

Earth Observation Veracity Proof of Concept Verification

Second Public Webinar



Virtual, 3rd of June 2026

Ref: EOVerPoCVerif.PRE.014

Please avoid printing this colourful slide. Let's save the planet together.

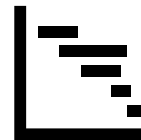


Agenda

- Welcome & Project Summary
- The Importance of Data Veracity
- Methods of Interference in EO Veracity
- Next Steps
- Deliverables and Benefits
- Interactive Q&A and Feedback

EO Veracity

PROOF OF CONCEPT VERIFICATION





Interactive Session

- We are using Mentimeter
- Answers are completely anonymous
- Please go to menti.com
- Enter the code **3250 0769**
- Alternatively scan the QR code:





Project Summary

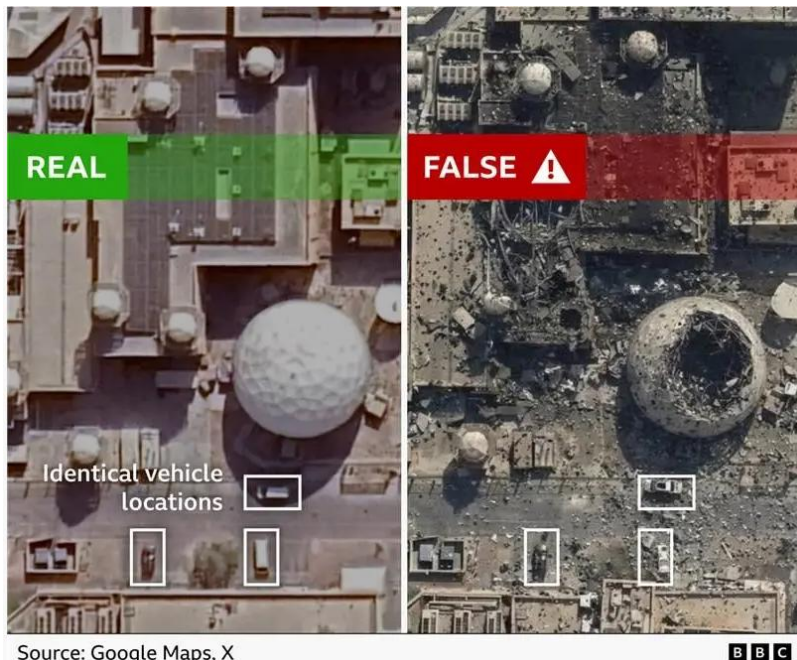


PROOF OF CONCEPT VERIFICATION

Why verify EO products?

Earth Observation scenes are open to **manipulation** and **misinformation**

Example of manipulated EO imagery



- Geopolitical misinformation
 - Influence **strategic decisions**
 - Affect **international opinions**
- Environmental manipulation
 - Exaggerate/reduce **natural phenomena**
 - Directly affect **policies and markets**
- Have you come across manipulated EO data?



The Project

ESA funded project

Kicked off in September 2025

Running until February 2027

Investigating:

- How EO data could be **interfered with**
- How to **counter this interference**, and
- How to **guarantee the veracity** of the information provided

Project Team

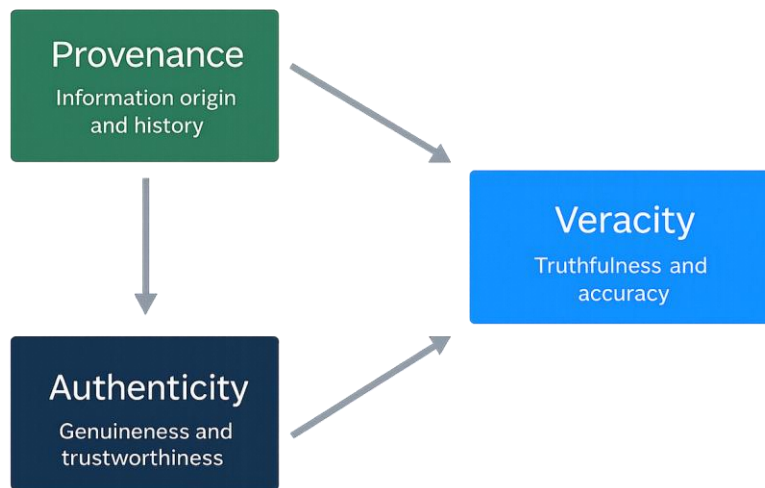




What does veracity mean?

