

RESISTO:

D10.7_ DISSEMINATION AND COMMUNICATION ACTIVITIES – SECOND



RESISTO

D10.7 – DISSEMINATION AND COMMUNICATION ACTIVITIES – SECOND

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_D10.7_190527_02	Version:	2.0
Deliverable:	D10.7	Date:	29/05/2019
		Status:	APPROVED

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

Approval Status	
Prepared by:	Federica BATTISTI (RM3)
Approved by: (WP Leader)	Bruno SACCOMANNO (LDO)
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
Marco Ferrero	APRE	Contributor
Maria Belesioti	OTE	Contributor
Silvia Bach	BUW	Contributor
Andrei Avădănei	BSS	Contributor
Marco Carli	RM3	Reviewer
Bruno Saccomanno	LDO	Reviewer

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
1.0	30/04/2019	All	All	First draft ready
1.1	23/05/2019	All	All	Revision and inclusion of the website statistics
1.2	27/05/2019	All	All	Update
1.3	28/05/2019	Annexes	All	Inclusion of the Annex
2.0	29/05/2019	All	All	Final release

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 – Genova (GE) – 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 second release of the dissemination plan to present the dissemination activities carried out during the first 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

1.	INTRODUCTION.....	9
2.	COMMUNICATION AND DISSEMINATION STRATEGY	9
3.	DISSEMINATION AND COMMUNICATION TOOLS.....	12
4	SUMMARY OF COMMUNICATION CHANNELS.....	21
5	EXECUTION OF DISSEMINATION STRATEGY.....	23
6	CONCLUSION	25
7	REFERENCES.....	26
8	ANNEXES	27

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 first release D10.6 Dissemination and communication activities – First.

The first year of the project has mainly addressed the update and consolidation of the system architecture, the definition of the system requirements, and the identification of the key performance indicators.

For this reason, the performed dissemination activities are mainly related to the overall approach developed within RESISTO and the analysis of cyber and physical threats to the telecommunication infrastructure.

As announced in 10.6, in D10.7 all activities foreseen and accomplished during the first project year are mapped and individual dissemination and communication actions per partner listed.

More specifically, Sections 3 to 5 have been updated with respect to 10.6.

2. COMMUNICATION AND DISSEMINATION STRATEGY

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 Initial identification of 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, at this preliminary stage:

1. 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.
2. 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.
3. 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 Organizations (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 organized by the EC, Experts working Groups, Critical Infrastructures Initiatives or Security Organizations.

3. DISSEMINATION AND COMMUNICATION TOOLS

In the following, the actions carried out during the first year of the project along with representative foreseen activities for the first project year are presented. These actions will be further specified and elaborated in the next version of this Deliverable, which will also elaborate the RESISTO vision for a more effective and appealing dissemination and communication strategy.

3.1 Project image

3.1.1 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.



Figure 1 - RESISTO logo

3.2 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);

Additional templates will be added as required.

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

3.3 Website

The project website allows the communication with the general public as well as communication among the consortium partners. The project website <http://www.resistoproject.eu/> 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, news broadcast channel for all public information. The website contains a dedicated space for all public documents and dissemination material produced as a part of the RESISTO project (e.g. press releases, project brochure, newsletter, conference and journal publications).

