D8.1 - Dissemination plan and calendar of activities

Work Package:	WP 8
Lead partner:	CNIT
Author(s):	Matteo Mauri (CNIT), Davide Ariu (CNIT), Barbara Pirillo (ENG), Marc Busch (AIT), Liliana Andrei (RATB), Roberto Puricelli (CEFRIEL), Yung Shin Van Der Sype (KU LEUVEN), Filipe Custódio (VISIONWARE), Nelson Escravana (INOV), Carlo Dambra (PROPRS), Nathan Weiss (ELTA), Enrico Frumento (CEFRIEL)
Submission date:	30/12/2015
Version number:	1.0 **Status:** Final

Grant Agreement N°:	653618
Project Acronym:	DOGANA
Project Title:	Advanced Social Engineering and Vulnerability Assessment Framework
Call identifier:	H2020-DS-06-2014-1
Instrument:	IA
Thematic Priority:	Trustworthy ICT
Start date of the project:	September 1st, 2015
Duration:	36 months

Dissemination Level	
PU: Public	✓
PP: Restricted to other programme participants (including the Commission)	
RE: Restricted to a group specified by the consortium (including the Commission)	
CO: Confidential, only for members of the consortium (including the Commission)	

Horizon 2020 European Union Funding for Research & Innovation

Project co-funded by the European Commission under the Horizon 2020 Programme.

Revision History

Revision	Date	Who	Description
0.1	01-10-2015	Matteo Mauri (CNIT)	Creation
0.2	10-10-2015	Barbara Pirillo (ENG) Marc Busch (AIT) Liliana Andrei (RATB) Roberto Puricelli (CEFRIEL) Yung Shin Van Der Sype (KU LEUVEN) Filipe Custódio (VISIONWARE) Nelson Escravana (INOV)	Partners Contributions
0.3	02-11-2015	Carlo Dambra (PROPRS) Nathan Weiss (ELTA)	Partners Contributions
0.4	01-12-2015	Matteo Mauri (CNIT) Davide Ariu (CNIT)	Revision
0.5	17-12-2015	Matteo Mauri (CNIT) Davide Ariu (CNIT)	Revision
0.6	23-12-2015	Enrico Frumento (CEFRIEL)	Revision
1.0	04-01-2016	Matteo Mauri (CNIT) Davide Ariu (CNIT)	Final

Quality Control

Role	Date	Who	Approved/Comment

Disclaimer:

Table of Contents

List of figures

List of Tables

Definitions and acronyms

CC	CyberConnector
CyberConnector	An internal knowledge collaboration site and social network that is used to share all the information among partners. Referred to also as CC.
DOW	Description of Work
DT BLOCK	Development of the DOGANA Toolchain, first project block
FF BLOCK	Foundations of the DOGANA Framework, second project block
FT BLOCK	Field Trials, third project block
GA PHASE	General Awareness Dissemination Phase (Phase 1)
MA PHASE	MArket potential Dissemination Phase (Phase 2)
OS PHASE	Other Stakeholders Dissemination Phase or Open Source Dissemination Phase (Phase 3)
MST	Management and Support Team
PC	Project Coordinator
SC	Scientific Coordinator

1. Introduction

In this document, we describe the first version of the "Dissemination Plan" of the DOGANA Project.

According to the European Commission, dissemination is *a planned process of providing information on the quality, relevance and effectiveness of the results of programs and initiatives to key actors. It occurs when the results of programs and initiatives become available*.

Therefore, in this report we propose a list of possible targets to which the research products must be disseminate. At the same time, we indicate a set of possible actions which can be performed in order to reach such targets.

The consortium members are fully aware that the arguments studied by DOGANA are extremely competitive and at the edge of security. The whole ICT security community, all around the globe is still struggling on which are the best solutions to mitigate the problems of social engineering and the human related weaknesses. The partners have therefore the intention to put a special attention to the dissemination efforts of the project in order to maximize the impact of DOGANA not only at the end-users level but also at the business and research levels.

In order to design an effective dissemination plan, we followed the main guidelines suggested by several EU education and culture programs:

- clear rationale for and objectives of dissemination and exploitation;
- strategy identifying which results to disseminate and to which audiences – and designing programs and initiatives accordingly;
- identification of organizational approaches of the different stakeholders and allocation of responsibilities and resources;
- implementation of the strategy by identifying and gathering results, and execution of dissemination and exploitation activities;
- monitoring and evaluation of the effects of the activities.

The objective is to maximise the visibility, credibility and impact of the project. To ensure that the project outputs will be further used and evolved, DOGANA outcomes will be disseminated to a **wide set of stakeholders**.

This knowledge and capacity will be leveraged to assure the necessary measures and engage all the relevant market players to maximise the project impact. Noteworthy, impact and dissemination of results will be facilitated by the large network of the project's coordinator, as well as other partners.

This planning consists in defining what will be disseminated, where, when and by whom. The evaluation criteria will be based on quantities (number of publications, number of attendees....) but most important it will be qualitative (level of the conference, quality of the feedback obtained, and profile of persons contacted).

Accordingly, this report is as follows. Section 2 describes the main targets involved in the dissemination plan. Section 3 describes a list of possible actions for each of above targets. Section 4 gives a brief report of current/under organization dissemination activities. Section 5 presents possible dissemination deadlines. Appendix I and II, show which actions are and/or will be carried on by DOGANA partners, jointly or individually, and the connection between dissemination and the projects main research blocks.

