RESISTO

RESIlience enhancement and risk control platform
for communication infraSTructure Operators

HORIZON 2020
#InvestEUresearch

RESISTO Project and Architecture

infocom world | infocom media

Maria Belesioti, M.Sc.

Dr. Ioannis P. Chochliouros

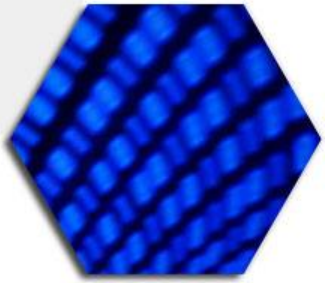
Hellenic Telecommunications Organization S.A.

Infocom World Conference 2019

November 26, 2019

Athens, Greece

ΟΤΕ
ΟΜΙΛΟΣ ΕΤΑΙΡΕΙΩΝ



RESISTO – This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No.786409

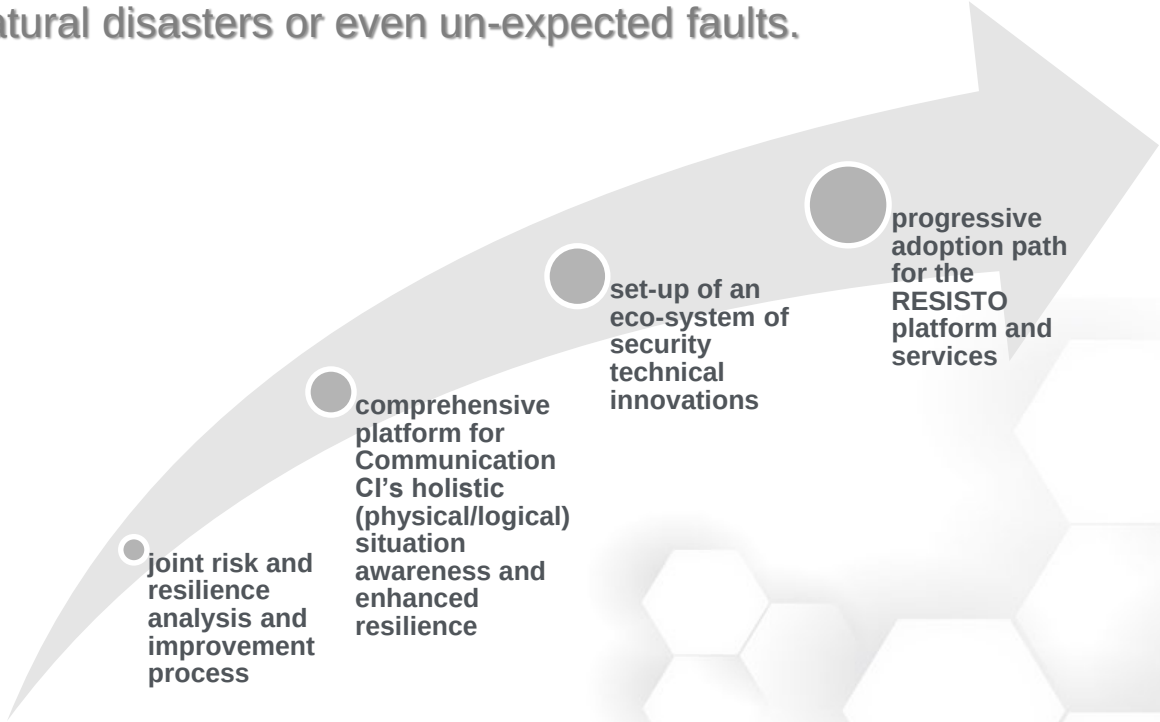
RESIST

RESIlience enhancement and risk control platform for communication infraSTructure Operators

OTE GROUP OF COMPANIES

- ***3 years*** (*May 2018-April 21*)
- **Topic(s): CIP-01-2016-2017 – *Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe***
- ***10M€ cost (8M€ funding)***
- ***17 partners*** (2 Large Enterprises, 6 Telco operators, 5 RTOs/Universities, 4 SMEs)
- ***Validation across 3 Verticals*:**
  - *current,*
  - *future and*
  - *interdependent comms infrastructures*

