

RESISTO:

D10.8_ DISSEMINATION AND COMMUNICATION ACTIVITIES – THIRD



RESISTO

D10.8 – DISSEMINATION AND COMMUNICATION ACTIVITIES – THIRD

Document Manager:	Federica Battisti	RM3	Editor
--------------------------	-------------------	-----	--------

Project Title:	RESilience enhancement and risk control platform for communication infraSTructure Operators
Project Acronym:	RESISTO
Contract Number:	786409
Project Coordinator:	LEONARDO
WP Leader:	LDO

Document ID N°:	RESISTO_D10.8_200527_01	Version:	1.0
Deliverable:	D10.8	Date:	27/05/2020
		Status:	APPROVED

Document classification	Public
--------------------------------	---------------

Approval Status	
Prepared by:	Federica BATTISTI (RM3) – Arianna MAGNI (APRE)
Approved by: (WP Leader)	Federica BATTISTI (RM3)
Approved by: (Coordinator)	Bruno SACCOMANNO (LDO)
Advisory Board Validation (Advisory Board Coordinator)	N.A.
Security Approval (Security Advisory Board Leader)	N.A.

CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Federica Battisti	RM3	Editor
Arianna Magni	APRE	Contributor
Jorge Carapinha	ALB	Contributor

DISTRIBUTION LIST

Name	Company / Organization	Role / Title
PMT	RESISTO CONSORTIUM	NA
Markus MULLER	EC DG REA	EC Programme Officer
General Public	NA	NA

REVISION TABLE

Version	Date	Modified Pages	Modified Sections	Comments
0.1	15/05/2020	All	All	First draft
0.2	18/05/2020	All	All	New text, revision
0.3	26/05/2020	40-45	Section 11	New section
1.0	27/05/2020	40-45	All	Final version

COPYRIGHT STATEMENT



© 2018-2021 This document and its content are the property of the RESISTO Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the RESISTO Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the RESISTO Partners. Each RESISTO Partner may use this document in conformity with the RESISTO Consortium Grant Agreement provisions.

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Program, under the Grant Agreement No 786409.

The views and opinions in this document are solely those of the authors and contributors, not those of the European Commission.

PROJECT CONTACT



LEONARDO
Via Puccini 2 – Genova – 16154 – Italy
Tel.: +39 348 6505565
E-Mail: bruno.saccomanno@leonardocompany.com

RESISTO PROJECT – PUBLISHABLE EXTENDED ABSTRACT

Communications play a fundamental role in the economic and social well-being of the citizens and on operations of most of the CIs. Thus they are a primary target for criminals having a multiplier effect on the power of attacks and providing enormous resonance and gains. Also extreme weather events and natural disasters represent a challenge due to their increase in frequency and intensity requiring smarter resilience of the Communication CIs, which are extremely vulnerable due to the ever-increasing complexity of the architecture also in light of the evolution towards 5G, the extensive use of programmable platforms and exponential growth of connected devices. The fact that most enterprises still manage physical and cyber security independently represents a further challenge. RESISTO platform is an innovative solution for Communication CIs holistic situation awareness and enhanced resilience (aligned with ECSO objectives). Based on an Integrated Risk and Resilience analysis management and improvement process availing all resilience cycle phases (prepare, prevent, detect, absorb, etc.) and technical resilience capabilities (sense, model, infer, act, adopt), RESISTO implements an innovative Decision Support System to protect communication infrastructures from combined cyber-physical threats exploiting the Software Defined Security model on a suite of state of the art cyber/physical security components (Blockchain, Machine Learning, IoT security, Airborne threat detection, holistic audio-video analytics) and services (Responsible Disclosure Framework) for detection and reaction in presence of attacks or natural disasters. Through RESISTO Communications Operators, will be able to implement a set of mitigation actions and countermeasures that significantly reduce the impact of negative events in terms of performance losses, social consequences, and cascading effects in particular by bouncing efficiently back to original and forward to operational states of operation.

EXECUTIVE SUMMARY

This deliverable contains the third release of the dissemination plan to present the dissemination activities carried out during the second year and to act as a roadmap for the upcoming activities.

This deliverable is an update of the existing main objectives and tools of the dissemination and communication strategy that the project has put in place to reach the largest audience as possible for sharing the details of the project and of its outcomes. This Deliverable is meant to act as the main dissemination and communication strategy document.

CONTENTS

ABBREVIATIONS	9
1. INTRODUCTION.....	10
2. COMMUNICATION AND DISSEMINATION STRATEGY: 2ND YEAR	11
2.1. Integrated Plan	11
2.2. Roles and Responsibilities	12
2.3. Dissemination and Communication POCs	13
2.4. Stakeholders, targeted audience and User Groups	13
3. RESISTO BRAND INDENTITY (BI).....	16
3.1. Guidelines for use of brand identity	16
3.2. Project logo.....	16
3.3. Guidelines for the EC funding	16
3.4. Project Templates.....	17
3.4.1. RESISTO Newsletter template	17
4. COMMUNICATION MATERIALS AND PRODUCTS.....	19
4.1. Brochure/Poster/Rollup.....	19
4.2. Business card	21
4.3. Background slide.....	21
4.4. Event card	22
4.5. Gadget	22
4.6. Booth Wall.....	23
4.7. Newsletter	24
5. SUMMARY OF DISSEMINATION / COMMUNICATION TOOLS AND CHANNELS	27
5.2. Social media channels	28
5.2.1. Twitter	28
5.2.2. Facebook	29
5.2.3. LinkedIn.....	29
5.2.4. YouTube.....	30
6. PROJECT PRESENTATION AT EXTERNAL EVENTS	31
6.1. Trade shows, exhibitions and clustering events.....	31
6.2. Conference.....	32
6.2. Workshop.....	33
6.3. Events participation: partner rules.....	35
7. PUBLICATIONS	36
7.1. Scientific Publications.....	36
7.2. Articles	36
7.3. Other Publications.....	37
7.2. Publications section on the website	38

8.	NETWORKING: EU CLUSTER FOR SECURING CRITICAL INFRASTRUCTURES	39
9.	SUMMARY OF RESISTO KPIs	40
10.	EXECUTION OF DISSEMINATION STRATEGY	41
11.	RELEVANT STANDARDS, GAP ANALYSIS AND RESISTO COMPLIANCE	42
11.1	Standards in RESISTO	42
11.2	Standards to be used by RESISTO	45
11.3	Other relevant documents	47
11.	CONCLUSION	48
12.	REFERENCES	49
	ANNEX 1: RESISTO INTEGRATED PLAN.....	50
	ANNEX 2: DISS AND COMM POCs contacts list	51
	ANNEX 3: List of the partners' social media accounts.....	52

ABBREVIATIONS

APRE	Agency of the Promotion of the European Research
BI	Brand Identity
COMM	Communication
DISS	Dissemination
DoA	Description of Actions
DX.X	Deliverable
ECSI	European Cluster for Securing Critical Infrastructure
EU	European Union
FB	Facebook
KPI	Key Performance Indicator
KSI	Key Success Indicator
LKD	Linkedin
M	Month
RM3	University of Roma Tre
TW	Twitter
WP	Work Package
YT	YouTube

1. INTRODUCTION

The main purpose of this Deliverable is to update the general roadmap towards the dissemination strategy and communication plan that was presented in the second release D10.7 Dissemination and communication activities – Second.

The second year of the project focused on the consolidation of the system architecture, the interfaces among all RESISTO components, the use cases that will be employed in the validation phase.

In this second year dissemination activities were carried out more extensively to cover a broader audience with respect to the first year. Moreover, we have created a group with one representative for each partner to strengthen their involvement in the dissemination activities.

As announced in D10.6, also in D10.8 all activities foreseen and accomplished during the second project year are mapped and individual dissemination and communication actions per partner listed.

2. COMMUNICATION AND DISSEMINATION STRATEGY: 2ND YEAR

The main goal of the dissemination strategy within RESISTO is the dissemination of the achieved results to the largest audience as possible. This includes the following objectives:

- the definition of mechanisms and strategies for an effective dissemination;
- the creation of a community composed by the project partners and interested stakeholders;
- the implementation of targeted communication activities for different recipients (e.g., stakeholders, research communities);
- the performance of dissemination activities to raise international awareness and interest in the project activities and in the achieved results;
- the dissemination of relevant project results to standardization bodies;
- to maximize the impact of RESISTO by creating a liaison with other EU, regional and national projects.

The dissemination activities are devoted to the establishment of a critical mass of stakeholders and research bodies. In order to achieve this goal, the results of the activities within RESISTO will be disseminated to the widest possible community through several means. The participation of entities outside the consortium and knowledge sharing will be encouraged through networking activities and events aimed at increasing the impact and enriching the scientific and industrial contribution to the project.

The goals of the dissemination strategy are:

- the preparation of a plan for the dissemination activities;
- the creation of an image of the project;
- the establishment of the project website, together with its continuous update;
- the use of social networking tools;
- the preparation of articles, publications, press releases and brochures/flyers;
- the participation to dissemination events.

The practices to be followed by the dissemination strategy refer to the following principles:

- definition of the various target audiences to whom the project will appeal;
- identification of the type and nature of the knowledge produced and production of targeted dissemination materials tailored to the characteristics of each audience segments;
- establishment of communication means and channels to reach these audience segments along with appropriate preparation of printed and electronic materials;
- selection of the most suitable time schedule to implement the items listed above in order to achieve the most effective dissemination possible.

2.1. Integrated Plan

The RESISTO Integrated Plan is a planning of the all main RESISTO dissemination and communication activities. This plan is stored in EMDESK in a dedicated folder named “integrated plan”, and it is accessible to all partners (<https://emdesk.eu/shared/5ebb89893dd29-c9133f1498f0a0990ff751f8e5479af7>)

The integrated plan (Annex 1) is an excel file composed by 4 sheets: the first three sheets represent the three years of the project; each column identifies a month and each row an activity (meetings, workshop, special events and main communication and dissemination products such as newsletter, project video and open access book articles).

