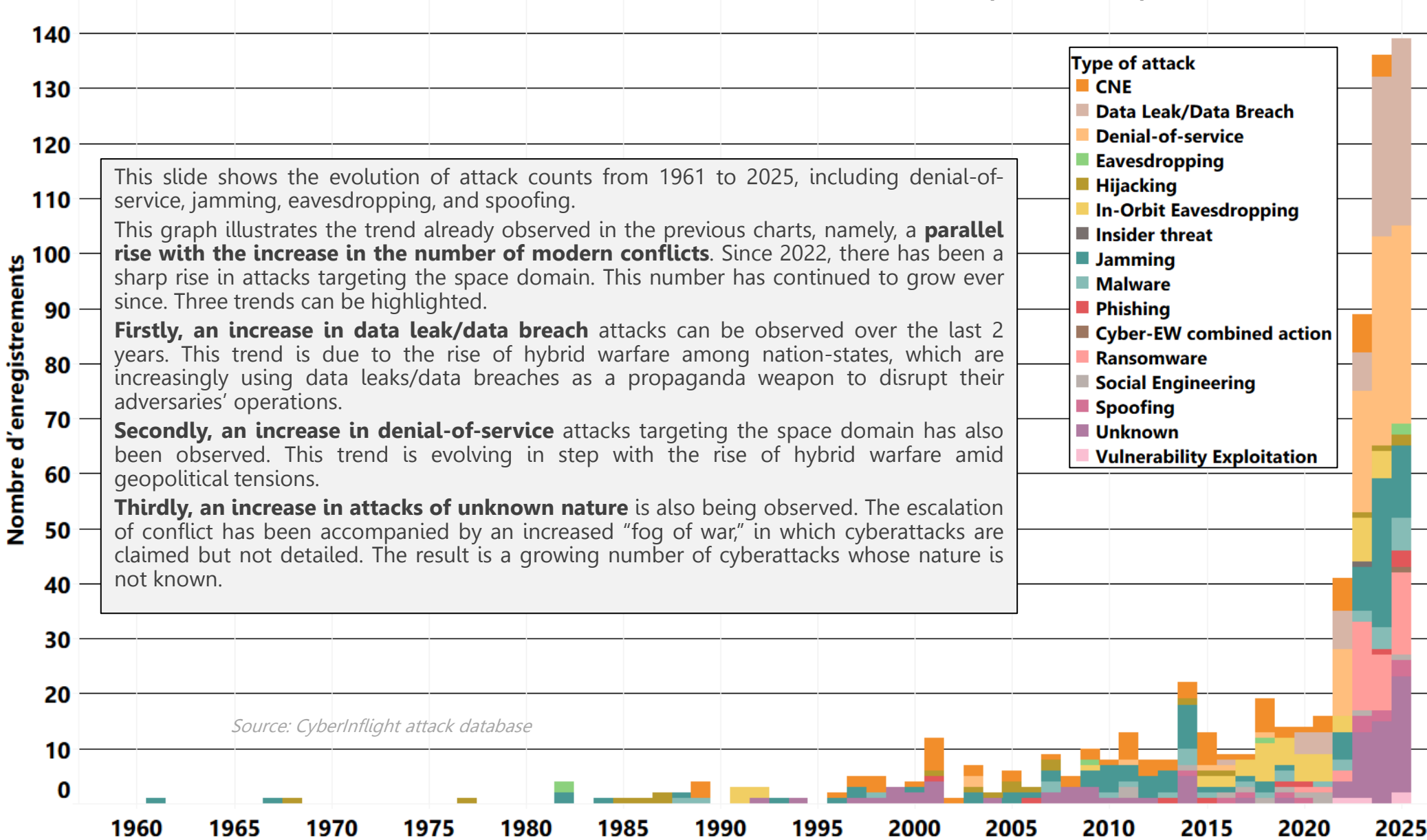
# Space cyber-threat landscape

## Evolution of the number of attacks (2/2)



### EVOLUTION OF THE NUMBER OF ALL TYPES OF ATTACKS (1961 – 2025)

Written on August 25, 2026



# Threat landscape and the signal segment

## Overview of the threat targeting the signal segment



Written on July 21, 2026

**154** Interferences events targeted the signal segment from 1961 to 2026.

### OFFENSIVE ACTIONS (1961 – 2026)

**50%** Of the attacks targeting the signal segment occurred after February 2022.

**63%** Of the attacks corresponded to jamming

**33%** Of the interference events corresponded to In-Eavesdropping

### REGIONS TARGETED AND ORIGINS OF ATTACKS

**56%** Of the attacks came from Russian Electronic Warfare Units and intelligence agencies (FSB, GRU)

**13%** Of the attacks came from U.S. Electronic Warfare Units

### ATTACKS MOTIVATIONS

**50%** Of the attacks targeting the signal segment were driven by political motives.

**33%** Of the attacks targeting the signal segment were driven by state espionage motives

**26%** Of the attacks targeting the supply chain were driven by military motives.

Source: CyberInflight database

