The Cyber Side of the Moon

Why space needs more than just astronauts, and how Belgium is leading the way in space cybersecurity

Living on the Moon – Technical challenges

Johan Helin – Senior Security Engineer & Team Lead, Nexova

with Matteo Merialdo – CTO Cyber, Sopra Steria and Nexova

Nexova

sopra steria

A Sopra Steria company

Nexova, a Sopra Steria company

Cybersecurity and space engineering, part of a European digital services group since 1 May 2026

30+
years of space engineering

2500
Cybersecurity experts in the Group

14
European countries

55,000
Employees in the Sopra Steria group

Nexova: cyber engineering, managed security (SOC) services, cyber ranges and compliance for space and critical infrastructure

- Full space mission lifecycle, from design to operations
- Customers: ESA, EUMETSAT, national space agencies, European defence ministries and space manufacturers
- Headquarters in Libin (Belgium), the same municipality as ESA's Redu site

sopra steria

Sopra Steria: about 55,000 people in nearly 30 countries, revenue of €5.8 billion (2024)

- Nexova and Starion joined on 1 May 2026, through CS Group, the Sopra Steria subsidiary for critical systems
- Nearly 2,000 people on space activities across the group, over €200 million of space revenue



Nexova and Starion headquarters, Rue des Etoiles, Libin (Belgium)



C2 - Restricted use


Space, closer than
you think
01

Your day runs on satellites

Space services you use before lunch, without noticing them

07:00

Phone clock

synchronised to the atomic clocks of navigation satellites (Galileo, GPS)

07:30

Weather app

Meteosat and MetOp satellites feed the 72-hour forecast

08:15

Bus and maps

Galileo positioning, used by 4 billion+ smartphones; EGNOS corrections for aircraft

09:00

Card payment

transactions and stock exchanges timestamped with satellite time

12:00

Breaking news

Copernicus images of floods and wildfires, emergency maps in under 3 hours

20:00

Video call

satellite links as the backup when terrestrial networks fail, and the only link at sea or in the air

~80% of critical infrastructure depends on satellite timing

4 billion+ smartphones use Galileo, free of charge, since 2017

< 3 hours from satellite image to Copernicus emergency map

Loss of satellite timing alone would hit telecoms, power grids and payments at the same time

C2 - Restricted use

Europe's space programmes

Four flagship programmes paid by EU citizens, and who runs them

Galileo and EGNOS

Europe's own navigation and timing; 4 billion+ users; an encrypted signal (PRS) reserved for police, emergency services and armed forces

Open Service since 2017

Copernicus

Earth observation with the Sentinel satellites; flood and fire maps, climate records, maritime and border surveillance

Data free and open for everyone

GOVSATCOM and IRIS²

secure satellite communications for governments and first responders; IRIS², the EU's own constellation of about 290 satellites

IRIS² services foreseen from 2030

Space surveillance and space weather

tracking debris, collisions and solar storms (EU SST), to protect the satellites themselves

Space Weather Data Centre hosted at ESEC Redu

Who does what:

European Commission → owns and funds the programmes

ESA → designs and develops them

EUSPA → operates Galileo, EGNOS and GOVSATCOM

Belgium pays into all of them: €1.1 billion pledged to ESA in November 2025, plus its share of the EU space budget