2. Targets of the Dissemination Plan

In this Section, we focus on the possible targets, in terms of public and private institutions, end-users, which may take advantage from news and research products of the DOGANA project.

The DOGANA project is supported by an extensive consortium throughout Europe. Consortium members have gained significant expertise in the areas of social engineering, cybercrime, risk assessment and cyber-terrorism (focusing on the technical, ethical and criminological aspects), both in research (including EU-funded research) and in commercial activities.

Several targets may be taken into consideration:

- **Government**. In particular, those government institutions directly involved in security issues, as law enforcement agencies, judicial authority and administrative offices. These institutions may be at different levels: local, national, and international.
- **Private and public companies**, involved in adopting or creating novel solutions for computer security, spear phishing, social engineering. Every year the cybercrime carried out through social engineering costs millions of euros to public and private companies.
- **Research community**. Social Engineering 2.0 risks and the development of defense tools are open problems day-by-day monitored by the research community. The consortium will bridge the gap between DOGANA and **related running projects** in the Security Theme in order to disseminate results and contribute valuable knowledge.
- **End-users**. Due to the large diffusion of social networks, many users are constantly exposed to privacy violations. DOGANA project should try to inform them at best and should try to “teach” them, if possible, which are the real risks of the social networks.

3. Actions

In this Section, we indicate several possible actions that can be done in order to disseminate the research products of DOGANA, to increase the visibility of the project partners and reach the targets listed in the previous Section.

As reported in Figure 1, dissemination planning is split into three steps.

- **GA PHASE** - General Awareness Dissemination Phase (Phase 1)
- **MA PHASE** - MArket potential Dissemination Phase (Phase 2)
- **OS PHASE** - Other Stakeholders Dissemination Phase or Open Source Dissemination Phase (Phase 3)

Figure 1 – Dissemination planning phases
GA Phase – MA Phase – OS Phase

In this planning, a list of the activities suggested by the consortium is reported, indicating the corresponding dissemination phase.

3.1. GA PHASE - General Awareness Dissemination Phase (Phase 1)

During the first phase, the main purpose will be to create general awareness about DOGANA's objectives and expected results and establish links with related initiatives and projects. The dissemination will be focused on the description of the project's aims and objectives, the explanation of how to attain them, the envisaged results and expected benefits.

During this **first phase**, the main dissemination activities will include:

- **Project brochure and posters**, which will provide an overview of the objectives, approach, consortium and targeted results, giving particular emphasis to the scale of breakthrough/innovation expected to be achieved;
- **Project website**, providing project description, partners profile and expertise, and regular information on the project progress.
  The project website has been already released at the time of creating this document, and it is available following the URL: http://dogana-project.eu/
  It will play several roles, such as facilitating the exchange of information within the consortium as well as with the public in general. The website will also be used to coordinate various activities among the partners, as well as hosting the digital content distributed during the workshops, that the partners select for public release. It will also

facilitate contacts with other researchers, companies, public bodies, agencies and all potential stakeholders, aiming to create an informal international network. The main content of the website includes information about the project and its goals; information about the project consortium; publications and material produced during the project; details on any events organized during the project; public documents; multilingual press releases. As the website's goal is mainly intended to raise awareness about the project activities, the website's target will be non-specialists people. Hence, the language used in the website is non-technical. The website is better described in the **DOGANA Public Deliverable 8.2. - Project Website and Social Networking accounts**.

- **Press releases** in specialised journals.
- **Presentations at meetings and workshops**, to which, researchers, companies, government bodies, decision makers, (in general all the relevant stakeholders) will be invited. **Media coverage will be also ensured**. As already discussed in the WP8 presentation, two workshops have been already planned. During the first Workshop, the tool developed during the first 24 months of activity will be exposed. At the final Workshop, both the project's results and the tool, will be presented and discussed. Workshops will also facilitate the creation of synergies between current running EU research projects, improving the coordination of DOGANA results with European and national efforts.
- **Whitepapers and public reports** will be released, primary making a publicly available version of deliverables **D2.1** (The role of Social Engineering 2.0 in the evolution of attacks), **D3.1** (Report on existing tools, their evaluation and the gap to be filled by DOGANA development), **D4.1** (Human Attack Vectors in SE 2.0), and **D5.5** (Legal and Ethical Recommendations) in form of whitepaper or similar. All such documents will be made available through the project's website. To maximize the project's impact, the consortium will consider the possibility of splitting the whitepapers in order to make them more easily readable.
- **Social Media accounts**, as fast and effective channels of communication and interaction with the general public. Public audience will be reached and involved also through **Social Networks**, e.g. on YouTube, where it will be possible to share **videos of workshops presentations and interviews**. To complement the online presence of the project, a Twitter account will be created and can be used to push short announcements to the community of the project and relevant news about the subject studied by DOGANA. The latest Twitter posts could also be mirror on the homepage of the project's website as well as on Facebook. The partners will contribute posting news in order to transform the site in an influential social engineering source. The consortium is also evaluating the possibility to create a **video tutorial** showing how the tool works, and to create a "**viral" video** showing **the risks of sharing private information in the social networks**. The aim is to become an authoritative hub of news on social engineering, sharing as much as possible the knowledge collected by DOGANA partners and the relevant news and trends.