- ***MAIN RESISTO's OBJECTIVE***
  - *is to **IMPROVE RISK CONTROL AND RESILIENCE** of modern Communication CIs, **AGAINST a wide variety of CYBER-PHYSICAL THREATS**, being those malicious attacks, natural disasters or even un-expected faults.*



Detailed objectives

1. **Help managers of Communication CIs to guarantee improved business and asset continuity, by delivering an INNOVATIVE PLATFORM for OPTIMIZED DECISION SUPPORT in the face of physical, cyber and combined cyber-physical threats** *taking account of critical schemes of infrastructure, functions and services and possible (cascading) event trajectories*

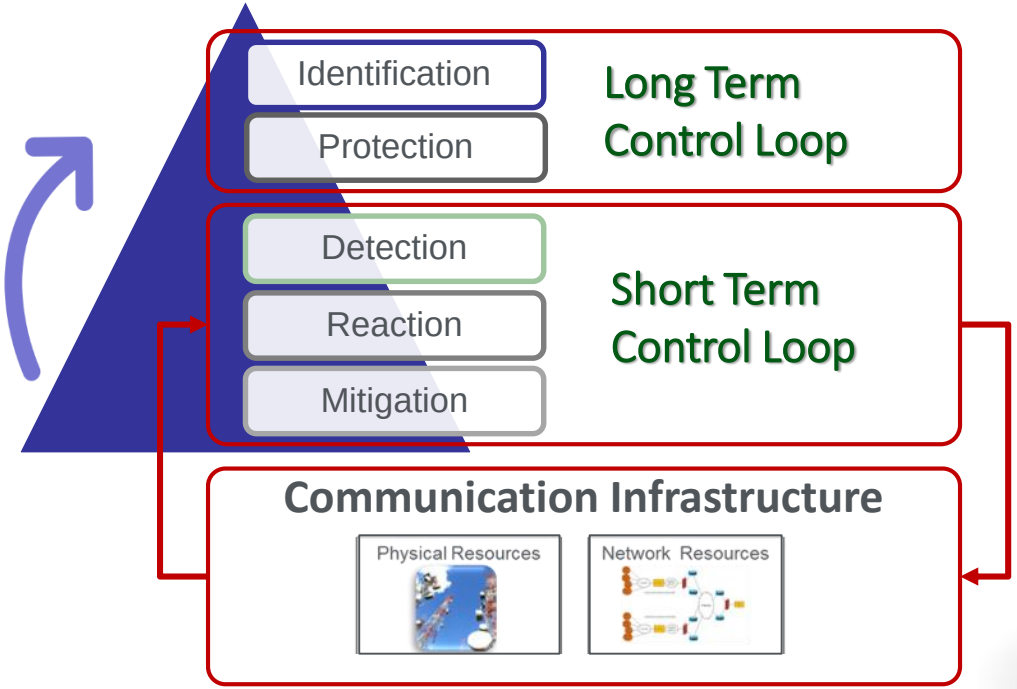
2. **Develop an INTEGRATED RISK AND RESILIENCE ANALYSIS AND MANAGEMENT TOOL for improved preparedness and prevention in the communication domain** *that takes account of cyber and/or physical threats and disruptions jointly at the level of telecommunication service functions and performance functions, including systemic security management*

3. **Provide, experiment and assess a suite of innovative cyber/physical security solutions for prevention/protection, detection and reaction** *that can deliver unprecedented cost-effective performances in a holistic technology framework*

4. **Support a progressive adoption path for the RESISTO platform and services through extensive validation in relevant use cases for Communication Infrastructure protection** *directly involving relevant Communication CI operators, arising awareness and promoting a joint approach to resilience*

