RESISTO

RESIlience enhancement and risk control platform for communication infraSTructure Operators

HORIZON 2020

#InvestEUresearch

RESISTO Project: An Overview

Security Threats in Telecom Infrastructures

Maria Belesioti & Ioannis Chochliouros

Fixed Network R&D Programs Section

Hellenic Telecommunications Organization S.A. (OTE)

infocom world | infocom media

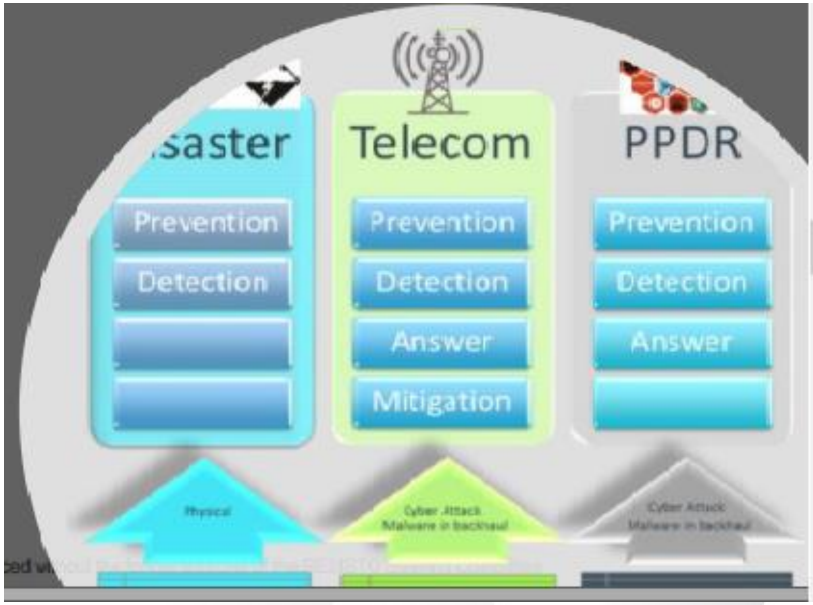
OTE

ΟΜΙΛΟΣ ΕΤΑΙΡΕΙΩΝ

This document is produced under the EC contract 786409. It is the property of the RESISTO Parties and shall not be distributed or reproduced without the formal approval of the RESISTO Steering Committee

RESIlience enhancement and risk control platform for communication infraSTructure Operators

- *3 years (May 2018 – April 2021)*
- *10M€ cost (8M€ funding)*
- *19 partners:*
  6 End-Users (Telco Operators), 3 Large Enterprises, 5 Research & Technology Organizations and 5 SMEs
- *Validation across 3 Verticals: current, future and interdependent communication infrastructures*
- *Ambitious exploitation plan (with specific focus on Public Protection Disaster Relief-PPDR)*



This document is produced under the EC contract 786409. It is the property of the RESISTO Parties and shall not be distributed or reproduced without the formal approval of the RESISTO Steering Committee

Project Overview

- **RESISTO is an innovative solution for Communication Critical Infrastructure (CI)** providing holistic (cyber/physical) situation awareness and enhanced resilience.

- **It aims 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 unexpected faults.

- **RESISTO will deliver a holistic platform** that, implementing innovative security models, methodologies and technologies and, *by interacting with pre-existent security components of a Communication Infrastructure*, **will increase the overall level of cyber-physical security providing a quantifiable benefit for the end-users**, *in terms of resilience improvement and enhanced protection*.

This document is produced under the EC contract 786409. It is the property of the RESISTO Parties and shall not be distributed or reproduced without the formal approval of the RESISTO Steering Committee

Project Ambition

- The **main ambition** of the RESISTO consortium is to ***develop the necessary concepts and a solid technological baseline*** **so that to create a comprehensive solution that allows:**
  - (i) *faster detection of new cyber/physical threats, and;*
  - (ii) *better informed decision-making and achievement of a joint understanding of cascading effects within the CI and across interconnected Cis, and;*
  - (iii) *enhanced resilience of Communication Infrastructure and CIs that rely on it.*

- ***RESISTO will support progress beyond the state-of-the-art in communication CI protection and the EU strategy on Cybersecurity.***

This document is produced under the EC contract 786409. It is the property of the RESISTO Parties and shall not be distributed or reproduced without the formal approval of the RESISTO Steering Committee

Objectives

- **Help managers of Communication CIs** to guarantee improved business and asset continuity, 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.*

- **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.***

- **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.