Past activities are noted in black and future activities are noted in red. This document is updated monthly.

The fourth sheet reports all the key words of the project and the main topics highlighted by the coordinator and technical coordinator (Figure 1). They are useful indications for communication and dissemination activities, especially when attending an event and presenting the project.

RESISTO - Key-words & Topics

KEY WORDS (for events selection)	PERIOD		TOPICS (for papers, presentations, newsletters, ...)	PERIOD
A. CRITICAL INFRASTRUCTURE PROTECTION	always		RESISTO Project (context, needs, general solution)	M01 - M24
B. RISK & RESILIENCE MANAGEMENT	always		RESISTO Architecture	M01 - M24
C. 5G NETWORK SECURITY	always		Critical Infrastructures Modeling	M22 - M27
D. PHYSICAL SECURITY	always		Cascade effects prediction	M22 - M27
E. MACHINE LEARNING	M25 - M36	Only for the last year of the project	Workflows for an effective Decision Making Support	M22 - M27
F. ARTIFICIAL INTELLIGENCE	M25 - M36	Only for the last year of the project	... TBD (eg Validation, Benefits for the end user)	M28 - M36
			Resilience Assessment	M01 - M24
			RIs (Resilience Indicators) quantification	M19 - M24
			SDS (Software Defined Security)	M22 - M27
			5G Orchestrator	M22 - M27
			Anomaly detection with active and passive sensors	M19 - M24
			... TBD	
			... TBD	

Figure 1– RESISTO Integrated Plan: Key-words & Topics

The topics are also reported in the first row of each sheet.

This document is meant to be reference point for past, present and future dissemination and communication activities.

2.2. Roles and Responsibilities

Interaction and communication with all consortium partners and interaction with all Work Packages are necessary to successfully disseminate the results of the project.

All consortium partners have to contribute to the implementation of the dissemination strategy.

RESISTO project partners are expected to acknowledge the Dissemination and Communication Manager in order to ensure the smooth implementation of the Communication and Dissemination objectives.

The Task 10.2 “Dissemination, Communication and awareness raising activities” defines the plans, the roles, and the responsibilities of the partners for the communication and dissemination activities. RM3 (with APRE support) is responsible for designing and scheduling the strategy at European level, as well as coordinating, monitoring, periodically evaluating and reviewing the dissemination strategy. Communication activities will be implemented by the whole consortium under the coordination of RM3 (with APRE support) and LEONARDO, as WP leader and project coordinator. Any communication choice is discussed first among the coordinator and RM3, to identify the presence of issues related to the confidentiality of some

activities of the RESISTO project, and then proposed to the whole consortium for improvements and approval.

All partners are responsible for carrying out specific dissemination actions and for ensuring the highest quality in the implementation of the dissemination activities. Each partner is responsible for adapting the dissemination activities and materials at their national level and for the performance of effective monitoring and follow up.

As far as the execution of the plan is concerned, an internal monitoring process will be put in place: RM3 (with APRE support), as Task 10.2 leader, will supervise the progress of the communication actions and provide further indication when needed.

2.3. Dissemination and Communication POCs

In order to improve the involvement of the entire consortium in the dissemination activities, an operative group has been created. It is composed by one representative (PoC – Point of Contact) from each partner. Monthly meetings are foreseen among the project coordinator, the communication and dissemination leader (with the support of APRE), and the PoCs for discussing about the current status and plan new dissemination activities. The list of PoCs is reported in Annex 2.

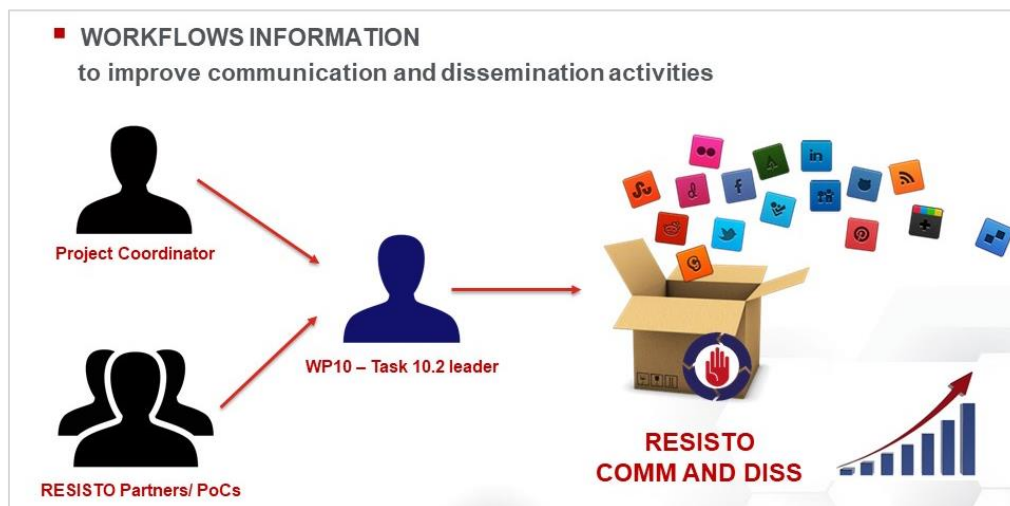


Figure 2– Workflow information comm and diss: scheme

2.4. Stakeholders, targeted audience and User Groups

In order to develop an effective dissemination and communication strategy, following the determination of its specific goals and objectives, the most critical step is the identification of the target audience for the project. It is clear that for each phase (requirements definition, development and integration, piloting implementation - as it will be described later in this Deliverable), different groups will be targeted so as to proactively and effectively provide the most relevant information to particular specific groups.

To this respect, and in order for the produced knowledge during the project to be disseminated and communicated effectively, the following groups have been initially identified:

Initial phase: requirements and architecture definition

- facility managers and working conditions advisors;
- IT engineers, cyber/physical threat avoidance workers and hardware / software developers;
- students, researchers, and the academic community;
- general public;
- telecom providers, end users and ISPs associations and security communities.

Development and integration phase

- policy makers in large telecom organizations or in government and ministries;
- critical infrastructures regulators, managers and grants providers;
- development partners and stakeholders from international and national cooperation agencies;
- public and private agencies and associations against cyber and physical threats;
- National and International Telecommunication associations.

Piloting implementation phase

- industry stakeholders and policy makers;
- telecommunications and security supplier companies and integrators;
- electronics and sensors manufacturers;
- mobile, web and IT developers;
- national and international Telecommunication Standardization Bodies;
- risk / resilience related players and associated agencies;
- the wider security community and associated markets;
- the wider critical infrastructures community and related national and international bodies since many of the project outcomes are foreseen to have significant applications and important impact to other critical infrastructures (i.e. transportation infrastructures, energy plants etc) apart from the telecom ones.

To this end, based on the above list, different mechanisms and actions will be employed in order to disseminate and communicate the goals and outcomes of RESISTO to the above wide variety of targeted groups. Attempting to make an initial classification of the various stakeholders of the targeted audience the following general groups are derived where respective dissemination and communication tools, means and channels will be applied to attract the major possible appeal:

1. Dissemination to European and nationally or internationally based industries: the RESISTO industrial partners and SMEs will disseminate the project scope and outcomes not only within their companies and organizations, but also out of their companies and through their client networks and communication channels. The expected mechanisms to be applied are:
 - informal awareness creation and knowledge transfer, through internal websites, portals and newsletters;
 - meetings of related staff with other personnel out of the project, to identify synergies early enough;

- clustering with other EU and national research projects and operational initiatives;
 - dissemination to related Business Interest Groups with the use of all dissemination and communication channels, such as electronic media and participation in conferences, fairs, exhibitions and joint events.
2. Dissemination to the academic and scientific research community: the RESISTO academic partners and Research and Technology Organisations (RTO) will disseminate the technological and scientific results that will be of major interest for the scientific and industrial commercial community. These results will be communicated, apart from the RESISTO website, at scientific, hardware and IT, telecom infrastructures and the general security society meetings, through publications in peer-reviewed conferences and journals, through press releases for popular technical magazines, along with social media and networking. Metrics such as the Impact Factor will be used to select the most appropriate and important journals for the scientific content while Open Access policies will be also promoted. Special sessions organizations in international and IEEE Conferences and workshops will be pursued.
 3. Dissemination to the wider public, the media and potential users: the attraction of a wider public is planned to be accomplished through the creation and inclusion in web sites, the social media and popular channels along with press releases in magazines and newspapers or newsletters, adjust the content each time to the specific target group.
 4. Dissemination to policy makers, security organizations and End Users (Telecom groups and Standardization Bodies): this activity includes a variety of actors including those players that determine the legal framework in national and international level since the RESISTO affects legal and ethical issues (such as personal data) as well. The above category ranges from the EU Committees and Agencies related to critical infrastructure protection up to Law Enforcement Agencies (LEAs), Non-governmental organizations (NGOs) and International Standardization Bodies (IEEE groups, ETSI and ECC etc). The related activities are foreseen to take place in the later stages of the project where the proof of concept and the piloting implementation will result in successful validation and evaluation results. Thus, representatives of these entities will be invited to observe the operational RESISTO platform during the piloting implementation, while targeted actions are envisioned: participation to large security and critical infrastructures related scientific or market events, fairs, exhibitions, conferences and expos in combination to exploitation actions.
 5. Clustering with other research and operational initiatives: Intra-project dissemination and clustering with relevant EU or national projects will be pursued to achieve essential and important collaboration between researchers within Europe. Currently running or already finished EU or national research projects with disciplines related to RESISTO will be contacted to establish relationships and investigate potential common interests or even combined implementations and approaches, exchanging views and information, fostering cooperation and feedback with other players on the field and enabling stakeholders' interaction. This will be facilitated through participation in Clustering Events organised by the EC, Experts working Groups, Critical Infrastructures Initiatives or Security Organizations.