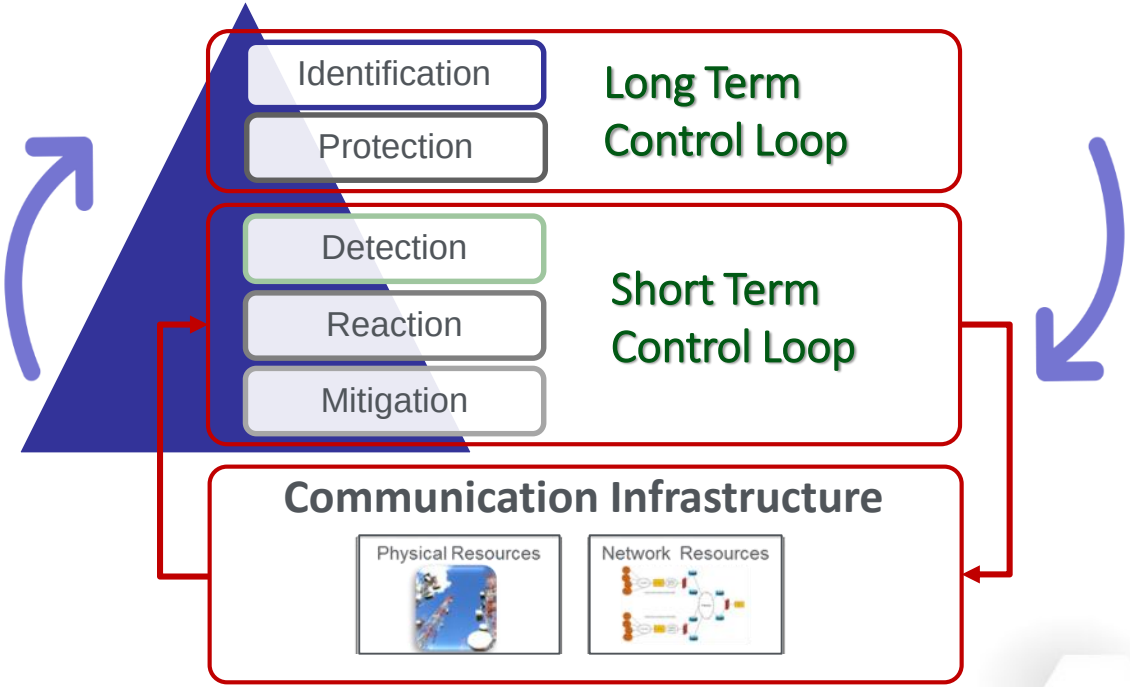
5. **Contribute to the European Programme for Critical Infrastructure Protection and, *in particular,* to the objectives of the Cybersecurity Strategy of the European Union,** *providing suitable inputs also to the Cybersecurity PPP*

Main functional concepts



- **The Long Term Control Loop (LTCL) is based on the *Risk and resilience assessment analysis.***
- For each loop cycle **a set of Resilience Indicators (RIs)**, *relevant to critical threat event typologies*, **are estimated and stored in a Knowledge Base (KB).**
- **LTCL is performed on a periodic basis** *(annually, quarterly or even monthly)* **or when particular events take place.**