### Targeting the signal segment

The signal segment represents **the oldest and most direct pathway for conducting an attack in the space domain**. The first attacks against the signal segment occurred in the 1960s, when Soviet fishing ships equipped with SIGINT antennas conducted low-intensity jamming and attempted to hijack U.S. satellite signals. Until the late 1990s and early 2000s, from a technical standpoint, **most of the attacks were not sophisticated** (but efficient). Hijacking attacks overpowered uplink or downlink signals, replacing them.

Threat actors **began developing advanced capabilities in the 2000s**. They **began operating them in real conditions in the 2010s**. For instance, Russian electronic warfare troops started to operate GNSS jamming and spoofing systems after the annexation of Crimea in 2014. Since then, multiple **offensive** actions (mostly jamming), **defensive** actions (such as spoofing), and **intelligence** actions (such as in-orbit eavesdropping) were carried out. However, there was a **significant surge in 2022**, coinciding with the start of the war in Ukraine.

In the long term, interference targeting the signal segment becomes **increasingly difficult to track** because, in some areas (The Baltic Sea, the Black Sea, and Ukraine, it is permanent).

Most of the interference and offensive actions **were carried out by military units**. They are the only threat actor with the necessary capabilities to carry out sophisticated or large-scale interference.

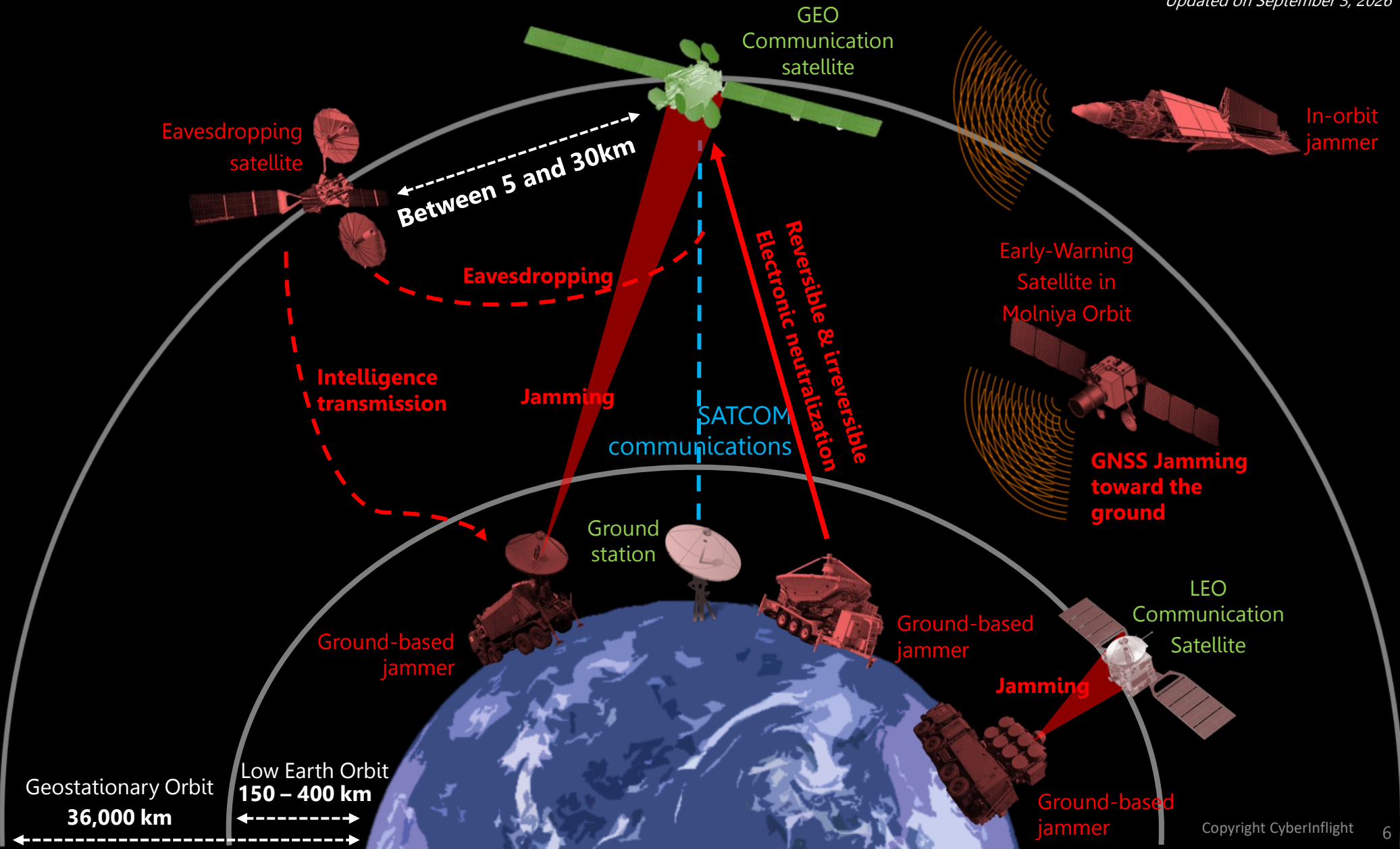
Interferences or other offensive actions targeting the signal segment **are driven by various motives**. Interferences targeting GNSS signals in times of peace are based on **political motives**. The aim is to strengthen the pressure on the identified adversary. When these interferences are carried out in times of war, the motives are **military**. Other actions (such as Eavesdropping) are driven by **state espionage motives**. A significant share of attacks against the signal segment have unknown motives.

