ESA Technology Vision 2024 – 2040
Security for Space Systems

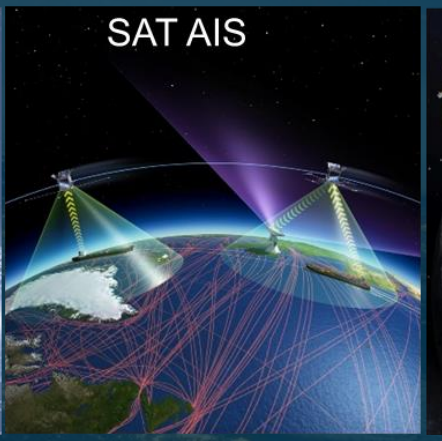
2024 Security for Space Systems Conference (3S)
27-28 May 2024, ESTEC, the Netherlands

Massimo Crisci (TEC-ES) / Antonios Atlasis (TEC-ESS)
security4space@esa.int
Directorate of Technology, Engineering and Quality

Importance of Space for Modern Life

Massive Use of Space Systems

Critical Space Infrastructure



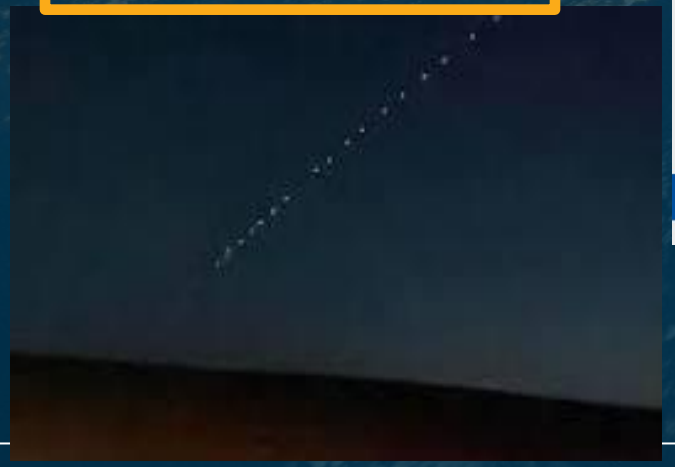
Security now Integral Part of the Development process of our Space Systems

Boost of commercial and new space initiative

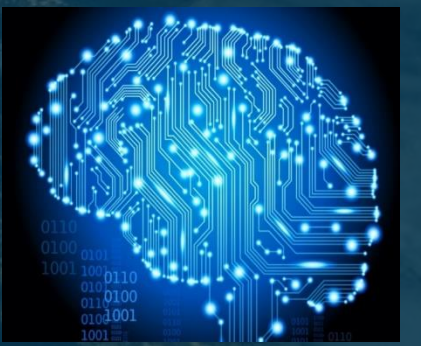
New Space

New Approach

New Responsibilities



New Techno



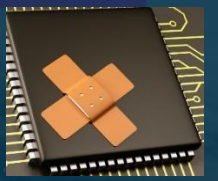
The challenges

Space Specific

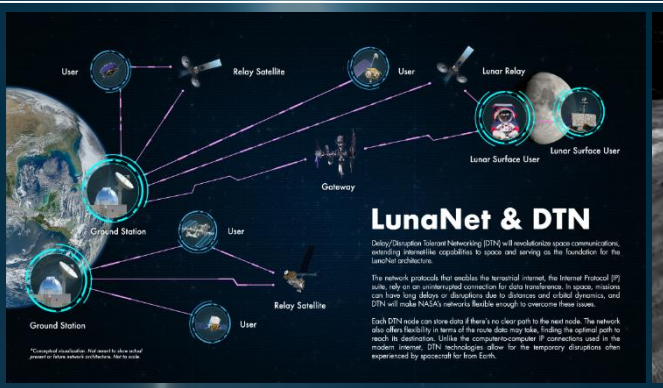
- Constrained and harsh environment (power, EM radiation damaging electronics, weight/space, safety/critical oriented, vacuum/thermal constraints limiting choice of materials, etc.)
- Distributed architecture ground / space / user /Lack of physical access (for space segment)
  - ➔ High degree of Autonomy and complex FDIR
  - ➔ Recovery is possible only remotely
  - ➔ Patching is more challenging (esp. at space segment
- Physical / Cyber hybrid systems /Large attack surface
- Massive service coverage area / Millions of users in footprint
- Long development cycles / Long lifetime of the missions / Obsolescence issues
- Large distance / Long Comms delay / Intermittent communications
- Etc.

