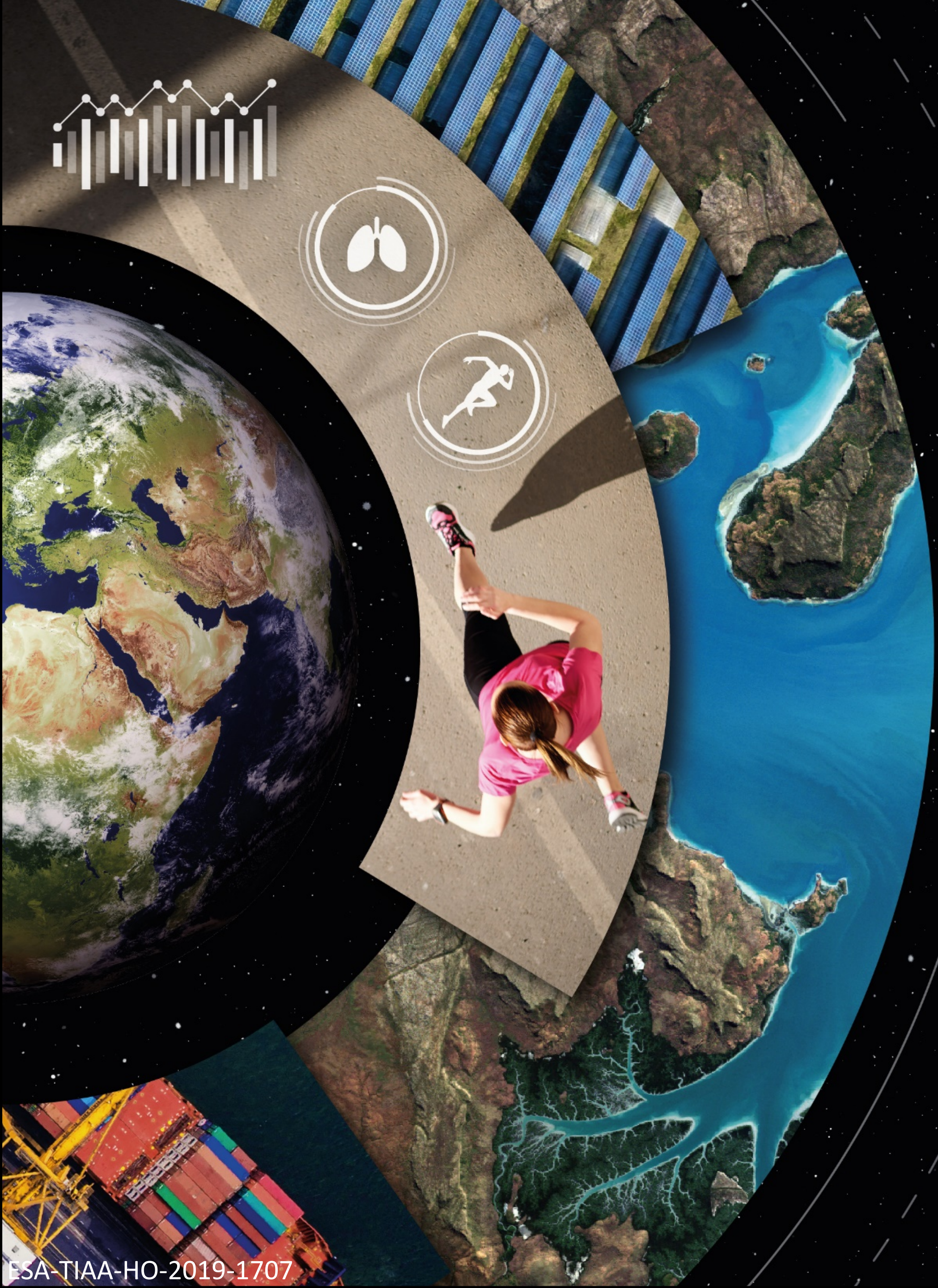


→CYBER SECURITY AND SPACE BASED SERVICES Webinar

21/08/2019 11:00 CEST - 12:00 CEST

Laurence Duquerroy – Laurence.Duquerroy@esa.int

European Space Agency

WELCOME TO THE WEBINAR! Before we start…

- Due to the number of attendees, please keep your microphones muted at all times and switch off the webcam function

- You can use the conversation function anytime to submit your questions. They will be addressed during the Q&A at the end of the webinar

➔ AGENDA

- ➢ What ESA Business Application offers

- ➢ Space as cyber security enabler

- ➢“Cyber Security and Space based services” call for tenders
  - Opportunity
  - Objectives
  - Partners
  - User & Stakeholders involvement
  - Other requirements

- ➢How to apply

- ➢Open Questions & Answers session

Purpose of ESA

"To provide for and promote, for exclusively peaceful purposes, cooperation among European states in **space research** and **technology** and their **space applications.**"