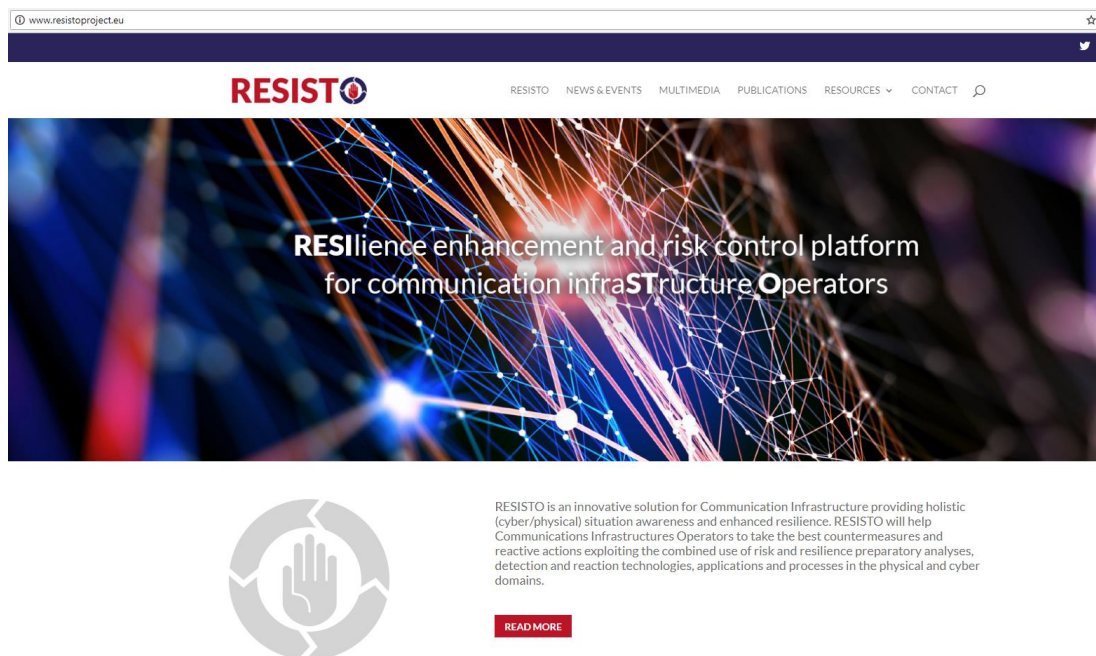


Figure 2 - RESISTO website.

3.4 Deliverables

The public RESISTO deliverables are listed on the website and are be available for download upon request. This allows the interested audience to follow the project development.

3.5 Brochure/ Poster/ Roll-up

In order to reach the wider audience as possible, different dissemination materials has been produced. Dissemination materials include RESISTO logo, a brief description of the project and of its structure, and the list of partners.

The produced dissemination material is published on the website and is available for download at <http://www.resistoproject.eu/communication-materials>. They will be also distributed at the events attended by the partners in order to increase the visibility of the project and extend our network and contacts.

Moreover, a roll-up has been printed to be used in the dissemination activities.

“

The main ambition of the RESISTO consortium is to develop the necessary concepts and a solid technological baseline to create a comprehensive solution that allows faster detection of new cyber/physical threats, better informed decision making and achievement of a joint understanding of cascading effects within the CI across interconnected CIs providing enhanced resilience of Communication Infrastructure and CIs that rely on it. RESISTO will concretely support progress beyond the State of The Art in Communication CI protection and the EU strategy on Cybersecurity.

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 ECSO.

RESISTO PARTNERS

LEONARDO, ROMA TRE, TIM, OTE, BT, orange, retevisión, altice, ERICSSON, Fraunhofer, iscom, INTEGRASYS, guardtime, adfess, treelogic, SENTINEL, APRE

(RM3 third party) is responsible of Dissemination, Communication and awareness raising activities

COORDINATOR

Federico Frosali
LEONARDO - SOCIETÀ PER AZIONI
federico.frosali@leonardocompany.com

www.resistoproject.eu

www.resistoproject.eu

THE RESISTO PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO. 786409.

Figure 3 - RESISTO brochure, outer part.





**RESilience enhancement and risk control platform
for communication infraSTructure OPerators**

WHAT IS RESISTO PROJECT?

RESISTO is an innovative solution for Communication Infrastructure 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.

WHAT ARE THE OBJECTIVES OF THE RESISTO PROJECT?

RESISTO will:

- 1 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.
- 2 Develop an Integrated Risk and Resilience analysis and management tool, that takes account of cyber and/or physical threats and disruptions jointly at the level of telecommunication service functions and performance functions.
- 3 Provide, experiment and assess a suite of innovative cyber/physical security solutions for prevention, protection, detection and reaction that can deliver unprecedented cost-effective performances in a holistic technology framework.
- 4 Support a progressive adoption path for the RESISTO platform and services through extensive validation in relevant use cases for Communication Infrastructure protection (TRL 7) directly involving relevant Communication CI operators, arising awareness and promoting a joint approach to resilience.
- 5 Contribute to the European Programme for Critical Infrastructure Protection and to the objectives of the Cybersecurity Strategy of the European Union.

