The ATSEP Role in CNS/ATM Cybersecurity events

The ATSEP must *(among other)**:***

- ***distinguish*** *whether any problem/degradation identified is a Technical failure or due to a Cyber event* (space or Ground)
- **respond** to **tactically** address any cybersecurity issue
- ATSEP Sup to **coordinate** with the ATCO Sup locally or remotely in ATSUS of delegated airspace
- **mitigate** degradation to ensure CNS/ATM service continuity

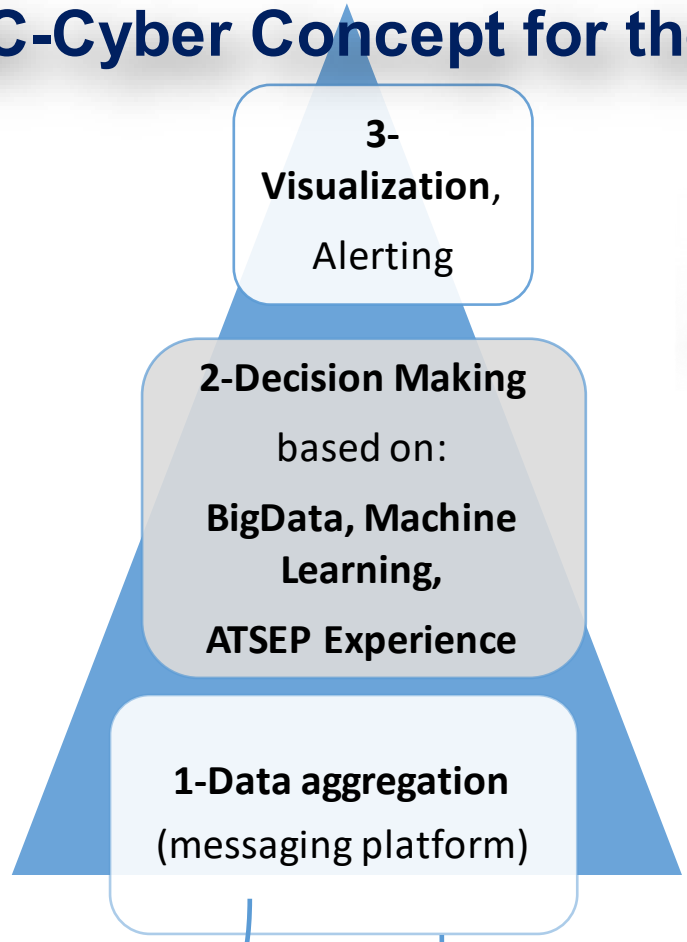
Addressing this cyber incident would be a challenge given that **tools for shared awareness of security threat level and total system state and health awareness, have not been fully researched and developed yet.**

IFATSEA proposes a *Technical Supervision model* ***instantiated in each ATSEP WP***

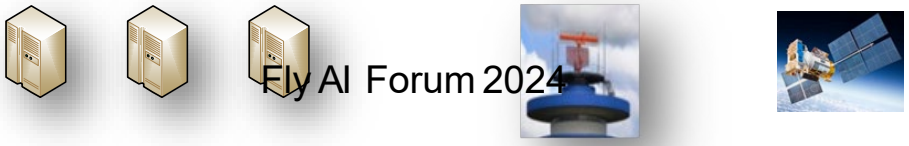
"an event object mechanism assisted by AI, interfacing with individual systems (or Service providers) with predictive capabilities based on specific sensors activity monitoring (s/w and h/w) and displaying their health status in the SMC domain **able to detect, classify and propose solutions to pure technical or Cyber related degradations"**

IFATSEA SMC-Cyber Concept for the ATSEP WP

Total system situational awareness



ATSEP WPs



event
object

Impact on ATSEP Training

- Training (basic and on the job) on cyber-attack / cyber-terrorism (EASA/ICAO ongoing)
- Develop **ATSEP WP SIMULATORS (based on digital twins?)** developed for ATSEP Training (including cross country coordination).
- Increasing utilization of Artificial Intelligence and clarification/elaboration of Human – Machine interdependencies **(Digital assistants?)**
- Language requirement established for efficient communication beyond borders
- New recruitment procedures (background checks?). Career development for experts **(lack of ATSEP-interest of professionals/scientists/engineers)**
- Cybersecurity taken into account in all ANSPs processes (cooperation with IT and Cyber experts strategically and offline)