# Threat Landscape, electronic warfare, and the signal segment

## Threat overview



Updated on September 3, 2026



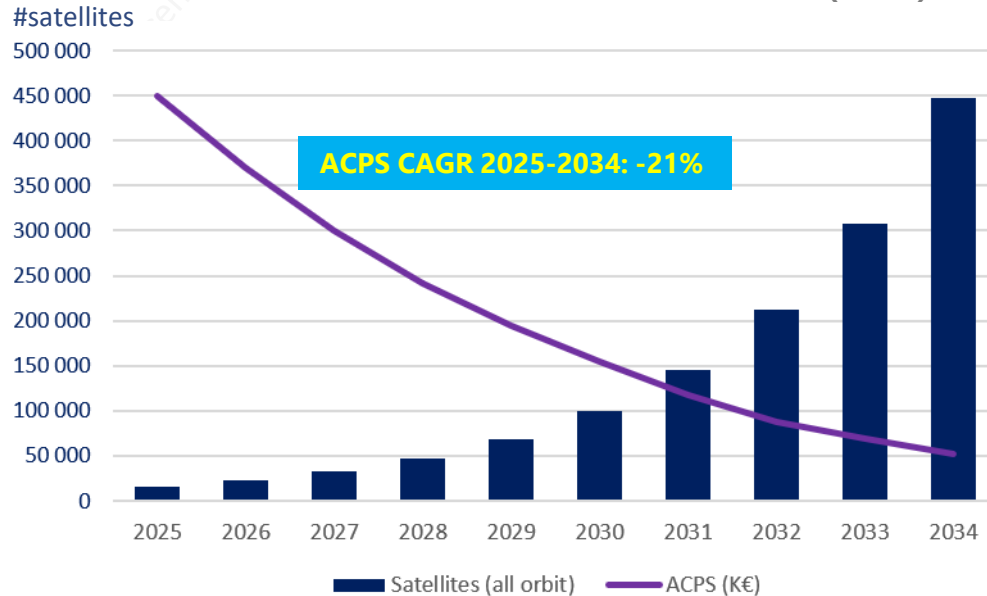
# Space Cybersecurity Economy

## Average costs of cybersecurity



Updated on August 28, 2026

### AVG. COST OF CYBERSECURITY PER SATELLITE (ACPS)



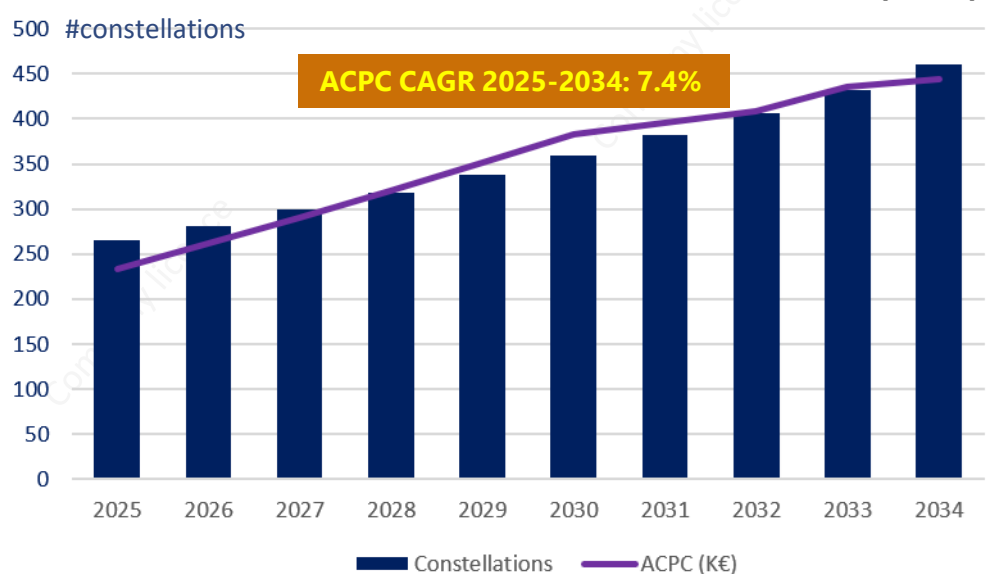
K\$

### Average cost of cybersecurity per satellite

Satellite operators may find it relevant to have an average metric to **estimate if their investment level per satellite is enough** each year. Such a metric encompasses CAPEX and OPEX per satellite, as the average cost of cybersecurity per satellite is revised annually. The metric is built by dividing the total number of satellites by the total investment level in cybersecurity.

In 2025, the **total number of satellites in orbit is estimated to be roughly 15,000**. This value is expected to grow each year significantly by a 45% CAGR in order **to reach at least 445,600 satellites by 2034** (which can still be considered as conservative with the number of mega-constellations projects which have been announced). Mechanically, the ACPS should decrease and is **expected to be around \$82K in 2034**. This is **explained by economies of scale**, as cybersecurity practices can benefit the entire fleet of a satellite operator.

### AVG. COST OF CYBERSECURITY PER CONSTELLATION (ACPC)



K\$

### Average cost of cybersecurity per constellation

A certain number of constellations have been deployed and continue to expand. **In 2025, we estimate the number of operational constellations to be around 265. This number is projected to reach around 460 in 2034**, although it may vary significantly depending on the financial sustainability of constellation projects.