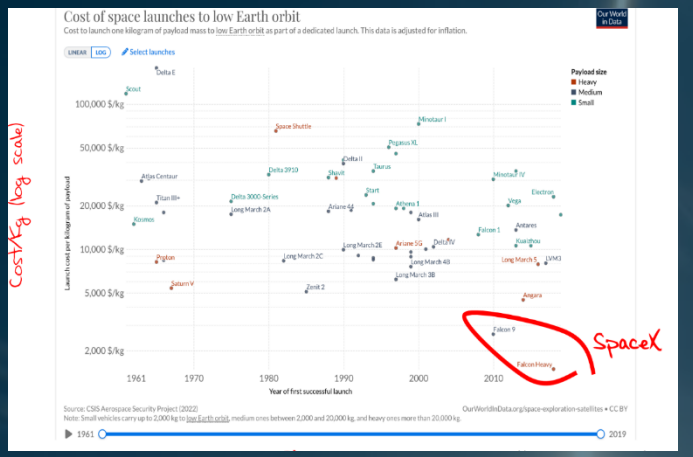
General and/or new to Space

- Scale up to new system architecture (e.g. large const.)
- Integration with terrestrial (e.g. 5G etc.)
- Emerging Quantum Threats for crypto
- AI and Security
- Optical and Quantum Comms security
- Cope with COTS solutions also onboard satellite
- Enhanced situational awareness
- Supply chain security
- Securing Mission and Securing infrastructure
- Etc.



Space Scenario 2040 - Key Elements





SpaceX Starlink Gen 1	4,408
SpaceX Starlink Gen 2	29,988
OneWeb, Phase 1	718
OneWeb, Phase 2	6,372
Amazon Project Kuiper	7,774
China Guowang	12,992
Astra	13,620
Boeing	5,842
Globalstar	3,080
Lynk	2,000
Telesat Lightspeed	1,969
Spin Launch	1,190
TOTAL	**89,953**
E-Space	337,323

Space Vision 2024 - 2040 – Preliminary Techno Themes

Technology Themes (Push)

Quantum

Artificial Intelligence

Cyber-Security

Hypervelocity Travel

Low Latency Information

AI Driven Materials Development

Human Augmentation (Cognitive/Physical Enhancement)

Resilient Space System

Next Generation Batteries

Humans/Avatars for Mars

Demisable Systems for Sustainable LEO/Cis-Lunar/Planetary

Very Large Telescopes

Human Protection for Solar System Travel and Settlement

Embodiment of AI

Digitalisation Advanced Modelling

Deep Space Power Generation

Genetically Engineered Life Forms to survive in Extreme Environments

Advanced Robotics and Autonomous Systems

Innovative Propulsion and Guidance (Nuclear/Take-off and Landing/Planetary)

Orbital/Planetary/Asteroid Manufacturing, Assembly, ISRU

Next Generation Rovers

Advanced Manufacturing

Wireless Power Transmission

Data Storage In Space

Technologies for Cost Reduction

Technology Themes (Mission Pull)