3. RESISTO BRAND INDENTITY (BI)

3.1. Guidelines for use of brand identity

RESISTO project developed a distinct, recognizable brand, which was identified after some time of the project lifetime, its activities and its capacity, by the various stakeholders. The brand identity “RESISTO” comprises all visual and contextual content including logo, colours, fonts and accompanying slogan.

All partners in both their internal and external communication have to adhere to the guidelines for maintaining a consistent brand identity in order to build awareness and brand. The logo of partners responsible for specific actions (e.g. organisation of workshops or dissemination presentations) may also appear along with the project logo and after the consent of the Task 10.2 leader or the Project Coordinator.

The partners are required to follow the guidelines and directions established in the “RESISTO Brand Identity Manual” [D10.1 – Communication materials - first].

3.2. Project logo

The project logo is one of the key elements in the identity of the project. Its main goal is to effectively represent the core objectives of the project. The logo must capture the vision, mission and objectives of the RESISTO project, and therefore the project logo has already been designed in the first month of the project.

The project logo is in Figure 3.



Figure 3 – RESISTO logo official color_black_white

3.3. Guidelines for the EC funding

Projects funded by the European Commission (EC) are required to indicate this support received using a corresponding sentence on all public appearances of the project as well as the EC logo.



This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No **786409**.

This acknowledgement must appear in ALL external communication material produced by the project.

3.4. Project Templates

The templates for different document types have been prepared (.doc, .ppt). The use of shared templates allows the project to be represented in a uniform way. All templates are available for the consortium partners on Emdesk (<https://emdesk.eu/cms/?p=334>).

Currently the following templates are available:

- RESISTO Periodic report template (Microsoft Word);
- RESISTO Minutes of Meeting template (Microsoft Word);
- RESISTO Deliverable template (Microsoft Word);
- RESISTO Presentation template 16:9 (Microsoft PowerPoint);
- RESISTO Presentation template 4:3 (Microsoft PowerPoint);
- RESISTO Newsletter template A4 (Adobe Indesign)

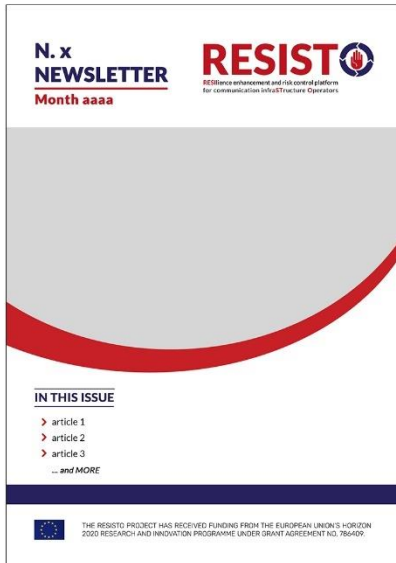
Additional templates will be added as required.

All documents and presentations in RESISTO will be created by using the appropriate templates.

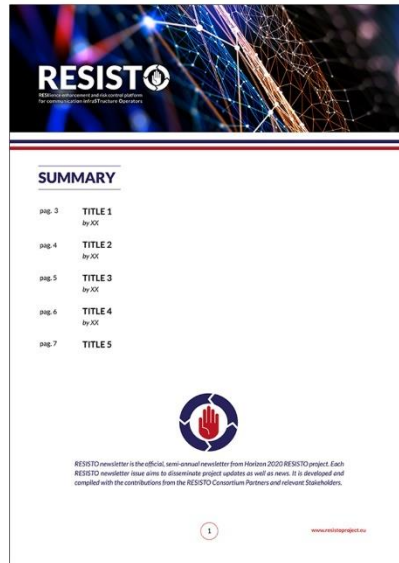
3.4.1. RESISTO Newsletter template

RESISTO newsletter is the official, semi-annual newsletter from Horizon 2020 RESISTO Project, designed by APRE and realised by RM3 with the contribution of all partners [see *paragraph 4.7*]

The RESISTO Newsletter template is designed respecting the brand identity of the project (palette colors, logo, background, font, etc.). The design has been conceived to be modern and appealing.



COVER



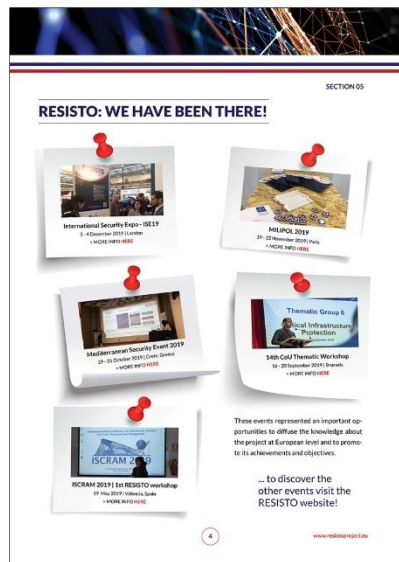
INDEX



WELCOME PAGE



ARTICLE PAGE



EVENTS PAGE



BACK COVER

Figure 4 – RESISTO newsletter template

4. COMMUNICATION MATERIALS AND PRODUCTS

While there is a wide variety of dissemination methods, it is important to select the right one(s) to get the project message to the target audience and achieve the project's purposes.

Dissemination materials represent the formats, structure and presentation of the content as the RESISTO information provided to user to make it easily useable.

- posters, brochures, roll up can create awareness about the project;
- brochures with summaries promote the objectives and outputs of the project. Brochures in printed form can be handed out at conferences. An electronic version (e.g. PDF file) can also be circulated electronically;
- a poster or a roll up at a conference may be more appropriate when you cannot make a presentation as a speaker. It may not be as effective as giving a presentation in the auditorium, but it is an excellent way to engage people, gauge their reactions, and get one-to-one feedback.

In the framework of the RESISTO project, APRE is responsible for the creation and development of the communication material.

A comprehensive set of communication materials has been designed and produced by APRE. It aims at improving the brand awareness and sharing information about the project's mission among the defined targets. It has been designed in total accordance with the RESISTO brand identity.

The RESISTO Communication material includes several tools/materials that each project partner will use during events, meetings and in any communication activity performed.

The RESISTO communication material is shared with the partners on EMDESK (RESISTO Intranet: collaboration and project management tool used by RESISTO consortium), in the "WP10" folder and it is possible to download the material from <http://www.resistoproject.eu/communication-materials/>

Currently [M24], the RESISTO communication material includes Brochure/Poster/Rollup, Business card, background slide, event card, gadgets, booth wall, and newsletter.

4.1. Brochure/Poster/Rollup

The brochure contains information on the main thematic of the project including the overall structure of the project, its objectives, and foreseen outcomes. The brochure will be distributed in public events and to interested parties during the lifetime of the project.

The brochure is designed respecting the brand identity of the project (palette colors, logo, background, font, etc.). The design has been conceived to be modern and appealing.

The brochure is available in hard and electronic version and it is downloadable from the project website. Printed versions will be made available to be distributed at key events in Europe and worldwide, electronics versions will be sent to target groups via e-mail.

All partners are required to distribute the leaflet:

- within events related to the project themes;
- within key events where the audience is mainly composed of stakeholders for the topic of RESISTO;
- during face-to-face meetings with targeted stakeholders.



Figure 5 – RESISTO brochure

The objective of the roll up and poster is to attract people attention, thus to impress in their mind some brief but strategic information about the RESISTO project with the aim of inducing them to look for more details on the website and be aware of the project objectives. The information conveyed through the roll-up or the poster should take the form of short self-understandable message.

The rollup or the poster, being a self-standing communication tool, can be positioned in wide and strategic places at conference premises, serving at best its dissemination purposes.

The roll up and the poster are designed respecting the brand identity of the project (palette colors, logo, background, font, etc.).



Figure 6 – RESISTO poster and roll-up

4.2. Business card

The objective of the business card is to facilitate the dissemination of contacts regarding the RESISTO project.



Figure 7 – RESISTO business card

4.3. Background slide

The background slide, being a self-standing communication tool, can be projected in all conference screens, in strategic position at conference premises, serving at best its dissemination purposes.

The background slide is designed respecting the brand identity of the project (palette colors, logo, background, font, etc.).



Figure 8 – RESISTO background slide

4.4. Event card

A dedicated card will be created for each new event or workshop to be opened. These cards will be used only for the social media communication.

The examples below have been created for:

- International Security Expo 2019, London, December 03, 2019;
- EGU 2020 General Assembly “Sharing Geoscience Online”, online event, May 08, 2020.



Figure 9 – RESISTO event cards

4.5. Gadget

The gadgets, branded with the RESISTO logo, will be distributed during major events to increase the knowledge of the RESISTO project by the community.



Figure 10 – RESISTO gadgets

4.6. Booth Wall

The RESISTO “wall”, being a self-standing communication tool, can be positioned in wide and strategic places at conference premises, serving at best its dissemination purposes.

The wall is designed respecting the brand identity of the project (palette colors, logo, background, font, etc.).



Figure 11 – RESISTO “booth wall”

4.7. Newsletter

RESISTO newsletter is the official, semi-annual newsletter from Horizon 2020 RESISTO Project, designed by APRE and realised by RM3 with the collaboration of all partners. Each RESISTO Newsletter issue aims at disseminating project updates as well as news. It is developed and compiled with contributions from the RESISTO Consortium Partners, Advisory Board’s members and the relevant Stakeholders.

With the aim of providing relevant information to the ecosystem while gaining stronger engagement from the RESISTO stakeholders, the newsletter is designed as follows:

- **Insight from the RESISTO project coordinator:** a welcoming message from the coordinator suggesting the most appropriate keys to go through the newsletter;
- **What’s hot:** hot topics analysed from RESISTO partners or AB members (a collection of articles with different themes);
- **Technical highlights:** technical update on the project by the technical coordinator of RESISTO;
- **RESISTO: we have been there!** a collection of all dissemination and communication events in which the RESISTO project partners participated.