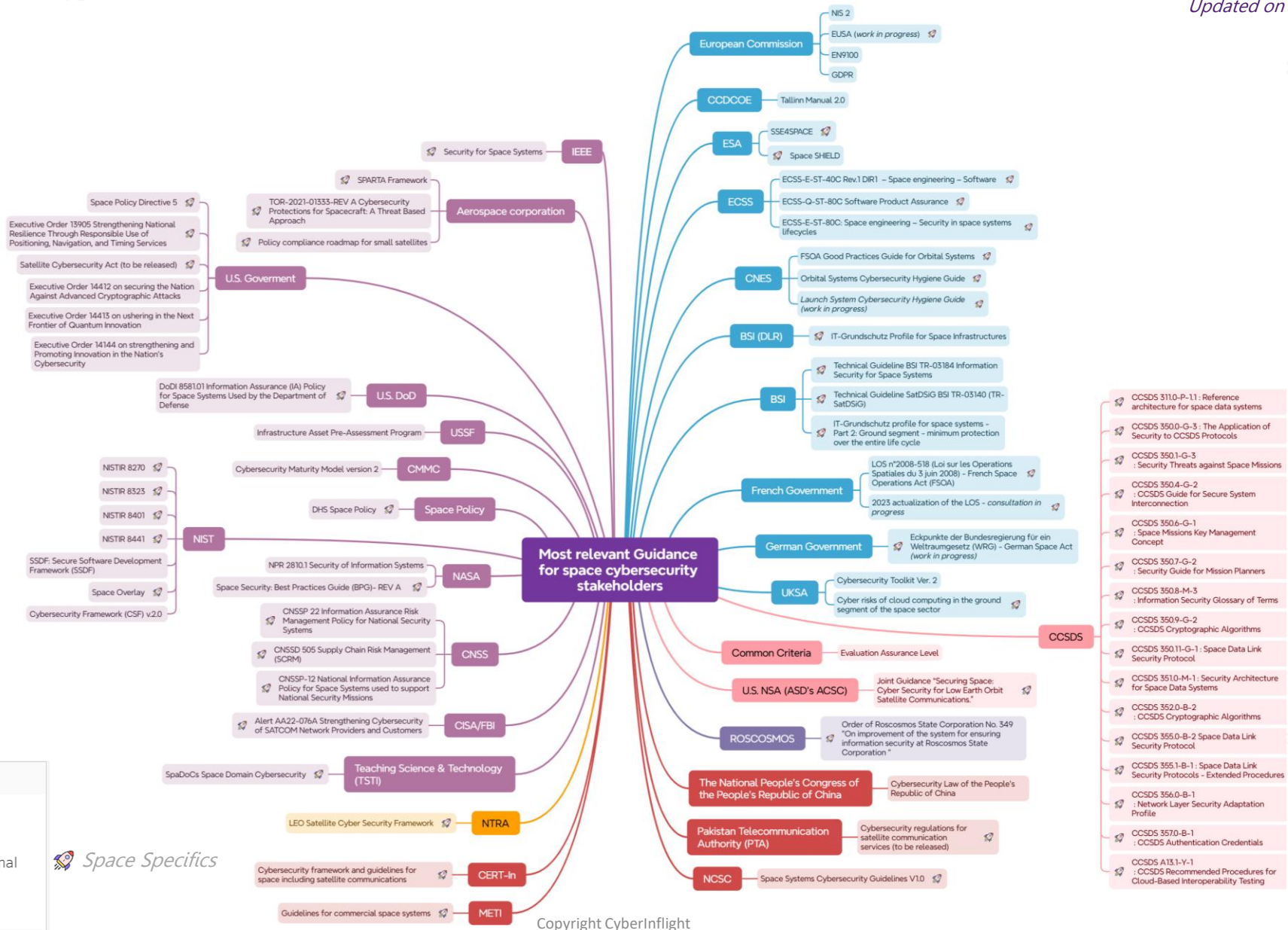
Based on this number, we propose a new metric called ACPC (Average cost of cybersecurity per constellation). The **ACPC is estimated at around \$41M in 2025** and is expected to grow steadily to reach \$80M in 2034, following a 7.5% 10-year CAGR.

This metric is mainly driven by the fact that the increasing number of satellites will mechanically increase cybersecurity expenses.