3.1.1. Promoting and organizing International and multidisciplinary contests

Organization of international competition on several topics of computer security could be done in order to involve research communities, universities, companies and end-users from several countries. The aim is making the point about the current technology on Computer Security and Social Engineering risks.

During a final meeting there could be a multidisciplinary award ceremony.

DOGANA partners could establish one or two awards from the following list:

- **"Best tale regarding Social Engineering 2.0"**: a contest for short tales (dystopian or positive tales) regarding Social Engineering 2.0, in which the author must appoint at least once the DOGANA project.

  Each short story will be published on the DOGANA website and must be shared by the own author over the Facebook Social Network and/or over the Twitter Social Network (to be defined). Among the 30 most shared tales, a qualitative jury will award three stories. The most shared tale will be also awarded.

- **"Best one-page comic/poster/image regarding social engineering 2.0"**: a contest for one-page comics or graphic posters/images regarding Social Engineering scenarios, in which the author must apply the DOGANA logo.

  Each comic/poster/image will be published on the DOGANA website and must be shared by the own author over the Facebook Social Network and/or over the Twitter Social Network (to be defined). Among the 30 most shared objects, a qualitative jury will award the best comic/poster/image. The most shared contribution will be also awarded.

- "**Best short video regarding social engineering 2.0**": a contest for short videos regarding Social Engineering scenarios, in which the author must apply the DOGANA logo.

  Each video will be published on the DOGANA website and must be shared by the own author over the Youtube Social Network. Among the 30 most viewed videos, a qualitative jury will award the best one and it will become the official project's video. The most shared contribution will be also awarded.

- **"Best newspaper article regarding the DOGANA project"**: a contest for short articles regarding the project.

  Each article must be published in a real existing online newspaper and will be published also on the DOGANA website and must be shared by the own authors over the Facebook social network and/or over the Twitter Social Network (to be defined). Among the 30 most shared articles a qualitative jury will award the best one. The most shared contribution will be also awarded.

- **"Best thesis regarding innovative solutions against Social Engineering attacks"**: a contest for M.Sc. theses. A qualitative jury will award the best thesis.

Prizes have yet to be determined and may be obtained by successful candidates only if they will be present during the closing ceremony.

3.2. MA PHASE - MArket potential Dissemination Phase (Phase 2)

The **second phase** will aim at increasing the market potential of DOGANA and will be results oriented; this phase includes the presentation of the tangible/exploitable results of the DOGANA project, presentation of the DOGANA functionalities and protection mechanisms to potential **users**.
During this phase, the dissemination will be based on presentations, e.g. publications and presentation in relevant scientific conferences and industrial exhibitions.

3.2.1. Publishing and presenting project results

A number of conferences and journals could be publication targets.

Joint publications will help to reinforce and demonstrate the collaboration between DOGANA partners. Accepted papers will acknowledge the support provided by DOGANA and will be made available for download on the project website. Worth remarking, this list is not exhaustive; thus, novel events may be added as dissemination activities of DOGANA partners proceed.

- Software Practice and Experience
- Journal of Object Technology or Information and Software Technology
- International Journal of Secure Software Engineering (IJSSE)
- Computer Networks
- IET Information Security
- Elsevier Computers and Security
- EURASIP Journal on Information Security
- International Journal of Information Security
- Journal of Systems and Software (JSS)
- ACM Transactions on Information and System Security (TISSEC) or Software and Systems Modeling (SoSyM)
- Elsevier Computers & Security journal
- IEEE Transactions on Information Forensics and Security.
- IEEE Security & Privacy

3.2.2. Other academic events. Courses, seminars, schools.

The consortium as a whole will take up the aforementioned dissemination activities, with all partners, by utilizing existing capabilities such as their respective websites, newsletters, blogs, social networking accounts etc. Furthermore, specified partners will undertake the additional

activities that were described, such as the implementation of the project website, the organization of workshops and training or educational sessions. Also, the consortium will use its large networking capacities based on its personal contacts, project cooperation's, memberships and affiliations to reach all the possible stakeholders interested in and affected by DOGANA results. DOGANA project and its results will be presented also during academic annual events (e.g. University of Cagliari organizes **Building Trust in the Information Age**, annual International summer school on Computer Security and Privacy, http://comsec.diee.unica.it/summer-school/; CEFRIEL hosts a master track for executives of SMEs and enterprises on Information Security Management, which is in 2016 at its 11th edition, http://www.securman.it).

3.3. OS PHASE - Other Stakeholders Dissemination Phase or Open Source Dissemination Phase (Phase 3)

The **final phase** will go on beyond the end of the project and will aim at stimulating the participation of other individuals, SMEs and other organisations through the **DOGANA open source project**.

Access to the stakeholders group might be mainly "direct". "Direct" access via the consortium means that a particular partner is in some capacity a member of the Agency, Forum, Association, or Working Group that will be targeted by the dissemination activity. The most relevant stakeholder organizations to the dissemination of DOGANA results include:

- AFCEA Portugal – a non-profit organization dedicated to increasing knowledge in information technology, communications and electronics for the defence, homeland security and intelligence communities.
- ANSSI – Agence nationale de la sécurité des systèmes d'information (national information system security agency).
- APWG – Anti Phishing Working Group - global industry, law enforcement, and government coalition focused on unifying the global response to cyber-crime through development of data resources, data standards and model response systems and protocols for private and public sectors.
- DGA (general directorate for armament – French agency of the ministry of Defense).
- CSIRTS network.
- Cyber defence centre in Portugal.
- DCC – Microsoft Digital Crimes Community.
- DANOTEC Portugal – Association of Defence, Armament and New Technologies.
- DGA – Division of General Armaments of the French Ministry of Defence (the main French cyber security actor in the military domain).
- EDA – European Defence Agency.
- EECTF – European Electronic Crimes Task Force.
- ENISA European Union Agency for Network and Information Security.IMG-S – Integrated Mission Group for Security - is an open forum bringing together security technology

experts from Research and Technology Organisations (RTOs), Universities, Industry and Small/Medium Enterprises (SMEs) with the aim to support the European Commission and its Member States to build world-class technology capabilities for Security.
- La Nouvelle France industrielle Cyber Security working group.
- NATO Computer Incident Response Capability.
- NATO NIAG – participation in Cyber Security and Defence studies.
- NATO Cooperative Cyber Defence Center of Excellence (NATO CCDCOE)
- Portuguese Government Agencies and Ministries - providing direct communication to Ministry of Defence, Ministry of Internal Affairs, Ministry of External Affairs, Ministry of Economy, among others.
- ShadowSEC – a company in the field of Information Security, Cyber Security and IT
- System@tic – French competitiveness cluster for security and defence, transports, telecommunications, ICTs and sustainable cities.
- SWITCH – company providing internet services for the Swiss universities and internet users

3.3.1. Notes on exploitation of results

OS PHASE and MA PHASE are closely related to the exploitation of DOGANA results, that will be better defined in the Deliverable *8.4 Exploitation Plan*, due in the 18th month of activity.

3.4. Target-Action Connection

In this section, we briefly link the set of actions, described in the previous pages, with the possible targets listed in Section 2. The following table summarizes, for each target, the possible set of actions that can be carried out.

Table 1 – Target-Action connection table

Target	**Action**
Government	• "Tutorial" meetings • Participation to events organized by public institutions • Organisation of workshops
Research community	• Publications on Journals and Conferences • High-profile magazines • Organization of contests or competitions • Social networks (LinkedIn and Twitter in particular)

	• Awards for best thesis regarding social engineering 2.0 • Organisation of workshops
Public and private companies	• Organization of contests or competitions • Tutorial workshops and meetings • Social networks (LinkedIn, Twitter and YouTube especially) • Participation to international expo (posters, brochure, proof-of-concept presentation) • Newspapers, magazines and high-profile Internet publications • Attractive website
End-users	• News segments, Magazine, Newspaper • Social networks (Facebook, Twitter and YouTube in particular) • Raise awareness events on “computer security” • Attractive website • Multidisciplinary contests • Video tutorial on the functioning of DOGANA

4. Current or under organisation dissemination activities

In the following, we briefly report some dissemination activities that DOGANA partners, jointly or independently each other's, are conducting.

- (Completed) DOGANA official logo
- (Completed – Under constant editing) DOGANA public website
- (Current) DOGANA official presentation templates
- (Completed) DOGANA presentation during SINNOVA Exhibition. More information are available on the DOGANA website, Events section. http://dogana-project.eu
- (Completed) DOGANA presentation during Security Summit Cagliari 2015. More information are available on the DOGANA website, Events section. http://dogana-project.eu
- (Completed) DOGANA presentation during European Cyber Security Month 2015. More information are available on the DOGANA website, Events section. http://dogana-project.eu
- (Current) Dissemination of DOGANA official press release and media coverage
- (Planned) Dissemination of DOGANA's goals through the partners' official websites
- (Current) Organizing of Building Trust in the Information Age 2016: annual international summer school on computer security and privacy. During a poster session the results of the project will be shown.
- (Planned) Submission of papers to the Conferences or Journals listed in section 3.2.1 of this document

5. Deadlines for a first evaluation of the dissemination activities

In this Section, we suggest a set of specific actions with related deadlines in order to give a first concrete evaluation of the dissemination activities of DOGANA partners. The following table Table 2 summarizes some possible proposals. We put in brackets the possible leader of each activity. The feasibility and the opportunity of realize each of these activities have to be discussed between partners.

Table 2 – Preliminary evaluation of dissemination activities table

Target	**Action**	**Deadline**
Government	Deciding the event/workshops to organize/participate in order to invite institutions	MONTH 18 (All consortium)
	Evaluation and report of the first Workshop	MONTH 24 (ENG, CNIT, CEFRIEL)
Research community	First list of submitted/accepted papers to conferences/journals. In particular, which scientific communities are the targets	M12 (All consortium)
	Deciding about realization of a tutorial video of DOGANA project	M12 (ENG, CNIT, CEFRIEL)
	Deciding about thesis contests, awards, and prizes	M12 (ENG, CNIT, CEFRIEL)
	Deciding about creation of specific DOGANA account on LinkedIn/Twitter	M6 (ENG, CNIT)
	Deciding about participation to common events involving DOGANA and similar research projects	M12 (All consortium)
	Evaluation of collaboration with related research projects	M18 (All consortium)
Public and private companies	Preparation of brochures and posters specific for DOGANA	M10 (ENG, CNIT, CEFRIEL)

	Deciding about creation of specific DOGANA open source strategy	M12 (All consortium)
	Deciding about integration between dissemination strategy and exploitation strategy	M12 (All consortium)
End-users	Deciding about creation of specific DOGANA account on Facebook, Twitter and YouTube	M6 (ENG, CNIT)
	Deciding about multidisciplinary contests, awards, and prizes	M12 (ENG, CNIT, CEFRIEL)
	Improving the attractiveness of current website pages for end-users	M6 (ENG, CNIT)
	Evaluation of website's users visits and statistics	M12 - M24 - M36 (ENG, CNIT, CEFRIEL)
	Improving digital presence among the participants' official webpages	M8 (All Consortium)
	Improving media coverage	M6 (All Consortium)
	Preliminary dissemination report	M18 (CNIT)

6. Appendix I: Partner-Action connection

Table 3 presents the individual contributions of the DOGANA partners.

