Challenge #1: Enhancing Defence & Security with Geospatial Intelligence

In today's world, where data availability and confidentiality are paramount, Geospatial Intelligence (GEOINT) is evolving to encompass not only the extraction and analysis of imagery and geospatial data but also ensuring its veracity and safeguarding GEOINT capabilities from cyber threats. This includes a focus on Earth Observation (EO) cybersecurity, which addresses vulnerabilities within the EO data collection and processing systems.

Geospatial intelligence continues to describe, assess, and visually represent physical features and geographically referenced activities on Earth. It encompasses various disciplines, including mapping, charting, imagery analysis, and imagery intelligence. Its applications are increasingly being exploited by civilian, defence and private sector organisations in areas such as telecommunications, surveillance, transportation, public health and safety, and real estate, contributing to the enhancement of everyday life quality.

In this challenge, we invite participants to leverage all available European space data, information, and signals from Copernicus, Galileo, or exploiting possible future services to be provided by IRIS2. The goal is to develop innovative products and services that can be readily utilised by planners, emergency responders, and decision-makers. We encourage participants to explore the following areas:

- **Geospatial intelligence for Defence, Humanitarian aid, Contingency Planning, and Security Surveillance:** Optimising resource allocation and delivery for disaster relief; Predicting and preparing for potential security threats; Enhancing defence missions, border control, counter-terrorism, anti-piracy, illegal fisheries, drug trafficking, and illegal crop monitoring.
- **Geospatial intelligence new services:** What future services Copernicus should be developed to better support security and defence missions, emergency management and humanitarian aid, critical infrastructure and surveillance applications?
- **Cybersecurity for remote sensing:** From a cybersecurity standpoint, assess the potential vulnerabilities of a generic EO system, including ground segments, EO satellites, Signals, Users, etc., and imagine ways to improve its cyber resilience
- **Ensure authentication of EO data:** Validate facts and other remote sensing data with historical patterns and Copernicus data, applying technologies such as blockchain.

Challenge #2: Unmanned Drone Applications for Defence & Security Operations

Unmanned aircrafts, more commonly known as drones, hold a huge potential for developing innovative defence, security and civil protection applications across a broad spectrum of sectors. These applications not only benefit European society but can also contribute to EU Member States capabilities, and to the creation of new businesses and job opportunities. Within the next 20 years, the broader European drone sector is projected to generate an economic impact exceeding €10 billion per year, primarily in services. Maintaining situational awareness and tracking incidents form a crucial part of any operational strategy, particularly for defence, surveillance and rescue services like fire departments and police forces.

In this challenge, we invite participants to create products, devices, or services that utilize European space data, information, and signals from Copernicus, Galileo, or exploiting possible future services to be provided by IRIS2. The aim is to enable sustainable and impactful solutions in the following areas:

- **Information gathering**: Develop systems for real-time data collection and distribution during defence, security and civil protection operations.
- **Emergency responder safety**: Protecting personnel during hazardous situations like defence operations, wildfires or natural disasters.
- **Cybersecurity of drone operations**: Design measures to assess and mitigate potential security risks in drone operations, ensuring reliable tracking, communication and positioning.
- **Data integrity**: Propose methods to ensure the authenticity and accuracy of data collected and transmitted by drones.
- **Misuse of drones**: Innovative solutions to detect and respond to misuse of drones, enhancing public safety and security.

Challenge #3: Orbital security – Navigating the collision frontier

In this challenge, participants are invited to delve into the critical field of Space Situational Awareness (SSA), with a particular emphasis on improving the safety of space operations through advanced collision avoidance techniques. The scenario involves a cybersecurity incident that has caused one of our satellites to veer off its intended course. As a consequence, Space Surveillance and Tracking (SST) services have issued a warning about space debris and satellites on a potential collision trajectory with the recovered satellite.

Participants will be provided with a dataset comprising Conjunction Data Messages (CDMs), derived from realistic conjunction scenarios involving the debris and satellites. The objective is to meticulously analyse the CDM data to assess the collision risk between the recovered satellite, the approaching debris, and other satellites. Teams must carefully evaluate whether this risk represents a significant threat that necessitates immediate action or if it can be reasonably disregarded as negligible.

Participants will get access to software tools and CDM data to help them solve this challenge. Participants are encouraged to also look at potential business models to commercialise their solution.