The risk governance model for the supply chain cyber security in space

Ana Maria Matejic

Director Cyber Services and Operations

Gen.B. (aus.) Roberto Mazzolin

Chief Defence, Security and Technology Strategies

Matteo Merialdo

Business Director, Security Engineering & Products

Delia Spinu

Regulatory Consultant

ECCO Community-driven Knowledge Sharing Events

Disclaimer

- ***These sessions are ECCO community-driven and expert-led, reflecting the collective knowledge and contributions of the members of the ECCO Community Groups. They are designed as knowledge-sharing events to build/animate the cybersecurity Community Groups on key topics and share valuable insights among stakeholders.***
- ***The information and opinions in this document are provided "as is" for general purposes only.***
- ***Experts are encouraged to ensure their presentations are accurate and up-to-date.***
- ***The views expressed in this webinar are purely those of the experts and may not, in any circumstances, be interpreted as stating an official position of the European Commission (EC), the European Cybersecurity Competence Centre (ECCC), the ECCO project, or any other EU institution, body or agency. The European Commission does not guarantee the accuracy of the information included in this webinar, nor does it accept any responsibility for any use thereof.***
- ***References to specific commercial products, processes, or services do not imply endorsement or recommendation, and this webinar should not be used for advertising purposes.***

How can NCCs contribute to cybersecurity supply chain in the space sector?

- Promoting collaborative research
- Liaising with the ECCC
- Encouraging cross-sector partnerships
- Education and training

ECCO

European Cybersecurity COmmunity

How are cyber security and space supply chain connected ?

Why the supply chain matters for space

As more nations and private companies enter the space race, the attack surface expands

Threats to the space supply chain are becoming a reality

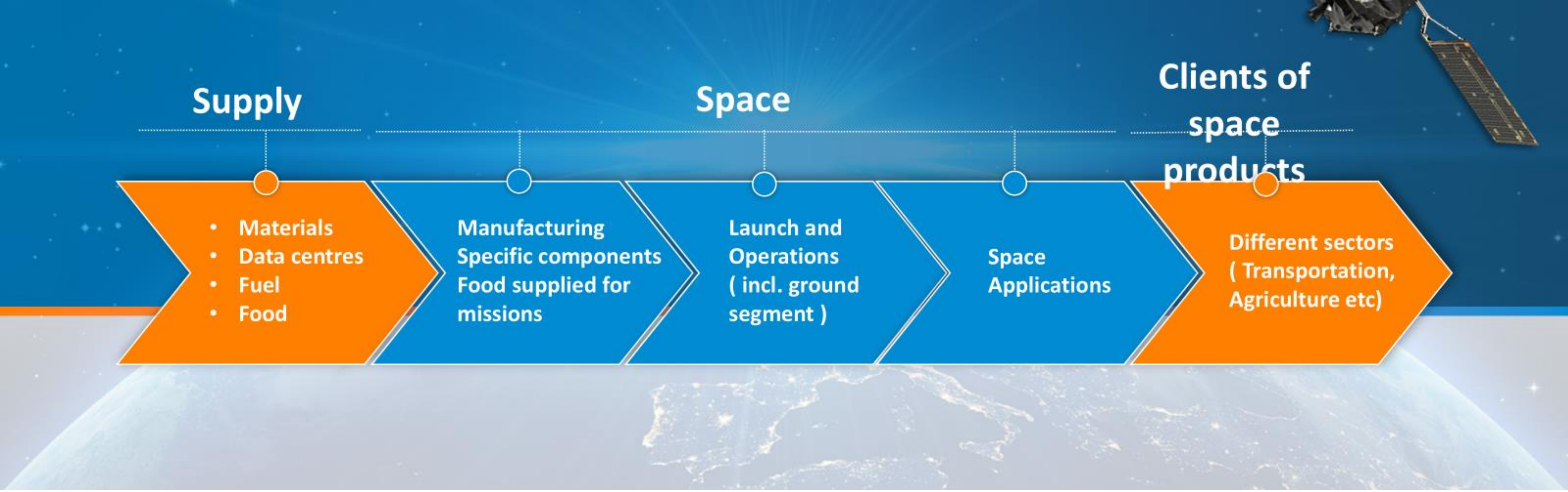
- **Key Questions:**
  - How can we ensure the integrity of components sourced globally?
  - What happens if a vulnerability is exploited after deployment in space?
  - How do we balance innovation with cyber security?
- The consequences of a cyberattack on space infrastructure range from temporary disruption to complete mission failure

In 2022, an American company, Viasat, operated by Skylogic(subsidiary of Eutelsat), encountered a significant cyber attack targeting the supply chain connecting the commercial sector with space operations

- Impact on internet subscribers
- Disruption to German energy company
- Supply chain vulnerability exposed

Can we govern the (un)controlled ?

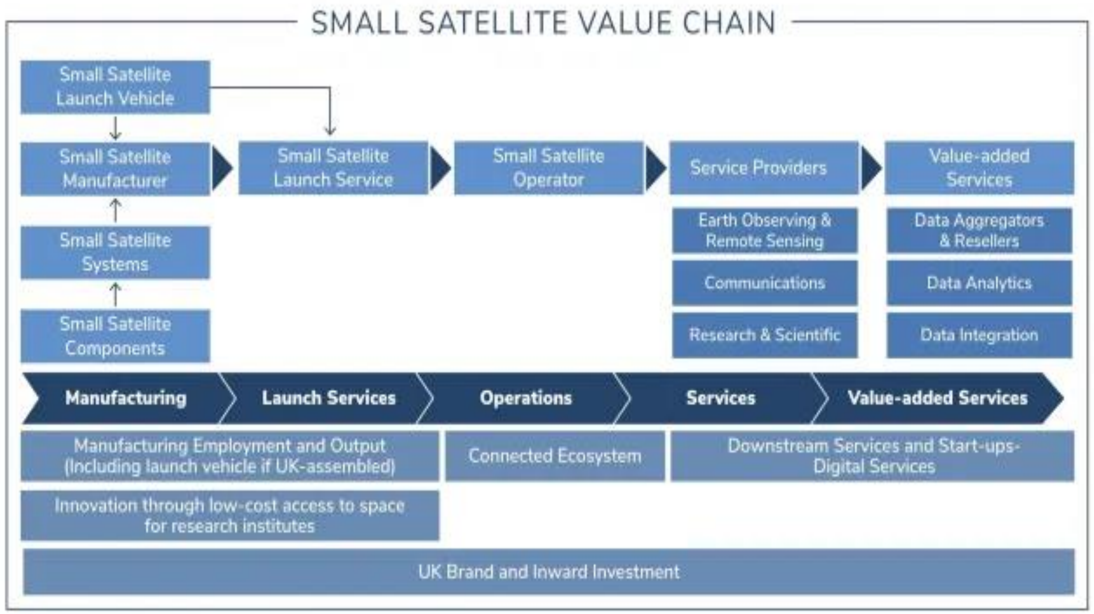
- Space governance looks in 3 directions
  - International governance (cooperation and law)
  - Cyber and Risk
  - Future global challenges (sustainability)
- Cyber security in space starts before the assets are built and become operational
- In the space value chain > supply chains are the trust foundation in the sector
- Governance is .. ?
  - Do we have consistent and adequate procedures throughout our supplier network to identify cybersecurity risks **before** they arise?
- How much is too much ?
  - Can we address the whole supply chain ? Where does the coverage stop ?