# Most relevant guidance for cyber-space stakeholders



Updated on August 27, 2026



## Region

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

Space Specifics

Copyright CyberInflight

# Key Electromagnetic Warfare events in space (2/2)



Updated on September 15, 2026

- **Late 2022 – Creation of Dedicated Space-EW Directorate within Russian EW Troops (REB):** Under Lieutenant General Yuri Lastochkin (Chief of the Electronic Warfare Troops of the Russian Armed Forces), creation of a dedicated electronic warfare department specifically tasked with space operations and countering orbital assets.
- **2022–2023 – The Starlink EW Campaign (*Tobol* & *Tirada-2S* Deployments):** Russia used *Tobol* and *Tirada-2S* systems to jam Starlink downlink/uplink channels, prompting automated frequency-hopping countermeasures.
- **Late 2025 – 2026 – Russian Ground-Based EW Station in Kaliningrad Jams German Bundeswehr Military Satellite:** German defense authorities confirmed that a German armed forces (Bundeswehr) military satellite link suffered targeted uplink/downlink RF jamming, causing a temporary loss of satellite communication for several hours. Triangulation and intelligence assessments traced the high-power interference directly to a Russian military electronic warfare ground complex located in the Kaliningrad exclave (associated with the *Tobol* / Baltic Jammer EW installation).
- **Mid-2025 – Operation Sindoor – Intensive EW Contestation & Targeted Jamming of Indian Military Space Links:** During the Operation Sindoor, Indian military assets, including EO (RISAT/Cartosat), NavIC GNSS, and dedicated SATCOM links (GSAT-7 series), faced severe electronic warfare counter-measures. Ground and theater-level operations experienced high-intensity RF jamming and GNSS disruption attempts across the Western and Northern theaters, triggering an emergency acceleration of India's Space-Based Surveillance (SBS Phase 3) program to deploy 52 EW-resilient, dedicated military satellites.
- **2023–2025 – Deployment and GEO Stalking Operations by *Luch-5X* / *Olymp-K-2*:** executed multiple close-proximity rendezvous maneuvers (RPO) within tens of kilometers of critical European and commercial telecommunications satellites, including Eutelsat 3B, Eutelsat Konnect VHTS, Astra-4A, and Intelsat-39.
- **2023–2024 – Baltic Sea "Jamming Bubble" (Kaliningrad / Baltic States):** Persistent GNSS jamming and circle-spoofing from Kaliningrad affected thousands of commercial flights and maritime navigation in Northern Europe.
- **May 2024 – Orbit Insertion of *Cosmos 2576* (Russia / US):** Russia launched *Cosmos 2576* into the co-planar orbit of US reconnaissance satellite *USA 314* as a potential non-kinetic EW and inspection platform.
- **2025 – Space "Bleed-Over" Jamming Phenomenon (Global):** Terrestrial high-power jammers in combat zones emitted high RF energy upward, blinding GPS receivers on LEO satellites orbiting overhead.
- **Summer 2026 – Operational Deployment of *Volna-Kupol-Garant* (Russia / Ukraine):** Russia fielded the *Volna-Kupol-Garant* system, shifting tactics from terminal jamming to **LEO satellite uplink saturation**. It transmits narrow-beam RF across Starlink's 8 Ku-band channels (14.0–14.5 GHz) to overload satellite receivers over a local area.

# Satellite constellations

## Starlink under attack (4/6): Volna Kupol Garant



Written on June 19, 2026

### "Volna Kupol Garant"

#### Operation

The system emits powerful interference targeted at a specific Starlink satellite, **flooding it with ground-based interference. It cuts the satellite off its connection to ground stations.** A single complex consists of six trailers equipped with satellite dishes concealed beneath randoms, **covering approximately 20 km<sup>2</sup>**, which is quite small compared to Starlink's coverage. Mechanically, the system **targets the 14-14.5 gigahertz reception band**, dividing the interference across eight distinct channels to blind the satellite.



Volna Kupol Garant System

### "Volna Kupol Garant"

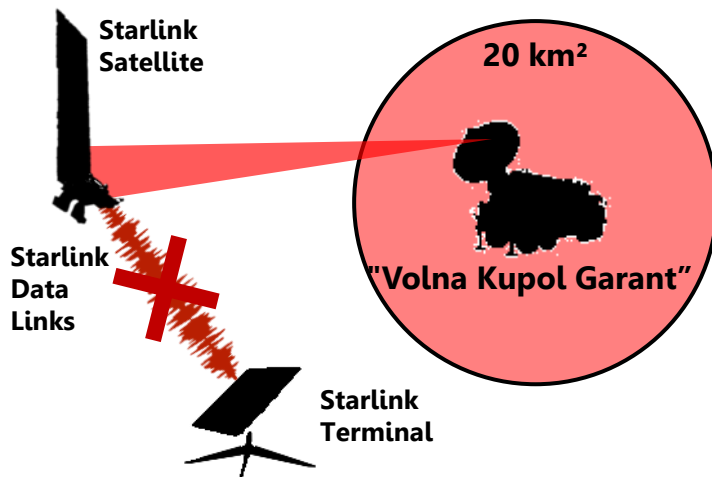
This electronic warfare system consists of a network of satellite antennas and targets 8 communication channels, each with a bandwidth of 62.5 MHz.