- **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.

- **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.

This document is produced under the EC contract 786409. It is the property of the RESISTO Parties and shall not be distributed or reproduced without the formal approval of the RESISTO Steering Committee

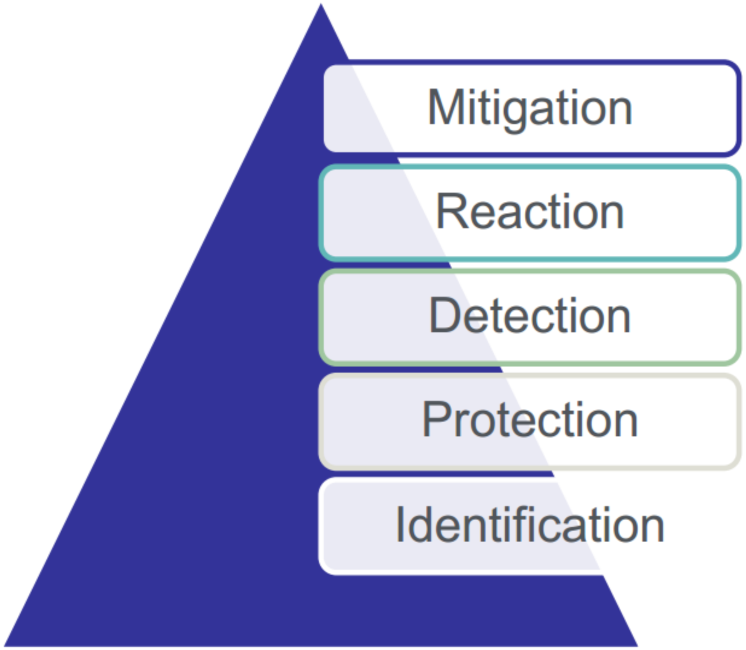
Key Innovation Areas

The RESISTO project will foster the following key innovation areas:

- ***Enlarged Threat Landscape considered*** *(Cyber/Phy/ Cyber+Phy)*
- ***Holistic approach to System Modelling***
- ***Integrated Risk and Resilience management***
- **Convergence of PSIM and Cyber Protection technology**
- ***Perspective:* *New challenges posed by 5G* evolution** *(IoT/IoE, Low-Power WAN)*
- ***New Technology for detection/protection/response*** *(blockchain, drones, machine learning algorithms, software defined security)*
- ***Cyber Intelligence***

This document is produced under the EC contract 786409. It is the property of the RESISTO Parties and shall not be distributed or reproduced without the formal approval of the RESISTO Steering Committee

Functionalities



Identification – *Define and maintain a knowledge base on physical and cyber security risks to systems, assets, data, and capabilities characterizing Telecommunication CIs.*

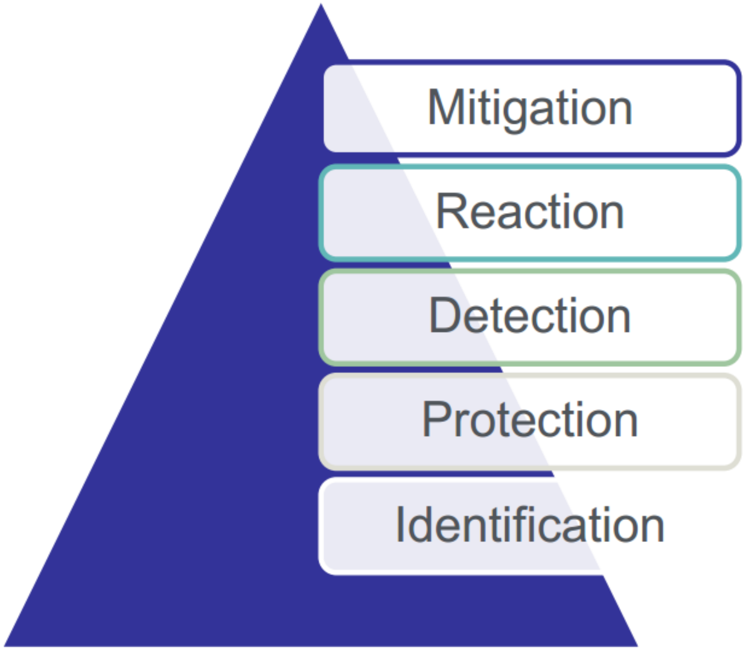
Protection – *Develop and implement the appropriate safeguards to ensure delivery of CI services.*