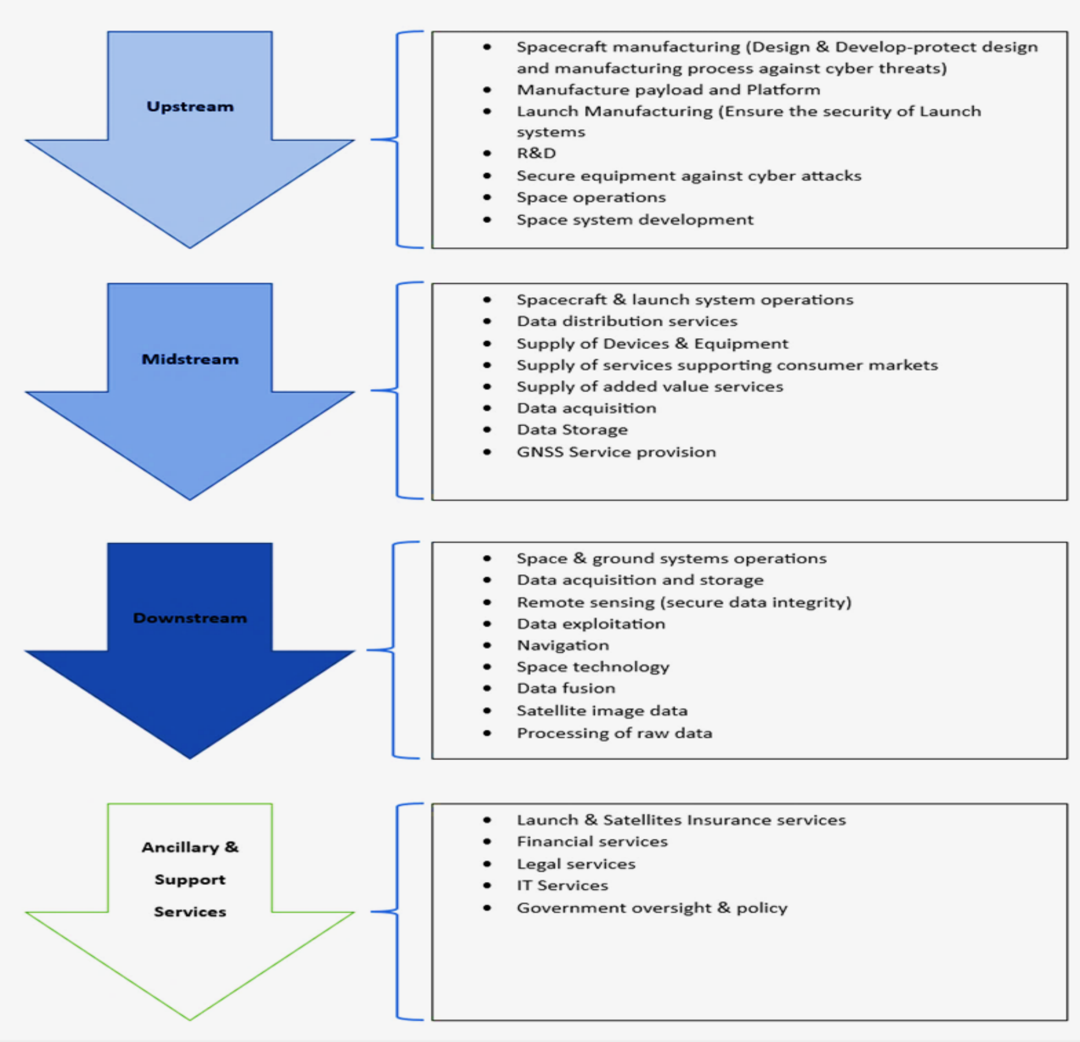
The space supply chain

- In the space value chain > supply chains are the trust foundation in the sector

Space cybersecurity value chain stages



Source: Frost & Sullivan



ECCO

European Cybersecurity COmmunity

Cybersecurity risks in the space sector's supply chain

Cyber threats that affect space supply chain

- Threats in the space supply chain derive from its complexity, length and dependencies/interconnections

The multiple 3rd parties required provide various open doors for malicious actors

- A single compromise of one supplier could result in a supply chain compromise
- Poor information security practices by lower-tier suppliers
- Compromised software or hardware purchased from suppliers

How space supply chain attacks work?

- **Initial Entry Point**

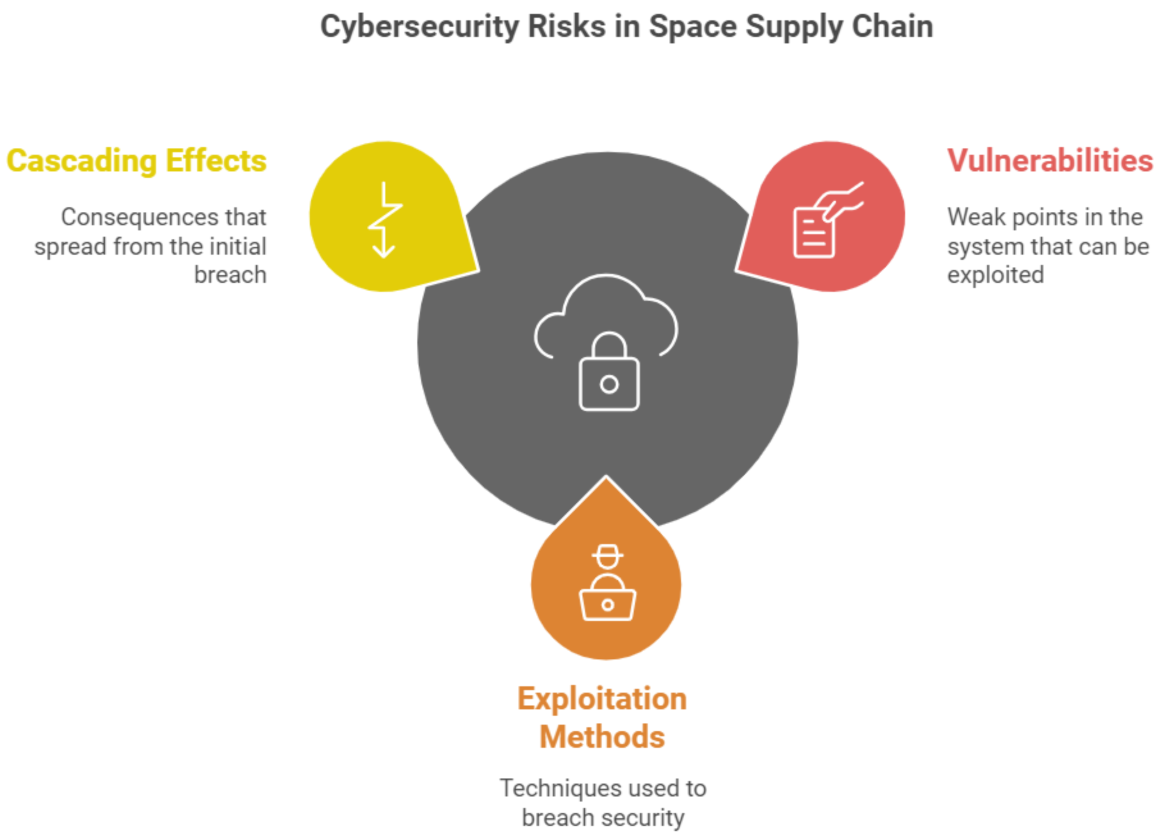
The first line of defense in the space supply chain is often compromised by vulnerabilities that can exist in various forms. Each of the entry points presents an opportunity for malicious actors to infiltrate the supply chain

- **Exploitation**

Once a weak link in the supply chain is identified, it can be exploited to carry out malicious actions. This exploitation may involve the manipulation of software updates, insertion of compromised components, or unauthorized access to sensitive data.