Table 3 – Contribution of partners to the overall dissemination activity

Participant	Dissemination activities
ENG	ENG will disseminate the DOGANA results in **two different communities** where it is active. In the **CYSPA environment**, ENG will publish information on the community portal, a membership based community with a sector per sector focus (currently transport, government, energy and finance). ENG will also analyse if / how DOGANA results could be directly incorporated on the CYSPA community portal to make them available to the community. In the **ACDC environment**, ENG is cooperating with the public authorities to set up the Italian national Web site to support fighting against botnets. This is part of a European wide activity to fight botnets – a key topic in terms of SVA, as the increased awareness targeted by DOGANA can contribute to decrease the deployment of botnets.
CEFRIEL	CEFRIEL will prepare dissemination talks and papers for various cybercrime groups such as **Microsoft DCC** and the **EECTF** and **CERT-IT**. Results of DOGANA will also be disseminated to all partners of the **CEFRIEL consortium** (i.e. ICT companies, public bodies and Universities). Furthermore, DOGANA insight will be brought to the training track through specialized **training courses** and will be exposed to the public via institutional communication channels, such as the web, social media and very high quality white papers published under a Creative Commons license, the CEFRIEL innovation paper series. CEFRIEL will also act as a liaison with the various organizations that it is able to reach. Being CEFRIEL the scientific coordinator of the proposal, it will publish main results during the project to the most relevant security conference, with a special attention to the European Conferences.
AIT	The dissemination of results by AIT will be realized by multiple paths to address a broad audience and a wide range of stakeholders. Dissemination on a scientific level will be done by publicizing at international recognized conferences and in scientific journals. Possible conferences that will be targeted by this activity will be **ACM Human-Computer Interaction (HCI), the Symposium On Usable Privacy and Security (SOUPS), Nordic Computer Human Interaction (NordiCHI)**.
CNIT	The CNIT research unit and the University of Cagliari will **coordinate Dissemination and Exploitation Activities**, being responsible for both the "Dissemination plan" (D8.1.1) and the "Dissemination reports". CNIT will be responsible for both the intermediate report (provided at M18, D8.1.2), and

	for the final report (D8.1.3). In addition, CNIT will guarantee the coordination of DOGANA with other relevant projects (D8.4.1). CNIT is also responsible to design, develop, and maintain the **project official website**, the main channel to distribute all the publicly available material. At the begin of the project CNIT will prepare the official starting press release, that will be released to the Italian press by CNIT itself. An English version of the press release will be provided to the partners for them to release to the relevant press agencies in their respective countries. CNIT plans to present the DOGANA achievements in peer-reviewed scientific papers published in international venues (either conferences and journals), and to disseminate the project results during the public events (regional, national, and international) to which the involved research unit regularly attends and participates. CNIT also expects to dedicate a day of the 2016 and 2017 editions of the summer school **"Building Trust in the Information age"** (organized by the involved research unit) to the topics addressed in the DOGANA project, having then the opportunity to present the results of the project. Poster sessions are usually organised during the school that are usually a suitable venue for this purpose. The event is also endorsed by GIRPR (Italian group of researchers in Pattern Recognition). CNIT will use **GIRPR newsletter** to disseminate DOGANA's presentation during the summer school's editions. Finally, CNIT plans to use the existing YouTube channel of the research unit involved to distribute all the video material produced during the project.
INOV	INOV plans to present DOGANA related papers in national and international reference publications and participate in local workshops with public and private potential end users for presentation of project results. Additionally a wide direct dissemination of the project results, via meetings, will be carried out in Portugal encouraging an active dialogue with local authorities to facilitate the fast adoption of the project results and usage by local end users**.**
NCSRD	NCSRD will participate in the dissemination of project results by: a) sharing knowledge through relevant conferences, workshops and open-access research publications, so as to maximize visibility of project results. Relevant journals and conferences include, for example, **IEEE Access**, the **European Alliance for Innovation International Conference on Pervasive Games** etc. A full list of scientific dissemination outlets will be constructed within WP8 "Dissemination and Exploitation". b) presenting results within our **educational activities**, thus providing fast access to research results to a new generation of researchers, c) presenting results to relevant industry groups, through our participation in the **Integrated Mission Group for Security**. NCSRD participates as member of **IMG-S in the technical areas (TAs), TA1 – Surveillance and Identification, TA2 – Communications, TA4 – Resilience**.