To date, two RESISTO newsletter have been issued. Each RESISTO newsletter has been disseminated following the RESISTO Communication Campaign approach. Open average: 56% (source: google analytics)

Links to the RESISTO newsletter issued during the reporting period (M1 – M24):

- [n.1 RESISTO Newsletter | December 2019 \[here\]](#)
- [n.2 RESISTO Newsletter | April 2020 \[here\]](#)



Figure 12 – RESISTO newsletter cover: 1st issue and 2nd issue

The RESISTO newsletter is disseminated through:

- Website;
- Social media channel (Twitter/Facebook/LinkedIn);
- Mailing to partners and contacts;
- Contacts subscribed via the website form;
- APRE database [6000 contacts];
- APREweekly (bulletin).

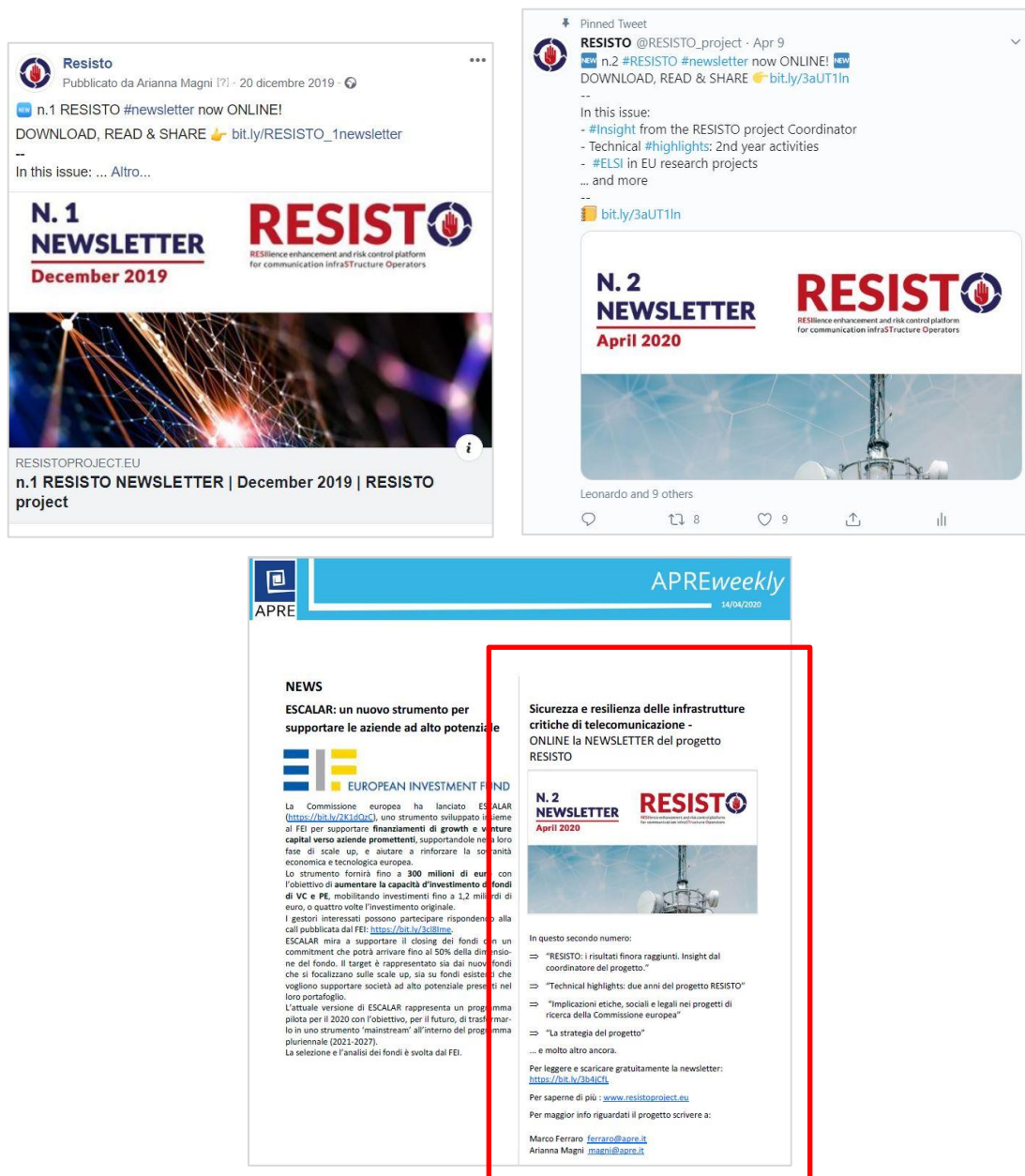


Figure 13 – RESISTO newsletter: dissemination through social media channels and APREweekly

5. SUMMARY OF DISSEMINATION / COMMUNICATION TOOLS AND CHANNELS

A number of communication tools is employed by the project for communication purposes in order to achieve the planned objectives. Each tool has a different goal, target audience and engagement factor, the purpose being to cover the whole target audience through complementarity.

5.1. RESISTO website: main analytics and figures

The project website allows the communication with the general public as well as the one among the consortium partners. The project website has been established within one month from the kick - off meeting and will be maintained and continuously updated through the whole duration of the project.

The project website is also used as a hub for all dissemination activities, and news broadcast channel for all public information.

The RESISTO website is online at www.resistoproject.eu

As shown from the website Map [D10.3 – Project Website], the Homepage serves as an entry point to all relevant sections. All the access points are provided for in the horizontal menu, while visual evidence through dedicated sections are provided when scrolling the homepage, as follows:

- About the RESISTO project
- Latest news
- Calendar Events
- Social media feed RSS
- RESISTO partners
- Resources
- Contact form

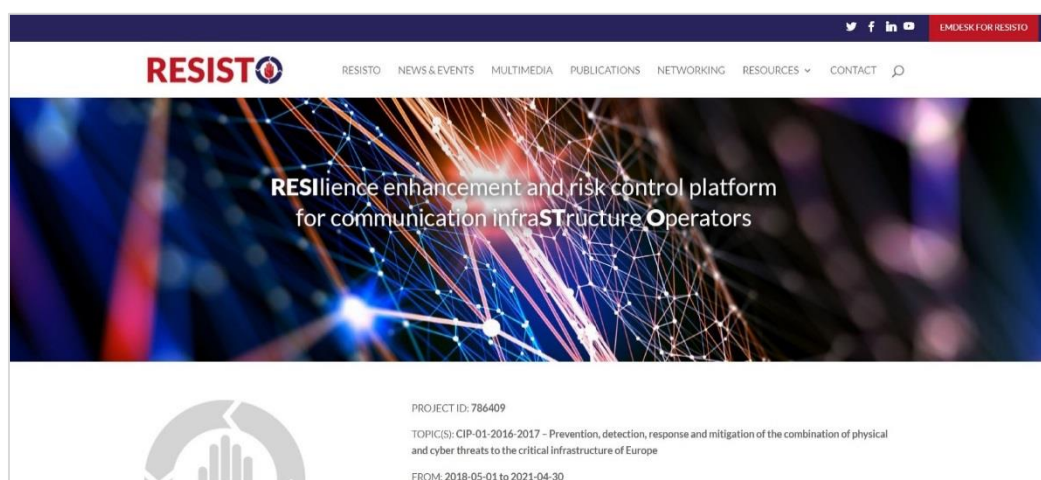


Figure 14 – RESISTO website: home page

The RESISTO website has been constantly monitored by the Communication team through the RESISTO Google analytics account. **Errore. L'origine riferimento non è stata trovata.** reports the main performance results at M24 (April 2020).

Analytics – www.resistoproject.eu (M24)	
Users	n. 734
Page views	n. 1567

Table 1 - Website Analytics (M12-M24) Source: Google Analytics

Table 2 reports a resume of content publishing activities on the website.

Publishing activities on - www.resistoproject.eu (M24)	
News and events	n. 28
Multimedia	n. 11 album
Publications/Resources	n. 23

Table 2 - Website – Publishing activity by content type

5.2. Social media channels

The RESISTO project is promoted all along its duration through four social media, namely Twitter, Facebook, LinkedIn and YouTube. It is understood that Social Media as a mean of communication require time and an editorial calendar to become effectively functional.

The social media will be promoted at any given chance, in all communication activities or material, by all partners. Therefore, links to all social media accounts will appear on the Website, flyers and brochures, reports intended for the public and official project presentations. It is also necessary for project partners to promote the social media in their exchanges with clients and other stakeholders.

5.2.1. Twitter

User name: [@RESISTO_project](https://twitter.com/RESISTO_project)

Twitter - brief (M24)	
Followers	n. 146
Tweets	n. 233
Retweets	n. 88
Views	n. 5,7 K

Table 3 - Twitter – brief (source: Twitter Analytics)

The partners are required to participate on spreading the word on Twitter. It is necessary that each project partner has an official account for interacting with RESISTO. Moreover, the partners will automatically receive an email whenever they have to interact with the RESISTO Twitter profile. The tweets shared by the RESISTO account will be retweeted by all the official partners' accounts (**Annex 3**).

5.2.2. Facebook

User name: [@RESISTO.eu.project](https://www.facebook.com/RESISTO.eu.project)

Facebook - brief (M24)	
Followers	n. 132
Post	n. 56
View	n. 757

Table 4 – Facebook – brief (source: Facebook Analytics)

The partners are required to participate to the dissemination on Facebook. It is necessary that each partner has an official account for interacting with RESISTO. The posts made at the RESISTO account will be shared by all the official partners' accounts (**annex 3**).

5.2.3. LinkedIn

User name: [@RESISTO project](https://www.linkedin.com/company/RESISTO-project)

Linkedin - brief (M24)	
Followers	n. 71
Post	n. 48
View	n. 1193

Table 5 - LinkedIn – brief (source: LinkedIn Analytics)

The partners are required to participate to the dissemination on LinkedIn. It is necessary that each partner has an official account for interacting with RESISTO. The posts made at the RESISTO account will be shared by all the official partners' accounts (**Annex 3**).