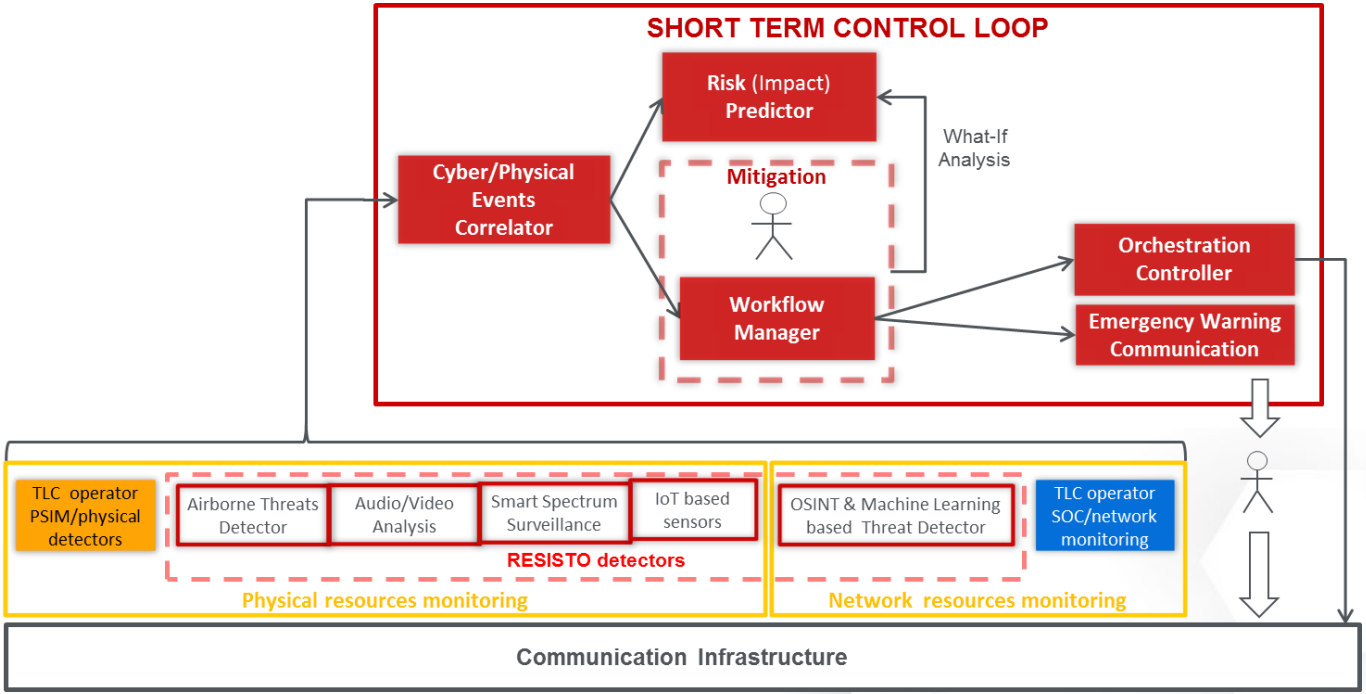
Main functional concepts



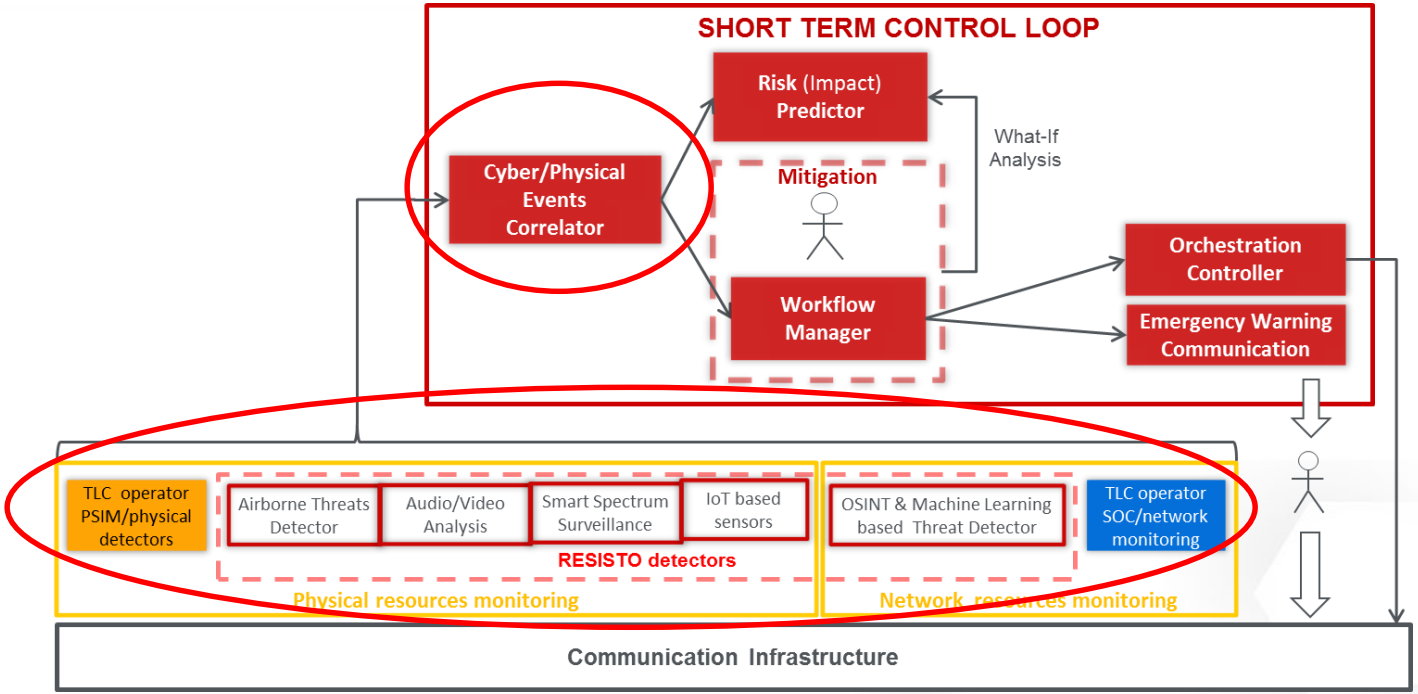
- **The Short Term Control Loop (STCL) reacts in real time to detected cyber/physical attacks and events,** *that may impact the operational life of the system.*
- It **enhances situation awareness** and **provides operators with a Decision Support System cockpit** *able to implement the best reactions.*