	d) presenting results to the general public, through our public, free-to-access activities (such as the **Researchers' Night,NCSRD Summer School** etc.), our **Newsletter** and our Public Relations department which disseminates results to the Hellenic press and media.
SUPSI	SUPSI has an established continuous communication and dissemination strategy, including local newspapers, radio and TV appearances. The DOGANA project and its outcomes will be promoted in the frame of events (**workshops, exhibitions, specialized fairs**) to which SUPSI regularly takes part or even leads and coordinates, thus creating an important network of stakeholders and awareness actions. In addition to the use of the project foreground in the frame of internal courses, the training of companies and public bodies in Switzerland is one of the activities carried out by the SUPSI security team. Last but surely not least, the dissemination is also guaranteed in the research community: the security team is in fact active as partner and scientific coordinator in research projects at Swiss and European (FP7) level.
KUL	The Interdisciplinary Centre for Law and ICT is an academic research centre at the KU Leuven aiming to further develop its existing knowledge at the crossroads of 'Law and ICT' and to deepen its research on the interaction of new information technologies with existing European legal provisions and policies. The results from the work performed under DOGANA will be disseminated mainly towards the **broader society by academic publications in scientific journals** and by participating in **high-level workshops** and/or conferences.
HP	HP will contribute to disseminate DOGANA both internally and externally. Internally, it will use institutional channels like **Business Unit newletters**, internal fora, Intranet website, knowledge repositories and technical conferences. A dedicated internal event for DOGANA presentation and demonstration could be planned. Externally, HP will target publications and industrial conferences. Among targeted conferences/fora there could be **CSA (Cloud Security Alliance) EMEA**, **Clusit Security Summit**, **Cisco Secure Tour**, **Italy Forum PA**, and other sector conferences. As a stretch goal, top HP worldwide events (**HP DIscover** and **HP Protect**) will be addressed if viable. In terms of publications, specialized sector magazines like "ICT Security" will be addressed, along with internal abstract publications to HP worldwide knowledge base. In compliance with corporate polices, a press release will be sought.
GNS	GNS will disseminate DOGANA mainly using the current **newsletter** and publishing useful information on the **new Site of the National Cybersecurity Centre**.
RATB	RATB will disseminate DOGANA by different communication channels, focused on the specific target **groups of professionals working in public transport**, by organizing workshops; publishing specialized articles in

	different local and international publications, newsletters; making presentations in different national and international events; using the own web-page for publishing information about the project progress and creating a link to DOGANA web-site**.**
HMOD	HMOD through **Cyber Defence Directorate** which is the responsible authority for cyber defence in national level will publish and distribute the outcomes of the project to all relevant stakeholders taking advantage its key role in the overall national cyber security activities. Additionally as the **national representative in NATO and EU cyber defence** communities will communicate the benefits of the project in order to promote how it can be integrated into existing cyber security programs and implementations.
DBI	DBI will add its long standing experience and relations with customers from the security technology industry. During the project phase, DBI will catch their attention, inform them on the project's results and on the advantages of improving resilience against Social Engineering cyber attacks. DBI's main communication channels will be: the **company magazine**, LinkedIn groups and partners' websites, like the **Danish Advanced Technology Group's website** (http://en.gts-net.dk). Participation and presentations at specialized conferences and events will also foster communication of the project results. By the end of the project phase, DBI will be able to produce and distribute a report with the most significant results, including the testimonies from stakeholders involved in the testing of the product.

7. Appendix II: Project Blocks-Action Connection

As presented in Section 3, dissemination planning is split into three steps: **GA PHASE**, **MA PHASE**, **OS PHASE**.

At the same time, the DOGANA project is organised in 3 main blocks:

- **Foundations of the DOGANA Framework - FF Block**
- **Development of the DOGANA Toolchain - DT Block**
- **Field Trials – FT Block**

In the following pages, the list of actions presented in the Section 3 and Appendix I is related to the DOGANA main blocks.

7.1.1. Foundations of the DOGANA Framework

Goal #1 ENG	
Purpose	Increase DOGANA visibility in the Cybersecurity landscape
Target	ACDC and CYSPA communities
Means	Publish information about the DOGANA approach in the ACDC and CYSPA communities (description of the DOGANA initiative and participants, objectives and expected outcomes, as well as periodic news about DOGANA activities and results)

-

Goal #2 ENG	
Purpose	Increasing DOGANA visibility in the Cybersecurity landscape
Target	CSWG cybersecurity working group in EOS (European Organisation for Security), http://www.eos-eu.com/Middle.aspx?page=cybersecurity
Means	Engineering Ingegneria Informatica chairing the CSWG

-

Goal #3 ENG	
Purpose	Increasing DOGANA visibility both as a project and as a research initiative operating in the Social Engineering domain.
Target	Public audience interested in the topic of Social Engineering and specifically looking for information about the DOGANA project.
Means	Public website to be set up

-

Goal #4 ENG	
Purpose	Raising interest in DOGANA, both as a project and as a research initiative operating in the Social Engineering domain.
Target	Public audience interested in the topic of Social Engineering
Means	Social media channels set up (i.e. DOGANA Twitter account, or Linkedin profile). Starting interactions and generating active discussions with stakeholders who may be interested in liaising with the DOGANA project; • Informing stakeholders about the benefits and results offered by the DOGANA research • Raising awareness about Social Engineering

-

Goal #3 ENG	
Purpose	Supporting the creation of dissemination material with the objective to increase the visibility of the DOGANA project and to position DOGANA as key player in the Social Engineering domain.
Target	All the Stakeholders identified as target audiences for the DOGANA project. The stakeholders will benefit from the dissemination material by increasing their awareness and knowledge about the DOGANA project and – in case of wider dissemination activities – about Social Engineering.

Means	Dissemination material (online content, poster, leaflets, flyers, brochure, etc. – to be selected according to the dissemination objective and the target audience identified).