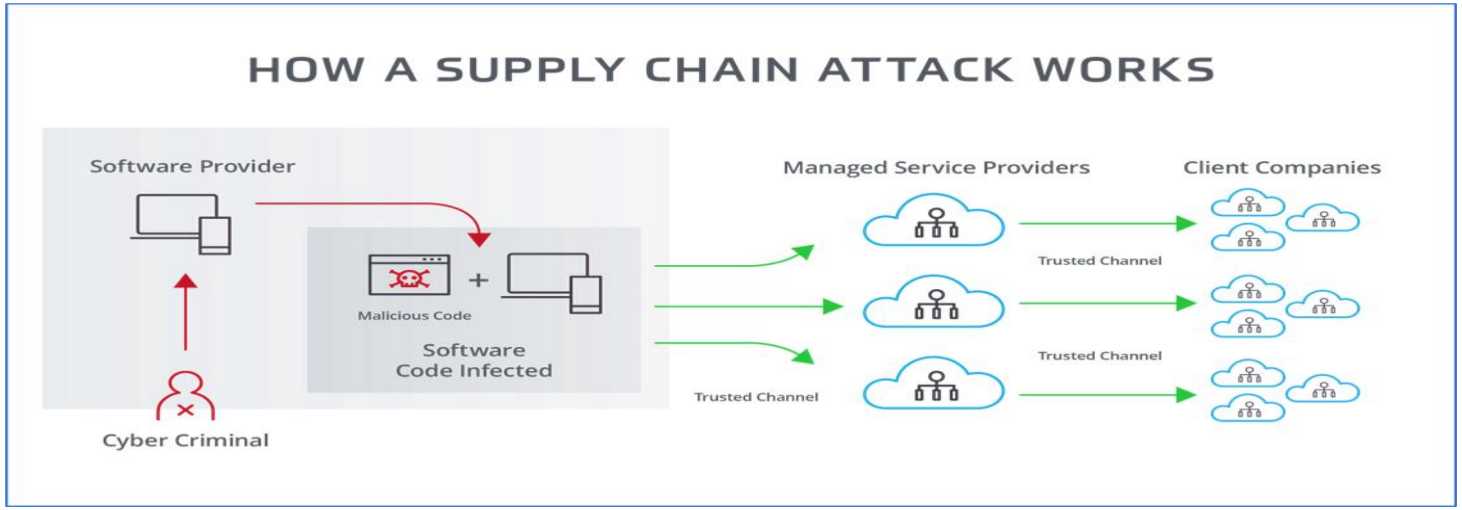
- **Spread**

A breach in one system can trigger cascading effects across multiple networks. This interconnectedness is particularly pronounced in the space sector, where various systems and services rely on each other for functionality.



A few examples

- Unauthorized access or data breaches can lead to information theft, espionage or unauthorized use of classified information
- Denial of Service (DoS) attacks
- Physical security threats
- Space-based communication systems are susceptible to interception, manipulation or jamming
- Regulatory compliance challenges



ECCO

European Cybersecurity COmmunity

The starting point

Define an approach

- Ensure a minimum supplier checklist for cybersecurity hygiene > mostly related to the practices

- Have a risk-based approach in relation with the supply chain

  - Adopt a framework (or a mix) that supports both a risk-based approach towards supply chain and that addresses the space

  - MITRE’s System of Trust framework
    - Having a common taxonomy of supply chain risks for suppliers, supplies, and services
    - Creating consistent supply chain security assessments and risk discussions.
    - Informing data driven decisions about supply chain risks.
    - Supplying a broad understanding of the available sources for supply chain risk assessment information

  - NIST for Commercial Space Operations

In the operational environment

- Incident Response Plan

  Understanding how to tackle a potential supplier/subcontractor breach and to assess the exposure risk

  Isolation and forensics analysis play a critical role in the plan

- Source Code Analysis

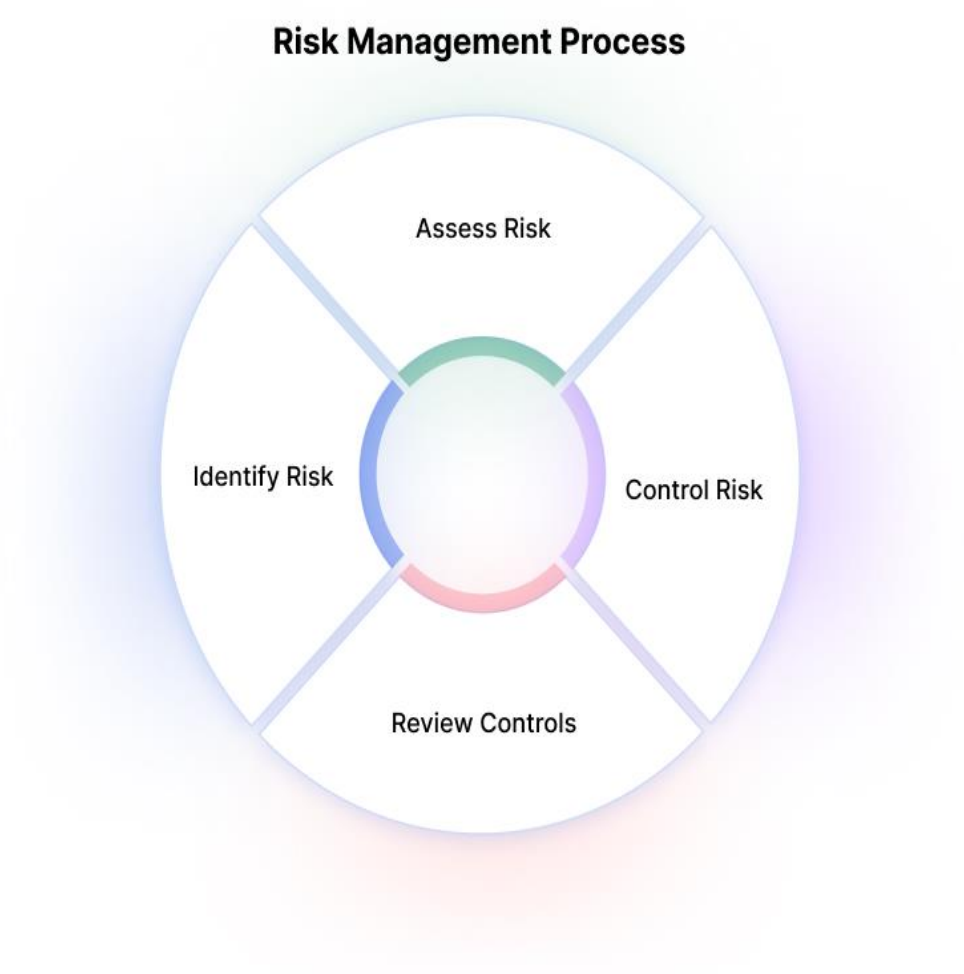
  Conduct source code analysis to detect potentially suspicious code blocks or malicious software