Living on the Moon needs network and complex IT/OT systems

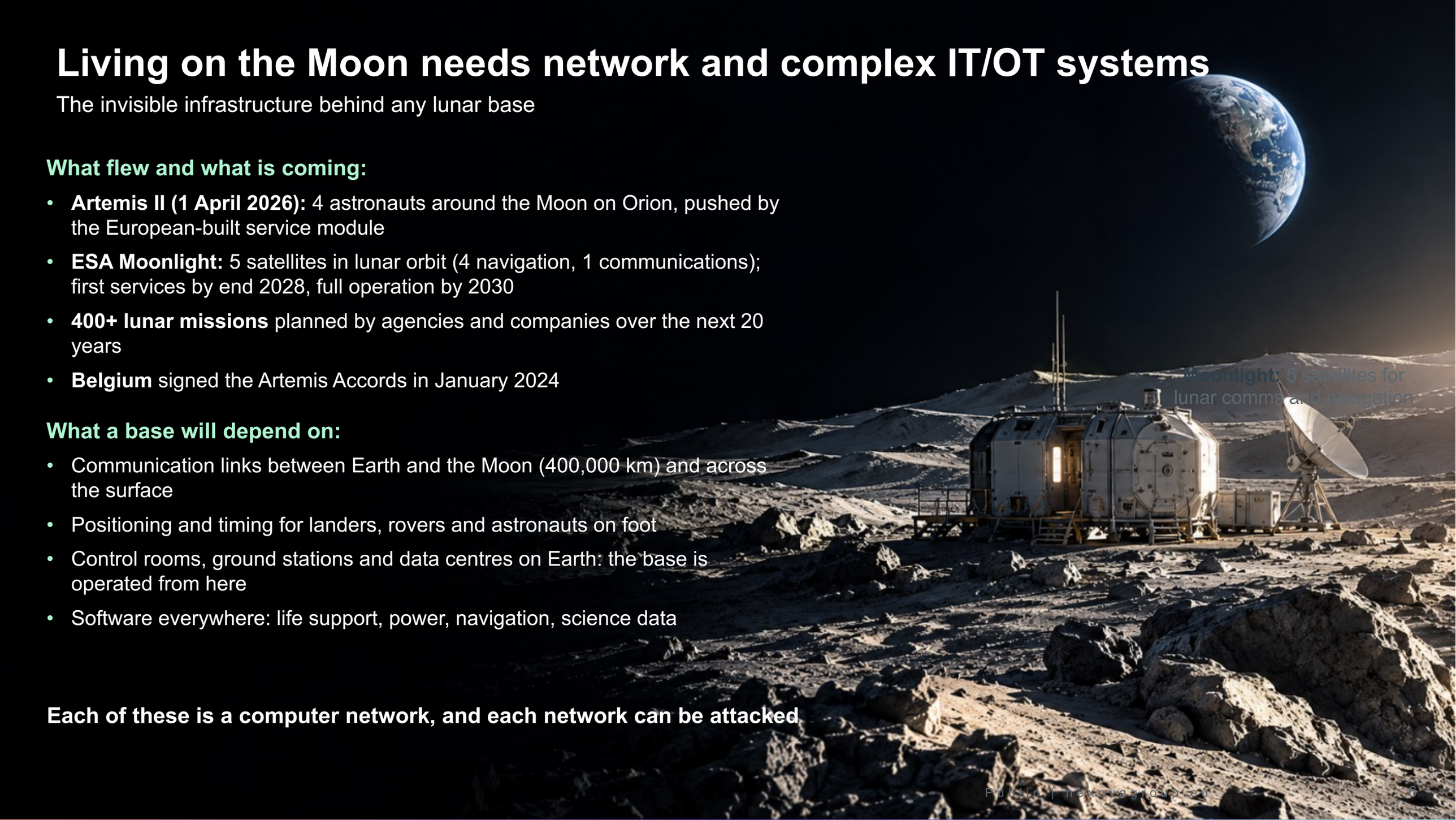
The invisible infrastructure behind any lunar base

What flew and what is coming:

- **Artemis II (1 April 2026):** 4 astronauts around the Moon on Orion, pushed by the European-built service module
- **ESA Moonlight:** 5 satellites in lunar orbit (4 navigation, 1 communications); first services by end 2028, full operation by 2030
- **400+ lunar missions** planned by agencies and companies over the next 20 years
- **Belgium** signed the Artemis Accords in January 2024

What a base will depend on:

- Communication links between Earth and the Moon (400,000 km) and across the surface
- Positioning and timing for landers, rovers and astronauts on foot
- Control rooms, ground stations and data centres on Earth: the base is operated from here
- Software everywhere: life support, power, navigation, science data



Each of these is a computer network, and each network can be attacked

A space mission, end to end

Four segments; only one of them is in orbit

Space segment

the satellite: a computer with radios and solar panels, 15 to 20 years in orbit, software written on Earth and rarely updated

Weak point: a flaw that cannot be patched

Link segment

uplink for commands, downlink for telemetry and data; radio waves in open air, anyone with an antenna can listen or interfere