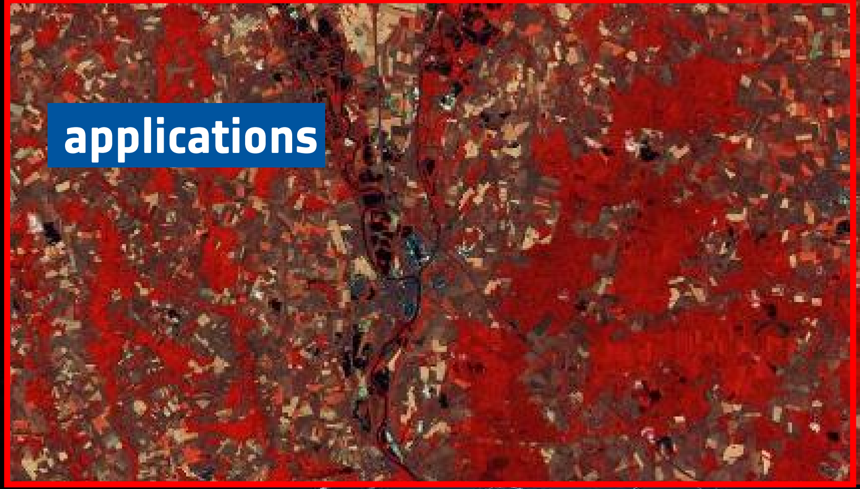
Article 2 of ESA Convention

ESA facts and figures

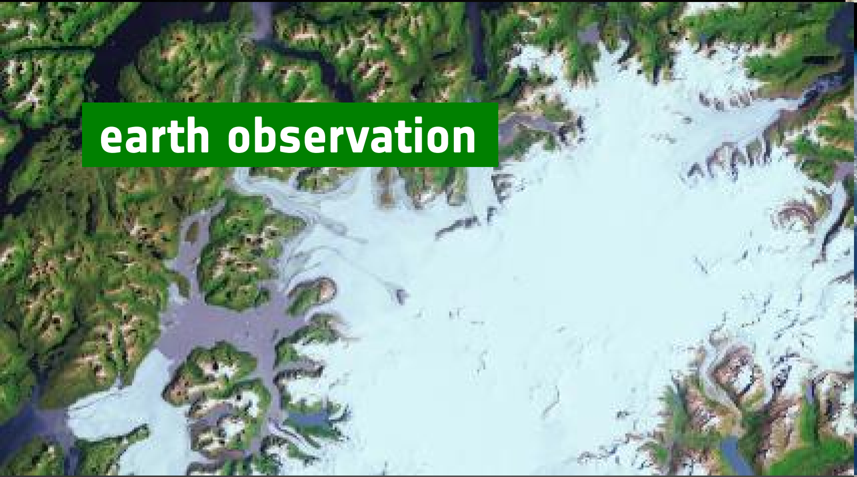
- Over 50 years of experience
- 22 Member States
- Eight facilities in Europe, about 2300 staff
- 5.75 billion Euro budget (2017)
- Over 80 satellites designed, tested and operated in flight