STARLINK AND  
ELECTRONIC WARFARE ATTACKS

M14 Highway

RUSSIA

UKRAINE

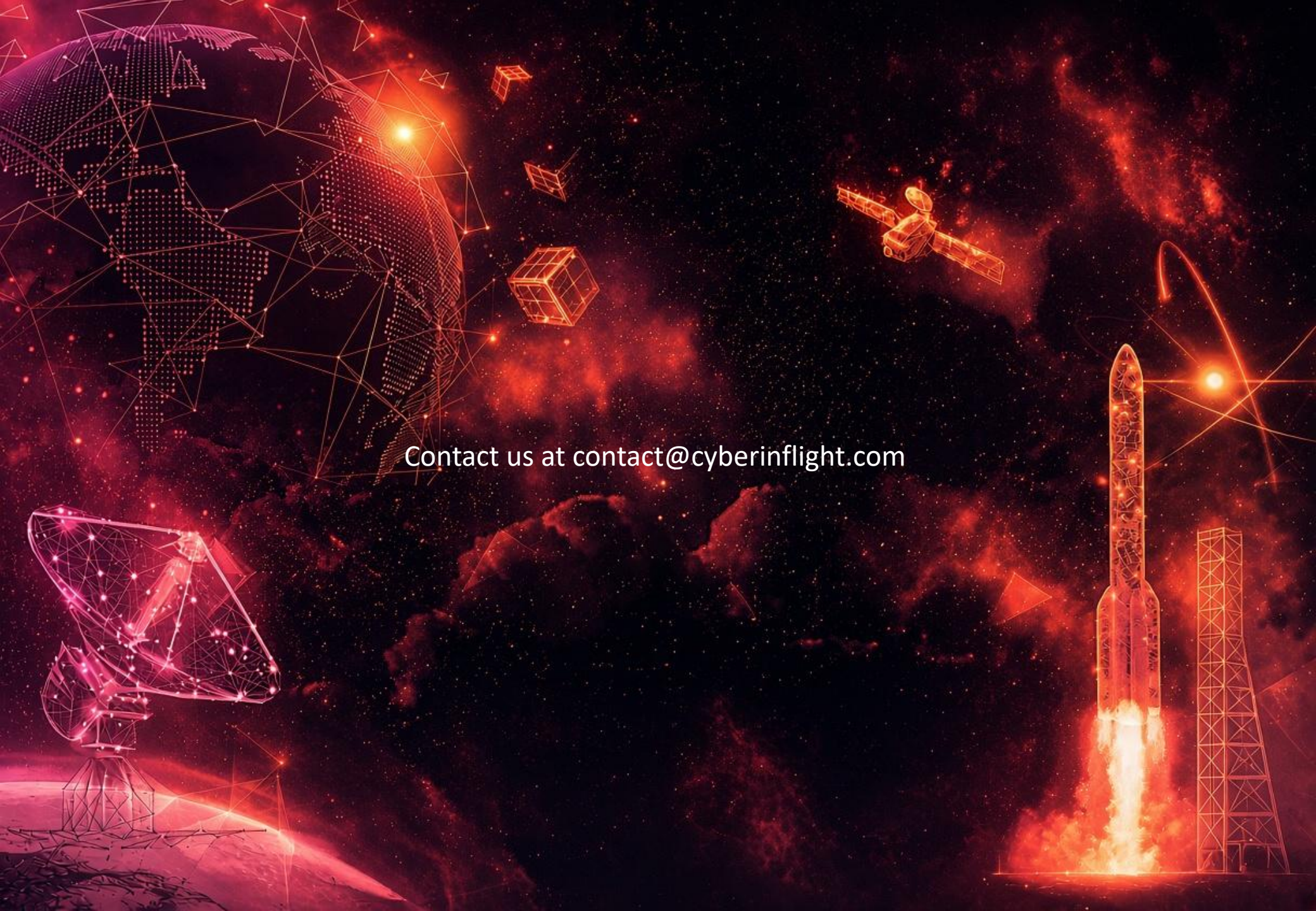


### "Volna Kupol Garant" Manufacturer

The system, designated as Volna Kupol Garant, is manufactured by the Simferopol-based **company Kupol**. According to Ukrainian sources, Kupol sold these mobile jamming units to the military for **\$1.5 million per complex**. In early September, Russian media mentioned the fact that the system's serial production had started.



It is currently being actively **used to protect the M14 highway from Ukrainian drones**. Ukrainian forces have noted that this new development is causing "significant problems." However, there are drawbacks: the electronic warfare system is currently quite bulky and conspicuous, although this issue is expected to be resolved in the future. Mass deployment of this technology was not observed again until 2026, following successful Ukrainian mid-range strikes on Russian logistics networks. Copyright CyberInflight



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