Long Term Control Loop

Short Term Control Loop



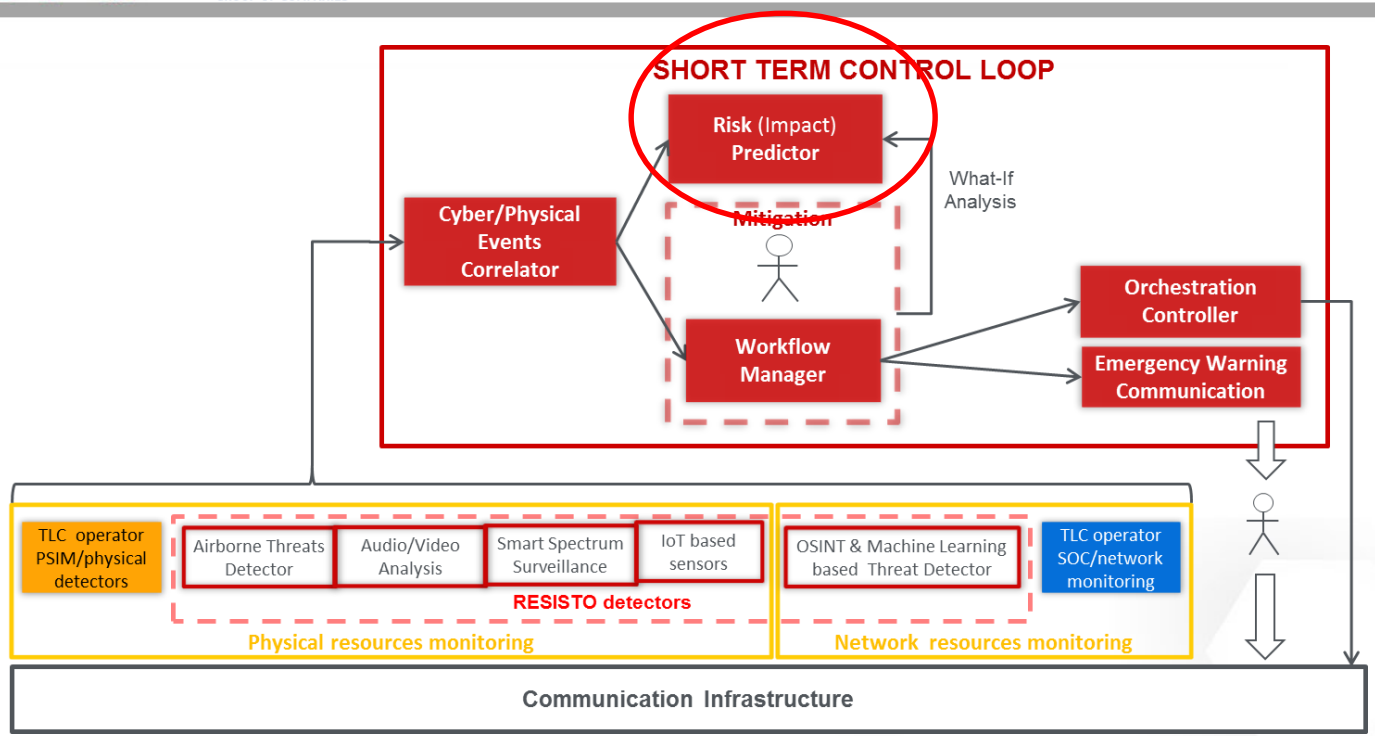
Short Term Control Loop



The Short Term Control Loop:

- **monitors the physical and cyber security status of the infrastructures**, *correlating the physical and cyber domain events and network monitoring data to detect anomalies and provide early warnings on security attacks by detecting threats in advance.*