-

Goal #1 VISIONWARE	
Purpose	Increasing DOGANA visibility in the Cybersecurity landscape
Target	Portuguese Cybersecurity community (prospective end-users)
Means	Present the goals of the project within VisionWare's client base.

-

Goal #2 VISIONWARE	
Purpose	Increasing DOGANA visibility in the Cybersecurity landscape
Target	Portuguese Cybersecurity community (cybersecurity experts)
Means	Present the goals of the project in specialized forums.

-

Goal #1 RATB	
Purpose	Dissemination of DOGANA Project
Target	RATB Employees Public transport professionals – local, regional, national and European level Universities Local Authority
Means	RATB newsletter RATB website Workshops E-mails

-

Goal #1 INOV	
Purpose	Dissemination of DOGANA project
Target	Portuguese CSIRTs
Means	Presentation in the Portuguese CSIRT network

-

Goal #2 INOV	
Purpose	Dissemination of DOGANA project
Target	Students in IT field
Means	Presentation at universities

-

Goal #1 AIT	
Purpose	Spreading Scientific Excellence
Target(s)	Scientific conferences: a) CHI – Conference on Human Factors in Computing Systems b) CSCW – Conference on Social and Collaborative Work c) CHI PLAY – Conference on Human Factors in Play d) SOUPS – Symposium on Usable Privacy and Security e) Persuasive Technology conference Scientific journals: a) Computers in Human Behavior b) International Journal of Human-Computer Studies
Means	Publication of research papers **Organization of workshops**

-

Goal #2 AIT	
Purpose	Dissemination of the DOGANA brand
Target(s)	National and international (business) events)
Means	Talks or demonstrations about/of DOGANA or DOGANA-related activities

-

Goal #1 KU LEUVEN	**GA PHASE** In this phase, KUL contributes to the dissemination of the DOGANA project by raising awareness for the topic of social engineering and by promoting the project itself at high-level workshops and conferences.
Purpose	Dissemination of the DOGANA brand by raising awareness in the cybersecurity landscape
Target	Industry
Means	Organisation of and participation in high-level workshops and conferences: - e-ID conference, Marseille - ICT2015, Lisbon

-

Goal #2 KU LEUVEN	**GA PHASE**
Purpose	Dissemination of the DOGANA brand by raising awareness in the legal academic landscape
Target	Academics
Means	Organisation of and participation in high-levels workshops and conferences: - Gikii 2016: with this conference an interesting legal academic audience is reached in an innovative manner. Besides academics, the conference also attracts journalists (success: cfr article in The Technologist by Michael Brooks “The rise of the geek lawyers”)

-

Goal #3 KU LEUVEN	**GA PHASE**
Purpose	Dissemination of the DOGANA brand by raising awareness of future employees
Target	Students
Means	Courses at the law and computer science faculties of the KU Leuven: - ICT Bachelor seminar, - ICT Law for computer science and law students, - ICT Law courses in the department's LLM program.

-

Goal #4 KU LEUVEN	**MA PHASE** In this phase, the role of KUL is primarily aimed at providing contextual support for the consortium to undertake activities to create market potential. Hence, KUL's dissemination activities in this phase do not have a direct impact on the market potential of DOGANA, but contribute to the contextual background for the DOGANA framework by spreading scientific excellence towards the broader society.
Purpose	Spreading scientific excellence towards peers
Target	Academics
Means	Academic publications in scientific journals: - Targeted journal: Computer, Law and Security Review (Elsevier) The academic publications will be disseminated through the CITIP KUL and iMINDS network

-

Goal #5 KU LEUVEN	**MA PHASE**
Purpose	Spreading scientific excellence towards future employees

Target	Bachelor and master students
Means	Courses (see above)

-

Goal #6 KU LEUVEN	**OS PHASE** In the third phase, KUL will mainly contribute by the publication of a white paper and by continuously raising awareness of future employees.
Purpose	Spreading scientific excellence towards the broader society
Target	Policy-makers
Means	D5.5 'Legal and ethical recommendations' will be made publicly available in the form of a white paper or similar document. This paper will be made available through the project's website and distributed through the CITIP KUL network and proposed to the Belgian National Data Protection Authority.

-

Goal #7 KU LEUVEN	**OS PHASE**
Purpose	Spreading scientific excellence towards future employees
Target	Bachelor and master students
Means	Courses (see above)

-

Goal #1 ELTA	
Purpose	Increase visibility of DOGANA as well as awareness of Social Engineering in our internal (company) environment
Target	IAI employees

Means	• Include articles on DOGANA and Social Engineering in our internal corporate newsletter • Meet with company employees involved in marketing and public relations to emphasize the importance of Social Engineering and DOGANA. • Include information on the threats of Social Engineering and the benefits of DOGANA on our internal corporate website. • Offer courses on Social engineering to our employees.

-

Goal #2 ELTA	
Purpose	Increase visibility of DOGANA as well as the threats of Social Engineering in the public domain.
Target	General Public
Means	• Include articles on DOGANA and Social Engineering in periodic newsletters on IAI that are published for the general public. • Include information on DOGANA and Social Engineering on our external website – accessible to the general public. • Press Releases. • Include mention of DOGANA in news media and magazine articles that relate to our company's activities • Include Social Engineering awareness as part of voluntary courses which are given by our employees to local schools.