science

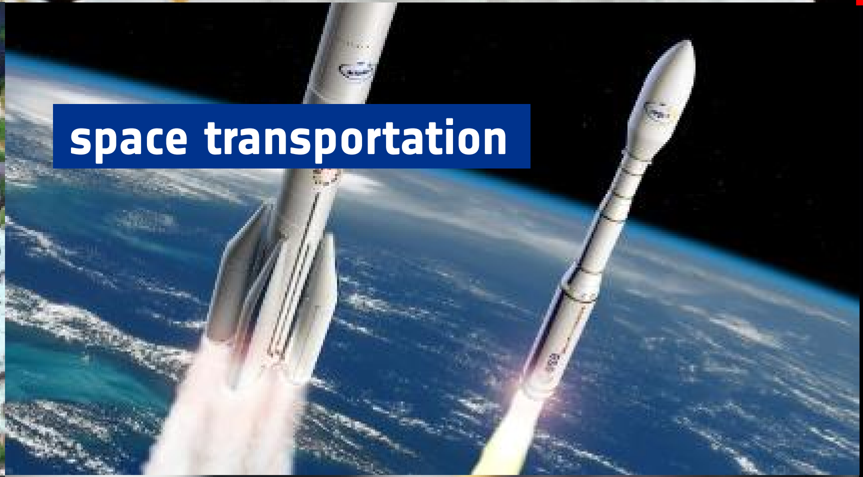
human spaceflight



applications



earth observation

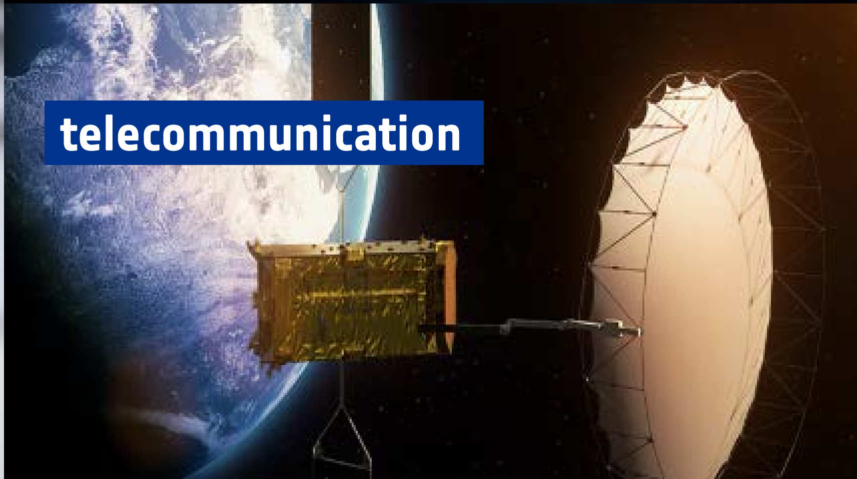


space transportation

navigation

exploration

technology



telecommunication

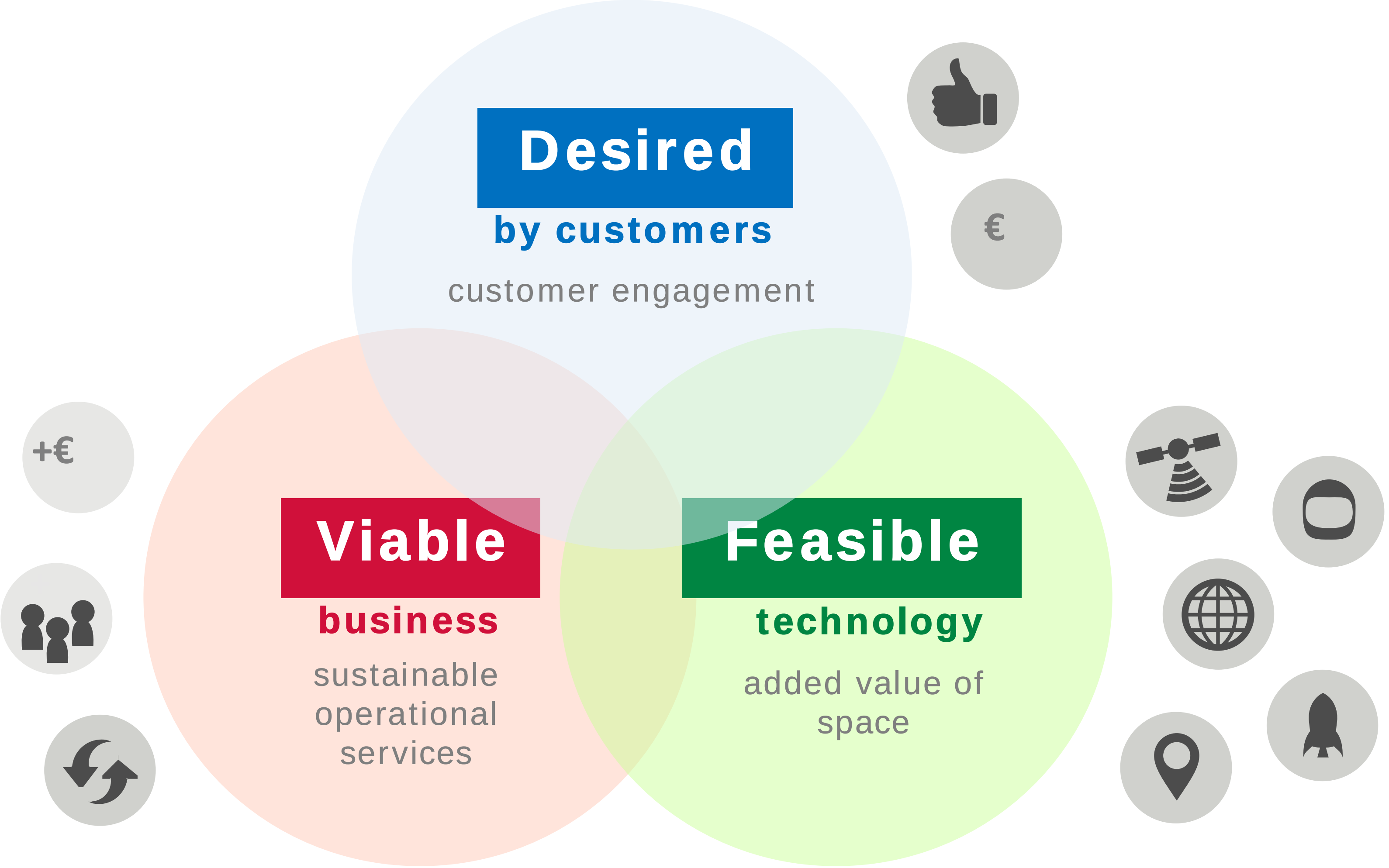
→ FUEL FOR YOUR BUSINESS

Could you be leveraging Space technology and data for the benefit of life on Earth?