5.2.4. YouTube

User name: [RESISTO project](#)

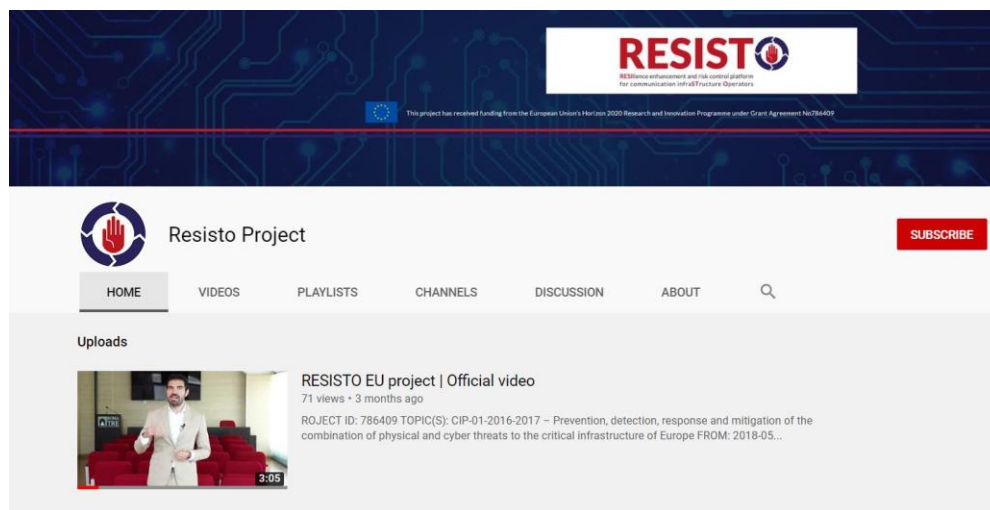


Figure 15 – RESISTO YouTube channel

The information content of the YouTube channel will be restricted to videos of events (mainly workshops and trainings) which would be of interest to target audience and the stakeholders.

6. PROJECT PRESENTATION AT EXTERNAL EVENTS

All partners will participate at external events relevant to the project in order to present the project and its results, increase the project visibility and establish new contacts.

6.1. Trade shows, exhibitions and clustering events

Consortium partners who will have a presence at international, national or regional events will represent the project. The dissemination will be performed by using the available templates and flyers\brochures.

During the second year, RESISTO was presented in the events reported in Table 6.

Authors/Presenters	Event name	Participant Number
Mirjam Fehling-Kaschek	European Safety and Reliability Conference, 22-26/09/2019, Hannover	500
Alberto Neri	14 th Meeting of the Community of Users on Secure, Safe, Resilient Societies, 16-19/09/2019, Brussels	100
Alberto Neri	Critical Infrastructure Protection & Resilience Europe (CIPRE), 16/10/2019, Milan	500
Maria Belesioti	Mediterranean Security Event, 29-31/10/2019, Greece	200
Arianna Magni, Marco Ferraro	MILIPOL, 19-22/11/2019, Paris	100
Federica Battisti, Sara Baldoni, Michele Brizzi	INTERNATIONAL SECURITY EXPO, 3-4/12/2019, London	10000
Stefano Panzieri, Fabio Cocurullo, Bruno Saccomanno, Agostino Longo	RESISTO project at Ufficio del Consigliere Militare del Presidente del Consiglio dei Ministri, 18/02/2020, Rome	50

Table 6 - List of talks presented in the first year of the project

Future venues considered for presentation include:

- the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (EU-LISA) associated events;
- relevant clustering events with research projects organised by: the European Commission and especially the Directorate-General of Migration and Home affairs (DG HOME); the Joint Research Center (JRC) Initiative (DG-JRC) of the European Commission and related units of European Security Agencies;
- IEEE Societies, Technical Committees and Working Groups or IEEE National Chapters that simultaneously are in charge or organise International Conferences or Journals, since members of the RESISTO consortium are relevant Chairs or Contributors;

- Authorities, Agencies and Bodies such as Authority for the Information and Communication Security and Privacy, working groups of Standardization bodies (i.e. ETSI etc) to enable also future exploitation aspects;
- EU's Research groups and initiatives such as AENEAS, ARTEMIS etc...

6.2. Conference

Dedicated conferences will be an excellent platform for disseminate our findings and start direct conversations with the audience.

Within the second year, the talk in Table 7 has been presented in international conferences. In this second year it is possible to notice a reduction to the number of conference since the consortium focused on other dissemination activities. We plan to increase this contribution in the third year.

Authors/Presenters	Talk Title	Conference Name	Participant Number
Mirjam Fehling-Kaschek	A Systematic Tabular Approach for Risk and Resilience Assessment and Improvement in the Telecommunication Industry	European Safety and Reliability Conference, 22-26/09/2019, Hannover	500

Table 7 - List of talks presented in the first year of the project in international conferences.

A partial list of upcoming conferences where partners plan to present the technical activities in the project is the following:

- IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC);
- International Conference on Information and Communication Technology Convergence (ICTC);
- IEEE Resilience Week (RWS);
- European Workshop on Visual Information Processing (EUVIP);
- International Conference on Protective Structures;
- Conference for Information Systems for Crisis Response and Management;
- Information systems for crisis response and management (ISCRAM);
- European Conference on Networks and Communications (EuCNC);
- International Conference on Artificial Intelligence Applications and Innovations (AIAI);
- InfoCom World;
- Romanian International Conference on Communications (IEEE Romania);
- International Conference on Pattern Recognition Application and Methods;
- IEEE World Congress on Computational Intelligence;
- European Signal Processing Conference;
- IEEE International Conference on Image Processing (ICIP);
- Annual Conference on Neural Information Processing Systems (NIPS);
- Annual Network and Distributed System Security Symposium (NDSS);
- IEEE Radar Conference (RadarCon);

- SPIE Defense + Security Conference, including SPIE Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security, Defense, and Law Enforcement;
- ICDSA - International Conference on Defense and Security Analysis.

6.2. Workshop

The first RESISTO Workshop was held in Valencia on May 2019 (host event: ISCRAM 2019) and had a significant and qualified participation



WORKSHOP/TUTORIAL:

“Physical and cyber threats: the new challenges for TLC Critical Infrastructures”

host event: **ISCRAM 2019** | 16th International Conference on
INFORMATION SYSTEMS FOR CRISIS RESPONSE AND
MANAGEMENT

“Towards individual-centric emergency management systems”

Workshops/Tutorials: May 19th, 2019 | **Conference:** May 19nd-22th, 2019

Venue: Valencia – Spain, Universitat Politècnica de València (UPV)

Figure 16 – First RESISTO Workshop

The Workshop will addressed the following topics:

- Protection of Telecommunication Infrastructures and Citizens
- Facing Cyber and Physical Threats: Technological & Operational aspects
- Modeling and analysis of disaster resilience
- Simulation modeling and analysis
- Challenges posed by 5G evolution

Here below the workshop agenda.



WORKSHOP/TUTORIAL:

"Physical and cyber threats: the new challenges for TLC Critical Infrastructures"

DATE: May 19th, 2019 | **VENUE:** Valencia – Spain Universitat Politècnica de València (UPV)

Time	Presenter	Title
9.45 – 10.00	Chairs	Welcome
10.00 – 10.30	A. Neri (Roma Tre University)	The problem of the protection of Telecommunication Infrastructures at a glance
10.30 - 11	F. Pascucci (Roma Tre University)	Technologies for cyber threats: an overview of the issues for the critical infrastructures
11.00 - 11.30	Coffee break	
11.30 - 12.15	R. Makri, I. Constantin, S. Bach	WG1: Technologies for physical threats WG2: Technologies for cyber threats WG3: Citizens in-the-loop: situation awareness and perception
12.15- 12.45	Moderator: M. Puggioni Panelists: R. Makri, I. Constantin, S. Bach	Round table
12.45 - 13.00	Closing	

Figure 17 – First RESISTO Workshop: agenda

6.3. Events participation: partner rules

Each time a consortium partner presents the project in an external event, it is important that he\she follows these simple and appropriate communication and dissemination actions:

- **pre-event:** share the info with T10.2 leader;
- **during the event:** take photos in which the RESISTO logo is visible (it is important to document the participation at the event). And if possible, send the photos to APRE (RESISTO social media manager) the day of the event. In this way we have the possibility to write a live post for the RESISTO social media;
- **post event:** if possible and if relevant for the communication, send a brief follow-up to T10.2 leader (e.g., report the important moments of the event, if any relevant meeting with stakeholders took place).

■ Partners contribution during the EVENTS: ACTIONS TO FOLLOW

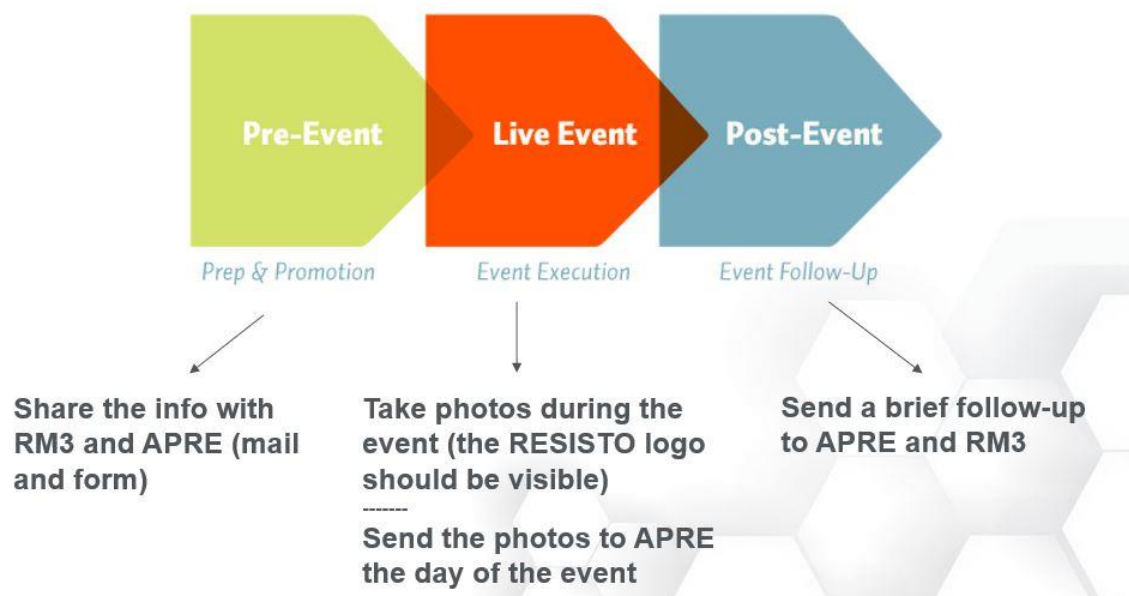


Figure 18 – Partners contribution during the EVENTS: scheme

7. PUBLICATIONS

7.1. Scientific Publications

Journal papers are an effective dissemination tool. The consortium partners will publish reports and scientific articles with specific target to open access journals. This will ensure the long lasting impact beyond project duration, particularly in relation to the academic world.