Navigation and Telecommunications Systems in the Solar System

Interplanetary/Interstellar Travels

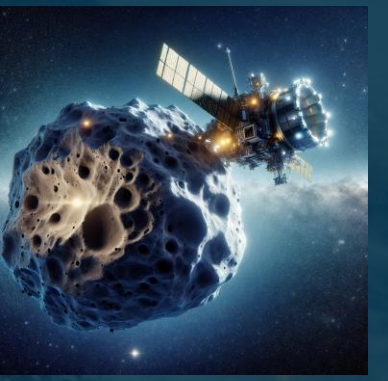
Asteroid Mining

VLEO

Sample Return from Outlying Planets

Life on the Moon

Orbital/Planetary Sustainable Habitats



ESA Security for Space Systems Task Force

- Recognising the importance of Security for Space Systems (but also on Quantum and AI), following ESA Executive Board mandate a Taskforce has been formed, led by the Director of Technology, Engineering and Quality, to establish a disruptive ecosystem and prepare the European ecosystem on Artificial Intelligence, Security and Quantum technologies.

- Objectives:
  - Propose an **ESA and European Strategy on security technologies for space missions** to prepare and establish the relevant European ecosystem in this domain.
  - **Identify the capabilities, including laboratories and competencies**, needed to support space security technology developments, and associated programmatic activities on the ESA side.

Our Vision for Security for Space Systems

- ***Categorise missions*** *to derive commonalities and similarities in security approach*
- ***Develop/Associate*** *knowledge of the* ***threat landscape*** *and possible* ***countermeasures***
- ***Secure-by-design*** approach, using a ***modular security reference architecture*** and a ***building blocks*** approach.
- Each mission, following a treat assessment / risk analysis approach can ***tailor*** the security architecture to its needs, and ***select*** the building blocks required to implement it (considering risk appetite, cost, etc.).
- No need to re-invent the wheel by new missions
  - Improved schedule/ Optimised cost
  - Increased security posture
  - Increased commercialisation opportunities
  - Boost on research
- Make available ***security products***, that can be used in a modular approach, suitable to fulfil identified security needs → ***Standardisation*** is key.
- Identify key security technology themes for development in a long run or through an accelerated approach

Categorisation of Missions

GENERIC CATEGORISATION

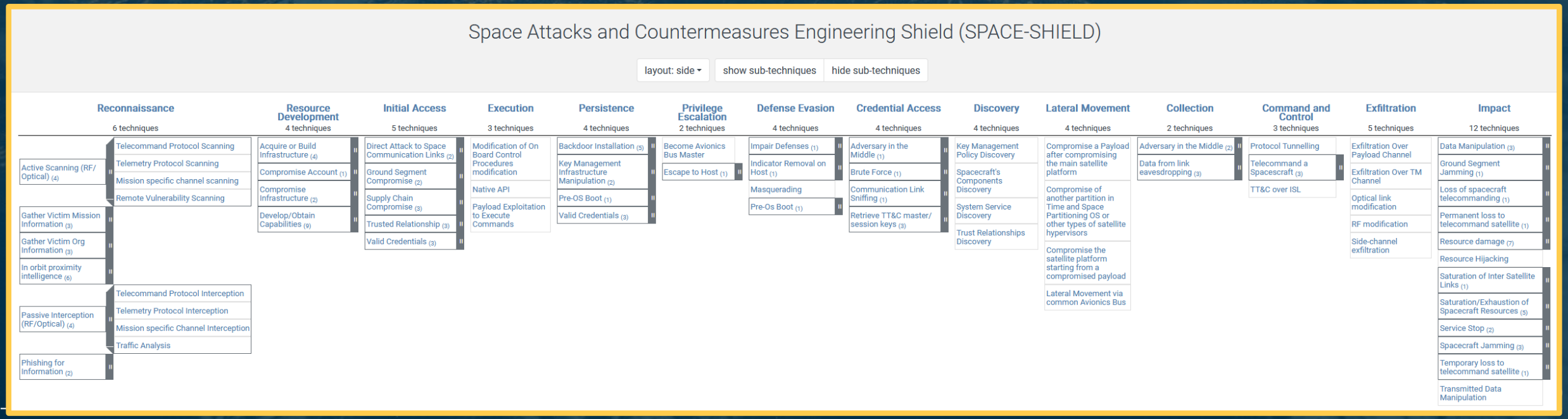
- ***Space critical infrastructure, potentially classified***, with strong security protection needs.
- **Unclassified institutional missions**, which will always require a good, commensurate protection of their assets and their services.
- Other ***unclassified institutional missions, of a potentially lower criticality*** in terms of security protection (e.g. Scientific missions), but still important from an investment and reputation perspective.
- ***Multitenant/Multipurpose missions hosting equipment*** (e.g. payloads) from different actors with different objectives, requirements, and level of trust whose challenge is the segregation.
- ***Commercial missions***, which are business driven and security comes as a business need to protect the services to the customers.
- ***"New space" missions***, driven by low cost and schedule demands, constituting a potential threat for the entire space ecosystem due to potentially relaxed security requirements.

