ECCO
European Cybersecurity COmmunity

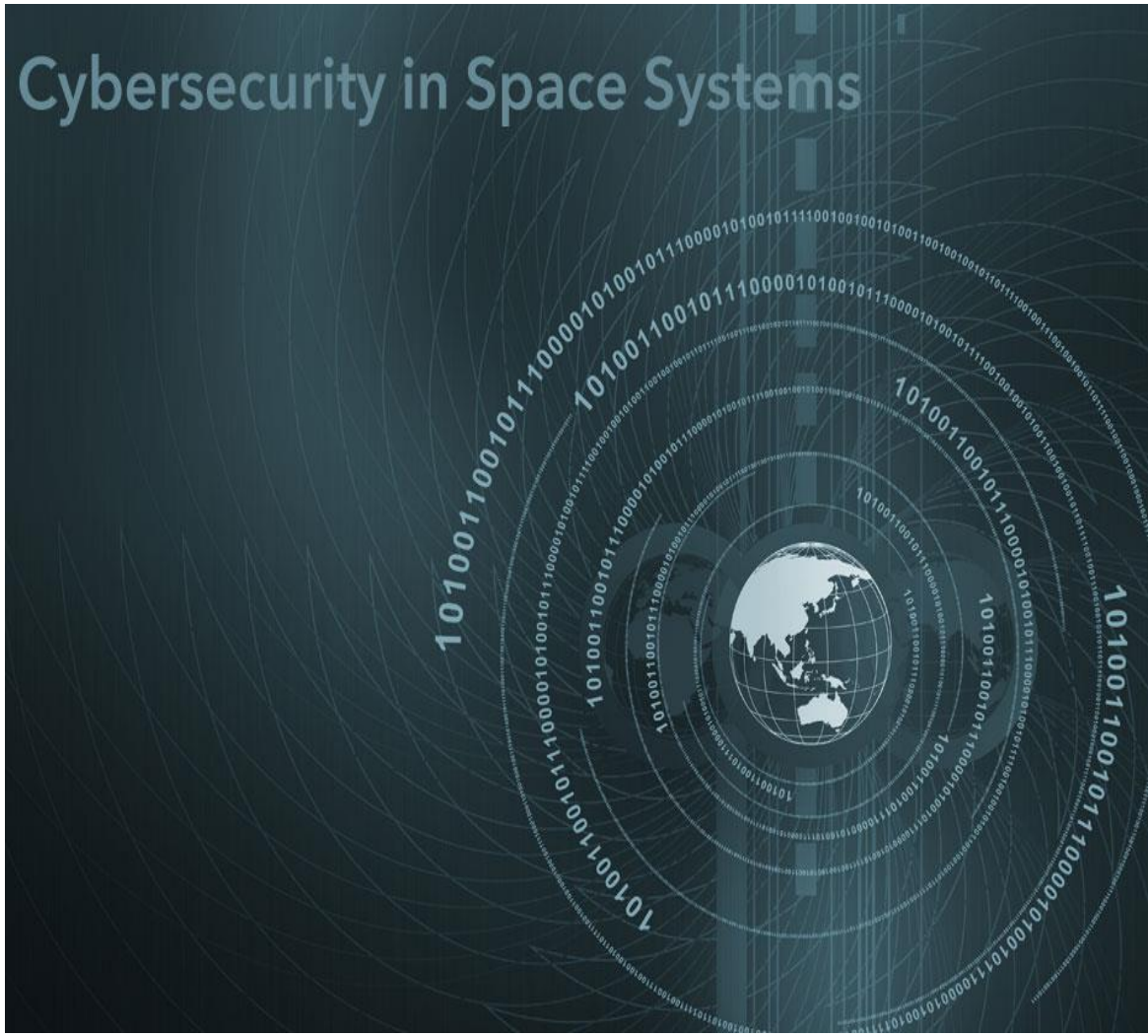
Introduction of the ECCO Community Group on synergies in cybersecurity for civilian and space applications

Matteo Merialdo

Business Director, Security Engineering & Products at RHEA Group

Overview of the ECCO community Group's missions and objectives

- Identifies and promotes **dual-use** cybersecurity technologies and practices between the civilian and space sector;
- Fosters **collaboration** and **knowledge** exchange with the industrial and the governmental space ecosystems;
- May develop actionable **recommandations** for the European Commission and the ECCC;
- Supports community **development and policy alignment** within the EU's cybersecurity landscape;