- Space Weather
- Earth Observation
- Satellite Navigation
- Satellite Communication
- Human Spaceflight Technologies

- Maritime
- Healthcare
- Transport
- Environment
- Agriculture
- Media
- Energy
- Education
- Aviation
- Financial

→ LOOKING FOR PROMISING SERVICES



WHAT ESA OFFERS

We'll work together to make your idea commercially viable, with:

Zero-Equity Funding (€60k-€2M+)

Tailored Project Management Support

Access to Our Network & Partners

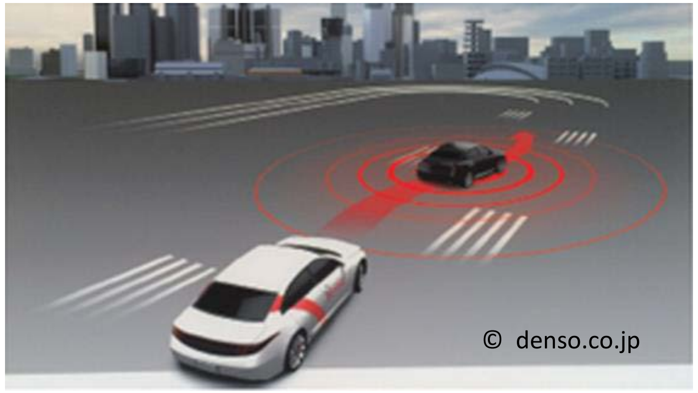
Use of the ESA Brand for Credibility

Space as cyber security enabler

➔ SPACE AS CYBER SECURITY ENABLERS: EXAMPLES

- ❑ GALILEO Authenticated services
  - ❑ **Open Service** will provide **Navigation Messages Authentication (OS-NMA)** enabling the detection of spoofing attacks and thus increasing reliability and the trustworthiness of position and timing information
  - ❑ **Galileo Commercial Service**: high accuracy combined with authentication services based on signal encryption for an increased robustness

- ❑ Satellites to be used for **watermarking**, to verify the position of a device based on recorded RF signals combined from different broadcasting satellites


© denso.co.jp

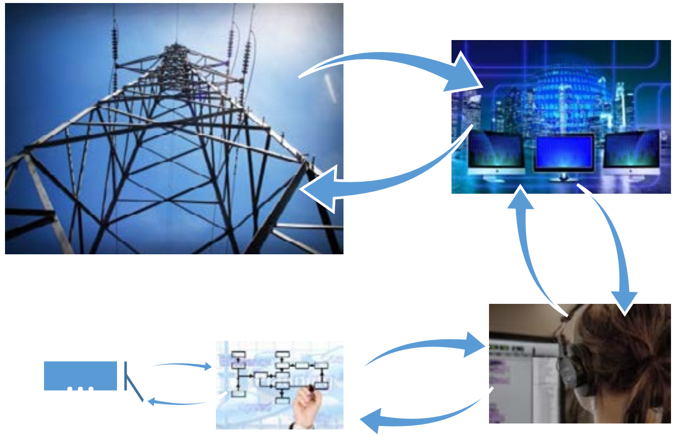
- ❑ Applications : For services requiring **authenticated geo-referencing and/or time-stamping, or geofencing**, i.e.
  - ❑ autonomous vehicles
  - ❑ transactions in financial sector,
  - ❑ sensor network / IoT of critical infrastructures…

➔ SPACE AS CYBER SECURITY ENABLERS: EXAMPLES

- Secure Satellite Communications

  - **Unique alternative to the transmission of data through the terrestrial internet** where they can be more subject to potential malicious attacks.

  - With the development of **free space optical communications with ground or between satellites**, which offer an **increased robustness** against interference, jamming and eavesdropping, Satcom systems and constellations will be even more secure and allow **worldwide exchanges of data bypassing terrestrial networks**.



➔ Use secure Satcom as primary communication means or as back-up to terrestrial networks, to enhance the security of sensitive data transmissions

➔ For Governmental applications (GovSatCom), Critical transport communications, critical infrastructures, financial sector, autonomous transport, public safety networks, etc.

→ SPACE AS CYBER SECURITY ENABLERS: EXAMPLES

- New initiatives emerging for establishing **secure Cloud in Space** for **storage of sensitive data** in satellites.

- Development of **Satellite quantum keys distribution** for use in geographically dispersed networks (c.f. ESA QUARTZ project) .

- Applications : telecommunication operators, financial organizations, infrastructure providers, institutions/governmental organizations.