CATEGORISATION BASED ON COMMUNICATION LINKS SPECIFICITIES

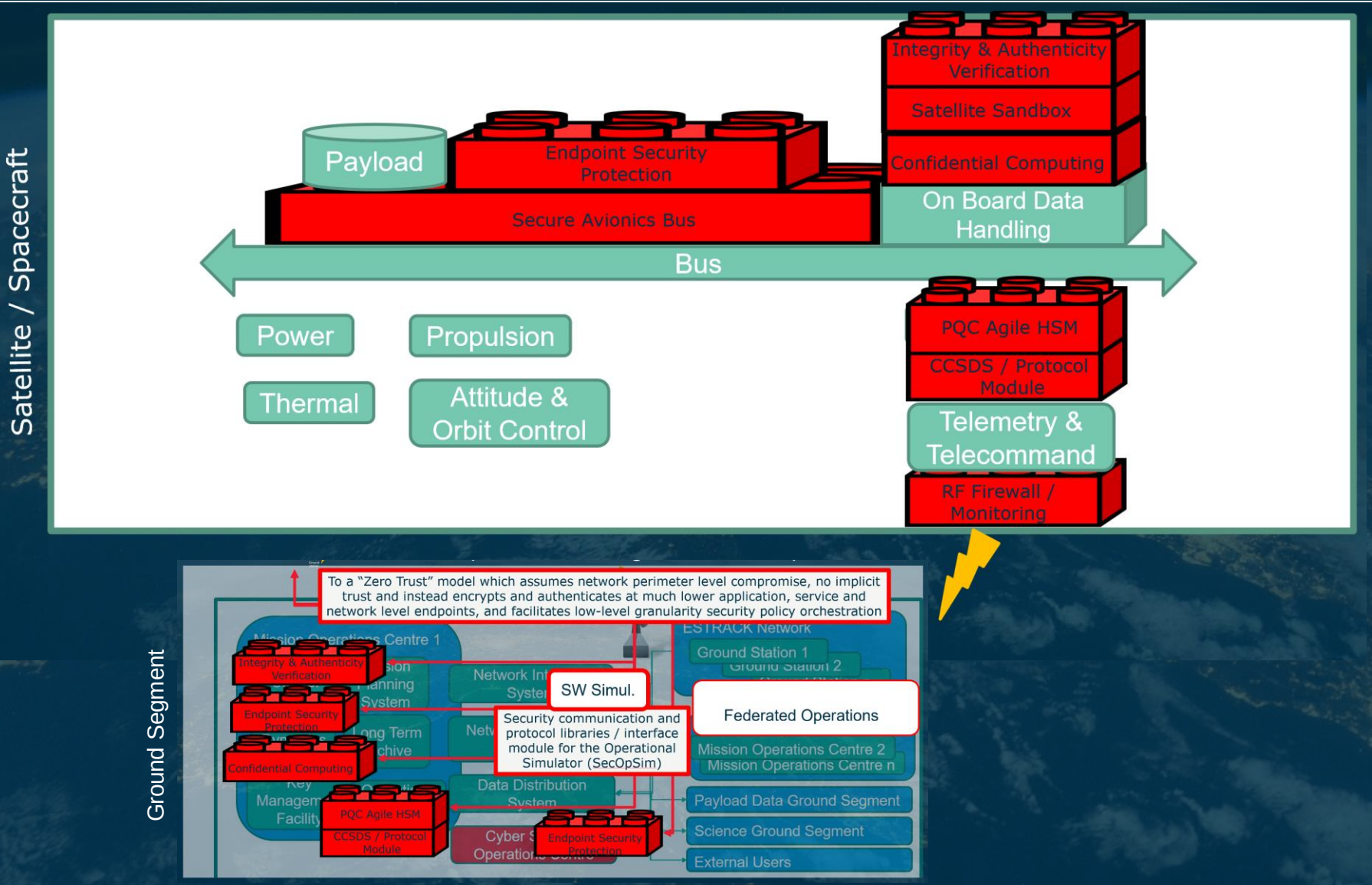
- Missions employing ***large (-mega) constellations***, requiring highly scalable cryptographic solutions, not always compatible with the traditional symmetric key exchange.
- ***Federated (e.g. inter-agency) missions***, with crypto solutions facilitating synergies with other missions and actors.
- Space missions, capable to operate ***over very long distances and propagation delays, potentially over third-party untrusted nodes***.
- Classified or even unclassified missions requiring ***accredited or certified*** cryptographic solutions.
- Any ***other space mission*** (e.g. Scientific missions) with no specific cryptographic requirements that need to rely on mature solutions, but for which adopting new technologies could ensure future-proofed security and interoperability.