ECCO

European Cybersecurity COmmunity

Overview of the EU and National space landscape

Current cyber landscape in the EU and National space sector

- Growing interconnection and interdependence between the space sector and the cyber domain;
- They both wield significant influence at both National and European levels;
- In the space sector, the integration of cybersecurity is imperative to protect critical space assets from potential cyber threats and attacks;
- Space militarization: utilisation of satellites and other space technologies for military purposes;
- The economic realm exhibits a duality between cyber and space, where both domains intersect to shape commercial activities and strategies;


science
human spaceflight
applications
earth observation
space transportation
navigation
exploration
technology
telecommunication
Credits: ESA

Why are space infrastructures vulnerable?

- Adversary nations have explicitly stated their intention to target **commercial space systems** operating in mission classes including Earth observation, communication and intelligence
- Many of the successful attacks on space systems are carried out via complex **supply chain attacks**
- Cybercriminals can **take control of vital systems**, manipulate controls and steal confidential data
- **Limited resources** in space sector can lead to low security measures in place

- **Ground attack vectors**: facilitates access to control and track space assets via terrestrial networks, simplifying space system attacks
- **Space attack vectors**: exploit electronic attacks and software vulnerabilities, gaining unauthorized access to critical services
- **Communication channel attack vectors**: jamming, spoofing, eavesdropping
- There are many old space assets more easily prone to cyberattacks due to **weak security controls**

Challenges at a National and European level

- Satellites bear exploitable vulnerabilities
- Modern security measures are often missing
- There's often no protection of telecommand via encryption or authentication

- Everything in space is more difficult: it is sometimes not easy to patch or fix a vulnerability on a space asset
- Attackers can relatively easily intercept communications
- Space assets became more and more critical for their essential role in society

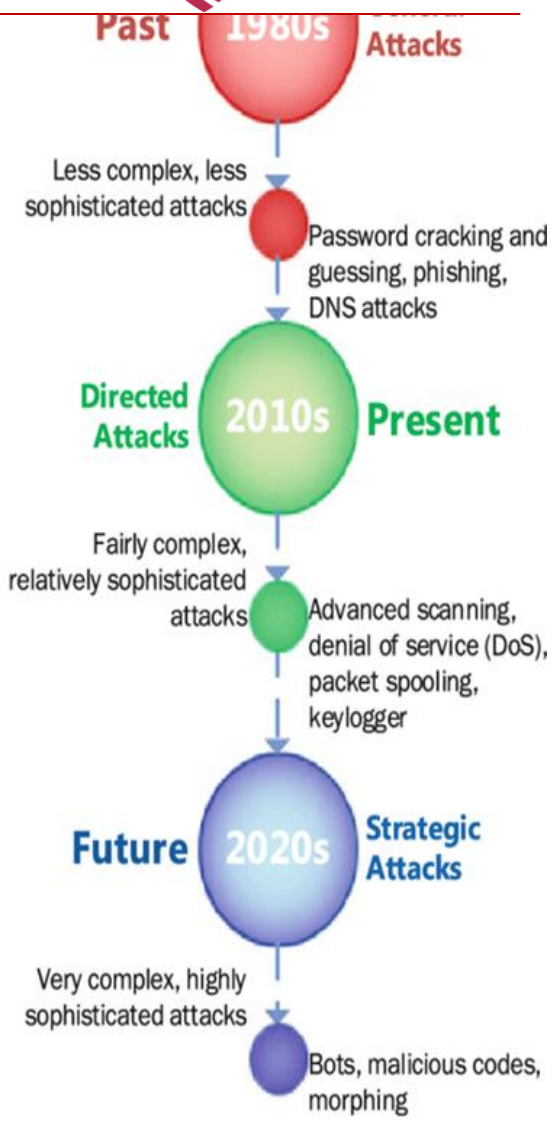
TOP 10 EMERGING CYBER-SECURITY THREATS FOR 2030

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

Cybersecurity threats in the space sector

Cyber threats must be taken into consideration as much as **electronic** threats and **physical** threats