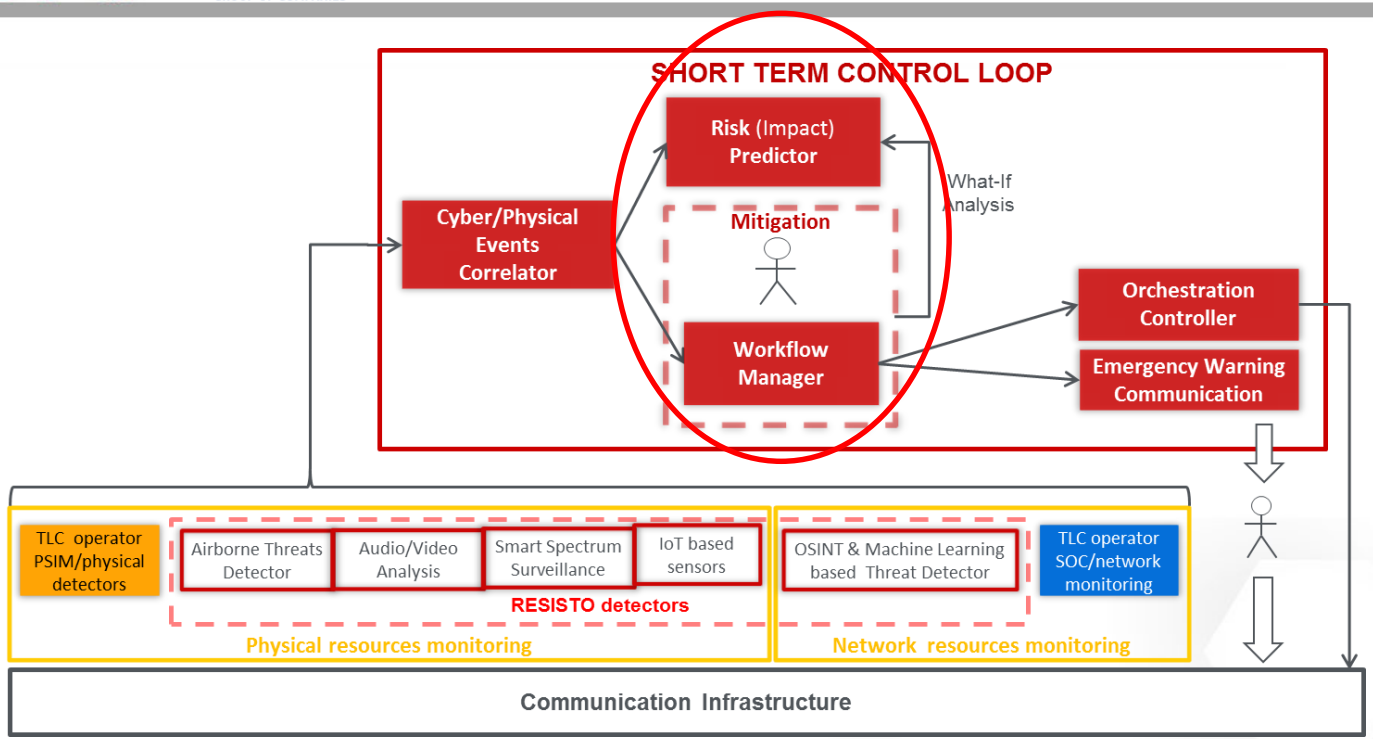
Short Term Control Loop



*The **Short Term Control Loop:***

- **evaluates the attack impact** with *respect to performance degradation of detected anomalies and security attacks on the communication CI, and interlinked CIs if known, based on the cascading effect*