Threat-Based Driven Approach

- We need to know our “enemy” (i.e. the potential security threats against space systems) – here we focus on the technological ones.
- Cyber space is well advanced on this (e.g. MITRE ATT&CK® knowledge base).
- Aerospace Corporation compiled SPARTA. ESA prepared SPACE-SHIELD.
  - Approach based on analysis rather than on real-world TTPs ➔ Facilitates the identification of needed technology developments + TTPs mapped to countermeasures / mitigations.
- Call to community for collaboration; outcome to be backed up by standardisation.



Satellite Security Reference Architecture



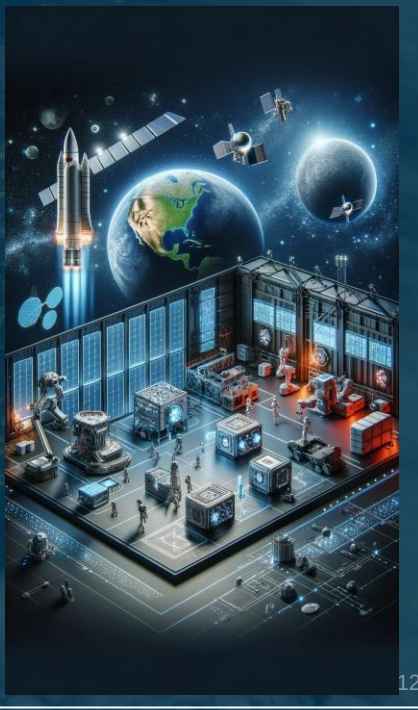
Space Security Technologies (Preliminary List)

Space Security Technologies (Push)

- Quantum Resistant Cryptography
- RF Security Protection / Antijamming
- Optical Security
- Crypto Agility
- Quantum Technologies for Security
- Supply Chain protection
- Physical / Hardware Security
- High Speed TRNG
- Trusted Platform Modules / Trusted Execution Environments
- Zero-trust, cloud native & next gen access control
- Segregated payload & ground segment ops
- AI for Security / Security for AI
- Satellite Active Défense
- Homomorphic Encryption
- Space Threat Intelligence / Situational Awareness
- Secure Space Protocol Implementation
- Space Digital Forensics and Spacecraft Recovery

Space Security Technologies (Mission Pull)

- High Speed Crypto (HydRON, IRIS2)
- Avionics (hardware, software) segregation (HydRON, IRIS2)
- (Asymmetric) PQC (IRIS2)
- 5G/6G Security (IRIS2, LEO PNT)
- Quantum Resistant Space PKI (Lunanet)
- BPsec, IPsec (Deep Space / Interplanetary Missions, Lunanet)
- Quantum Security (EuroQCI)



A Bit of a History, and short-term plans

The need to secure our space missions is not something new; ESA has initiated the development of technologies for security its space missions for years.

