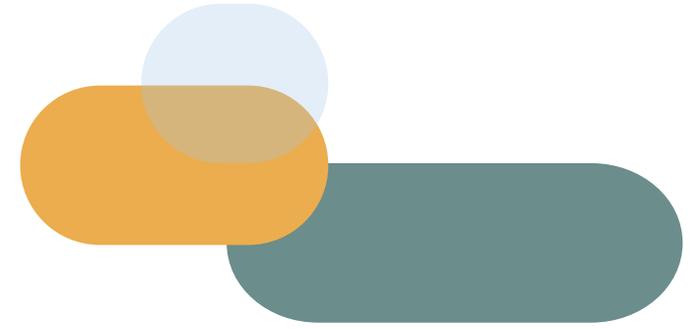


From Research to Operations: The Copernicus SESA Perspective



**Maria
Tamame**

**Project Manager at Copernicus Service on
Support to EU External and Security Actions (SESA)**

The European Union Satellite Centre

EU operational agency supporting security and external action

- Provides geospatial intelligence to support EU CFSP and CSDP decision-making.
- Supports EU institutions, EEAS, CSDP missions, and Member States.

Operational service provider

- Produces intelligence, situational awareness and early warning products.
- Integrates Earth Observation and contextual data into operational services.

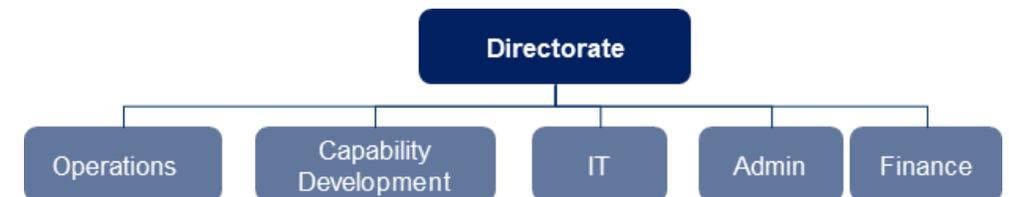
Bridge between space capabilities and operational users

- Translates EO data and research innovation into operational services.
- Contributes to Copernicus Security Service, including Copernicus SESA.



200 Staff,
21 Nationalities

Mix between **civilian & military** backgrounds



Copernicus SESA Service



- Provides operational services based on free and open access satellite and geospatial data.
- Security component implemented by EMSA (Maritime), Frontex (Border), and SatCen (SESA)
- SESA is the **Copernicus Security Service Component on Support to EU External and Security Actions**



- Initially focused on EU external action (CFSP/CSDP).
- Expanded to additional policy groups addressing internal security and EU law monitoring.
- Growing user base including EEAS, EC services, and Member State institutional users.



Copernicus SESA: Service Evolution

User-driven operational service

- Supports 11 application areas including crisis monitoring, climate security, and conflict analysis.
- Provides operational products tailored to institutional user needs.

Continuous service evolution

- Integration of new tools, datasets, and analytical capabilities.
- Transition of research and innovation outputs into operational services.

SESA as bridge between research and operations

- Validates and integrates innovative solutions from EU-funded projects.
- Facilitates operational uptake of new early warning and risk monitoring capabilities.



Operational Integration Challenges

Barriers encountered when transitioning research into operations

Technical Integration

- Solutions must comply with strict security, infrastructure, and interoperability requirements.
- Research solutions are often not directly compatible with operational workflows and data standards.
- Significant effort is required to adapt prototypes for operational deployment.

Operational Readiness

- Research outputs often remain at prototype or pre-operational stage.
- Limited validation under real operational conditions.
- Additional qualification and testing are required before operational deployment.

Transition and Operational Ownership

- No clear transition path after project completion: Significant delay between identification of operational needs and operational availability.
- Dependencies on external partners, data, or infrastructure limit operational autonomy.
- Ownership, licensing, or restricted access to processing chains may prevent operational deployment.

Lessons Learned: Enabling Operational Uptake

What is required to successfully transition research into operational services

Early Operational Involvement (solves compatibility and usability issues)

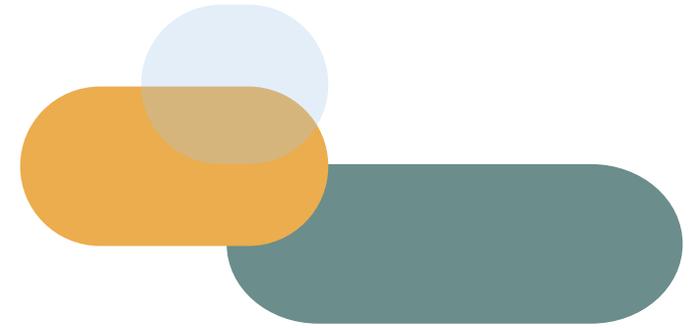
- Ensures alignment with operational needs and user requirements.
- Provides continuous feedback throughout development.
- Enables fitness-for-purpose validation from an operational perspective.

Operational Validation and Maturity (solves readiness and maturity gap)

- Test solutions in operational-like environments.
- Validate performance, reliability, and security.
- Ensure operational qualification before deployment.

Clear Transition and Operational Ownership (solves sustainability and autonomy risks)

- Define transition mechanisms beyond project completion.
- Ensure entrusted entities can deploy, run, and maintain solutions independently.
- Establish clear ownership, access to processing chains, and sustainability.



CENTAUR and Climate Security Early Warning

Illustrates both the potential and the operational challenges of integrating research into Copernicus SESA.



POTENTIAL - Valuable Early Warning Capability for Climate-Security Risk

- Climate-security indicators linking drought, fragility, and conflict risk
- Predictive models enabling anticipatory regional conflict risk analysis.
- Valuable analytical capability supporting climate-security monitoring.



OPERATIONAL REALITY - Significant Effort Required Before Operational Deployment

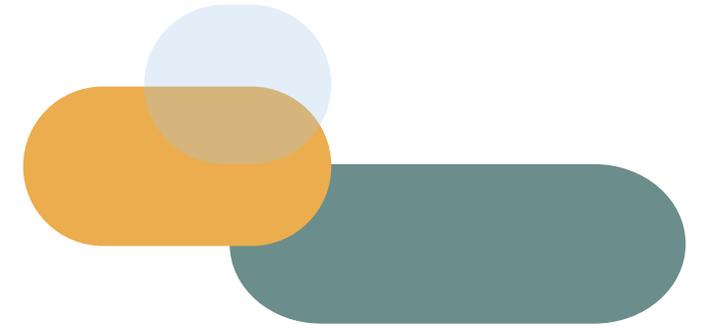
- Solutions remain at prototype or pre-operational stage.
- Require integration, validation, and adaptation to SatGen secure infrastructure.
- Dependencies, ownership, and access to processing chains must be addressed.



CURRENT PATH FORWARD - Exploring Operational Integration Pathways

- Ongoing discussions to assess feasibility of integrating specific components.
- Alignment with operational initiatives such as the CESDA Hub
(Climate and Environment Security Data and Analysis Hub)
- Focus on operational independence, sustainability, and security compliance

Conclusion



Research

Research and innovation are essential to evolve Copernicus operational capabilities



Transition

However, transitioning research into operational services remains a complex and structured process



Operations

Entrusted entities enable sustainable operational uptake.

Structured transition mechanisms are essential to transform research into operational Copernicus capabilities

Early operational involvement, structured validation, and dedicated service evolution pathways are key to maximise research impact.