WHY RESISTO PROJECT?

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.

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, LPWAN)
- New Technology for detection/protection/response (blockchain, drones, machine learning algorithms, software defined security)
- Cyber Intelligence

Figure 4 - RESISTO brochure, inner part.



Figure 5 - RESISTO poster.

3.6 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.

3.6.1 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 first year, RESISTO was presented in the events reported in Table 1.

Authors/Presenters	Talk Title	Conference Name	Participant Number
I. Constantin	Anatomy of A Cyber-Attack	Orange Educational Program, 2 October 2018	50
C. Patachia	Using Big Data Analytics to enhance cyber security Resilience	Internet and Mobile World, 3-4 October 2018	150
L. Enescu	Orange Romania- 2018 Security initiatives and achievements	Orange Group European Security Seminar, 15 October 2018	50
S. Panzieri	The H2020 RESISTO project (RESilience enhancement and risk control platform for communication infraSTructure Operators)	ATENA H2020 WORKSHOP: A new cybersecurity for interdependent Critical Infrastructures, 24 October 2018	40
M. Skitsas	RESISTO - RESilience enhancement and risk control platform for communication infraSTructure Operators	Nicosia Risk Forum, 14 November 2018	20
A. Neri	The RESISTO project and its architecture	The 5G network: criticalities and perspectives, 14 March, 2019	100
S. Bach	RESISTO: Risk and Resilience Assessment	Joint final conference of the H2020 projects SmartResilience and SAYSO, 15-17 April, 2019	100

Table 1 - 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 organized 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 organize 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.

3.6.2 Conferences

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

Within the first year, the talks in Table 2 have been presented in international conferences.

Authors/Presenters	Talk Title	Conference Name	Participant Number
M. Belesioti, I.P. Chochliouros, F. Frosali and R. Makri	Enhancing Critical Infrastructure Protection: The RESISTO Concept	Special Session of the European Conference on Networks and Communications, 18-21 June 2018, Ljubljana, Slovenia	50
I. Constantin	Needles and Haystacks: Using Machine Learning and Threat Intelligence to detect, prevent & mitigate advanced cyber-physical threats to the communications critical infrastructure of Europe	Balkan Cryptsec, 20-21 September 2018	200
C. Patachia	Public-Private Partnerships in research: an overview of ongoing research activities (Horizon 2020) in areas such as: Smart City, 5G, IoT, Connected Mobility, Factories of the Future, Cyber Security	Balkan Cryptsec, 20-21 September 2018	200
I. Häring	Technical approach to resilience for sustainable infrastructure systems	2-nd International Workshop on Resilience, 2-nd IRW, 31 October- 2 November 2018	50-100
I. Constantin	A holistic approach to resilience enhancement for C.I. operators	DefCamp - International Hacking and Information Security Conference, 8-9 November, 2018	30
C. Patachia	Connect & Inspire	DefCamp - International Hacking and Information Security Conference, 8-9 November, 2018	500
S. Bach, M. Carli	RESISTO: Risk and Resilience Assessment	INQUIMUS, 3-5 December 2018	50
M. Belesioti, I. Chochliouros	Perspectives for Enhancing Critical Infrastructure Protection within the Context of the RESISTO EU-funded Project"	Infocom World 2018 21 November 2018, Athens, Greece	80-100

Table 2 - 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.

3.7 Publications

3.7.1 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.

3.7.2 Other publications

Apart from peer review scientific papers we will also publish in industry magazines and newsletters, such as:

- Cyprus Safety & Health Association;
- Orange Business Internet Security Cyber Threat Report, H1 2018 (bi-annual report on current trends and threats discovered in ORO's MSS infrastructure. The data in this report is gathered from multiple network security appliances, end-points and servers and ingested, correlated and presented by a custom-built Events Log Management system. This report provides actionable intel for its consumers in order to better understand the current threat landscape and the steps needed to protect one's information, brand and reputation);
- Horizon, the EU Research & Innovation Magazine;
- IEEE Computational intelligence Magazine.