A preliminary list of journals is in the following:

- International Journal of Critical Infrastructure Protection, Elsevier;
- IEEE Access;
- IEEE Transactions on Information Forensics and Security;
- IEEE Transactions on Industrial Informatics;
- IEEE Systems Journal;
- IEEE Wireless Communications;
- IEEE Control Systems;
- Reliability Engineering and System Safety;
- Journal of Safety Research;
- IJBCRM, International Journal of Business Continuity and Risk Management, InderScience;
- Risk Analysis, Wiley;
- Artificial Intelligence;
- Information Fusion An International Journal on Multi-Sensor, Multi-Source Information Fusion;
- International Journal of Information Management;
- IEEE Transactions on Pattern Analysis and Machine Intelligence;
- Computers & Security;
- International Journal of Risk Assessment and Management;
- IEEE Systems;
- Journal on Signal Processing, Elsevier Science;
- IEEE Transactions on Microwave Theory and Techniques; IEEE Transactions on Communications.

7.2. Articles

In the second year two articles have been published on magazines targeting the stakeholders and the general public.

Title	Authors	Magazine
RESISTO: Resilience Enhancement and Risk Control Platform for Communication Infrastructure Operators (http://www.resistoproject.eu/wp-content/uploads/2020/05/Polaris_2020_N41_Aonzo_Neri.pdf)	E. Aonzo, A. Neri	POLARIS Innovation Journal. Edition: 41 – February 2020
TARGETING SECURITY: Integrating cyber and physical security to protect critical communication infrastructure (https://view.publitas.com/platinum-online/2020-marzo_ing/page/118-119)	A. Neri, B. Saccomanno	Platinum Edition: March 2020

Table 8 - List of articles published in magazines.

7.3. Other Publications

In this second year we participated to the preparation of a book entitled “Cyber-Physical Threat Intelligence for Critical Infrastructures Security” that will be published on line with open access by Now (<https://www.nowpublishers.com/>).

This book is the result of a tight cooperation with four other European Projects (FINSEC <https://www.finsec-project.eu>, SAFECARE <https://www.safecare-project.eu>, SPHINX <https://sphinx-project.eu>, and DEFENDER <https://defender-project.eu>).

Currently (M24) the final version of the chapters have been delivered and we are waiting for the publication on the publisher website and the delivery of the hardcopies.



Figure 19 - Preview of the book.

7.2. Publications section on the website

All publications are listed in a dedicated part of the website <http://www.resistoproject.eu/publications/> that summarizes all contributions in terms of Newsletters, Articles, Relevant Presentations and Scientific Publications.

8. NETWORKING: EU CLUSTER FOR SECURING CRITICAL INFRASTRUCTURES

Since November 2019 RESISTO is part of **ECSCI** (European Cluster for Securing Critical Infrastructures).

The cluster aims at promoting the interaction among European projects addressing the topic of security of critical infrastructures. It is composed of 9 partners beside RESISTO:

- FINSEC <https://www.finsec-project.eu>
- SAFECARE <https://www.safecare-project.eu>
- SPHINX <https://sphinx-project.eu>
- DEFENDER <https://defender-project.eu>
- ANASTACIA <http://www.anastacia-h2020.eu/>
- INFRA STRESS <https://www.infrastress.eu/>
- STOP-IT <https://stop-it-project.eu/>
- SATIE <http://satie-h2020.eu/>
- SecureGas <https://www.securegas-project.eu/>

The main activities within the cluster have been the organization of:

- the First ECSCI Workshop originally planned to be held at DG Home premises in Bruxelles from March, 26 to March, 27. Due to the spread of COVID-19 the workshop has first be postponed to May and then moved to a completely virtual event whose dates need to be settled;
- the 1st International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (<https://sites.google.com/fbk.eu/cps4cip20>) co-located with ESORICS 2020 that will take place in September 18-20, 2020.

9. SUMMARY OF RESISTO KPIs

Key Performance Indicators (KPI) or Key Success Indicators (KSI), are set as performance measurement to define and measure progress toward the set goals along with its impact to the targeted audiences. Initial means for verification of the success of the dissemination activities are presented in the following and will be further elaborated in the next version of this Deliverable.

The following table shows the achieved results in comparison with the overall KPIs, related to the Communication and dissemination activities.

	Targets	Metrics (Goals)	RESISTO results [M24]
Project website	Everyone	#website = 1 # visitors > 100/month	#website = 1 #visitors > 126/month
Social media	Exploitation partners, research community, end user	# channels > 3 # posts > 10/month # conversations > 3/month	# channels = 4 (fb,tw,linkd,youtube) # posts > 10/month # conversations > 2/month
Newsletter	Everyone	#newsletter = 4	#newsletter = 2
Project Video	Everyone	#video > 1	#video = 1
Articles or press release	-	#articles > 4	#articles = 2
Scientific publications	Research community, exploitation partners	# scientific pub > 15	# scientific pub = 8
Conferences /events	Research community, end users, exploitation partners.	# conf/events > 15 #Audience > 1,000	# conf/events =22 #Audience > 1,000
Workshop	End-Users, Industry, Researchers, European Commission Staff, Key Influencers, EU and national politicians and international experts in the field of CI protection and communication security, ECSO members	#workshop > 2	#workshop = 1 (ISCRAM 2019 1st Workshop 19/05/2019 @Valencia) (the second workshop was planned at M23 but it was postponed to M25 due to the CORONA virus outbreak)

Table 9 - KPIs related to the Communication and dissemination activities

10. EXECUTION OF DISSEMINATION STRATEGY

The key to the effective dissemination of project results is to communicate important achievements in the right time and to the right stakeholders. Thus, as denoted in Section 2, the dissemination and communication activities will follow a time plan compliant to the main project phases:

- The initial project phase incorporating Definition of user and architecture requirements will be accompanied by an initial awareness creation phase (year 1) towards dissemination and communication actions, during which the concept and project objectives will be communicated to a wide range of stakeholders;
- The project development and integration phase will be accompanied by a focused market and stakeholders attraction phase (year 2), during which early outcomes will be published and communicated;
- The piloting implementation phase will be accompanied by a more aggressive strategic dissemination phase (year 3), during which pilot trials with end users will be held to boost stakeholders and market penetration and to pave the way for the commercial exploitation after the end of the project.

There are 7 deliverables foreseen in the workplan which are associated with the dissemination strategy, as listed in **Errore. L'origine riferimento non è stata trovata.** that will materialize the above-mentioned dissemination and communication actions timeplan.

Deliverable	Due date	Responsible partner
D10.1 Communication material - first	4	RM3
D10.2 Communication material - final	36	RM3
D10.3 Project Web Site	2	RM3
D10.6 Dissemination and Communication Activities - first	2	RM3
D10.7 Dissemination and Communication Activities - second	12	RM3
D10.8 Dissemination and Communication Activities – third	24	RM3
D10.9 Dissemination and Communication Activities - final	36	RM3

Table 10 - List of deliverables related to the dissemination.

11. RELEVANT STANDARDS, GAP ANALYSIS AND RESISTO COMPLIANCE

11.1 Standards in RESISTO

The following Table 1 provides an overview of all relevant standards from the perspective of the RESISTO project.

In relation to the level of relevance to RESISTO, three cases are considered:

1. Standards or specifications that are mentioned, or referenced, in RESISTO deliverables
2. Standards or specifications that are used by specific components of the RESISTO architecture
3. Standards or specifications that are candidate to be enhanced by RESISTO.

The cases where 2 or 3 apply are analyzed afterwards.