- ***The high degree of redundancy*** *that usually characterizes telecommunication networks* ***will be further emphasized*** *in order to implement solutions with high resilience, with respect to both physical and cyber-attacks.*
- ***Graceful degradation of performance****, when under attack,* ***will take advantage of Communication or NFV and SDN paradigms.***

This document is produced under the EC contract 786409. It is the property of the RESISTO Parties and shall not be distributed or reproduced without the formal approval of the RESISTO Steering Committee

Functionalities

Detection – *Early and timely discover the occurrence of physical and cyber security events*.

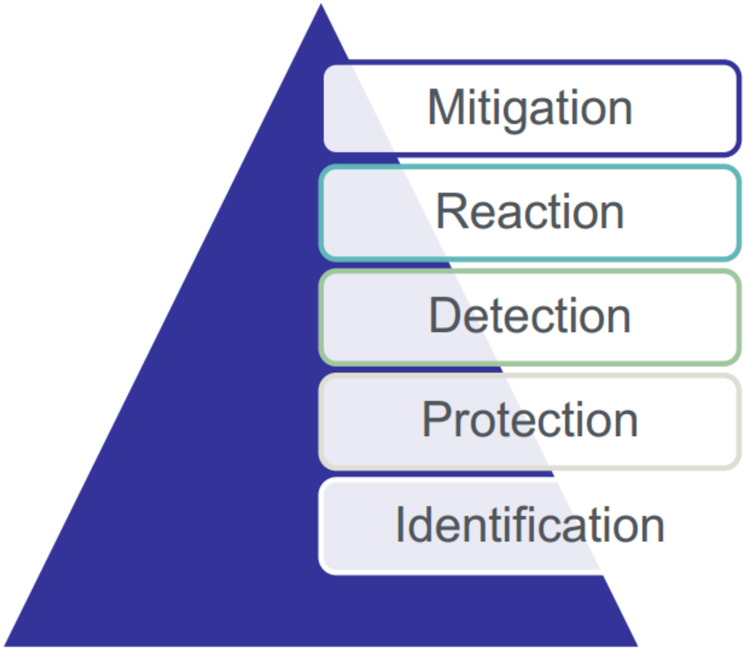


- *Based on evaluation of impacts, recurrent patterns, and the occurrence of complex events.*

- *With the aim of providing a timely detection of a cyber/physical attack, the project will leverage on use of innovative technologies delivered by partner SMEs and RTOs (Research and Technology Organizations), properly integrated with security solutions/components already available in the communication CI.*

This document is produced under the EC contract 786409. It is the property of the RESISTO Parties and shall not be distributed or reproduced without the formal approval of the RESISTO Steering Committee

Functionalities



Reaction – *Orchestrate and implement effective response to a detected security event*.