- **Advanced persistent threats** (APTs): Long-term, targeted attacks by skilled adversaries
- **Distributed denial-of-service** (DDoS) attacks: Overwhelming systems or networks with traffic to disrupt services
- **Phishing and social engineering**: Deceptive tactics to obtain sensitive information or compromise systems
- **Insider threats**: Unauthorized actions by employees, contractors, or partners with access to sensitive information or systems
- **Signal jamming**: Intentional interference with satellite communication signals, disrupting services.
- **Signal spoofing**: Transmitting false signals or data to deceive users or systems.
- **Interception**: Unauthorized access to communication signals, allowing eavesdropping or data theft.
- **Supply chain attacks**: Compromising third-party vendors or suppliers to gain access to targeted systems



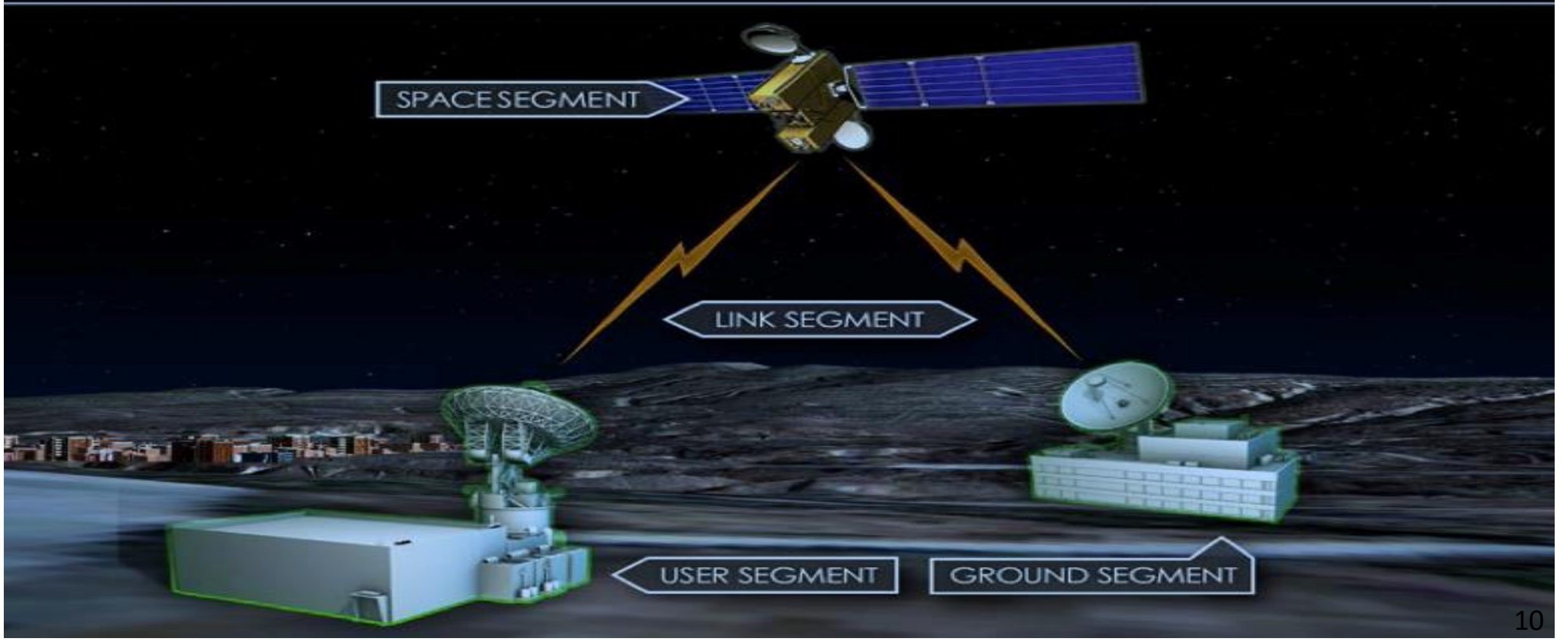
CYBER THREATS TO SPACE SYSTEMS

SPACE SEGMENT
- Command Intrusion
- Payload Control
- Denial of Service
- Malware