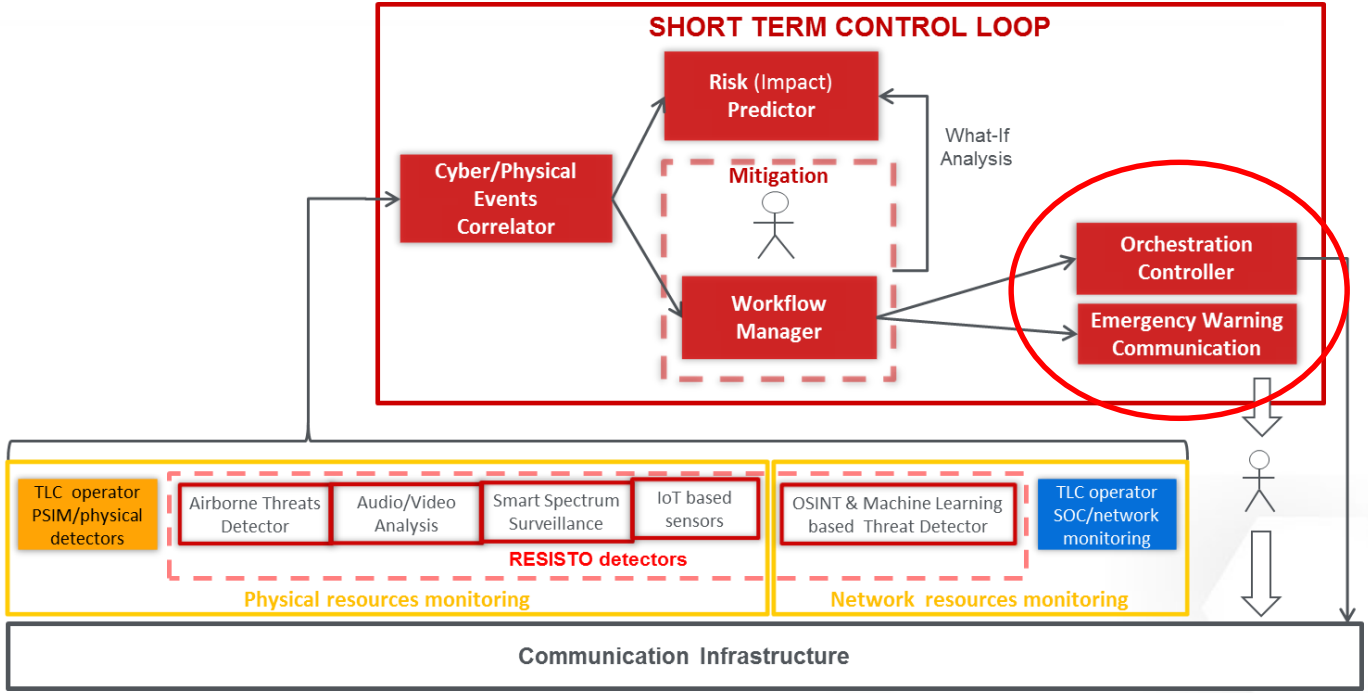
Short Term Control Loop



*The **Short Term Control Loop:***

- **supports decision making,** *by providing a qualitative and quantitative "What-If" analysis tool in order to evaluate the most resilient communication CI reconfiguration.*