3.8 Social media and blogs

The project will activate social channels in order to promote the finding of the project and promote the creation of collaboration among the partners and the interested audience.

Social media are a very dynamic environment and one of the most popular and fastest ways to promote the project and enhance its visibility; we plan to create LinkedIn, Facebook, and Twitter accounts that are the most effective media for reaching a wider audience. Policy papers, newsletter, the project video along with media communication and press releases will be also pursued.

4 SUMMARY OF COMMUNICATION CHANNELS

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, second version of this Deliverable. Google Analytics, Hootsuite and LinkedIn statistics will be also used to provide relevant statistics.

Table 3 summarizes communication channels and key performance indicators, which are relevant for the consortium partners with respect to the targeted audience.

Channel	Targets	Metrics
Project website	Everyone	# visitors > 100/month
Social media	Exploitation partners, research community, end user	# posts > 10/month # conversations > 3/month
Scientific publications	Research community, exploitation partners	# papers > 20 # citations
Other publications	End users, exploitation partners	# articles > 16 # Audience > 100,000
Conferences	Research community, end users, exploitation partners.	# presentations > 15 Audience > 1,000

Table 3 - Summary of communication channels.

Currently, the most exploited media is the website as reported by the statistics in Figure 6.

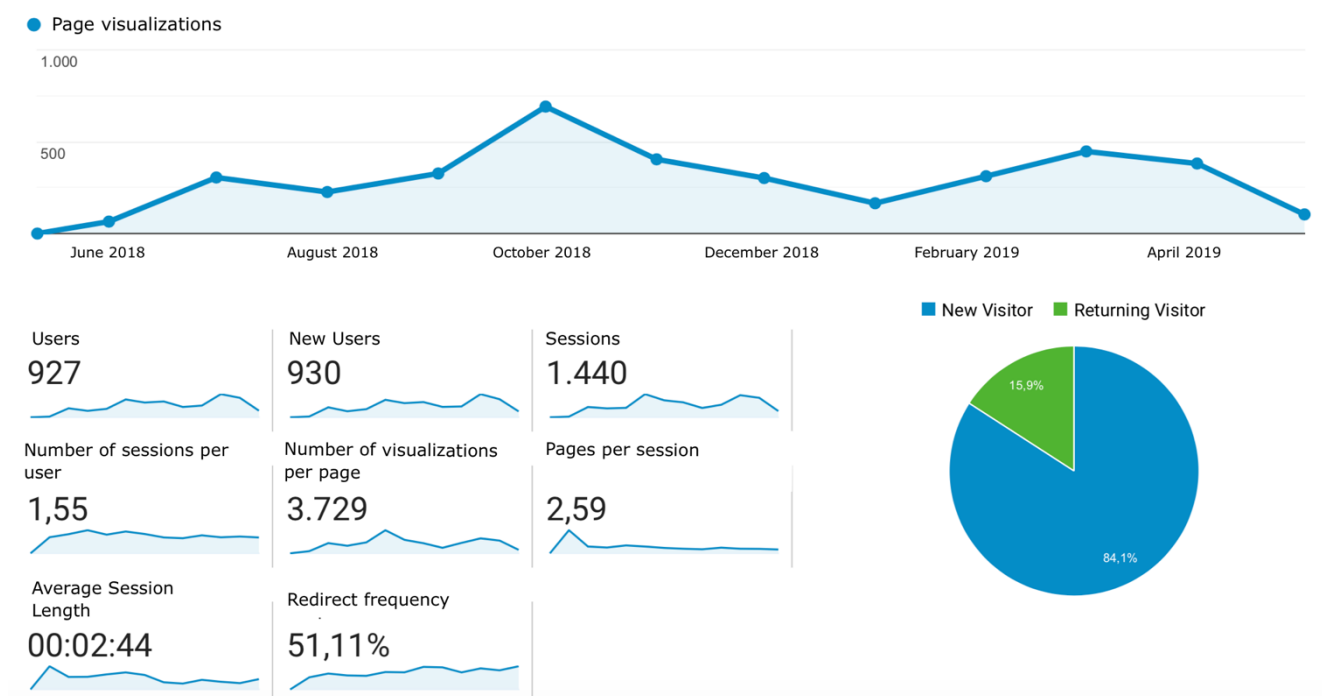


Figure 6 - RESISTO website statistics.