- Vendor Risk Management

  Continuous monitoring and regular assessments

- Firmware verification

  Especially applicable on memory chips (as a use case)



A case study: supply chain security in Manufacturing, Assembly, Integration and Testing processes

- MAIT processes are critical to developing reliable and functional space systems

- Ensures components are manufactured to specifications, assembled correctly, integrated seamlessly, and thoroughly tested
  - Within complex N-tiers consortia

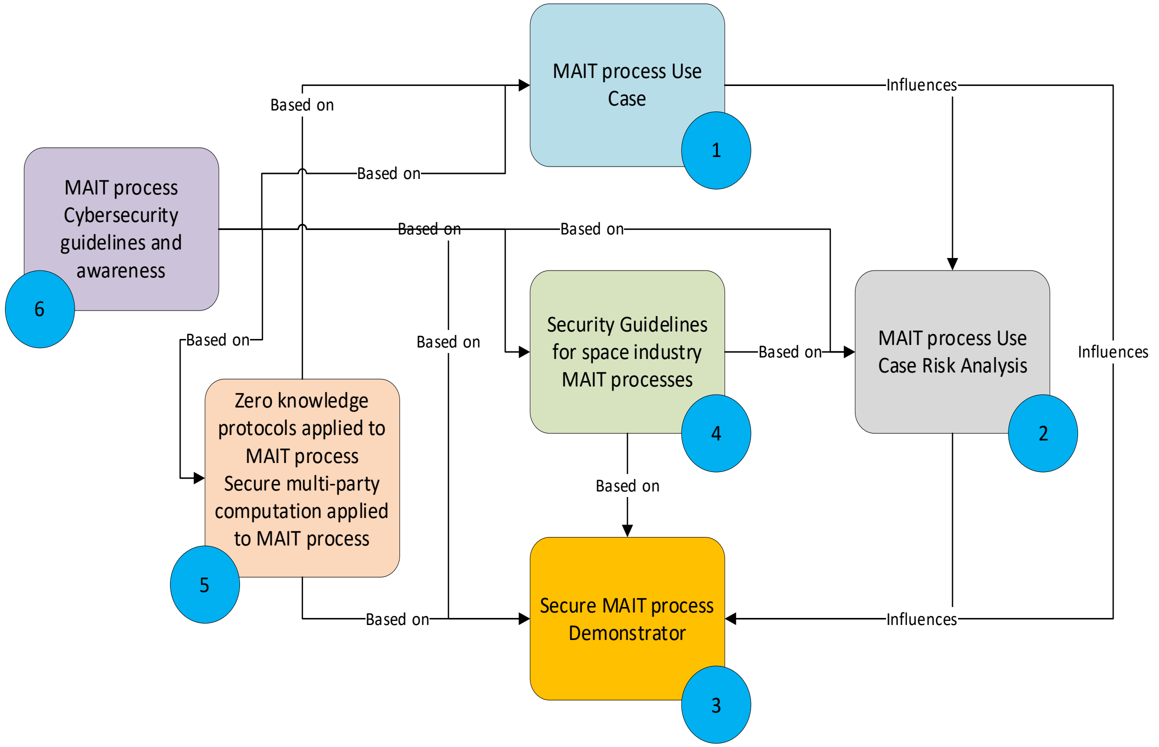
- Compromises in MAIT processes can lead to failures or malfunctions in the final product

Cybersecurity to Protect and Allow Exchange of Manufacturing Data

- PAEMD was a research activity within the ESA GSTP framework

Objectives

- Apply cyber security risk governance to protect data in MAIT processes
- Identify data protection needs and cyber risks
- Assess applicability and efficacy of security measures
- Select and tailor cyber security measures for specific MAIT processes
- Develop guidelines for secure data exchange in manufacturing