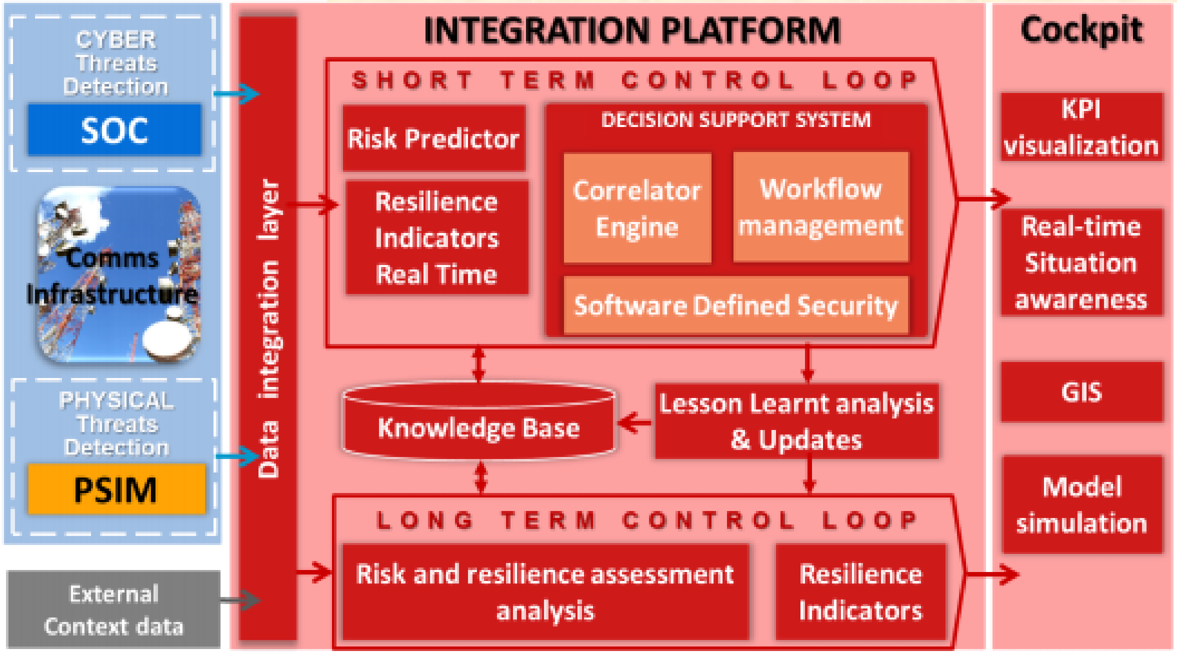
- *RESISTO will investigate the joint use of Security Function Virtualization and Software Defined Security.*
- *Moreover, identifying the best response requires significant advancements in the state-of-the-art, such as tools for the automatic impact assessment of the security risks and performance & effectiveness of potential countermeasures.*

Mitigation – *Develop and implement the appropriate activities to mitigate the impacts of the threat and to restore as much as possible capabilities or services that were impaired due to a security event.*

RESISTO

Logical architecture of the RESISTO platform (1/2)

Two different control loops



Long Term control loop

is

in charge of defining configuration of the system according to the security assessment, and updating it on a periodic basis or when particular events takes place

The ***Long Term control loop*** mainly consists of the:
"Risk and resilience assessment analysis" that identifies the context, analyzes the interdependencies (physical, cyber, logical and geographical) and the risks, evaluates semi-quantitatively and quantitatively those risks, suggests the risks treatment, *and;*
"Resilience indicators" as summarizing measures of resilience of the communication CI in its operational phase;

OTE
ΟΜΙΛΟΣ ΕΤΑΙΡΕΙΩΝ

This document is produced under the EC contract 786409. It is the property of the RESISTO Parties and shall not be distributed or reproduced without the formal approval of the RESISTO Steering Committee

Logical architecture of the RESISTO platform (2/2)

The ***Short Term control loop*** is in charge of promptly reacting to attacks and threats that may impact the operational life of the system.
It is the real-time component of the platform that:

- ***Monitors the Physical and Cyber security status of the infrastructures****, according to the real-time indicators identified by the Risk and Resilience assessment analysis, correlating the physical and cyber domain events in order to detect anomalies and provide early warnings on security attacks by detecting threats in advance, supported also by the innovative detection tools brought by the project.*

- ***Performs the "Interdependency analysis"*** *(Risk Predictor), by simulating the impact with respect to performance degradation of detect anomalies and security attacks on the communication CI and interlinked CIs, based on the cascading effect, to verify the resilience of the communication services*