The numbers of the social media are not yet very large (Twitter, 19 followers; Facebook, 31 followers, LinkedIn, 17 followers) but we expect to increase these numbers in the second year where we first results of the project will be disseminated.

5 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.

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

There are 7 deliverables foreseen in the workplan which are associated with the dissemination strategy, as listed in Table 2 that will materialize the above mentioned dissemination and communication actions time plan.

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 3 - List of deliverables related to the dissemination.

5.1 Consortium partners' contribution

Interaction and communication with all consortium partners and interaction with all WP are necessary to successfully disseminate the results of the project, especially because WP10 retrieves results and contents of WP 1-9 for dissemination and exploitation.

All involved partners will participate to the dissemination by:

- Contributing with contents and outcomes from the work packages they are involved in: press releases, presentations, pictures, video releases, articles, publications, etc.;

- Sharing dissemination opportunities;
- Participating and presenting the project at relevant events;
- Reporting the performed dissemination activities;
- Populate the section on EMDESK® dedicated to the dissemination activities (<https://emdesk.eu/cms/?p=334>).

5.2 Acknowledgement of European Union funding

All dissemination material needs to include the EU emblem and the following acknowledgement: “This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No. 786409.”

6 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 first year, where the requirement definition phase has been the main activity carried out. We expect the dissemination activities to grow in number and importance as the first results will be delivered.

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

7 REFERENCES

INDEX	REFERENCE
[1]	RESISTO – Grant Agreement. Project Starting Date: May, 1 st 2018
[2]	D10.6 Dissemination and Communication Activities - first

8 ANNEXES

8.1 RESISTO WORKSHOP DURING DefCamp

Brochure distributed to almost 2,000 attendees.

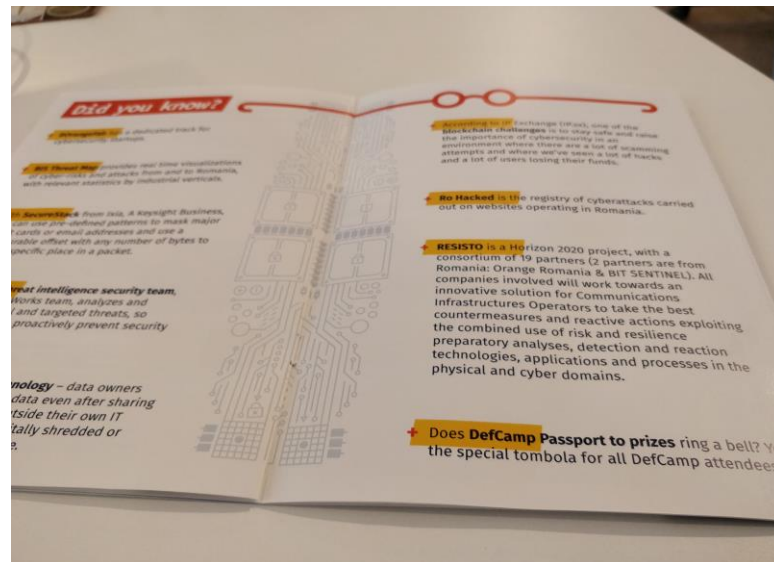


Figure 7 - Brochure advertising RESISTO distributed during DefCamp.

RESISTO

MasterClass: Risk and Resilience Frameworks

Lucian Nitescu - Senior IT Security Specialist

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

BIT SENTINEL
Your Safety is Our Business!

Figure 8 - RESISTO masterclass at DefCamp.