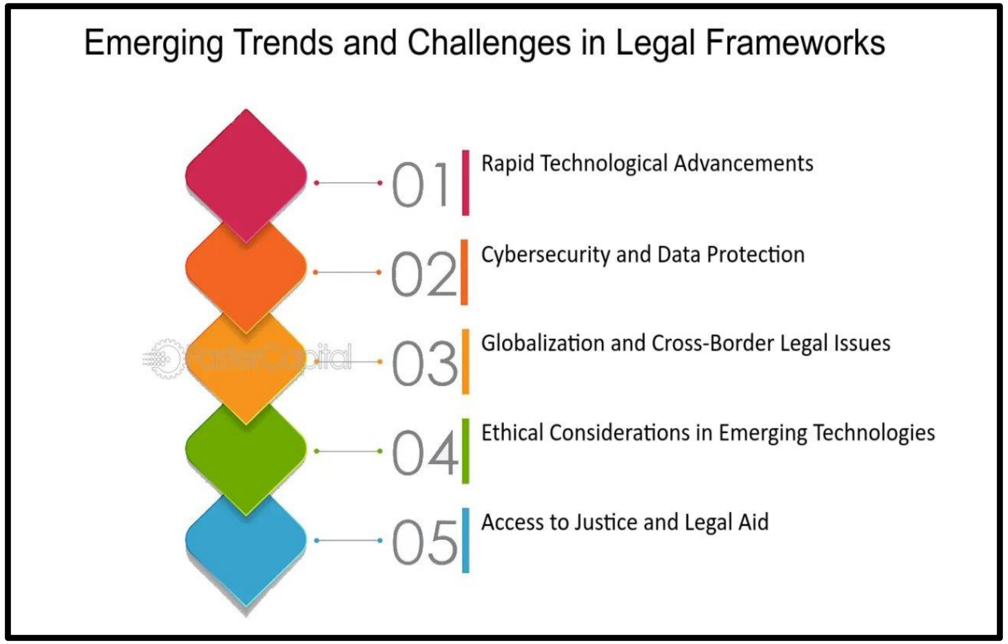


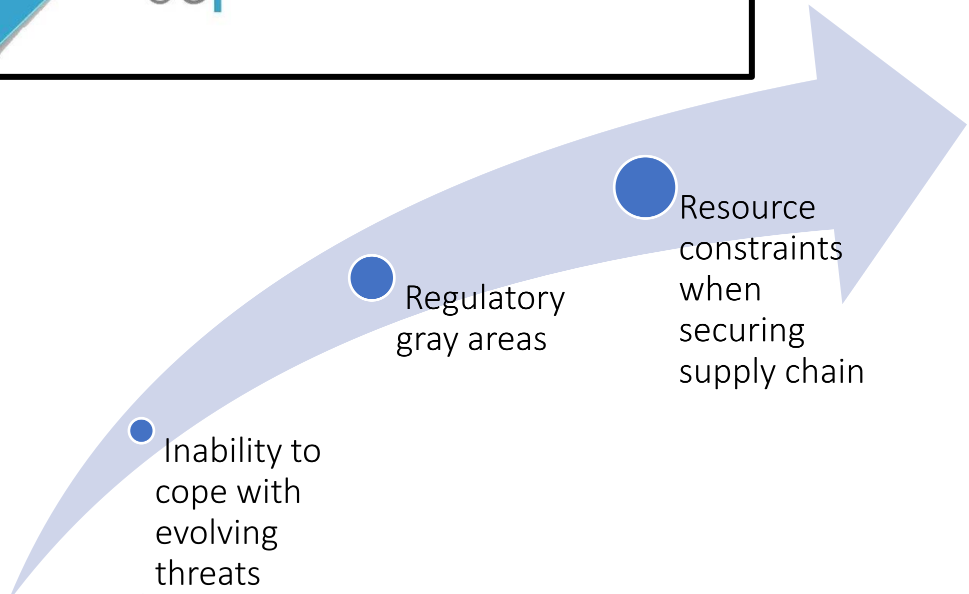
ECCO

European Cybersecurity COmmunity

From Regulatory gaps to robust supply chain security in the space sector

EU's legal framework: an old challenge





- Previous EU legal framework didn't address **supply chain security**

Member States were guided by strategic considerations and not by legal norms

- Complex jurisdictional challenges for regulatory bodies
- Difficulty in identifying responsibilities due to complex supply chains
- Heterogeneous legal approach to space cybersecurity
- Tensions arise with different interests

International laws

Outer Space Treaty (OST, 1967):

- State supervision and responsibility
- Non-appropriation of space and freedom of exploration
- Non-militarisation of space and disallowance of weapons of mass destruction

United Nations resolutions:

- Multiple principles including some on Direct Broadcasting (1982) and Remote Sensing (1986)

International conventions, including:

- **1972:** Convention on international liability for damages caused by space objects
- **1975:** Convention on the registration of objects launched in outer space
- **1979:** Agreement governing activities on the moon and other celestial bodies

UNCOPUOS guidelines:

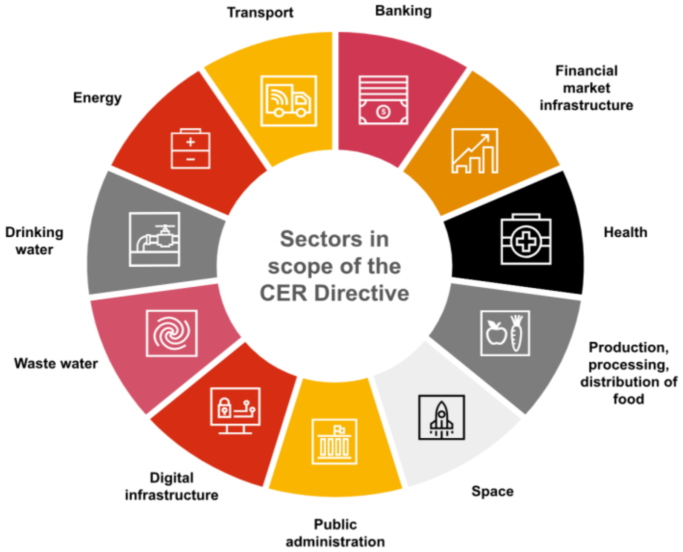
- **2010:** Space Debris Mitigation Guidelines
- **2019:** Space Activities Sustainability Guidelines

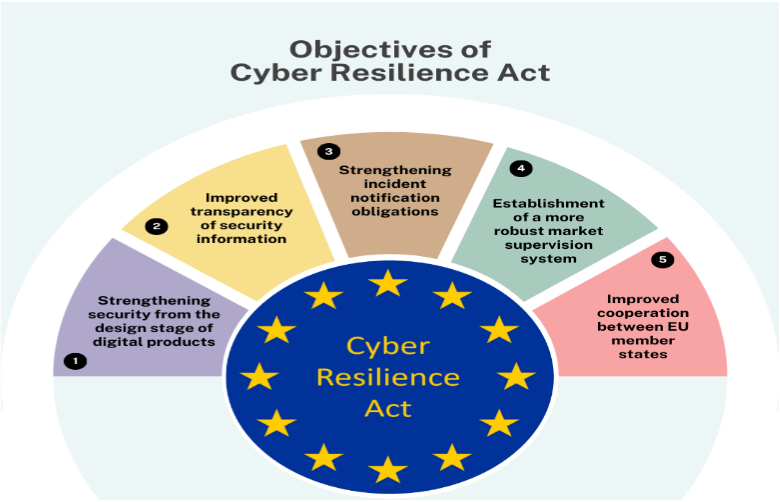
International Telecommunications Union (ITU):

- ITU Constitution and Convention
- ITU Radio Regulations and Frequency Allocations

Bilateral/Multilateral agreements, including:

- **2023:** Artemis Accords (36 nations signed so far)
- Regional space working groups
- **Agreements between space agencies and space corporate entities** (i.e. SpaceX/NASA agreements)





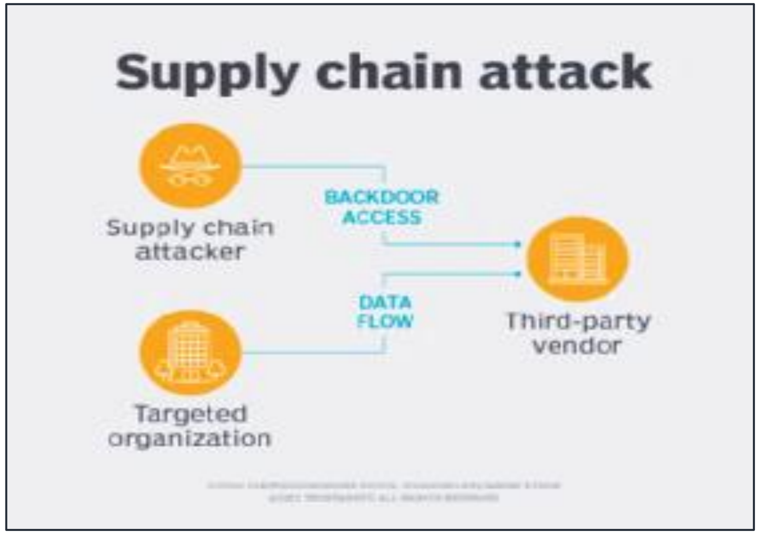
From an outdated legal framework to a robust regime

Why NIS2 is a milestone for space cybersecurity?

The space sector is a target of supply chain disruption attempts

Supply chain cyber security is crucial to ensure the integrity and reliability of assets

Increasing reliance on third parties demands a deep understanding of the risks associated



Key aspects to consider when selecting third-party suppliers in the space sector :

- ✓ They must comply with the NIS2 Directive's security guidelines
- ✓ Check whether suppliers have implemented robust cybersecurity measures

How NIS2 impacts the supply chain?