→ SPACE AS CYBER SECURITY ENABLERS: EXAMPLES

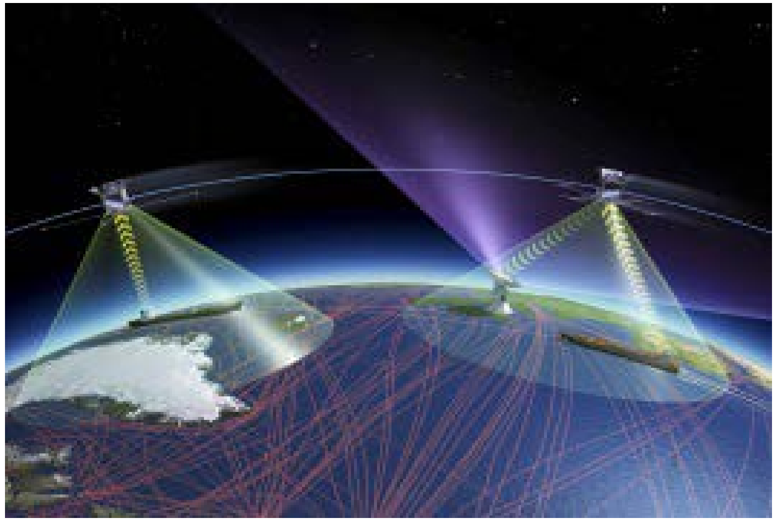
- Data collected from Space, i.e. Satellite Earth Observation, Sat-AIS and Space-based ADS-B data

- Combined with Big Data Analytics and Machine Learning,

- Possibly correlated with other sources

- Can contribute to detect new attacks and security breaches by identifying suspicious patterns or corrupted data wrt. historical patterns and data.

- Applications: transport (tracking and tracing), maritime surveillance, insurance, etc., to detect falsified information regarding reported positions .



CYBER SECURITY AND SPACE BASED SERVICES
Planned ESA’s funded invitation to tender

→ OPPORTUNITY

- Invitation to tender to assess the technical feasibility and the business case of **innovative services and solutions in support of cyber security** in the frame of a fully-funded Feasibility Study

- Potential services must:
  - **be enabled by Space technologies or data** (SatCom, SatEO, SatNav); and/or
  - contribute **to enhancing the end-to-end cyber security of space-based applications**.

- Services and solutions to be investigated can address **cyber security prevention, protection, detection and/or response activities**. Awareness, training, and information sharing activities are excluded.

- These services must address threats and challenges from one or more of the following vertical market sectors:
  - **Transport and Mobility (maritime, land, air, including autonomous vehicles)**
  - **Energy, Utilities and Critical Infrastructures**
  - **Financial Sector**
  - **Public Safety**

→ OBJECTIVES

- Assess the **technical feasibility** and **business case** of innovative cyber security services

- Get **anchor customers commitment** towards services implementation and **sustainable operation**, and validate **value proposition**

- Identify and assess the **technical and non-technical risks** associated with the implementation, commercialisation and operations of the services

- Consolidate the **business plan** for supporting an informed decision for investment in further activities

- Establish the **roadmap for service implementation, esp**. through a potential **follow-on (co-funded) demonstration project** within ESA Business Applications

→ PARTNERS

The Agency has established cooperation with the following key stakeholders

EUROPEAN DEFENCE AGENCY

EMSA

ENCS

enisa

EUROCONTROL

ING

who have provided areas and/or use cases of interest.

During the course of the study(ies), these stakeholders may provide feedback to the study results and contribute with inputs towards potential follow-on demonstration projects.

Set up in 2004 as an agency of the Council of the European Union, the European Defence Agency supports its 27 Member States - all EU countries except Denmark - in the improvement of their defence capabilities through European cooperation. An enabler and facilitator for Ministries of Defence looking to engage in collaborative capability projects, the Agency has become the central hub for European defence cooperation.

Areas of interest :

- GNSS threats’ detection: solutions capable of automatically detecting highly degraded and/or unreliable situations and adopting alternate strategies to provide reliable navigation services.
- Use of AI in geospatial information platforms using space and non-space data sources to increase situational awareness; another point of interest is the cybersecurity of the data used in these platforms for integrity purposes.

https://www.eda.europa.eu/

The European Maritime Safety Agency was established for the purpose of ensuring a high, uniform and effective level of maritime safety, maritime security as well as prevention of and response to pollution by ships within the EU.

1st Area of interest : Maritime Navigation

- Improving Network security on board ships (navigation marine equipment, Radiocommunication marine equipment)
- Improving authentication in SAT-AIS
- GNSS (AIS) spoofing detection
- False AIS-AtoN detection

2nd Area of interest : Maritime Autonomous Surface Ships cyber security

- Navigational systems, on-board sensor systems, (satellite) communication links, etc.

http://www.emsa.europa.eu/

ENCS

The European Network for Cyber Security is an independent non-profit organization owned by European grid operators with the mission to help improve their cyber-security.

Areas of interest : Critical infrastructure security, in particular for electricity grid operators (DSOs, TSOs)

- Secure time synchronization of grid substations (resilient to GPS spoofing)
- Secure data communication during power outages

https://encs.eu/

The European Union Agency for Cybersecurity is working to make Europe cyber secure since 2004. ENISA works with the EU, its member states, the private sector and Europe's citizens to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Since 2019, it draws up cybersecurity certification schemes.