USER SEGMENT
- Spoofing
- Denial of Service
- Malware

LINK SEGMENT
- Command Intrusion
- Spoofing
- Replay

GROUND SEGMENT
- Hacking
- Hijacking
- Malware



Impact of attacks on the space sector

Disruption of satellite communications

- Service disruptions for sectors reliant on satellite-based services such as telecommunications, navigation and remote sensing
- Can lead to communication blackouts and hinder critical operations

Compromised data integrity

- Manipulate or tamper with data transmitted by satellites, compromising the integrity and accuracy of information relayed to users
- Can undermine decision-making processess and erod trust in satellite-based data

National security risks

- Space assets are integral to national security for purposes such as surveillance, military communication, etc;
- Cyber attacks can undermine defense capabilities and compromise sensitive information

Impact of attacks on the space sector

Physical damage to satellites

- Physical damage to satellites through interference with their operation or by initiating destructive actions leading to malfunction or destruction
- Can result in the loss of critical space assets

Increased vulnerabilities

- The expanded attack surface provides adversaries with more opportunities to exploit vulnerabilities
- Can compromise assets

Loss of public trust

- Loss of public trust in space systems and programs and their reliability

Examples of Previous Cyber/Space Incidents

- **2014**: Chinese hackers target US National Oceanic and Atmospheric Administration (NOAA) satellite data
- **2018**: GPS jamming during NATO exercises in the Arctic, affecting navigation systems
- **2020**: Cyber attack on a satellite communications provider, causing severe service disruptions
- **2022**: Russian attack on Viasat terminals, partial interruption of KA-SAT's consumer-oriented satellite broadband service Europe-wide
- **Ongoing**: Cyber espionage campaigns targeting space industry intellectual property and sensitive information

ECCO

European Cybersecurity COmmunity

Identification of synergies and dependencies between space and cybersecurity in the EU

EU Policy and governance perspectives

Legislative developments

NIS 2 Directive :

- Covers space sector;
- Requires reporting of cybersecurity incidents;
- Promotes collaboration;

Critical Entities Resilience Directive:

- Covers space sector;
- Requires regular risk assessments;

EU Policy and governance perspective

Governance challenges and opportunities in ensuring cybersecurity for space activities

Challenges :

- Regulations;
- Interruption of activities due to cyber threats or attacks;
- Lack of skills, funding;

Opportunities:

- Technological advancements;
- Increased efficiency and competitivness of EU Space Sector;
- Development of solutions that ensure the safety of assets and critical infrastructure;

Technology and innovation perspectives

a) Innovations driving cybersecurity in the space domain

- **Technological advancements**: artificial intelligence, machine learning, quantum computing;
- **Adaptive security measures**: innovative cybersecurity solutions are essential to adapt to evolving threats and vulnerabilities;
- **Collaborative research and development**: collaboration between industry, academia and government agencies drives innovation in space cybersecurity;

b) Synergies between space technology and cybersecurity measures

- **Satellite communications security:** implementation of encrypted communication protocols for satellite communications;
- **Space mission protection:** deployment of anomaly detection systems on spacecraft to identify and mitigate cybersecurity threats;
- **Ground station security:** implementation of access control measures and intrusion detection systems at ground stations;

What are Institutions and Industry in EU working on?

Cyber threat sharing: establish robust channels for sharing cyber threats and attacks within the space sector

Policy development and compliance: develop and enforce comprehensive cybersecurity policies tailored to space sector requirements and aligned with national and european standards;

Incident response planning: formulate clear and effective incident response plans to swifty address cybersecurity incidents and minimise operational impact;

Collaboration: foster partnerships with Government agencies, industry and organizations;

Risk management: refine and tailor means to relatively easy monitor the risk in space systems;

Monitoring and evaluation: implement continuous monitoring systems to assess cybersecurity posture and evaluate effectiveness of security measures;

Capacity building: invest in training programs to improve cybersecurity skills and awareness