What word comes to mind when you think about data veracity?

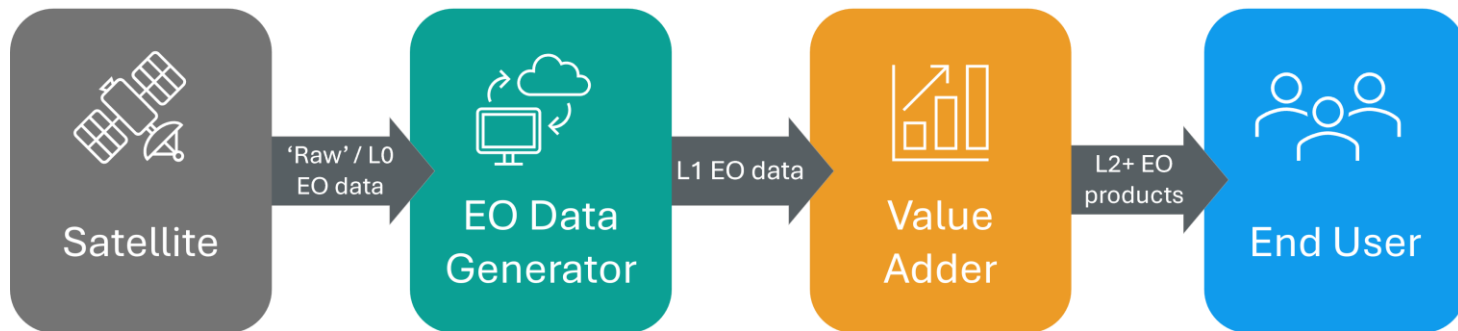
The Three Dimensions of Data Integrity





EO Supply Chains

Example EO Supply Chain



Which EO supply chain role best describes your work?

EO Supply Chains

- Activities focus on four example EO chains:
- **Sentinel-2:** data acquisition & processing (L0 → L2A) to dissemination
 - **SEonSE:** near real-time maritime situational awareness
 - **FloodSENS:** AI-powered flood mapping
 - **EUGENIUS:** Border Permeability Mapping





Objectives

Objective 1

Elaborate the EO end-to-end information generation chain that could be open to interference



Objective 2

Characterise types of potential interference and the expected consequences



Objective 3

Specify methods to detect potential interferences

Objective 4

Specify methods to counter interference and formulate a methodology integrating these methods



The Importance of Data Veracity



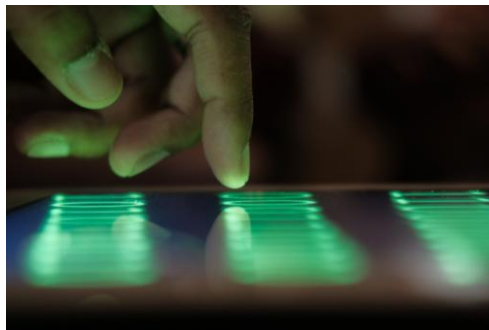
PROOF OF CONCEPT VERIFICATION





The Situation

-  Satellite imagery once considered a highly reliable source
-  Recent rise in fake information questions this
-  Ability for information to spread rapidly increases threat
-  EO data chains often don't consider potential vulnerabilities





The Problem

Are you certain of the **veracity** of the data you are providing or using?

- Do you know the **provenance** of your input data?
- How can you prove the **authenticity** of your EO products?
- Are you concerned about the veracity of the data you use?
- Recently, digital data, including EO data, is under attack more regularly – are we ready for it?