The audience at the Masterclass RESISTO was constituted by 30 attendees from the following industries:

- Healthcare representatives
- Big 4 Accounting representatives
- National Bank of Romania representatives
- Academia & Universities representatives
- Tactical military radios and defense electronic systems representatives
- Energy representatives
- ICT providers
- Telco representatives

8.1.1 RESISTO Dissemination at DefCamp

Website: <https://def.camp/technologies/#bitsentinel>

Period of promotion: September 2018 - July 2019

Expected reach (on the website): 30,000 unique visitors

Expected direct audience (on the page): 3,000 unique visitors

Bit Sentinel – Cyber Security Services

BIT SENTINEL provides services to private companies from European countries since 2015. Main services are related but not limited to offensive & defensive cyber security services such as penetration testing, code review, Cyber Attacks Recovery, Social Engineering (remote/physical), incident response, vulnerability management, PCI DSS security services etc for Web Application, Software Application, Mobile Application, Network Infrastructure, Wireless Infrastructure, Workstations, Blockchain Security.



Besides providing cyber security services & advisory for companies from different sectors such as Fintech, Healthcare, Real Estate, Retail, Ecommerce, Online, Startups, Blockchain, Critical Infrastructures etc. we are also:

- Involved as one of the key technical partners from the **RESISTO project**: an innovative solution for Communication CIs holistic situation awareness and enhanced resilience. During RESISTO, BIT SENTINEL will develop a fully-functional framework for Vulnerability Disclosure based on blockchain. Our goal is to embed standard functionalities of Vulnerability Disclosure Framework within the main RESISTO framework and provide an innovative way to threat the most critical features of a vulnerability disclosure framework such as voting, payments, privacy, accounting, identities and others with help of decentralized technologies such as blockchain, smart contracts and tokens. In this way, not only we will push forward the idea of privacy of the security specialists and companies but we also provide a feature rich platform that could help simplify rewarding process of Bug Bounty programs with help from innovative token based payments.
- Technical coordinator for the National Phase & Selection of National Teams of **European Cyber Security Challenge**, one of the most important cyber security competitions from Europe
- Developer & Technical Coordinator of **Business Internet Security Threat Map**, a technology developed by us for Orange Romania that presents the visualization from a high overview perspective of the data gathered from the Orange Romania Business Internet Security agents deployed across Romania
- Developer & Maintainer of **RO Hacked** – Register and Catalog Web Attacks Against Websites from Romania

Figure 9 - RESISTO advertisement on BIT SENTINEL webpage.



Figure 10 - Main Stage at DefCamp 2018.



Figure 11 - MasterClass Workshop organised by BIT SENTINEL & ORANGE ROMANIA at DefCamp 2018.

Dissemination has been carried out also through:

- LinkedIn: <https://www.linkedin.com/feed/update/urn:li:activity:6460811821006749696/>

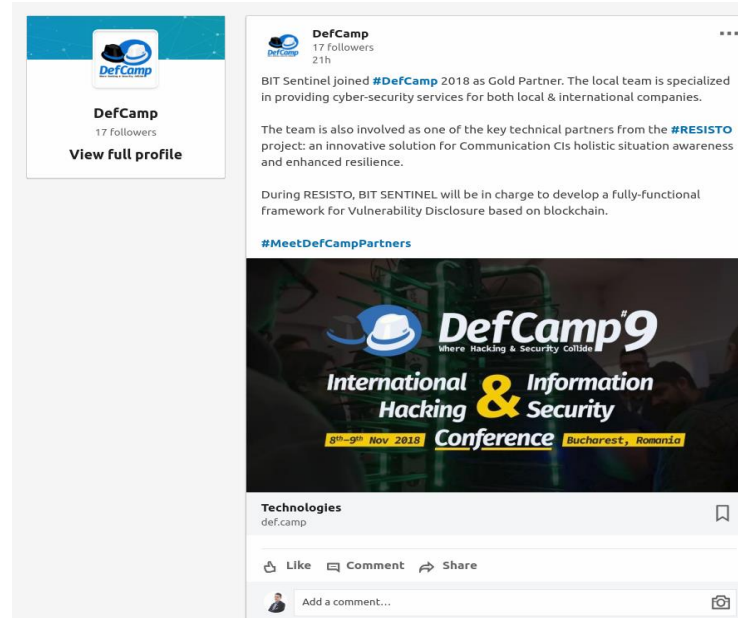


Figure 12 - RESISTO avertissement on DefCamp LinkedIn webpage.

- Facebook: <https://www.facebook.com/DefCampRO/posts/1775455312552243>



Figure 13 - RESISTO advertisement on DefCamp Facebook webpage.