- In the context of specific projects (e.g. NAV) & R&D programmes (e.g. ARTES-4S)
- As part of GSTP Cyber Security Compendia (2019, 2022) ➔ have been proven very successful, since 70-80% of the activities are being implemented.
- As part of Basic Activities to complement ESA Cyber Resilience
  - A ***modular security reference architecture*** will be kicked-off in the next few days (follow up at higher TRL is foreseen)

Coordination at ESA wide level under ESA Cyber Coordination Board

GSTP Cyber Security Compendium 2022

GEN - Generic Technologies - Cybersecurity

CD3 - Avionic Systems

Programme Reference	Activity Title	Budget (k€)
GT1Y-601ES	Intrusion detection prevention module for secure avionics bus	2,500
GT1Y-602ES	Confidential computing: implementing spacecraft operations using trusted execution environments	2,000
GT1Y-603ES	Security segregation and isolation in a satellite	2,000
GT1Y-604ES	Agile post-quantum space data link security protocol hardware module	3,300
GT1Y-605ES	End-to-end supply chain protection	3,000
GT1Y-606ES	CCSDS delay-tolerant networking BPSec module	2,000
GT1Y-607ES	IP over CCSDS including internet protocol security module	1,200
	Total CD3	**16,000**

CD5 - Radiofrequency & Optical Systems and Products

Programme Reference	Activity Title	Budget (k€)
GT1Y-608ES	Low-cost resilient software defined radio platform for satellite applications	450
GT1Y-609ES	Radiofrequency firewall for satellites	4,000
	Total CD5	**4.450**

CD8 - Ground Systems and Mission Operations

Programme Reference	Activity Title	Budget (k€)
GT1Y-610GD	Secure communication and operations for the operational simulator	2,000
GT1Y-611GD	Security architecture for federated operations	3,000
GT1Y-612GD	Zero trust architecture for mission ground segments	2,000
	Total CD8	**7,000**

CD9 - Digital Engineering

Programme Reference	Activity Title	Budget (k€)
GT1Y-613GD	Consolidation of a secure systems engineering toolset for space missions	5,000
GT1Y-614GD	Quantum qualification and certification technology platform	8,000
	Total CD9	**13,000**