- *Based on Risk Indicator target value and multi objective (operational, economic, social) analysis,* ***it suggests (Workflow Management)the operator the actions to be enforced (Software Defined Security)*** *to mitigate the risks or to recover from a damaged situation, and orchestrates them.*

Threats classification principles

- **Acceptability:** *The classification of logical and practices easy to be accepted by the majority.*
- **Mutual exclusivity:** *Every threat is classified in one category, excluding all others because categories do not overlap. Every specimen should "fit "in at most one category.*
- **Scalability:** *The classification method can adapt to technology, the ability to accurately define new types.*
- **Certainty:** *The characteristics of each category description are accurate.*
- **Exhaustive:** *The categories in a classification must include all the possibilities (all threat specimens).*
- **Unambiguity:** *All categories must be clear and precise, so that classification is certain. Every category should be accompanied by unambiguous classification criteria defining "what specimens to be placed in that category".*
- **Repeatability:** *Repeated applications result in the same classification, regardless of who is classifying.*
- **Universality:** *Can be adapted to different application requirements.*
- **Acceptance:** *All categories are logical, intuitive and practices easy to be accepted by the majority.*
- **Usefulness:** *It can be used to gain insight into the field of inquiry; it can be adapted to different application needs.*
- **Availability:** *Classification of the different fields of practical value.*

This document is produced under the EC contract 786409. It is the property of the RESISTO Parties and shall not be distributed or reproduced without the formal approval of the RESISTO Steering Committee

Security threats in telecom infrastructures

*A **security threat** is defined as a **potential violation of security**; a possible danger that might exploit a vulnerability to breach security and, therefore, cause possible harm.*

Examples of threats include:

- ***Unauthorized disclosure** of information;*
- ***Unauthorized destruction or modification** of data, equipment or other resources;*
- ***Theft, removal or loss of information** or other resources;*
- ***Interruption or denial of services (DoS)**, and;*
- ***Impersonation, or masquerading** as an authorized entity.*

This document is produced under the EC contract 786409. It is the property of the RESISTO Parties and shall not be distributed or reproduced without the formal approval of the RESISTO Steering Committee

Assets to be protected in telecom infrastructures

In telecommunications domain there is a need to protect assets for:

- **Customers/subscribers** *who need confidence in the network and the services offered, including availability of services (especially emergency services).*
- **Public community/authorities** *who demand security by directives and/or legislation, in order to ensure availability of services, privacy protection, and fair competition.*
- **Network operators and service providers** *who need security to safeguard their operation and business interests and to meet their obligations to customers, their business partners and the public.*

The assets to be protected also include:

- *Communication and computing services;*
- *Information and data, including software and data relating to security services;*
- *Personnel, and;*
- *Equipment and facilities.*