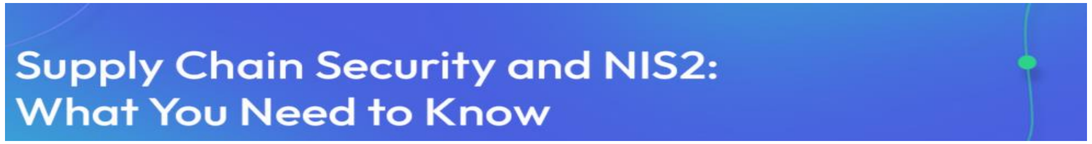
ECCO
European Cybersecurity COmmunity

- Cybersecurity risk management measures are integrated into agreements with suppliers and service providers

- Millions of organizations will have to comply as suppliers

- Not covered by NIS2 ≠ immunity on supply chain requirements : delivering services to in scope entity requires a **minimal cybersecurity maturity**

- The supplier will be supervised by his customer



How to ensure supply chain resilience in the space sector?

Categorization

- List all the organizations in the supply chain
- What is their criticality in your supply chain risk assessment?
- Based on the result, assign appropriate cybersecurity measures

Contractual obligations

- Cybersecurity clauses including each party's responsibilities
- Cybersecurity expectations
- Incident reporting timelines
- Risk management protocols
- Information security measures

Monitoring

- Audits
- Vulnerability scanning
- Penetration testing on the systems provided by suppliers

Incident response plan

- Integrate third party suppliers into the incident response plan
- Incidents must be reported promptly
- Any incident affecting a third party supply must be communicated to the primary entity

How do you link third party and incident response under NIS2?

- Report significant incidents → based on the consequences → Very simple notification in 24h
- Ensure that your third party suppliers have clearly instructions on how to communicate incidents that affect your operations

European Commission Regulation on NIS2:supply chain security

Supply chain security policy requirements

- Assess cybersecurity practices of suppliers
- Ensure suppliers' ability to meet cybersecurity specifications
- Evaluate the quality and resilience of ICT products and services
- Leverage security risk assessments in alignment with NIS2

Contracts should specify

- Cybersecurity requirements for suppliers
- Supplier requirements for employee training, awareness
- Obligations for incident reporting, vulnerability handling and audit rights

Supplier monitoring and evaluation

- Monitor reports
- Review incidents
- Assess needs for unscheduled reviews

Supplier directory requirements

- Maintain up-to-date registry of suppliers

Supply Chain Security for Space-ECCO

Gen.B. (aus.) Roberto Mazzolin

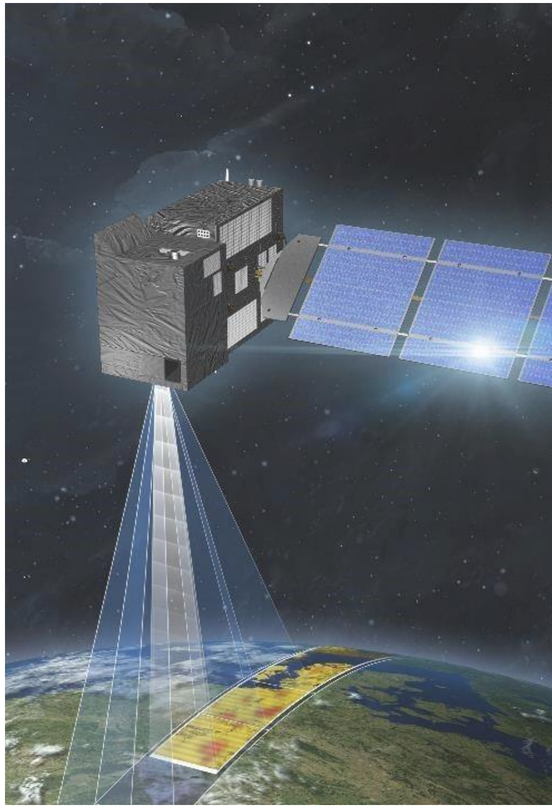
Chief Defence, Security and Technology Strategies

A World of Risks Threaten Supply Chains

Trends / conditions driving risks, including:

- Global markets, technology and industry with supply chains operating across geographical, political, social, cultural and economic environments
- Supply chains yield advantages and exposure to risks
- Competition and conflicts
- Climate change and Dynamic interplay of a wide array of risk types: Natural Disasters /Human-Made Disasters/Geopolitical & Economic Events/ Regulatory Actions/ Reputational / Political/ Fragile Supplier Enterprise Management Workforce / Talent Losses/ Single / Sole Sources/ Foreign Influence / Dependency Product / Service Security Cyberattacks Transportation / Logistics/ Litigation/ Coronavirus Pandemic

Limited Visibility into Supply Chains = Unknown Risk Exposure



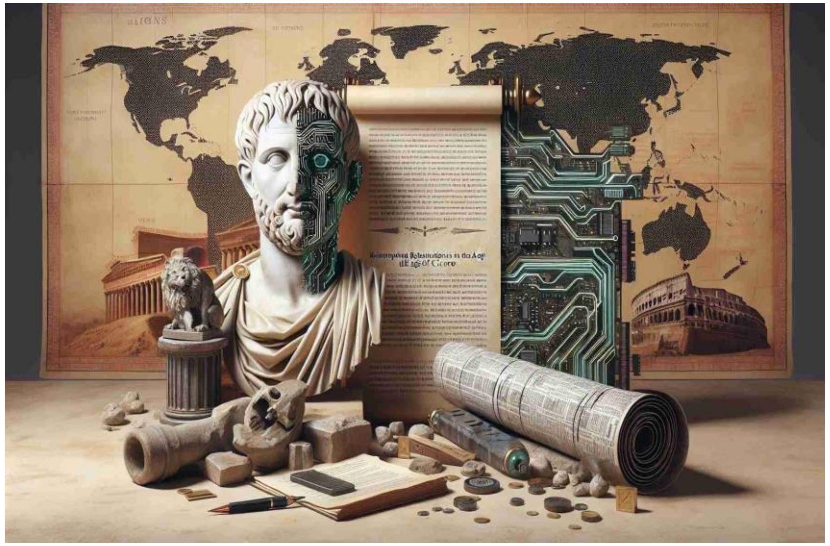
Geopolitical Context

- Covid and Russian invasion of Ukraine highlighted global industrial dependencies and strengthened concept of strategic autonomy – continued Russian threat

-China continues to develop offensive space capabilities

-Growing competition between space faring nations and militarization of outer space – response doctrine not normalized

-Increasing isolation of US - Administration policies/Executive Orders: “Made in America”/....maximize the use of goods, products and materials produced in, and services offered in, the United States /.. strengthen the resilience of supply chains across the nation’s space industrial base



Risk Examples – Impact all Levels of the Value Chain

- Growing demand and geopolitical crises disrupted supply of noble gases (neon, xenon, krypton) Russia's illegal annexation of Crimea disrupted Ukraines steel industry, which was source of 90% global neon gas supply- Shortage of neon gas disrupted Taiwan Semiconductor Manufacturing Company and others as neon is key input into semiconductor manufacturing.