Areas of interest: Cyber Security Infrastructure & Services

- Cryptoservices relying on Space, such as Quantum Key Distribution, or for new sources of randomness
- Novel security services (for mitigating GNSS spoofing attacks) and threat intelligence solutions for the transportation sector.
- Secure and highly accurate timestamping services
- Supporting Cyber Crisis management (with e.g. cyber threat intelligence enhancement using data collected from space, satcom as fall back communication solution)

https://www.enisa.europa.eu/

EUROCONTROL

EUROCONTROL is an intergovernmental organisation with 41 Member and 2 Comprehensive Agreement States, committed to building, together with its partners, a Single European Sky for Air Traffic Management and to supporting European aviation.

Areas of interest : Air Traffic Management

- Cyber resilience of Communication, Navigation and Surveillance (CNS) infrastructure relying on space and terrestrial systems for future Air Traffic Management
- Drones and U-Space cyber security
- Digitalisation : enhancing ATM system-wide information system (SWIM) integrity and addressing threats related to the use of AI in ATM safety critical operations

https://www.eurocontrol.int/

ING

ING is a global financial institution with a strong European base, offering banking services through its operating company ING Bank. The purpose of ING Bank is empowering people to stay a step ahead in life and in business. ING Bank's more than 53,000 employees offer retail and wholesale banking services to customers in over 40 countries.

Areas of interest: Financial services

- Reliability and continuity of financial services, with respect to various cyber security and not cyber related threats (technical outages, environmental threats and social threats).

https://www.ing.com/

→ USERS AND STAKEHOLDERS ENGAGEMENT

Bidders are invited to propose for investigation services and solutions relevant to the areas and use cases of interest to the previous stakeholders (alternative #1)

- ESA will facilitate the contact following the selection of the bidders.
- Tenderers shall not contact the afore-mentioned organisations during the bidding period.

Alternatively, it is possible for Bidders to propose for investigation services for other areas of interest and use cases, belonging to the vertical market sectors identified for this study (alternative#2).

For both alternatives, due to the customer/user-driven nature of the study and with the aim to investigate commercially viable services, Bidders shall engage with and involve in the study at least one potential user /customer.

- Letter(s) of interest/intent from this(these) user(s) shall be provided in the proposal.

→ ADDITIONAL REQUIREMENTS

- The study shall investigate technical solutions and business opportunities deemed to be available in the short (2 years) or medium term (2-5 years).
- Study shall focused on a reduced number of services (recommendation: not more than two services)
- The envisaged services/solutions shall benefit from one or more space assets (i.e. SatNav, Satcom, SatEO) or/and shall be aimed to protect space-based applications in an end-to-end manner. The space assets do not need to be limited to ESA's or European space assets
- Contractor team should be interested in developing and commercialising considered services and have the relevant technical and business capabilities.

→ MAIN TASKS AND KEY FACTS

Main tasks

- Use cases analysis and user requirements consolidation
- Technical Feasibility Assessment
- Commercial Viability analysis
- Roadmap for future implementation

100% funding, €200k

Duration: 9 months

Several parallel contracts possible

→ HOW TO APPLY

1. **Register** by completing online questionnaire on ESA-STAR Registration (minimum 'light registration') (https://esastar-emr.sso.esa.int)

2. **Download** the official tender **documentation** (Invitation to Tender) via EMITS '**AO9927' from 22nd August 2019** (http://emits.sso.esa.int/emits/owa/emits.main)

3. **Create** 'Bidder Restricted Area' in ESA-STAR

4. **Write your proposal** and obtain **Letter of Authorization** from your National Delegation

5. **Submit** your proposal via 'Bidder Restricted Area' in ESA-STAR Tendering by **14th November 2019 13:00 CET** (Don't wait until the last minute!)

➜ BASIC PRINCIPLES

Tender documentation:

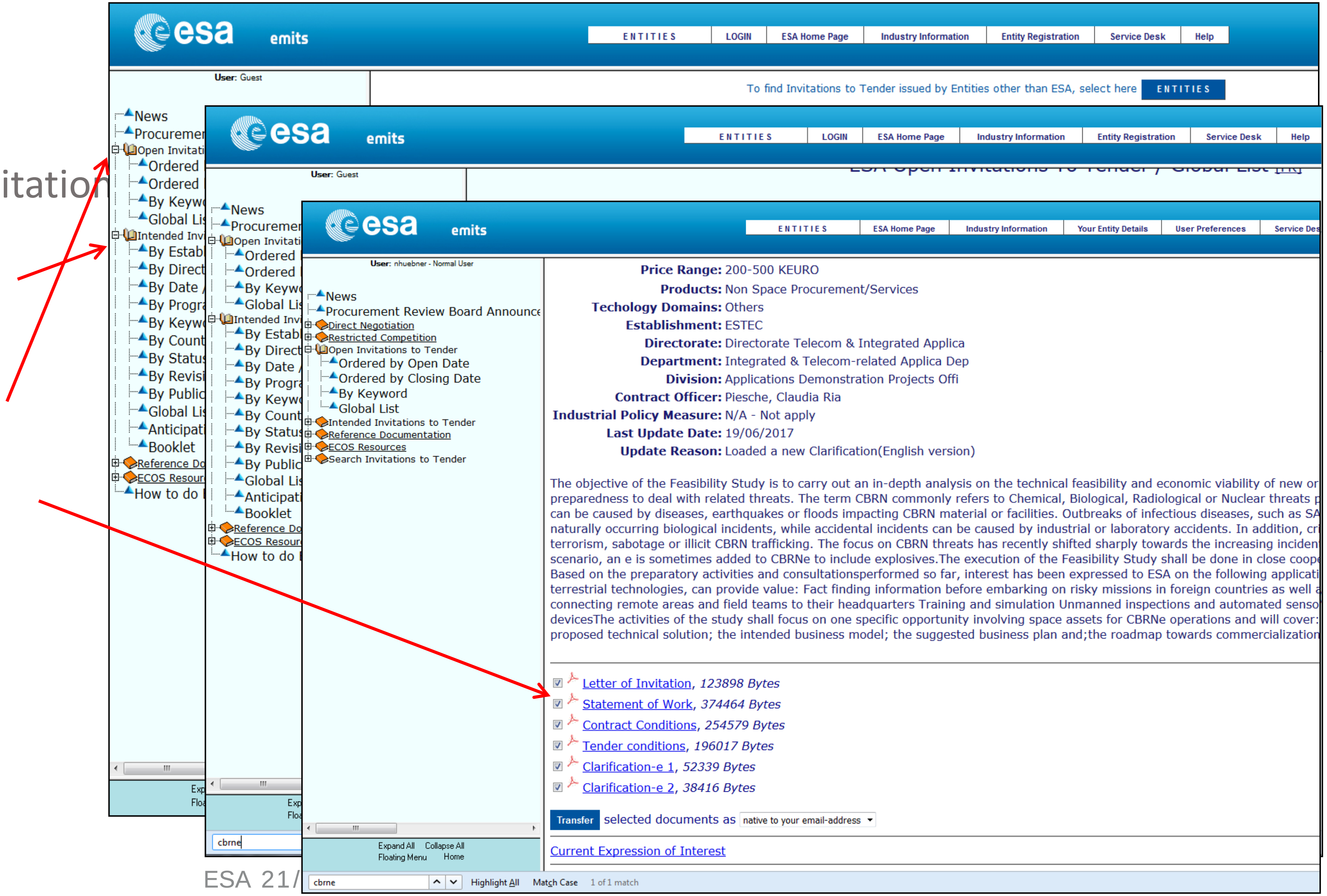
on **<emits.esa.int>**

Announced under “Intended Invitation to Tender (IITT)”

Published under “Open Invitations to Tender (ITT)”

(⇒ registration required to access tender documents)

Submission of proposals electronically in ESA-STAR



To find Invitations to Tender issued by Entities other than ESA, select here ENTITIES

Price Range: 200-500 KEURO
Products: Non Space Procurement/Services
Techology Domains: Others
Establishment: ESTEC
Directorate: Directorate Telecom & Integrated Applica
Department: Integrated & Telecom-related Applica Dep
Division: Applications Demonstration Projects Offi
Contract Officer: Piesche, Claudia Ria
Industrial Policy Measure: N/A - Not apply
Last Update Date: 19/06/2017
Update Reason: Loaded a new Clarification(English version)

The objective of the Feasibility Study is to carry out an in-depth analysis on the technical feasibility and economic viability of new or
preparedness to deal with related threats. The term CBRN commonly refers to Chemical, Biological, Radiological or Nuclear threats p
can be caused by diseases, earthquakes or floods impacting CBRN material or facilities. Outbreaks of infectious diseases, such as SA
naturally occurring biological incidents, while accidental incidents can be caused by industrial or laboratory accidents. In addition, cri
terrorism, sabotage or illicit CBRN trafficking. The focus on CBRN threats has recently shifted sharply towards the increasing inciden
scenario, an e is sometimes added to CBRNe to include explosives.The execution of the Feasibility Study shall be done in close coope
Based on the preparatory activities and consultationsperformed so far, interest has been expressed to ESA on the following applicati
terrestrial technologies, can provide value: Fact finding information before embarking on risky missions in foreign countries as well a
connecting remote areas and field teams to their headquarters Training and simulation Unmanned inspections and automated senso
devicesThe activities of the study shall focus on one specific opportunity involving space assets for CBRNe operations and will cover:
proposed technical solution; the intended business model; the suggested business plan and;the roadmap towards commercialization

☑ Letter of Invitation, *123898 Bytes*
☑ Statement of Work, *374464 Bytes*
☑ Contract Conditions, *254579 Bytes*
☑ Tender conditions, *196017 Bytes*
☑ Clarification-e 1, *52339 Bytes*
☑ Clarification-e 2, *38416 Bytes*

Transfer selected documents as native to your email-address

Current Expression of Interest

→ BASIC PRINCIPLES

- For **competitive tender activities (ITT)**, **interaction** with ESA experts is not possible during the opening period.