SDO	Title	Type					Referenced by RESISTO	To be used by RESISTO	To be enhanced by RESISTO
		Security	Risk mngt	Comm	Critical Infra	Other			
CSA	Cloud Security Alliance, Cloud Controls Matrix v.3.0	x					D5.1		
	Cloud Security Alliance, Top Threats to Cloud Computing: Deep Dive	x					D5.1, D6.1		
ETSI	Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes - ETSI TR 133 926 V14.0.0	x					D5.1		
	SOL005 NFV Release 2; Protocols and Data Models; RESTful protocols specification for the Os-Ma-nfvo Reference Point			x			D6.1	Orchestration controller (?)	
	ETSI OSM			x			D6.1	Orchestration controller (?)	
CESNET-CERTS	IDEA - https://idea.cesnet.cz/en/index	x					D6.1	x	
IETF Trust	IDMF Format details: RFC 4765 - https://tools.ietf.org/html/rfc4765 ; Details of the XML data model and associated DTD: RFC 4766 - https://tools.ietf.org/html/rfc4766 ; Recommended transport protocol (IDXP) RFC 4767 - https://tools.ietf.org/html/rfc4767	x					D6.1		
ISO	ISO 1989 Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture			x			D2.3		
	ISO 31000 Risk management - Principles and guidelines		x				D3.1		
	ISO/IEC 27000, 27001 and 27002 for information security management	x					D3.3		
	Message Queuing Telemetry Transport (MQTT) v3.1.1 - (ISO/IEC PRF 20922:2916 Information technology)			x			D6.1		

ITU	ITU-T Recommendation E.408: Telecommunication Networks Security Requirements.	x		x			D2.2, D4.1		
	ITU-T Recommendation X.1205: Overview of Cybersecurity	x		x			D2.2		
	ITU-T Recommendation X.800: Security Architecture for Open Systems Interconnection for CCITT Applications	x		x			D2.2, D3.1, D4.1		
	ITU-T Recommendation X.1205: Overview of Cybersecurity	x		x			D2.3		
NCCIC	National Cybersecurity and Communications Integration Center, 2014 DDoS Quick Guide, https://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf	x					D4.1		
NIST	Guide for Developing Performance Metrics for Information Security. NIST Special Publication	x					D3.7		
	Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 NIST				x		D5.1		
OASIS	Structured Threat Information Expression (STIX), https://oasis-open.github.io/cti-documentation	x					D2.2, D2.3, D6.1		
OMG	Business Process Model and Notation 2.0.2 https://www.omg.org/spec/BPMN/					x	D6.1	x	
ONF	SDN/OpenFlow			x			D6.1		

Table 11 - Overview of relevant standards.

11.2 Standards to be used by RESISTO

In this section, the standards to be used by RESISTO are briefly analyzed in relation to the relevant architecture component, including the relevance to RESISTO, the level of compliance expected to be accomplished by RESISTO and the identification of possible gaps, if any.

BPMN 2.0 (ACTIVITI)

Short description of the standard/draft	The Object Management Group (OMG) has developed a standard Business Process Model and Notation (BPMN). The primary goal of BPMN is to provide a notation that is readily understandable by all business users, from the business analysts that create the initial drafts of the processes, to the technical developers responsible for implementing the technology that will perform those processes, and finally, to the business people who will manage and monitor those processes. Thus, BPMN creates a standardized bridge for the gap between the business process design and process implementation. Another goal, but no less important, is to ensure that XML languages designed for the execution of business processes, such as WSBPEL (Web Services Business Process Execution Language), can be visualized with a business-oriented notation.
Link to standard/draft (if available)	https://www.omg.org/spec/BPMN/2.0.2/PDF
Relevant RESISTO component	Workflow Engine
Relevance to RESISTO	Workflow execution is carried out via Activiti, an open-source workflow engine written in Java that can execute business processes described in standard BPMN (Business Process Model and Notation) 2.0. The Workflow engine is an extremely effective tool for managing critical infrastructure security. It is a Business Process Model (BPM) engine for the configuration and execution of automatic or semi-automatic processes, consisting of sequences of actions and reactions, which can be triggered by a defined event. Given a certain alarm/event, it permits selecting and executing the most appropriate workflow, i.e. a conditional sequence of tasks.
Compliance of RESISTO	
Potential gaps	

CESNET IDEA

Short description of the standard/draft	The draft describes a data model to represent information exported by intrusion detection systems and explains the rationale for using this model. It is an Experimental Protocol for the Internet community. Discussion and suggestions for improvement are requested. The IESG has chosen to publish this document in order to document the work as it was when the working group concluded and to encourage experimentation and development of the technology. Readers of the RFC should exercise caution in evaluating its value for implementation and deployment.
Link to standard/draft (if available)	https://www.ietf.org/rfc/rfc4765.txt
Relevant RESISTO component	Workflow Manager

Relevance to RESISTO	In the RESISTO project the choice is to adopt the IDEA standard as a message exchange format. The reason for choosing the IDEA standard is mainly due to the following considerations: <ul style="list-style-type: none"> • simple data structure not too verbose or complex, • data model based on the JSON standard • easily extendable data schema to manage different types of events • incident classifications based on eCSIRT.net taxonomy.
Compliance of RESISTO	
Potential gaps	

ETSI NFV SOL005 / NFV IFA013

Short description of the standard/draft	ETSI SOL005 and IFA013 address the reference point between OSS/BSS and the management block of NFV (MANO). Although SOL005 and IFA013 are different specifications, they can be seen as different parts of the same standard, which defines the communication between an NFV Orchestrator and the OSS/BSS above. Essentially, IFA013 (stage 2) provides the information model and specifies requirements, whereas SOL005 (stage 3) specifies RESTful protocol and data models to fulfil those requirements.
Link to standard/draft (if available)	https://www.etsi.org/deliver/etsi_gs/NFV-SOL/001_099/005/02.04.01_60/gs_NFV-SOL005v020401p.pdf https://www.etsi.org/deliver/etsi_gs/NFV-IFA/001_099/013/02.01.01_60/gs_NFV-IFA013v020101p.pdf
Relevant RESISTO component	Orchestration Controller
Relevance to RESISTO	In a NFV-based environment (e.g. 5G), network management operations are done through this interface, including: <ul style="list-style-type: none"> • network service lifecycle management (e.g. instantiation, query, update, scaling, termination) of network services; • policy management of network services; • querying network service and VNF instances, forwarding events, usage, and performance of network service instances. From the NFV MANO perspective, the RESISTO orchestration controller will play the role of OSS/BSS, therefore this will likely be an interface to be supported by RESISTO, at least for NFV-based network infrastructures.
Compliance of RESISTO	Under evaluation.
Potential gaps	Under evaluation.

OASIS MTT

Short description of the standard/draft	MQTT is a Client Server publish/subscribe messaging transport protocol. It is light weight, open, simple, and designed to make communications implementation easy. These characteristics make it ideal for use in many situations, including constrained environments such as for communication in Machine to Machine (M2M) and Internet of Things (IoT) contexts where a small code footprint is required and/or network bandwidth is at a premium.
-----------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Link to standard/draft (if available)	https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html
Relevant RESISTO component	Message Broker
Relevance to RESISTO	Since the RESISTO platform must be interconnected with IoT sensors characterized by devices with poor hardware resources, it was decided to make use of MQTT technology either by directly using the appropriate connectors or through an MQTT proxy to be integrated it into the Kafka message broker protocol.
Compliance of RESISTO	
Potential gaps	

11.3 Other relevant documents

- European Directive 2009/140/EC (“amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services”) - <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF>
- European Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union - <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016L1148>)

11. CONCLUSION

The Dissemination plan is the guideline for the dissemination of the project and of its results. This plan presents dissemination tools for particular targeted audience and draft and is a living document.

The content presented in this Deliverable represents the outcomes of the second year, in which the system architecture has been consolidated together with all interfaces among modules and the selection of the use case scenarios.

All issues set herein will be continually monitored, updated and reported during the project.

12. REFERENCES

INDEX	REFERENCE
[1]	RESISTO – Grant Agreement. Project Starting Date : May, 1 st 2018
[2]	D10.1 Communication material - first
[3]	D10.3 Project Website
[4]	D10.6 Dissemination and Communication Activities - first
[5]	D10.7 Dissemination and Communication Activities - second

ANNEX 1: RESISTO INTEGRATED PLAN

[M1-12]

	May 2018 M01	June 2018 M02	July 2018 M03	August 2018 M04	September 2018 M05	October 2018 M06	November 2018 M07	December 2018 M08	January 2019 M09	February 2019 M10	March 2019 M11	apr-19 M12
DISS & COMM Topics	• RESISTO project (context, needs, general solution) • RESISTO Architecture • Resilience Assessment	• RESISTO project (context, needs, general solution) • RESISTO Architecture • Resilience Assessment	• RESISTO project (context, needs, general solution) • RESISTO Architecture • Resilience Assessment	• RESISTO project (context, needs, general solution) • RESISTO Architecture • Resilience Assessment	• RESISTO project (context, needs, general solution) • RESISTO Architecture • Resilience Assessment	• RESISTO project (context, needs, general solution) • RESISTO Architecture • Resilience Assessment	• RESISTO project (context, needs, general solution) • RESISTO Architecture • Resilience Assessment	• RESISTO project (context, needs, general solution) • RESISTO Architecture • Resilience Assessment	• RESISTO project (context, needs, general solution) • RESISTO Architecture • Resilience Assessment	• RESISTO project (context, needs, general solution) • RESISTO Architecture • Resilience Assessment	• RESISTO project (context, needs, general solution) • RESISTO Architecture • Resilience Assessment	• RESISTO project (context, needs, general solution) • RESISTO Architecture • Resilience Assessment
PROJECT MEETING (Progress meeting)	KoM [14-15/05/2018] @ Rome	01 PMT1 [22/06/2018] (telco)				02 PMT2 [05/10/2018] (telco)	03 PMT3 [22/11/2018] @ Rome			04 TECH [18-20/02/2019] @ Athens		05 PMT4 [11/04/2019] (telco)
REVIEW MEETING (EU review)												
AB MEETING (Supervision)												
RESISTO WORKSHOP												
MAIN DISSEMINATION EVENT (with booth)												
DISSEMINATION EVENT (partners invited to talk about the project)					Orange Educational Program [13/09/2018] @Bucharest Balkan Cryptsec 2018 [20-21/09/2018] @Romania Orange Group European Security Seminar [24/09/2018] @Moldova	Internet and Mobile World 2018 [4/10/2018] @Bucharest/ROMEKPO 2nd International Workshop on Resilience [31/10/2018] @Chengdu ATENA H2020 WORKSHOP [18/10/2018] @Luxembourg	Nicosia Risk Forum 2018 [14/11/2018] @Cyprus DefCamp 2018 [8-9/11/2018] @Bucharest	INQUIMUS 2018 [04/12/2018] @Venice				
Web Event												
NEWSLETTER												
OPEN ACCESS BOOK												
PROJECT VIDEO												

[M13-24]