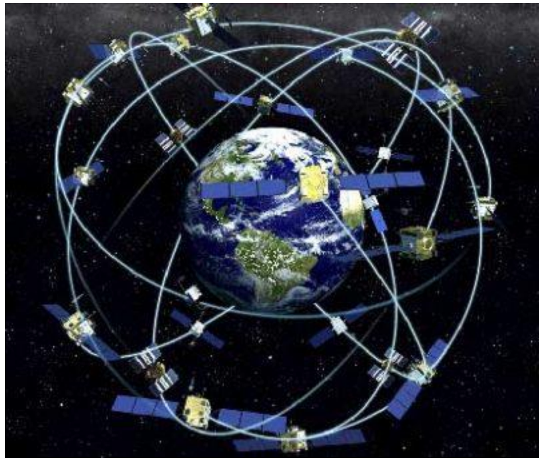
- Increasing Chinese development and production/US ban on NVIDIA chip export to China/Chinese development of military capabilities -US DARPA avoids Chinese components – reviewing suppliers with Russian ties

- Viasat KA-SAT network attacked February 2022 which distributes services via 3rd party during acquisition by Eutelsat

- OneWeb paused constellation deployment after suspending use of Russian Soyuz rockets

- BAE satellite manufacturers identified 5th party supplier of cameras was Chinese

- Increasing restrictions around technology sharing under US ITAR



Key Observations – So What?

- EU Space Sector missions rely upon multitiered, interconnected and global supply chains of commercial, non-profit and government organizations to develop and operate complex, high-value and innovative systems for the community

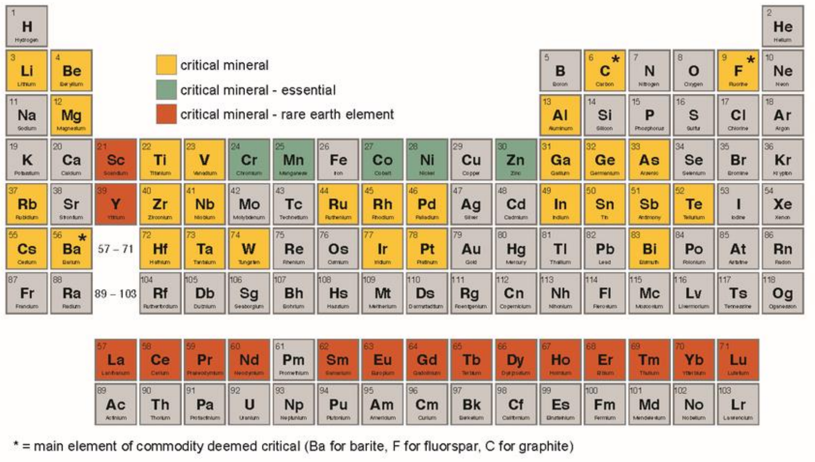
- EU is a space power with a significant industrial capacity & know-how but its value chain is exposed to supply risks / industrial dependencies

So what?

- More targeted criticality assessment is needed for key components and materials - This monitoring requires an adapted methodology based on a life-cycle thinking approach. The sector has been already successful with supply chain management, e.g. with obsolescence risk management programme…

Critical Elements

- Raw Materials – Metallic Alloys, Nozzles, Li-ion batteries, Electronics, Solar Cells, Propellant Tanks, 3D printing parts, Optical instruments, Sensors, Metallic Alloys, Reaction wheel
- Particular focus on Rare Earth Elements
- Titanium,- 40% global production from Japan/Russia/Kazakhstan Cobalt, Xenon - Ukraine, Krypton
- Key Technologies – Solar, Wind Turbines, Fuel Cells, Batteries, Motors Robotics, 3D Printing, Drones, Smartphones/Computers/Rockets/Satellites
- Sectors - Renewables, E-mobility, Energy Industry, ICT, Defence and Aerospace



Issues 1

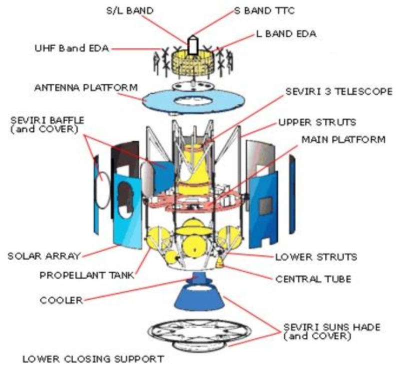
- Space communication technology impacts lives of non-terrestrially connected population – expected to create 1.2 Trilion Euros of retail revenues between 2020-2030 – influx of private actors where once was only government players

- Space Services support essential services such as military, utilities, aviation and emergency comms – directly drawn into geopolitical conflicts

- Increasing government focus on identifying users and providers profiting from space dependent technologies and securing end to end cyber resilience – need for collaboration – difficult given geopolitical situation and ITAR regulations

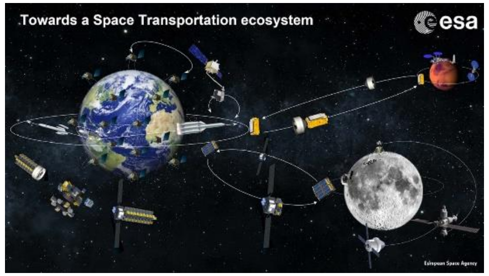
Typical Space System Complexity

Capability= spacecraft + instrument + Ground Segment + Launch Facility + User Community



-Just the satellite-

- Subsystems, assemblies, components, parts, materials
- Approx. 350 products tracked
- Approx. 70 suppliers, located in Europe and 5 other countries



Extends to Raw Materials, Advanced materials and Components, Design and Manufacturing, Final Assembly Lift Off, Use Phase data generation and storage, Post mission disposal (space debris mitigation)

Supply Chain Security in the Space Sector - It Starts with Cyber

- Space Assets, including related industry are high value targets-Data is main product

- Space Services used to be separated from Terrestrial networks-now interdependent

- Customization widespread – long term development- long lead times for materials – changes very difficult/impossible to effect post launch- need right partners

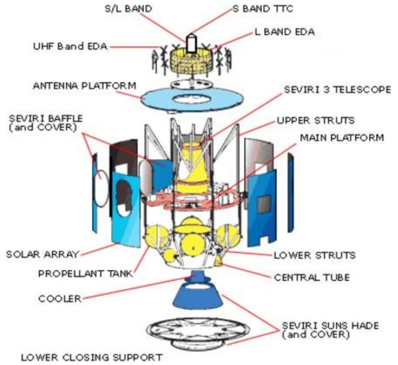
- Safety and resilience tests essential for electronics (radiation effects) and software in remote settings

- Testing for Ground control processes when breach occurs- opportunities for automated response systems

Unique Vulnerabilities of Space Technologies and Systems

- Not limited to ground stations, data links and satellites but vulnerable at multiple interconnection points

- Traditional satellite development was "boutique" – new space increasingly uses COTS components – therefore, all satellites are vulnerable if any part of shared supply chain is corrupted – with wide reaching impacts