The Solution

- **Understanding where** your EO chain could be open to interference
- Knowing what to do to **counter such interference**
- Putting in place methodologies that **safeguard your EO chain**
- Being able to **ensure your customers** of your EO data veracity



We can help!

EO Veracity

PROOF OF CONCEPT VERIFICATION





Methods of Interference in EO Veracity

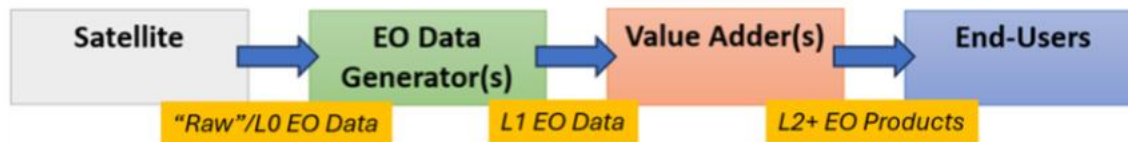


PROOF OF CONCEPT VERIFICATION





EO Data Chain Overview



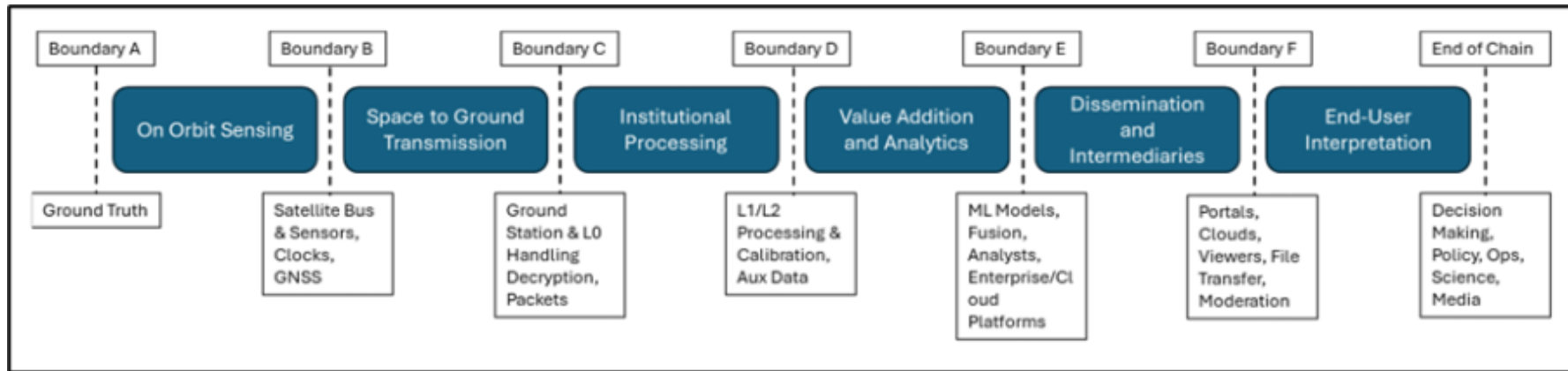
Identified in Task 1:

- End-to-end flow: sensor to user
- Multiple systems, organisations, and data sources
- Includes processing, fusion, and dissemination
- Trust built (and lost) at each stage



Trust Boundaries in EO Data Chain

- Trust is not continuous across the EO chain
- Boundaries where assurance becomes assumption
- Shift from technical integrity to interpretation
- Veracity risk increases downstream





Threat Actors

- Diverse actors with different motivations
 - Range from highly capable to opportunistic
 - Target data trust, not just systems
 - Often operate long-term and covertly
- 
- Nation-state actors
 - State-sponsored/APTs
 - Organised criminal groups
 - Hacktivists / ideological groups
 - Insider threats
 - Commercial competitors



Methods of Interference

- Data Tampering – altering data, metadata, or processing
- Unauthorised Access – gaining covert control within systems
- Intermediary Manipulation – changing how data is delivered or displayed
- Supply Chain Disruption – compromising trusted dependencies