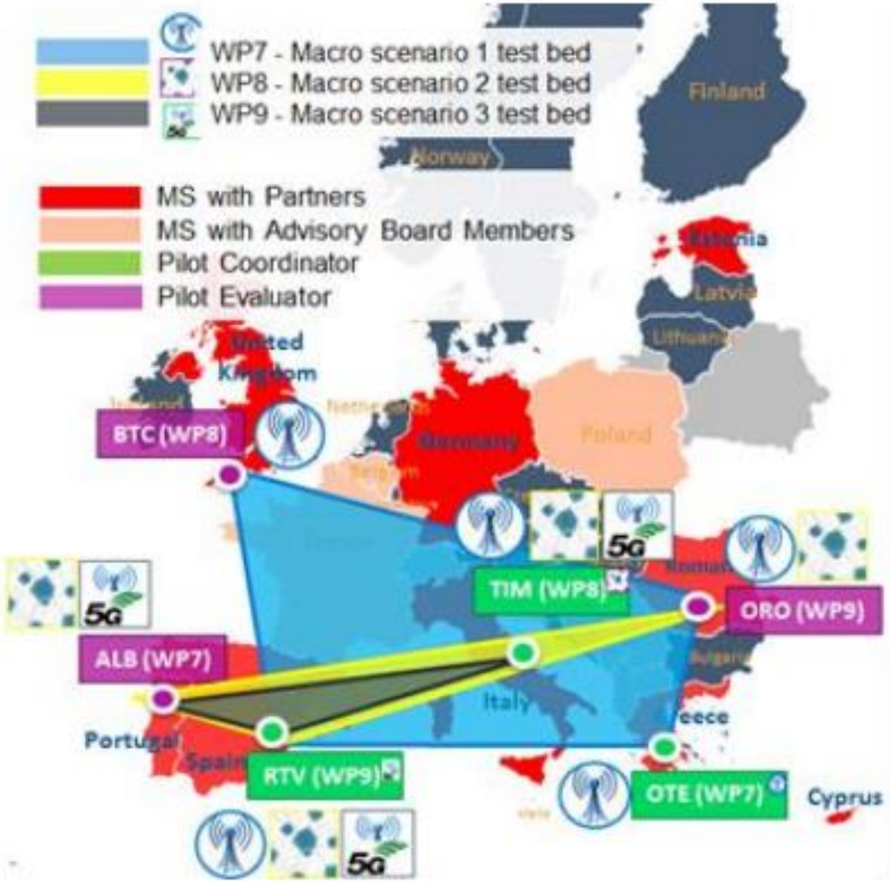
RESISTO Validation Framework

- **RESISTO is an experimentally-*driven* research for the design and deployment of solutions**, ***in line with H2020 Innovation Actions'*** *expected approach tailored to the Communication CI domain.*

- Thus, **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)*.

- **Consideration of three (-3-) (Macro)-Scenarios**, **each one involving a set of related Use Cases *to prove the RESISTO concept against physical and cyber threats for the Communication CIs***, covering the following domains in a progressive manner:
  - *Macro-Scenario 1* - *Protection of the current Telecommunication Critical Infrastructures*
  - *Macro-Scenario 2* - *Their interdependencies as providers of essential communication services to other interlinked CIs and related cascade effects in the vicinity*
  - *Macro-Scenario 3* - *Their evolution towards the future 5G networks and the emerging IoT world*

(Improving of resilience of) Current telco Infrastructures



- ***Exchange of data among the pilots*** *so as to react jointly*
- ***Sharing of the infrastructure (physical interconnection of pilots):*** *Pilot sites are physically interconnected.*
- ***End-users will actively work together*** *so as to properly cover all challenges*

- **Blue color** depicts the test-bed of **Macro-Scenario 1 *(OTE Coordinator)***
- **Yellow color** depicts the test-bed of **Macro-Scenario 2**
- **Grey color** depicts the test-bed of **Macro-Scenario 3**

Expected Results

- **State-of-the-art analysis** of physical/cyber detection technologies and risk scenarios of Communication CIs.
- **Innovative tools, concepts, and technologies** *for combatting combined physical/cyber threats to Communication CIs (RESISTO framework).*
- **Security risk management plans** *integrating systemic and both physical and cyber aspects.*
- **Extended validation of the RESISTO framework against physical/cyber threats** ***across three verticals:*** *current, future (towards 5G) and interconnected Communication infrastructures.*
- **Convergence of safety and security standards**, *establishment and dissemination throughout the relevant user communities of specific models for information sharing on incidents, threats and vulnerabilities.*
- ***Support to the European Cyber Security Organization (ECSO)***.

This document is produced under the EC contract 786409. It is the property of the RESISTO Parties and shall not be distributed or reproduced without the formal approval of the RESISTO Steering Committee

Thank you !

http://www.resistoproject.eu/

For more information:

Dr. Ioannis P. Chochliouros
Head of Fixed Network R&D Programs Section
Research and Development Dept., Fixed & Mobile
Core Network DevOps & Technology Strategy Division, Fixed & Mobile
E-Mail: ichochliouros@oteresearch.gr; ic152369@ote.gr;

Mrs. Maria Belesioti
Fixed Network R&D Programs Section
Research and Development Dept., Fixed & Mobile
Core Network DevOps & Technology Strategy Division, Fixed & Mobile
E-Mail: mbelesioti@oteresearch.gr;