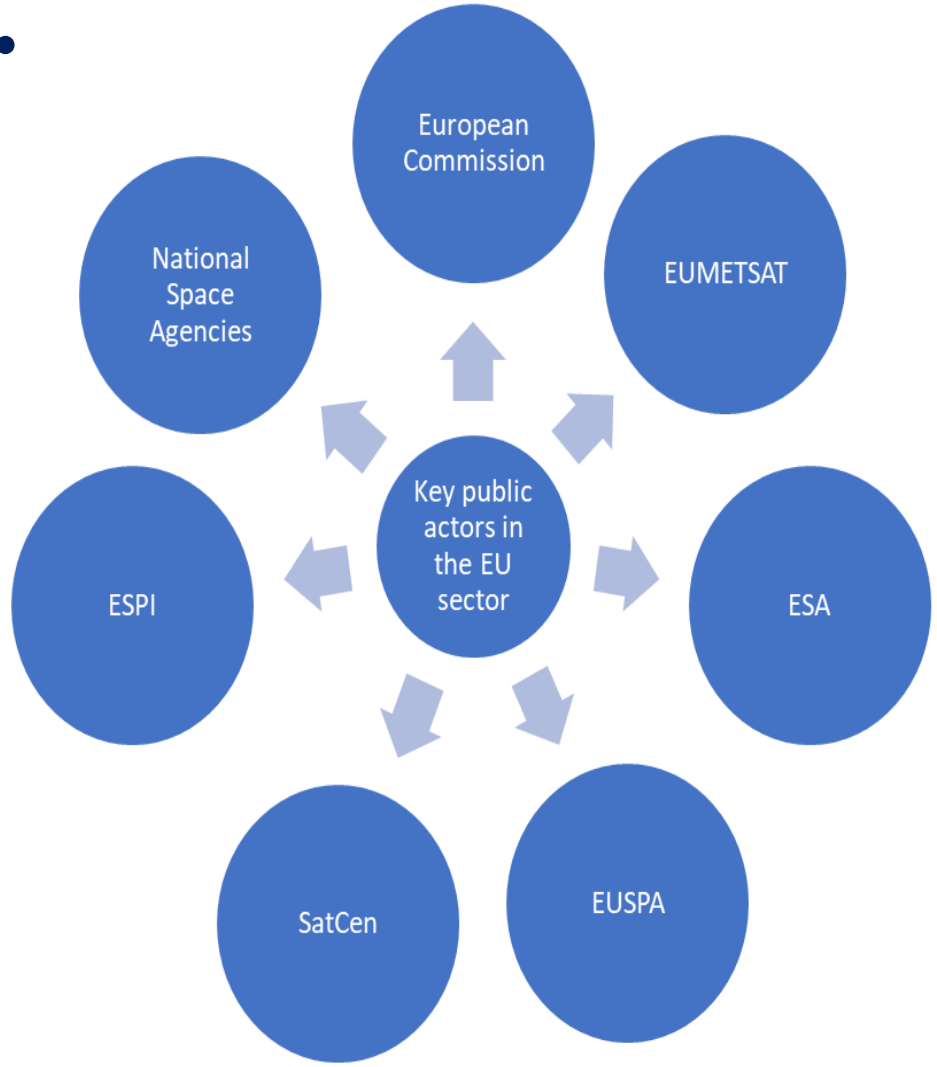
ECCO

European Cybersecurity COmmunity

Overview of main EU space stakeholders with relevant cybersecurity involvement:

Public actors in the EU space sector

- **European Commission:** actively bolsters the EU's cybersecurity role through a **robust regulatory framework** (for example, EU Space Law)
- **European Union Agency for the Space Programme (EUSPA)**: **Manages EU space programs**, ensures the security of space infrastructure, and supports the development of innovative space applications. Manages EU space programs, including Galileo and EGNOS, and oversees Copernicus and Govsatcom services
- **European Space Agency (ESA)**: Coordinates EU space policy and programs, and supports the development of **space-related technologies**
- **EUMETSAT**: provides Europe with a **resilient capability** to deliver global observations, data and user support services;
- **SatCen**: primarily serving as the **supplier of satellite imagery and geospatial intelligence** for the EU's common security and defense policy;
- **ESPI:** offers decision-makers **well-informed perspectives** on mid-to long-term issues pertinent to Europe's space endeavors;



National Space Agencies

- Numerous EU Member States boast their own national space agencies such as the French **CNES**, the Italian **ASI**, **Luxembourg's Space Agency**, German **DLR**, many others...