Short Term Control Loop



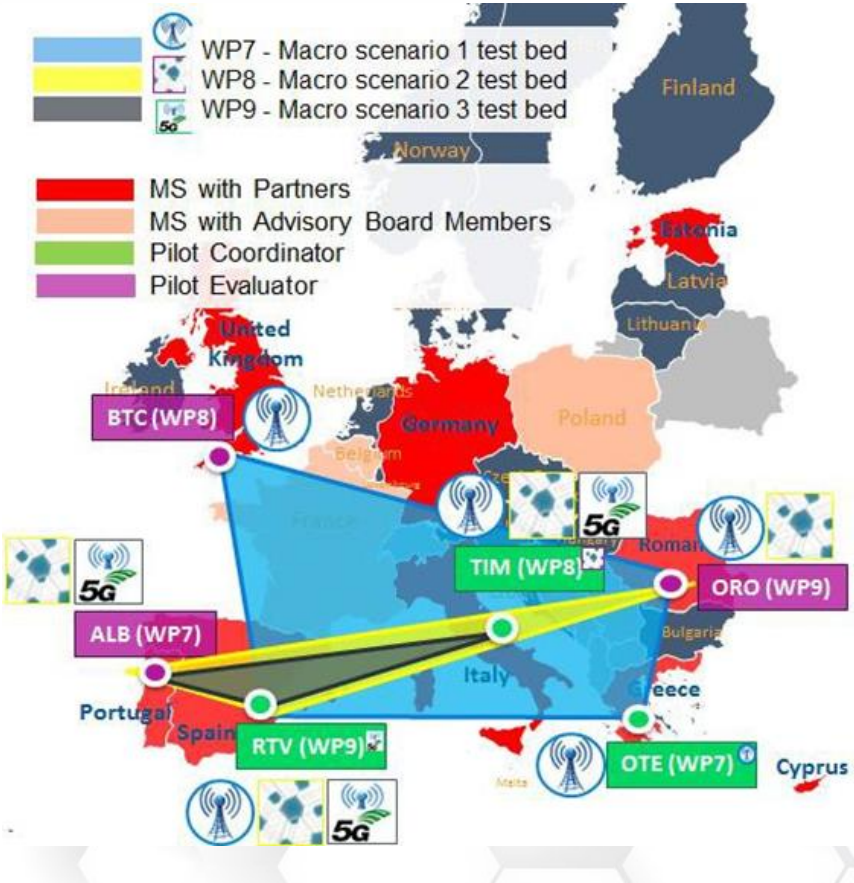
*The **Short Term Control Loop**:*

- **drives reaction and mitigation by means of action workflows** (*composed of directives to intervention teams, physical protection devices activation*) **and, *mainly*, of orchestrated Communication Network reconfiguration and protection function activation.**

RESISTO Validation Framework

- ***An extended validation is envisioned through a variety of operational Use Case pilots formed in sets configurations in terms of context, organization and impact, altogether consisting the RESISTO overall Validation Framework.***

- **Three (3) (Macro)-Scenarios**, *each one involving a set of related Use Cases to prove the RESISTO concept:*
  - ***Protection*** *of the* ***Current*** *existing* ***Telecommunication Critical Infrastructures***
  - *Their* ***interdependencies*** ***as providers of*** *essential* ***communication services to other*** *interlinked* ***CIs*** *and related cascade effects in the vicinity.*
  - *Their* ***evolution*** ***towards*** *the future* ***5G networks*** *and the emerging IoT world.*



Thank you for your Attention!!!!

For more info:

- **Mrs. Maria Belesioti, M.Sc.**

  Hellenic Telecommunications Organization –
  Fixed Network R&D Programs Section
  Research & Development Department, Fixed & Mobile
  mbelesioti@oteresearch.gr