	May 2019 M13	June 2019 M14	July 2019 M15	August 2019 M16	September 2019 M17	October 2019 M18	November 2019 M19	December 2019 M20	January 2020 M21	February 2020 M22	March 2020 M23	apr-20 M24
DISS & COMM Topics	• RESISTO project (context, needs, general solution) • RESISTO Architecture • Resilience Assessment	• RESISTO project (context, needs, general solution) • RESISTO Architecture • Resilience Assessment	• RESISTO project (context, needs, general solution) • RESISTO Architecture • Resilience Assessment	• RESISTO project (context, needs, general solution) • RESISTO Architecture • Resilience Assessment	• RESISTO project (context, needs, general solution) • RESISTO Architecture • Resilience Assessment	• RESISTO project (context, needs, general solution) • RESISTO Architecture • Resilience Assessment	• RESISTO project (context, needs, general solution) • RESISTO Architecture • Resilience Assessment • Rts (Resilience indicators) quantification • Anomaly detection with active and passive sensors	• RESISTO project (context, needs, general solution) • RESISTO Architecture • Resilience Assessment • Rts (Resilience indicators) quantification • Anomaly detection with active and passive sensors	• RESISTO project (context, needs, general solution) • RESISTO Architecture • Resilience Assessment • Rts (Resilience indicators) quantification • Anomaly detection with active and passive sensors	• RESISTO project (context, needs, general solution) • RESISTO Architecture • Resilience Assessment • Rts (Resilience indicators) quantification • Anomaly detection with active and passive sensors	• RESISTO project (context, needs, general solution) • RESISTO Architecture • Resilience Assessment • Rts (Resilience indicators) quantification • Anomaly detection with active and passive sensors	• RESISTO project (context, needs, general solution) • RESISTO Architecture • Resilience Assessment • Rts (Resilience indicators) quantification • Anomaly detection with active and passive sensors
PROJECT MEETING (Progress meeting)		06 PMT5 [18/06/2019] @Brussels	07 TECH [16-17/07/2019] @Austria			08 PMT6 [02/10/2019] @Pagan	09 TECH [09/10/2019] @Pagan	10 TECH [09-04/12/2019] @Sofia		11 PMT7 [01/02/2020] (telco)	12 TECH [17-18/03/2020] (telco)	
REVIEW MEETING (EU review)		1st Review [19/06/2019] @Brussels				AB meeting [02/10/2019] @Pagan						
AB MEETING (Supervision)												
RESISTO WORKSHOP	SCRAM 2019 1st Workshop [19/06/2019] @Valencia											
MAIN DISSEMINATION EVENT (with booth)												
DISSEMINATION EVENT (partners invited to talk about the project)					ESREL 2019 [22/09/2019] @Hanover 14TH MEETING OF THE COT [17/09/2019] @Brussels	Critical Infrastructure Protection & Resilience Europe (CIPRE) [16/10/2019] @Milan Mediterranean Security Event 2019 [28-31/10/2019] @Greece	MILIPOL 2019 [18-23/11/2019] @Paris	INTERNATIONAL SECURITY EXPO 2019 [13-14/12/2019] @London			EC3 workshop [26-27 March 2020] @Brussels [EVENT CANCELLED]	
Web Event												
NEWSLETTER								Newsletter N.1 December 2019				Newsletter N.2 April 2020
OPEN ACCESS BOOK									1st issue OPEN ACCESS BOOK			1st issue OPEN ACCESS BOOK (printed and shared)
PROJECT VIDEO			1st RESISTO project video									

[M25-36]

	May 2020 M25	June 2020 M26	July 2020 M27	August 2020 M28	September 2020 M29	October 2020 M30	November 2020 M31	December 2020 M32	January 2021 M33	February 2021 M34	March 2021 M35	apr-21 M36
DISS & COMM Topics	• Critical Infrastructure Modeling • Cascade effects prediction • Workflows for an effective Decision Making Support • SDI (Software Defined Security) • 5G Orchestrator	• Critical Infrastructure Modeling • Cascade effects prediction • Workflows for an effective Decision Making Support • SDI (Software Defined Security) • 5G Orchestrator	• Critical Infrastructure Modeling • Cascade effects prediction • Workflows for an effective Decision Making Support • SDI (Software Defined Security) • 5G Orchestrator	• TBD (eg. Validation, Benefits for the end user)	• TBD (eg. Validation, Benefits for the end user)	• TBD (eg. Validation, Benefits for the end user)	• TBD (eg. Validation, Benefits for the end user)	• TBD (eg. Validation, Benefits for the end user)	• TBD (eg. Validation, Benefits for the end user)	• TBD (eg. Validation, Benefits for the end user)	• TBD (eg. Validation, Benefits for the end user)	• TBD (eg. Validation, Benefits for the end user)
PROJECT MEETING (Progress meeting)												
REVIEW MEETING (EU review)		2nd Review [25/06/2020] @Online										
AB MEETING (Supervision)												
RESISTO WORKSHOP		EC3 workshop [17-18 June 2020] @Online [suggested dates]			ESORICS OPS4OP 2020 Workshop [14-18/09/2020] @Gulfport, United Kingdom	RESISTO Workshop (October 2020) [tbd]						
MAIN DISSEMINATION EVENT (with booth)							Security Research Event 2020 [24-26/11/2020] @Bonn, Germany					
DISSEMINATION EVENT (partners invited to talk about the project)	EGU 2020 General Assembly "Sharing Geoscience Online" [10/05/2020] @Online											RESISTO Final Conference [April 2021] [tbd]
Web Event												
NEWSLETTER						Newsletter N.3					Newsletter N.4	
OPEN ACCESS BOOK												
PROJECT VIDEO			2nd RESISTO project video									

ANNEX 2: DISS AND COMM POCs CONTACTS LIST

Contractor Short	Contractor	Email
LDO	LEONARDO - SOCIETA PER AZIONI	paolo.dimichele@leonardocompany.com
RM3	UNIVERSITA DEGLI STUDI ROMA TRE	federica.battisti@uniroma3.it
TIM	TELECOM ITALIA SPA	marco.mancini@telecomitalia.it; luca.lionetti@telecomitalia.it
OTE	HELLENIC TELECOMMUNICATIONS ORGANIZATION S.A. - OTE AE (ORGANISMOS TILEPIKOINONION TIS ELLADOS OTE AE)	mbelesioti@oteresearch.gr
BTC	BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY	zhan.cui@bt.com
ORO	ORANGE ROMANIA SA	cristian.patachia@orange.com
RTV	RETEVISION I SA	francisco.marcos@cellnexttelecom.com
ALB	ALTICE LABS SA	jorgec@alticelabs.com
TEI	ERICSSON TELECOMUNICAZIONI	cosimo.zotti@ericsson.com
Fraunhofer	FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V.	Mirjam.Fehling- Kaschek@emi.fraunhofer.de
ICCS	INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS	rodia@esd.ece.ntua.gr
BUW	BERGISCHE UNIVERSITAET WUPPERTAL	sbach@uni-wuppertal.de
INT	INTEGRASYS SA	jose.sanchez@integrasys-sa.com
GT	GUARDTIME AS	liis.livin@guardtime.com
ADI	ADITESS ADVANCED INTEGRATED TECHNOLOGY SOLUTIONS; SERVICES LTD	rb@aditess.com
BSS	BIT SENTINEL SECURITY SRL	andrei@bit-sentinel.com
TP-APRE	TP - APRE	magni@apre.it; ferraro@apre.it

ANNEX 3: LIST OF THE PARTNERS' SOCIAL MEDIA ACCOUNTS

Organisation name	Institutional Twitter account	Institutional Facebook account	Institutional LinkedIn account
ADITESS LTD	https://twitter.com/aditeesscy	https://www.youtube.com/channel/UCb4ooXc5-KCFOr19INakzjw	https://www.linkedin.com/company/aditeess/
BIT SENTINEL	\	https://www.facebook.com/bitsentinel/	https://www.linkedin.com/company/bit-sentinel/
GUARDTIME	@Guardtime, https://twitter.com/Guardtime	Guardtime, @Guardtime, https://www.facebook.com/Guardtime/	Guardtime, @Guardtime, https://www.linkedin.com/company/guardtime/
Altice Labs, S.A.	https://twitter.com/PTin	https://www.facebook.com/alticelabsofficial/	https://www.linkedin.com/company/altice-labs/
TIM S.p.A.	https://twitter.com/TIM_Official	https://www.facebook.com/TimOfficialPage/	https://www.linkedin.com/company/timbusiness/
University of Wuppertal	@Uni_Wuppertal	@uni.wuppertal	https://www.linkedin.com/company/50613
Leonardo	https://twitter.com/Leonardo_live	\	https://www.linkedin.com/company/leonardo_company
RETEVISION (cellnex Telecom)	https://twitter.com/cellnextelecom	\	https://www.linkedin.com/company/cellnex-telecom/
Fraunhofer	\		https://www.linkedin.com/company/fraunhofer-institute-for-high-speed-dynamics-ernst-mach-institut-emi
APRE	@APRE_it	@APRE.it	APRE - Agenzia per la Promozione della Ricerca Europea
Department of Engineering, Roma Tre University	@IngegneriaR3	@IngegneriaR3	\
Integrasys	@IntegrasysSA	\	https://www.linkedin.com/company/integrasys-s-a/
ICCS	\	\	ICCS - ΕΠΙΣΕΥ (https://www.linkedin.com/company/iccs-episey-ntua/)
OTE - HELLENIC TELECOMMUNICATIONS ORGANIZATION S.A.	\	\	\

Organisation name	Institutional Twitter account	Institutional Facebook account	Institutional LinkedIn account
BTC - BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY	@bt_uk	BTUK	https://www.linkedin.com/company/bt/?originalSubdomain=it
ORANGE ROMANIA SA	@orangeromania	@orange	\
ERICSSON	@ericsson	@Ericsson	https://www.linkedin.com/company/ericsson/