Methods of Interference

- Source Manipulation – injecting entirely fabricated but plausible data
- Content Fabrication – distorting interpretation and narrative





Impact on End Users

- Distorted situational awareness
- Incorrect or delayed decision-making
- Corrupted analytics and modelling outputs
- Reputational, operational, and financial consequences





Conclusions

- EO systems are robust but not inherently trustworthy
- Veracity degrades across the data chain
- Trust is often assumed, not verified
- Small, subtle interference can have large impacts



Next steps



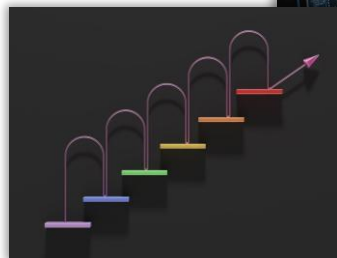
PROOF OF CONCEPT VERIFICATION





Detect and counter interference

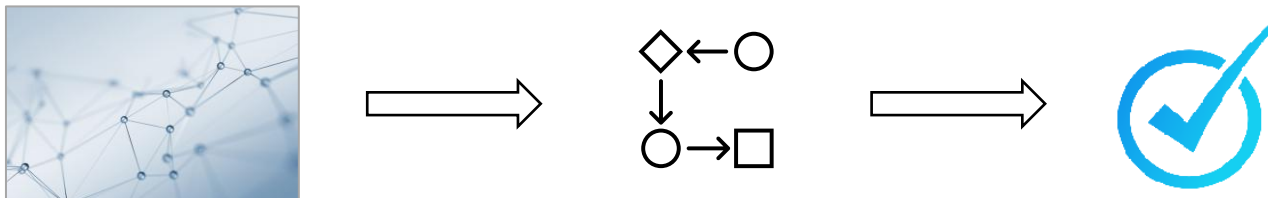
- **Focus** on potential interference identified in previous task
- **Identify** countermeasures to these potential interferences
- **Evaluate** countermeasures, which take the form of:
 - Technical solutions
 - Human-centred approaches
 - Procedural methods





Develop EO veracity methodology

- A process ensuring EO data veracity across the whole EO chain
- Approach follows three phases:
 - Development of **EO Veracity data model**
 - Development of **Standardised Assessment Methodology**
 - **Formalisation and Standardisation** of proposed Methodology





Deliverables and Benefits



PROOF OF CONCEPT VERIFICATION





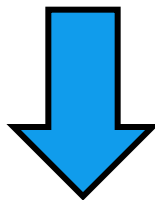
Project Deliverables

Report detailing assessment of elements of the end-to-end EO chain

Report characterising the nature of potential interferences

Report describing methods to detect and counter interference

Report outlining end-to-end veracity methodologies



**Roadmap for EO companies interested in
protecting the veracity of their EO information chains**



Public Outputs/Activities

- Event attendance to spread the word:
 - Geospatial World Forum – Apr/May, Netherlands
 - ESA Data Access and Preservation working group - May
 - GEO Symposium – May, Switzerland
 - ExpandEO – June, Belgium
 - VH-RODA – November, Italy
- Public project webinars – next end October
- Regular updates to the project website:
<https://eoveracity.ssl.telespazio.com/>





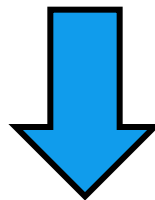
Why we need you!

We don't want to work in isolation

We want to **meet the needs** of EO industry

We want to **engage** with EO organisations

We need your feedback!



**Together we can produce a roadmap that is
thorough and practical to implement**



Interactive Q&A and Feedback



PROOF OF CONCEPT VERIFICATION



Questions and Answers

➤ We have some questions for you

- Please return to [menti.com](https://www.menti.com)
- Menti code: **3250 0769**





Feedback

Do you have questions for us on the EO Veracity project?



Do you have any feedback, suggestions or ideas to share?

If you would prefer to share these offline, please contact amanda.hall@telespazio.com



Thank you!



eoveracity.ssl.telespazio.com

Contact us via the website or at amanda.hall@telespazio.com