Weak point: jamming, spoofing, replayed commands

Ground segment

mission control centre, ground stations, data processing; ordinary IT and OT networks, run by people

Weak point: phishing, ransomware, insiders

User segment

receivers in phones and cars, satcom terminals, web portals and apps

Weak point: fake signals and compromised terminals

~12 career astronauts in the ESA astronaut corps

~66,000 people in Europe's space industry (2024), plus agencies, operators and universities

Three of the four segments are on the ground, and so are the people who run the mission

C2 - Restricted use

02

The cyber side



Why and where space gets attacked

High value, long life, hard to patch, easy to deny

Why space is a target:

Strategic leverage

one attack on navigation or communications degrades civil and military response at once

Long patch cycles

satellites fly 15+ years with software that is hard or impossible to update

Dual use

the same navigation, observation and satcom assets serve civilians and armed forces

Attribution gap

jamming, spoofing and intrusions can be subtle, deniable and slow

Where the attacks come from:

Kinetic

anti-satellite missiles, lasers, physical attacks on ground stations

Electronic

GNSS jamming and spoofing, interference on uplinks and downlinks

Cyber

intrusion into ground networks, supply chain compromise, ransomware on mission systems, manipulated telemetry

Logical

command injection, firmware exploits, protocol manipulation

The ground segment is the soft underbelly: ordinary IT, ordinary people, extraordinary consequences

C2 - Restricted use

Real-world incidents

Space is already a cyber battleground

2008

Terra and Landsat: repeated intrusions through a ground station in Svalbard (US-CERT). Lesson: remote stations need zero-trust access

2015

DLR, Germany: spear-phishing into the mission support network of the German space operations centre. Lesson: operators are the first target

2022

Viasat KA-SAT: wiper malware on satellite modems hours before the invasion of Ukraine; tens of thousands of terminals offline across Europe, 5,800 wind turbines in Germany lost remote control

2023

Ethical hacks: Thales took control of ESA's OPS-SAT nanosatellite at CYSAT (April); Italian students (team mHACKeroni) won Hack-A-Sat 4 on the Moonlighter satellite, the first hacking contest in orbit (August)

2024 to 2025

GNSS interference: jamming and spoofing around the Baltic Sea divert flights; interference reported on the European Commission President's flight to Plovdiv (August 2025)

In every case the entry point was a ground system or a radio link

C2 - Restricted use

Astronauts need Cyber Security as well.

In Redu, ESEC is Education Center



C2 - Restricted use

Astronauts needs Cyber Security as well.

In Redu, ESEC is Education Center

Trends Z | Trends LIVE BOURSE | tendances Trends

A la Une | Bourse | Entreprises | Mon Argent | IA & Tech | Events

TECH

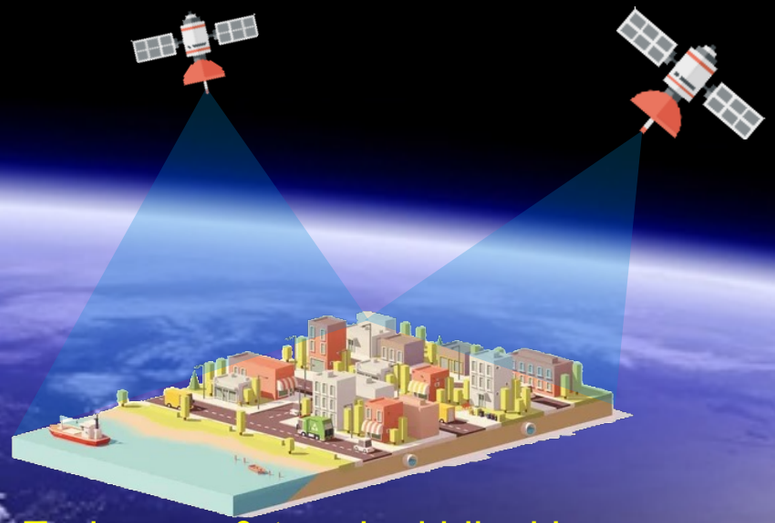
La station spatiale ISS infectée par un virus informatique

Partagez cet article:

28-08-2008, 11:00 • Mise à jour : 17-08-2022, 08:16 • <1 min. de lecture

La station spatiale internationale ISS est aux prises avec un virus informatique, et quelques 'laptops' à bord sont infectés.