- **These national space agencies face cybersecurity risks**, encompassing potential attacks on satellite systems, data breaches and disruptions to space missions;

Private actors

- Private companies have identified diverse **commercial opportunities in space**, spanning satellite communications, navigation, Earth observation.
- The private sector has played a pivotal role in **reducing the cost of accessing space** by developing reusable launchers and technologies.
- Private companies have introduced substantial **technological innovations** to the space sector, leveraging digitalization to design more efficient, cost-effective for satellites.
- Government space agencies have actively encouraged **public-private partnerships**, sharing costs and resources.

ECCO
European Cybersecurity COmmunity

Overview of possible EU space/cyber principal funding schemes

Horizon Europe

European structural and investment funds

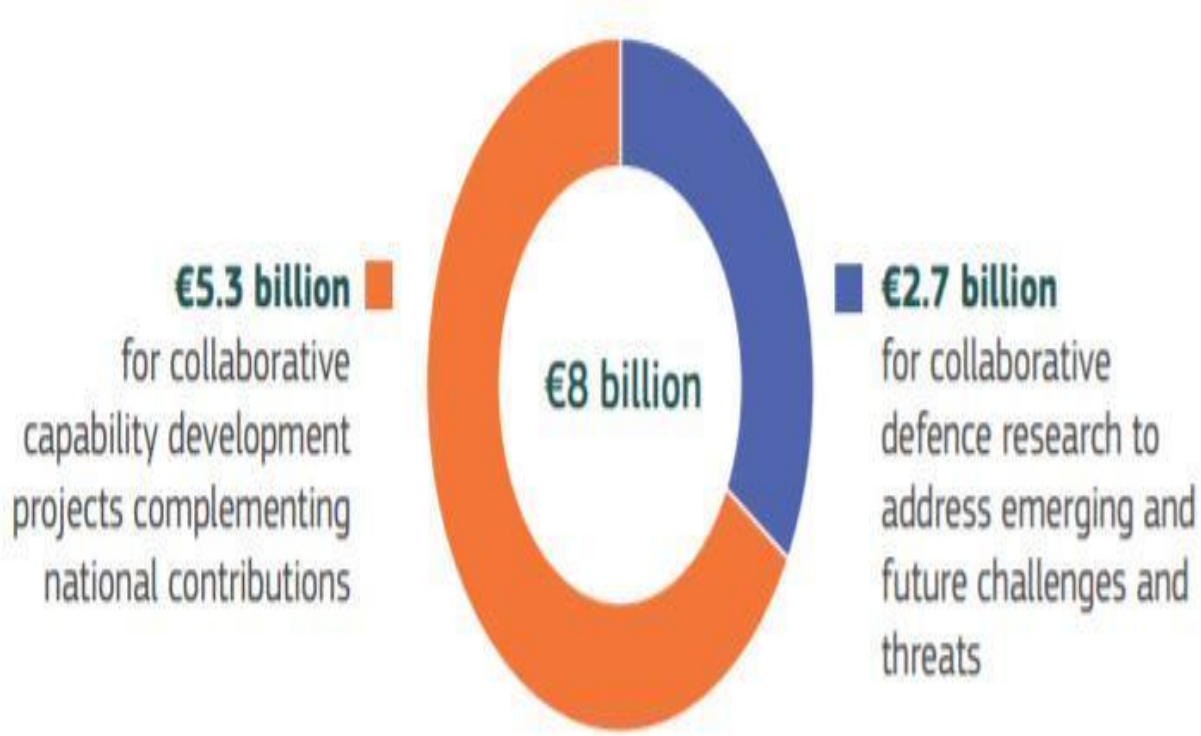
- The ESI Funds are embedded in a normative framework and follow an implementation process resulting from a negotiation between the European Commission and each Member State.

ESI Funds 2021-2027 set out common provisions for seven shared management funds at the EU level:

- CF: Cohesion Fund ;
- EMFF: European Maritime and Fisheries Fund;
- ERDF: European Regional Development Fund ;
- ESF+: European Social Fund Plus;
- AMIF: Asylum and Migration Fund;
- ISF: Internal Security Fund ;
- BMVI: Border Management and Visa Instrument ;

European Defence Funds

Supports initiatives to improve the resilience and security of space infrastructure and operations



EUROPEAN UNION
EUROPEAN DEFENCE FUND

Digital Europe Program

Holds programs to boost the common level of cybersecurity across the EU, underscoring the EU's Cybersecurity Strategy.