-

Goal #3 ELTA	
Purpose	Increase visibility of DOGANA among IT and Cyber professionals.
Target	IT and Cyber Professionals.

Means	• Include information on DOGANA as part of our presentations at several Cyber conferences and workshops such as: ◦ Europol-Interpol Cybercrime Conference (organized by Interpol Global Centre for Innovation – IGCI) ◦ AOC Conference (Association of Information and Electronic Warfare) ◦ ABS-MAS Technology Risk Seminar • Include awareness of DOGANA at meetings, events as well as in publications of Cyber Security organizations of which we are members.

-

Goal #1 PROPRS	
Purpose	To disseminate the DOGANA framework to the insurance industries with particular emphasis on the risk assessment methodologies and tools
Target	Insurance industries
Means	Workshop with insurance stakeholders

-

Goal #2 PROPRS	
Purpose	Identify novel approaches for SE2.0 attacks
Target	Industry
Means	SE hacker contest: to use one of the DOGANA users as target for an attack generated by the hackers participating to the context.

Table 4 – FF Block Actions

7.1.2. Dissemination of the DOGANA Toolchain

Goal #1 ENG	
Purpose	Increasing the visibility of the DOGANA Toolchain and project's results
Target	Disseminating DOGANA Toolchain and results through the Cyber Connector community, populated by the DOGANA members as well as by the already existing communities: CYSPA: 27 Organisations operating with more than 60 individual users ACDC: 70 Organisations operating with 150 users actively involved COURAGE: 16 Organizations operating with 28 individual users
Means	References to the DOGANA Toolchain will be included in the Cyber Connector portal, reaching out several communities operating in the cyber security area. Specifically, already existing community will provide DOGANA with an initial dissemination audience, made of stakeholders actively involved in the context of cyber security. Such initiatives are ACDC at http://www.acdc-project.eu CYSPA at http://www.cyspa.eu COURAGE at https://www.courage-project.eu

-

Goal #1 VISIONWARE	
Purpose	Increasing the visibility of the DOGANA Toolchain and project's results
Target	Portuguese end users, which are a target to social engineering attacks.
Means	VisionWare will actively search for end users where the DOGANA Toolchain can be implemented to reduce the risk from social engineering attacks.

-

Goal #2 VISIONWARE	
Purpose	Increasing the visibility of the DOGANA Toolchain and project's results
Target	Portuguese cybersecurity community
Means	Workshops and presentations of the project's results.

-

Goal #1 RATB	
Purpose	Raise awareness
Target	RATB IT specialist RATB employees Local Authority IT Department
Means	Local meetings E-mails

-

Goal #1 INOV	
Purpose	Dissemination of DOGANA tools
Target	Portuguese CSIRTs
Means	Presentation in the Portuguese CSIRT network

-

Goal #2 INOV	
Purpose	Dissemination of DOGANA tools
Target	Students in IT field
Means	Presentation at universities

-

Goal #1 ELTA	
Purpose	Increase awareness and visibility of the DOGANA Toolchain globally – with the ultimate goal of increased adoption of the toolchain
Target	IAI's customers and potential customers
Means	• Include information on the DOGANA toolchain in our marketing presentations to potential customers • Incorporate aspects of the DOGANA toolchain into our product offerings • Discuss the possibility of adoption of aspects of the DOGANA toolchain in our own corporate environment

Table 5 – DT Block Actions

7.1.3. Disseminating the outcomes of the field trials.

Goal #1 VISIONWARE	
Purpose	Increase the visibility of the DOGANA practical results
Target	Organizations similar to those used in the field trials
Means	Case studies and presentations to the prospective users.

-

Goal #2 VISIONWARE	
Purpose	Detect social engineering vulnerabilities in high value targets
Target	Organizations which are high value targets for social engineering attacks – public administration, finance sectors
Means	Propose a "free scan" as a means to identify volunteer organizations where the effectiveness of the DOGANA framework can be displayed and in turn the early detection of high value and high vulnerability targets can be identified.

-

Goal #1 RATB	
Purpose	Raise awareness
Target	RATB employees Public transport professionals – local, regional, national and European level Local Authority
Means	RATB newsletters Training courses Workshops Local meetings E-mails

-

Goal #2 RATB	
Purpose	Improve internal operating procedures
Target	RATB management and employees
Means	Internal meetings

-

Goal #1 INOV	
Purpose	Contribute to on-going research
Target	Scientific community
Means	Articles in conferences or journals

-

Goal #1 ELTA	
Purpose	Increase effectiveness of the defence against social engineering cyber attacks at our local company level
Target	IT professionals at IAI
Means	• A series of meetings and discussions with IT and Cyber professionals at IAI at which the results of the field trials

	are presented and the lessons learned are presented and discussed.

-

Goal #2 ELTA	
Purpose	Increase global awareness regarding the validation of the DOGANA toolchain in field trials
Target	IAI worldwide customers
Means	• Include, in our marketing presentations worldwide, information regarding the field trials, their results, and lessons learned. • Include information on the field trials as part of our presentations at talks given at conferences and meeting

Table 6 – FT Block Actions

8. References

[1] DOGANA Annex I – Description of Work (DoW)

[2] DOGANA Deliverable 8.2 - Project Website and Social Networking accounts

[3] European Commission, Communicating EU Research & Innovation – A guide for project participants, Luxembourg: Publications Office of the European Union, 2012, ISBN 978-92-79-25639-4, doi:10.2777/7985