Cyber Threats to the Space ECO-SYSTEM



End users & terminal hijacking

Supply chain compromise



Rogue Ground station

Command & Control interference

Laser interference

Satellite blinding

Virus infection
Trojan/Malware
Command takeover

Spying the signal
Eavesdropping

Ground network compromise

Electronic interference
Satellite jamming

Courtesy of ESA Security Office

The Space Security Operations Centre

A control room that watches the control room



Courtesy: ESA

On the floor: SOC analysts, mission engineers and RF specialists share the same playbooks; ESACERT (ESA's CERT, at ESRIN) handles the incidents with them

What a space SOC watches:

- Satellite telemetry, to spot anomalies (safe modes and eclipses are normal, a new pattern is not)
- Ground segment endpoints and networks (EDR/XDR)
- The radio spectrum, for jamming and spoofing
- Space-specific threat intelligence
- Incident response playbooks agreed with mission operators

Why it differs from a corporate SOC:

- Mission-critical systems with zero maintenance windows
- Proprietary protocols (CCSDS, PUS), no off-the-shelf parsers: protocol normalisation is 80% of the effort
- Safety-critical commands mixed with cyber telemetry
- Operators are engineers first; cyber is their second skill, so both teams train together
- A response that cuts a command uplink can be worse than the incident itself

ESA's C-SOC: inaugurated in May 2025, sites at ESOC Darmstadt and ESEC Redu, operated by Nexova with Starion and NVISO

C2 - Restricted use

Cyber ranges and digital twins

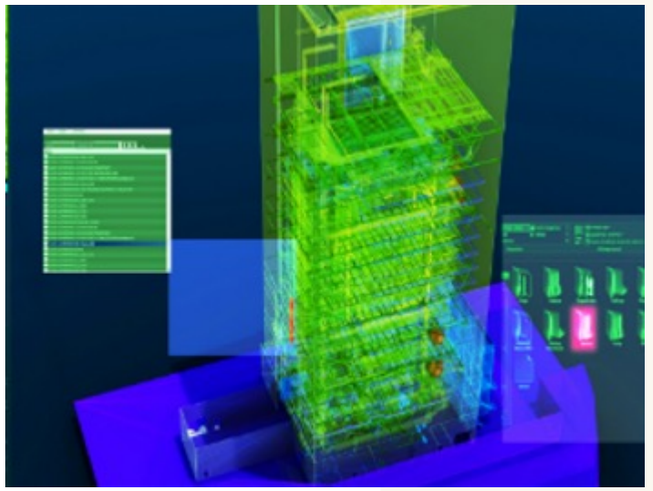
A flight simulator for attackers and defenders

What a digital twin is: a virtual (or hybrid) replica of the satellite, the radio links, the ground segment and the mission workflows, kept in sync with real telemetry

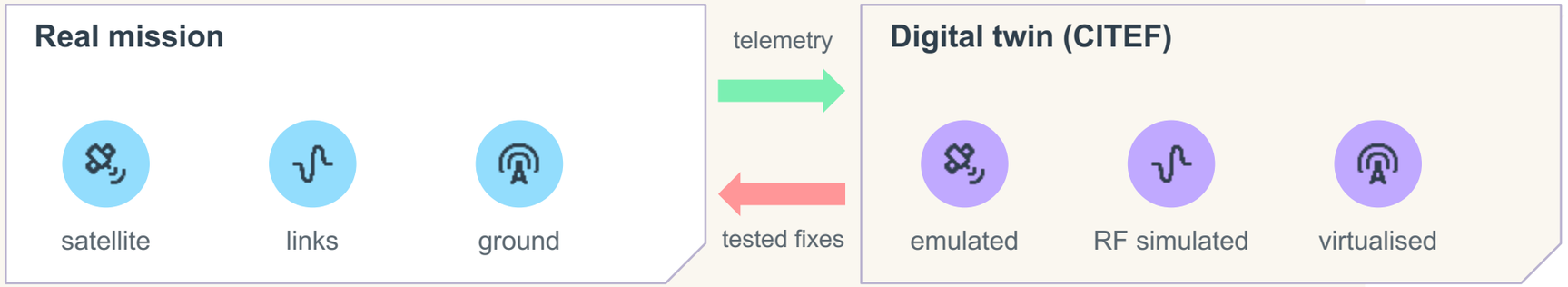
What it is used for:

- Replaying real attacks (Viasat, GPS spoofing) with no risk for the mission
- Testing a new satellite or ground system before launch
- Training operators, SOC analysts and RF teams together on the same scenario
- Producing evidence for compliance (NIS2, EU Space Act) and certification

Compared with a traditional testbed: hours or days to set up instead of months, a fraction of the cost, and it scales to full constellations



Courtesy: Nexova



attack scenarios injected here

At Nexova: CITEF (EU trademark) runs these twins for space, energy and defence customers; ESA's first space cyber range, ESEC Redu, 2016

The same twin serves testing, operator training and certification evidence

AI on both sides

The same tools serve the defender, the attacker and, sometimes, the target

AI for the defenders

- Anomaly detection on telemetry and network traffic, trained on what normal looks like
- Alert triage and summaries for SOC analysts, less false-positive fatigue
- Automated attack simulations (BAS) to test the defences continuously
- Agents that run the routine checks around the clock

AI for the attackers

- Phishing written for one named operator, in their own language
- Faster discovery of software flaws in ground systems
- Deepfake voices and video to talk their way into the control room
- Jamming and spoofing that adapt to the defences in real time

AI as the target

- On-board autonomy (image processing, navigation) fooled with crafted inputs
- Forecast and detection models poisoned through their training data
- A satellite that decides on its own can also be tricked on its own

Where the two meet: an AI model for a mission is tested like any other component, on the digital twin, with adversarial inputs

Skills in demand: data science and security together, plus people who understand the mission data

EU rules for space security

Why space engineers now read law, and lawyers read engineering

NIS2 Directive

2022

risk management, incident reporting and supply chain security for essential services; space ground segments in scope

For an operator: a risk register, incident notification within 24 hours, vetted suppliers

Cyber Resilience Act

2024

security requirements for products with digital elements sold in the EU, including the software and hardware of ground systems

For a supplier: secure development, vulnerability handling, a CE marking that covers cyber

EU Space Act

proposed June 2025

one EU rulebook for the safety, resilience and cybersecurity of space operators; under negotiation, trilogues expected late 2026, application around 2030

For an operator: cyber requirements as a condition of the authorisation

Space Threat Response Architecture

Council, 28 Sept 2026

how the EU monitors threats to its space systems and responds, with a yearly exercise