Operational objectives:

- **advanced cybersecurity equipment;**
- **knowledge**, capacity and skills related to cybersecurity; best practices;
- wide deployment of effective state-of-the-art **cybersecurity solutions**;
- **capabilities within Member States** and the private sector in support of the NIS Directive;
- **resilience**, risk-awareness;
- **enhancing synergies and coordination** between the cybersecurity civilian and defence spheres;

ECCO

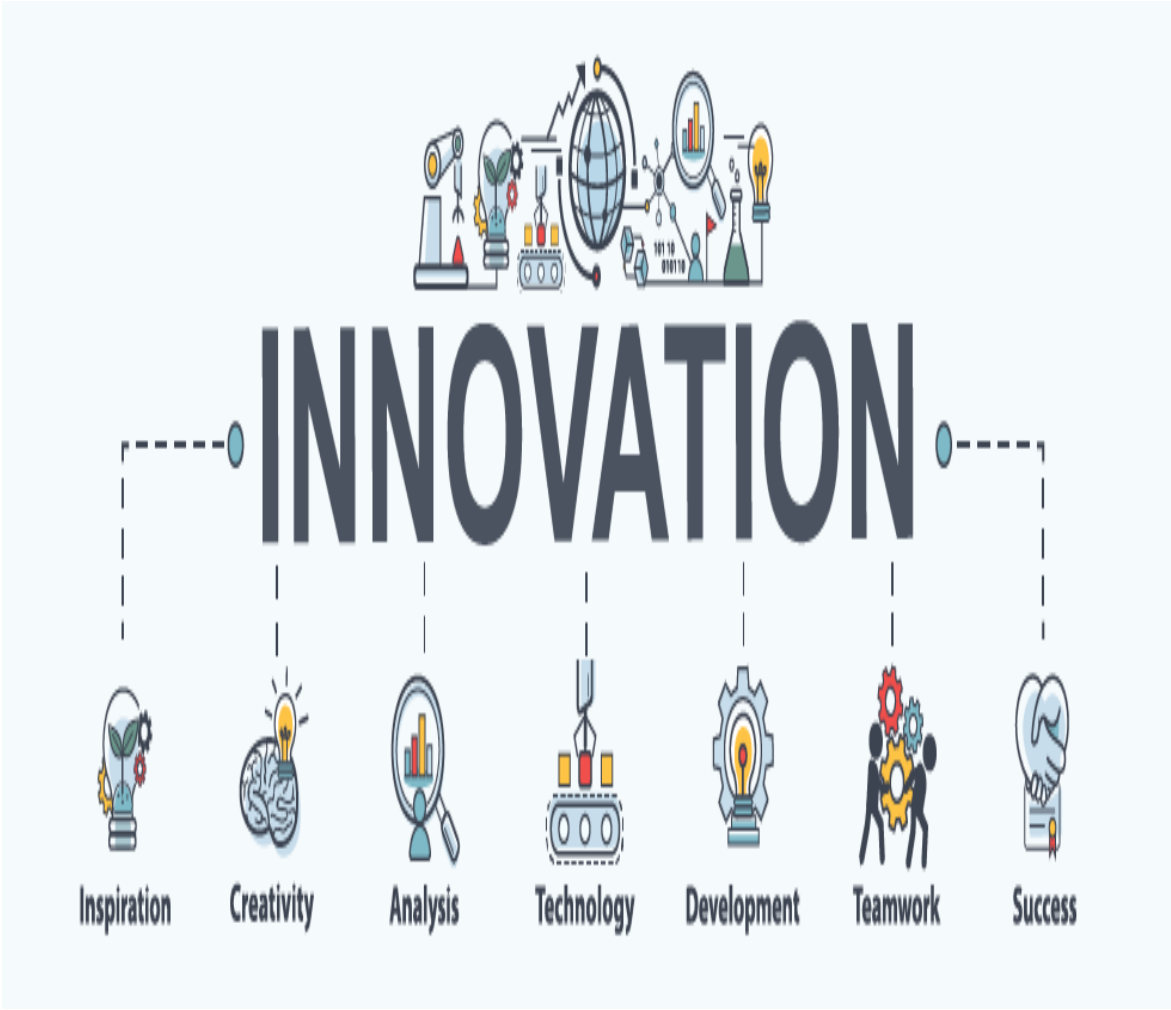
European Cybersecurity COmmunity

Commercial opportunities for space and cyber

Support innovative business

- **Technology transfer program**: facilitate the transfer of space-related technologies developed by government agencies to private companies for commercialization;