Timeline for ESA Vision 2040

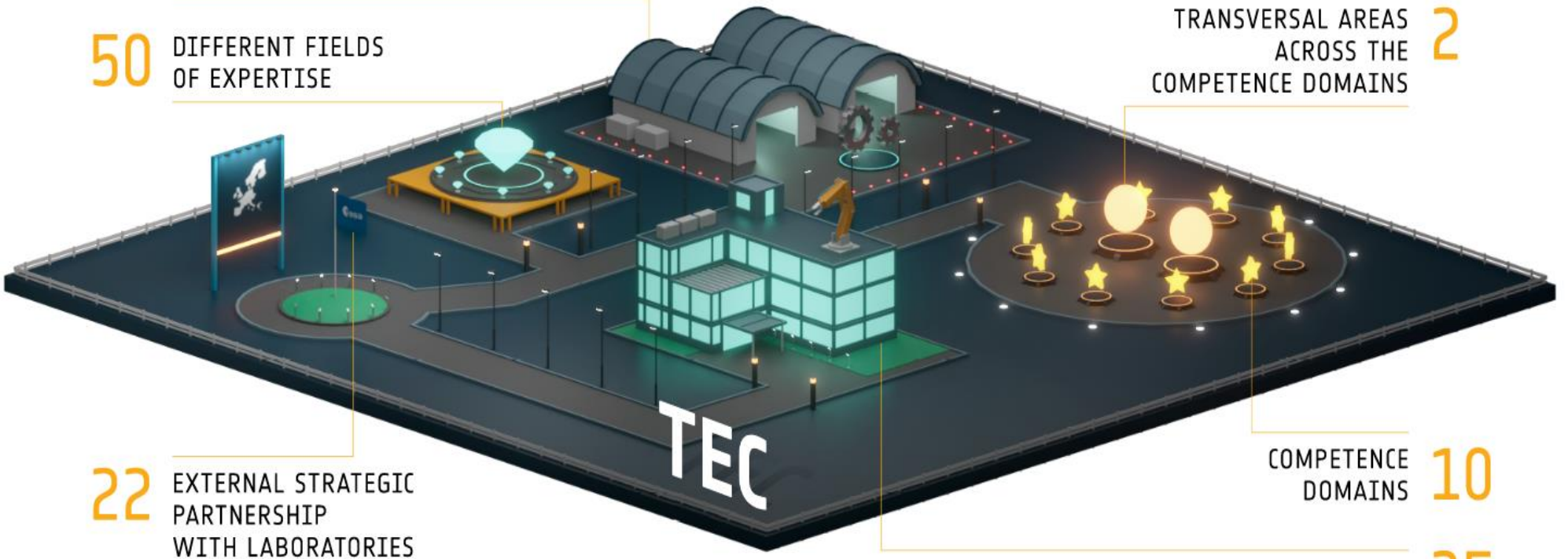
- Kick off performed on 2nd February 2024 ✓
- Internal Consolidation completed on 14th May. ✓
- Planned to be consolidated by end of June.
- To be issued mid July.
- Inputs from Industry, Academia, and (European) Space Agencies would be very much appreciated to prepare a ESA Vision on Security Technologies for Space for 2040.

Technology Development & Lab Capabilities

1 WORLD-CLASS TEST CENTRE

50 DIFFERENT FIELDS OF EXPERTISE

22 EXTERNAL STRATEGIC PARTNERSHIP WITH LABORATORIES IN ESA MEMBER STATES



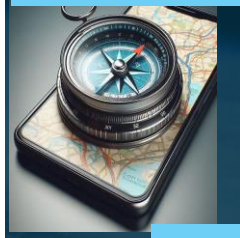
TRANSVERSAL AREAS ACROSS THE COMPETENCE DOMAINS 2

COMPETENCE DOMAINS 10

LABORATORIES 35

https://technology.esa.int/labs

Navigation Laboratory



Satcom / TTC Laboratory

Avionics Laboratory

Cyber Laboratory

A place where all technologies (avionics, crypto, NAV, RF, etc.) are gathered for end-to-end testing

We Need YOU

- Industry, Academia and Space Agencies **need to work closely together**, to:
  - Identify the **needs** of future space missions (institutional and commercial) in terms of required security technologies.
  - Follow **state-off-the-art research** on security aspects, with a focus on space missions.
  - **Work together** in driving future **research and development** on technological evolutions.
- Topics for discussion (also later for the panel):
  - What are the new technology-based threats?
  - What are the new security measures/benefits that technology can offer?
  - What are the gaps?
  - How security for space can benefit from non-space cyber security technologies?
  - How can the collaboration between Industry, Academia and space agencies become closer?
  - How can (security) technology development for space be accelerated?
- **For feedback**, **suggestions**, and any further communication on the topic, please contact with:
  - security4space@esa.int

2024 SECURITY FOR SPACE SYSTEMS (3S)

27-28 May 2024,
ESTEC, the Netherlands

organised by

esa

IEEE

esa academy

CYSEC

SYSGO EMBEDDING INNOVATIONS

THALES Building a future we can all trust

Logstail