- Increasing commality with terrestrial based IT protocols – many unencrypted

- Traditional satcom based ICT protocols well understood and legacy systems have weak/no encryption

- Satellites have limited hardware and storage, memory and power on board – what you see is what you get at launch – complicates insertion of defensive software

- Increasing adversaries placing assets in orbit to establish command link intrusions – risk of loss of operational satellite control

Solution Space – Operational Principles

-Strategy – do projections account for time/cost of cyber security protection in upstream operations

-Technology – Proactive management of opportunities for vulnerabilities ie equipment upgrades and system updates

-Service Delivery Models – Communication/coordination of precautions and procedures with customers to develop trust and confidence

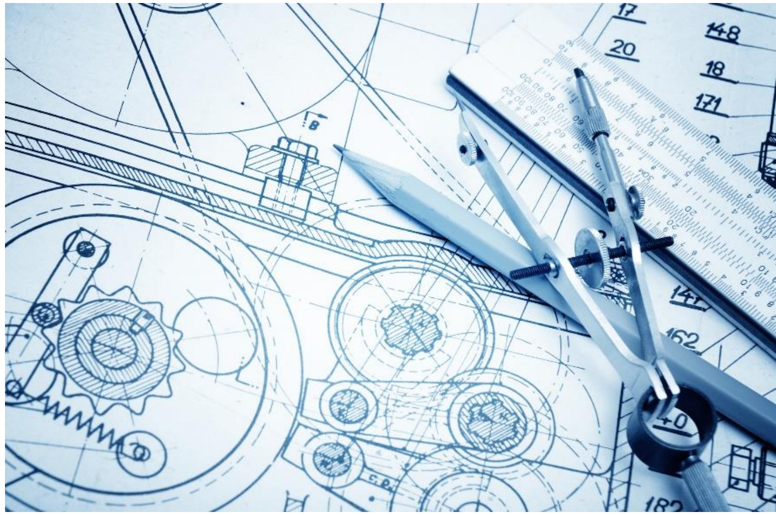
-Organizational Culture and Skills-Supplier and 3rd party workforce able to recognize breach attempts and trained to act

-Governance – Consistent and adequate procedures through supplier network to identify cybersecurity risks when they occur

-Increase collaboration and information sharing among government organizations, commercial industry, and international partners - ISAC

Solution Space – Design Principles

- Use of AI and related tools to guard against persistent attacks on satellite operator’s network
- Software development review in ground segment and space platform
- Incorporate cybersecurity into all stages of space system development – agile system engineering through Concurrent Design
- Increase collaboration and information sharing among government organizations, commercial industry, and international partners - ISAC
- Increasing adoption of government/military standards for space system development – baseline security standards for cyber components - US DoD Cybersecurity Maturity Model Certification (CMMC)



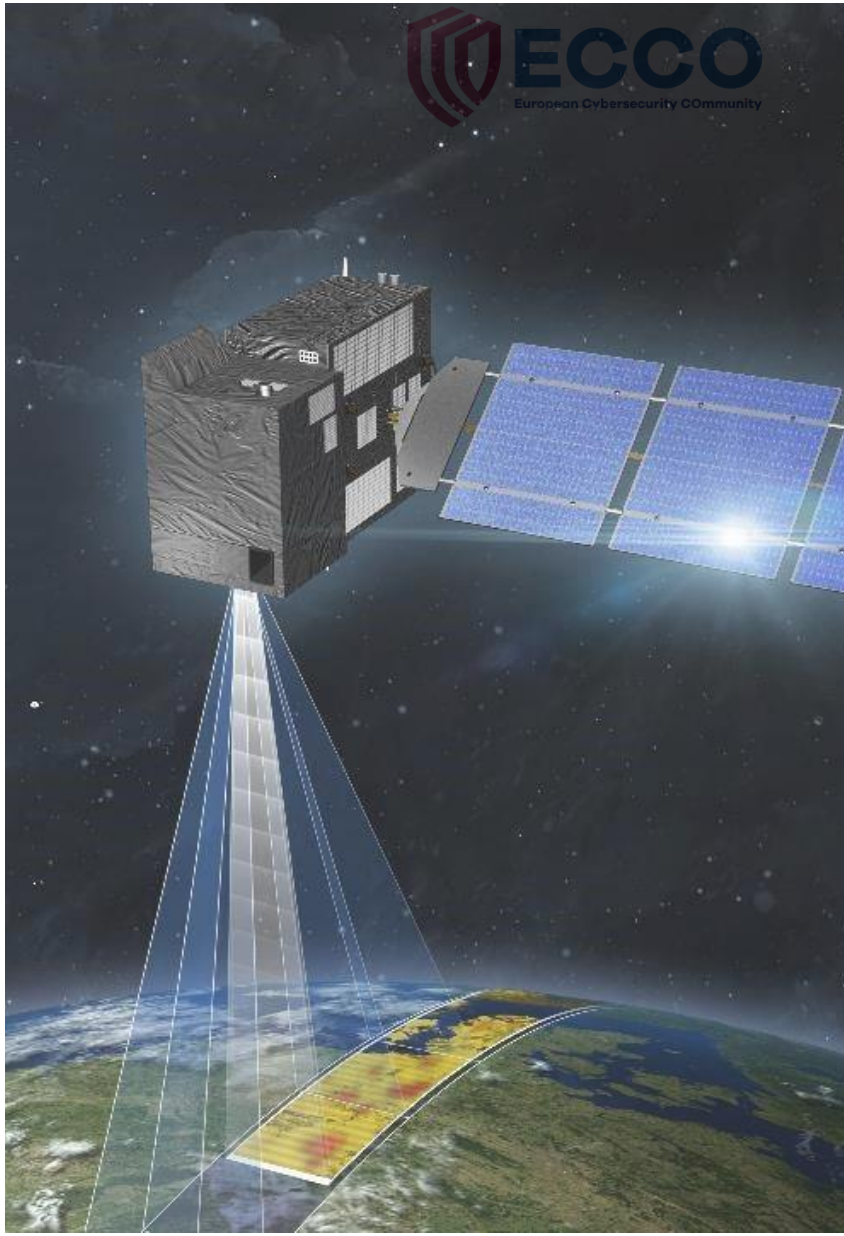
Solution Space – Resiliency through Defence in Depth

- Build resilience using Defence in Depth Model
    - Fortify systems at multiple levels
    - Redundancy in defences- ML based automated responses on both satellite and ground segment
    - Provide not only preventative but detection and recovery measures
    - Leverage modelling and simulation technologies (Cyber Ranges) to find weaknesses
- Move industry toward greater awareness
    - Cybersecurity built in to every layer of spacecraft design and supply chain – fundamental shift to operations
    - CSOCs

Composite of Critical Enablers

- Identify Supply Chain Risks
- Build Visibility and Shared Insight through
    - Data- Information – Knowledge- Wisdom
- Leads to Awareness and Foresight
- Results in Informed Decision Making
- To enable Actions at Strategic, Tactical and Operational levels

"You don't know what you don't know"




ANY
QUESTIONS?