For the EU: alerts, a space security toolbox, sanctions against the attackers

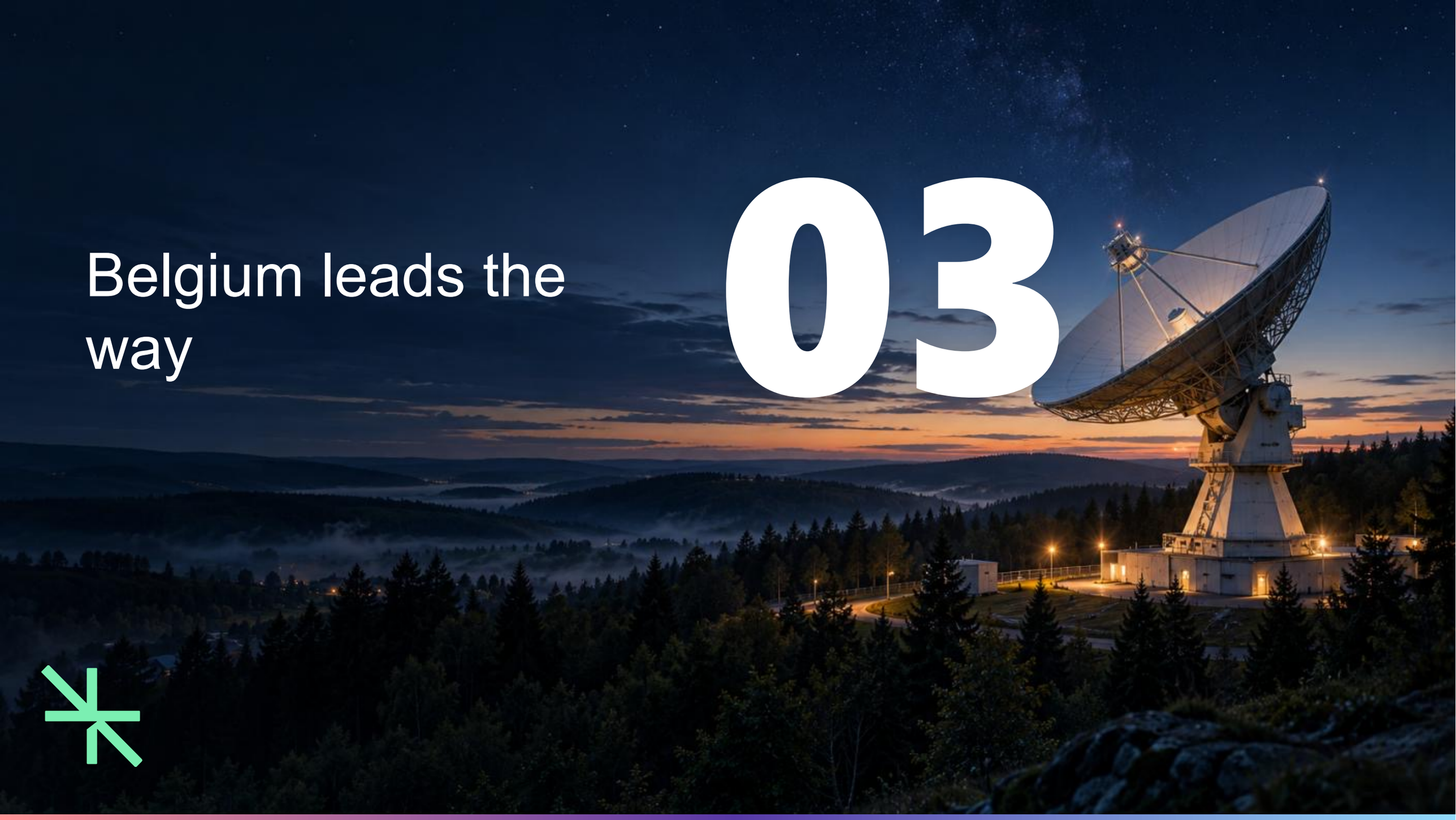
In practice: each text turns into system requirements, audits and evidence, work for engineers and lawyers who understand each other

Security is becoming a condition for the licence to operate in space, in Europe and elsewhere

C2 - Restricted use

03

Belgium leads the way



Belgium in space and in cyber

A founding member of ESA, and a country that built its own cyber institutions

1975
founding member of ESA

5th
largest ESA contributor, 2nd per capita

€1.1 bn
pledged to ESA, November 2025

6,500
jobs linked to ESA contracts

3
Belgian astronauts since 1992

Space:

- 100+ companies, 9 universities and 13 research institutes
- PROBA satellites, from Proba-1 (2001) to Proba-3 (2024), built under Belgian leadership (Redwire Space, Kruibeke)
- Thales Alenia Space Belgium (Charleroi): power supplies flying on 170+ satellites
- Aerospacelab (Charleroi): a factory for up to 500 satellites a year
- **Astronauts:** Dirk Frimout (1992), Frank De Winne (ISS commander, 2009), Raphaël Liégeois (ISS flight planned in 2027)
- Artemis Accords signed in January 2024

Cyber:

- **Centre for Cybersecurity Belgium (CCB):** the national authority, with the national CERT
- **Belgian Cyber Command** (October 2022), the Cyber Force since 21 July 2025, 5th component of the armed forces; a third of its people are civilians
- **ESA's cyber centre of excellence and C-SOC** at ESEC Redu (next slide)
- **Companies:** Nexova and Starion (Libin), NVISO (Brussels), with the Sopra Steria group behind them



€4.35 of industrial return for every euro Belgium invests in ESA

ESEC Redu, the space cyber hub of ESA

ESA's European space Security and Education Centre, in the Belgian Ardennes

The site:

- ESA ground station since 1968; 43 antennas, including the 20 m Galileo in-orbit test antenna
- PROBA mission control centre and the space weather data centre
- ESA Academy training facility for university students (2016) and CubeSat support facility (2018), next to the Euro Space Center
- ESA BIC Wallonie incubator for space start-ups (since 2012)

The cyber side:

- **2016:** first space security cyber range for ESA, built at ESEC by RHEA, today Starion
- **SCCoE:** the Security Cyber Centre of Excellence, developed with ESA for ESA and the space community
- **C-SOC:** ESA's Cyber Security Operations Centre, built by a 19-company consortium led by Leonardo; active since May 2024, inaugurated in May 2025, twin sites at Redu and Darmstadt
- **Operations:** run by Nexova, after a pre-operations phase to tune monitoring and response





Nexova headquarters, Rue des Etoiles, Libin, minutes from ESEC

1968 ESA station opens in Redu

2016 first space cyber range; ESA Academy arrives

2024 C-SOC active at ESEC

2025 C-SOC inaugurated, twin sites

2026 Nexova and Starion join Sopra Steria

The C-SOC covers ESA's missions from Darmstadt and ESA's corporate IT from Redu, each site backing up the other

04

Your place in it



Space cybersecurity jobs

8 roles that exist today, none of them in a spacesuit

Space SOC analyst

watches telemetry and ground networks, triages alerts, runs playbooks with mission operators

Background: networks, security operations

Satellite cyber engineer

secures on-board software and the command link, crypto for CCSDS protocols, thinks 15 years ahead

Background: embedded software, cryptography

RF and spectrum specialist

detects jamming and spoofing, designs links that survive electronic warfare

Background: electronics, telecom, signal processing

Cyber range and digital twin engineer

builds replicas of missions (software, hardware in the loop, RF) and the attack scenarios for them

Background: systems engineering, virtualisation

Space red teamer

hacks satellites and ground stations legally, OPS-SAT style, before someone else does

Background: ethical hacking, CTFs, reverse engineering

AI and data engineer

anomaly detection on mission data, models that resist adversarial inputs

Background: data science, statistics, mission data

Security accreditation officer

turns NIS2 and the EU Space Act into mission requirements and evidence for authorities

Background: law, engineering, project management

Threat intelligence analyst

tracks state actors and their techniques (SPARTA, ESA SHIELD), shares with the sector

Background: geopolitics, OSINT, security analysis

All of these roles are based on the ground, many of them in Belgium

C2 - Restricted use

How to get there

Paths into space cybersecurity, from any starting point

Study

- Computer science, electronics and telecom (RF), aerospace or systems engineering
- Mathematics and cryptography (post-quantum algorithms are coming to space protocols)
- Law, policy and management for the compliance side
- Belgium: 9 universities active in space, and cyber programmes at most of them

Practise

- Capture-the-flag contests: Hack-A-Sat, the European Cybersecurity Challenge, DEF CON
- Student satellites: ESA Academy 'Fly Your Satellite!' and the CubeSat facility at Redu
- Home lab: a software-defined radio, free Copernicus data, open satellite tools

Get in

- ESA Young Graduate Trainee programme and internships, including at ESEC
- Internships and junior roles at Nexova, Starion and Sopra Steria (Belgium and 8 other countries)
- Belgian Cyber Force: civilians are a third of its staff
- ESA BIC Wallonie in Redu for your own start-up

Where: the ESA Academy facilities and the Euro Space Center are in Transinne, next to Redu; Nexova and Starion are minutes away in Libin

Curiosity about how things break, plus one of the degrees above, is the usual entry ticket

C2 - Restricted use

Key takeaways

Space is infrastructure: timing, navigation, weather and communications for 4 billion+ users, and soon for the Moon

The attacks are real and they hit the ground: Viasat 2022, the DLR phishing of 2015, GNSS jamming today

Defence is a profession: SOC, cyber ranges, digital twins, AI and law, built in from the design phase

Belgium runs part of it: ESA's cyber centre and C-SOC at Redu, since the first space cyber range in 2016

There is a seat for you: 8 roles, all of them on the ground, many of them in Belgium

Thank you

A Sopra Steria company

sopra steria

Nexova

info@nexovagroup.eu

Rue des Etoiles 140
6890 Libin | Belgium

Nexova

nexova**group**.eu