- **Regulatory reform and policy advocacy**: advocate for regulatory reform to streamline licensing procedures and promote innovation in the space sector;



Stimulate private sector engagement in space exploration

- **Public-private partnerships**: establish collaborative ventures between government agencies and private companies to share resources, expertise and risks in space exploration projects;
- **Technology development in space/cyber**: support research and development initiatives;
- **Space based services and applications**: foster the development of space-based service and applications, including satellite imagery, Earth observation and weather forecasting;

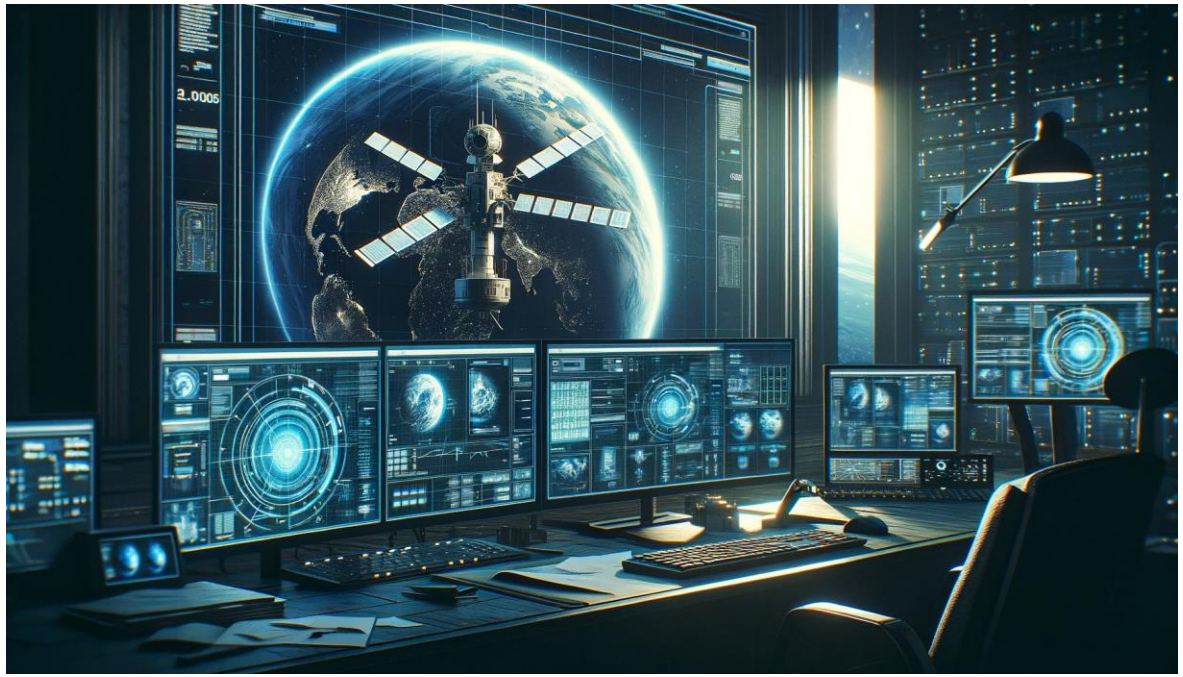
ECCO

European Cybersecurity COmmunity

Upcoming webinars – cyber and space synergies

Next ECCO cyber/space webinars draft topics

- European funding opportunities for space cybersecurity
- Engaging EU stakeholders in space cyber defense
- Strengthening supply chain cybersecurity in the space industry
- Detect and mitigate space cyber threats
- Cybersecurity opportunities in the space industry




ANY
QUESTIONS?