  During the opening period, questions have to be **formally** addressed to the **contracts officer** and will be answered via **clarifications** to the ITT **in EMITS**

- All submissions for activities as response to competitive tenders are based on **templates available in the tender package.**
- Proposal templates provide **additional explanations** on the **content**
- **Read carefully** the explanations and **answer to the point** (be concrete and focused)
- Do **not confuse quality of content with quantity**
- **Evaluation criteria can be found in the ITT Letter of Invitation**

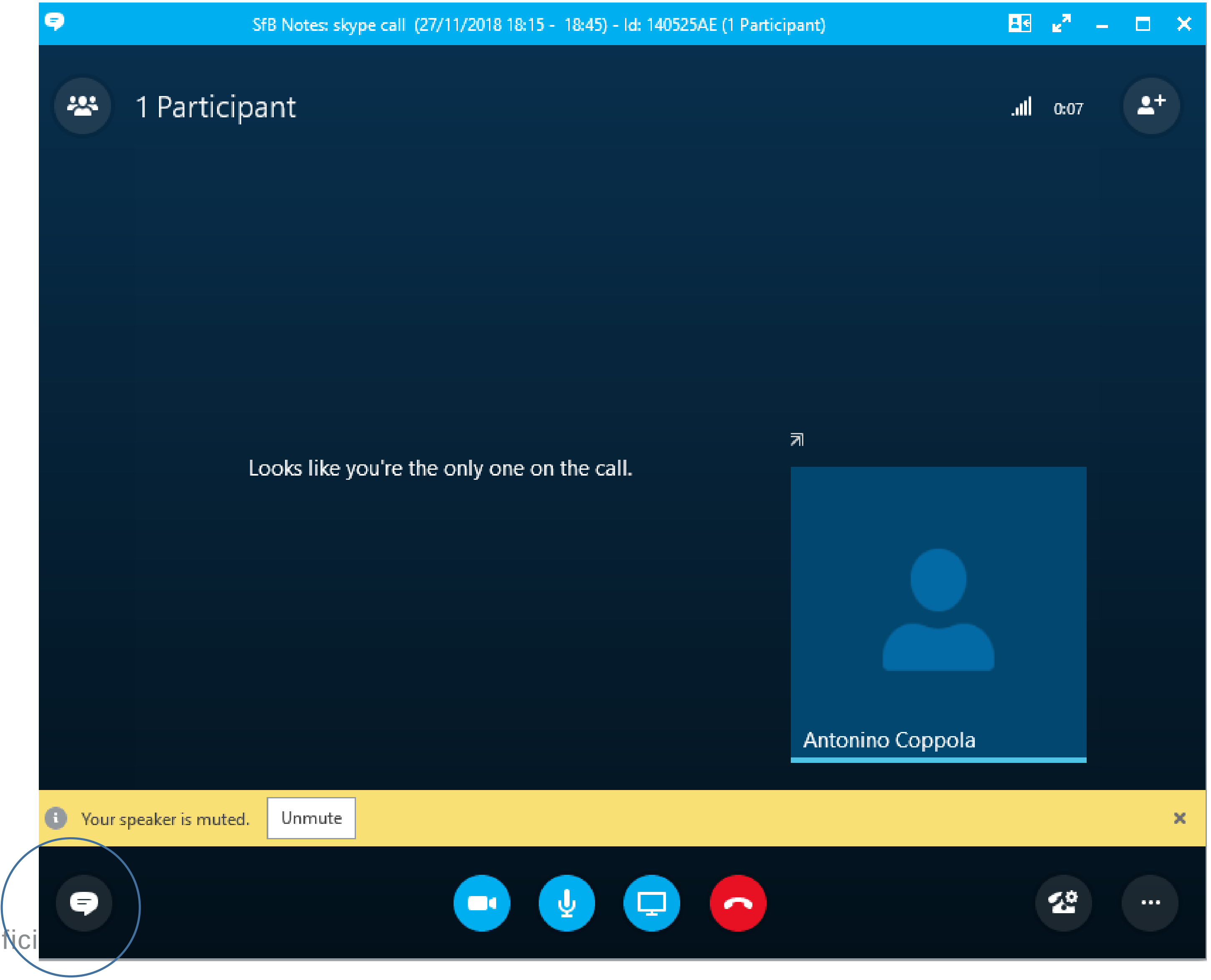
FUNDING ELIGIBILITY

- Open to any organisation, residing in any of those states that subscribed to the ARTES IAP programme (to date: Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxemburg, The Netherlands, Norway, Poland, Portugal, Romania, Sweden, Switzerland and the United Kingdom)

- **Letter of Authorisation from bidding team's national delegation(s) is needed and must be submitted as part of the Bidder's proposal. Without this letter, the proposal is not eligible.**

- The contacts of the National Delegations can be found at https://business.esa.int/national-delegations

OPEN QUESTIONS & ANSWERS SESSION



SfB Notes: skype call (27/11/2018 18:15 - 18:45) - Id: 140525AE (1 Participant)

1 Participant

Looks like you're the only one on the call.

Your speaker is muted.

→ Q&A

→ THANK YOU FOR PARTICIPATING

European Space Agency

https://business.esa.int/funding/invitation-to-tender/cyber-security-and-space-based-services