SHIELD

SECURING AGAINST INTRUDERS AND OTHER THREATS
THROUGH A NFV-ENABLED ENVIRONMENT

[H2020 - Grant Agreement No. 700199]

Deliverable D6.1

Project Dissemination and Communication Plan

Editor A. Lioy (Politecnico di Torino)

Contributors M. Terranova (AgID), L. Jacquin (HPE), B. Gastón (I2CAT), D. Katsianis (INCITES), A. Litke (INFILI), E. Trouva (NCSRD), N. Davri (ORION), G. Gardikis (SPH), A. Pastor (TID), R. Preto (UBI)

Version 1.0

Date February 28th, 2017

Distribution PUBLIC (PU)











Executive Summary

The dissemination and communication actions of SHIELD will target at the following groups:

- network operators and managers, in order to help them understand the additional capabilities offered by SHIELD with respect to a standard NFV deployment;
- security designers and managers, in order to help them value how SHIELD improves the security of a network infrastructure and supports the cybersecurity of an ICT system;
- the academic and industrial R&D community interested in/dealing with cybersecurity, networking, and big data, to make them aware of SHIELD results;
- general public, to let them know the progress accomplished by SHIELD with respect to the general cybersecurity problem.

The foreseen channels include quick availability of the project deliverables on the web, publishing the project results on major journals and magazines, information spreading via various social, media (LinkedIn and Twitter), and participation to industrial fairs and EC concertation events. Last but not least, the project will organize two focussed events: a summer school for academic and industrial researchers, and a workshop for the industrial sectors that could exploit the project's results.

Table of Contents

1. INTRODUCTION

This document outlines the dissemination and communication plan of SHIELD, emphasising on the general approach as well as the individual plans of the partners.

This document is strictly related to WP6 and does not have any reference or dependency on other project's deliverables, but the actions described here have of certainly various dependencies upon the projects results.

The rest of this document is organized as follows: Section 2 describes the general approach of the project regarding the dissemination and communication while Section 3 contains the plans of each partner. Finally Section 4 contains some brief conclusions.

2. OVERALL DISSEMINATION AND COMMUNICATION PLAN

This section describes the overall plan, later detailed in the next section as individual plans of the various partners.

2.1. Target groups and key messages

The dissemination and communication actions of SHIELD will target to the following groups:

- network operators and managers, to help them understand the additional capabilities offered by SHIELD with respect to a standard NFV deployment;
- security designers and managers, to help them value how SHIELD can improve the security of the network infrastructure and provide additional detection and reaction capabilities;
- the academic and industrial R&D community interested in/dealing with cybersecurity (especially network-based security), networking (especially NFV), and big data (especially for attack detection), to make them aware of the SHIELD results and to potentially incorporate them as part of more a complex/complete solution or product;
- general public, to let them know the progress accomplished by SHIELD with respect to improved security features of modern networks and how they can contribute to the overall security of an ICT infrastructure.

2.2. Channels

The project aims to achieve its dissemination and communication objectives by appropriately using a mixture of channels.

Public deliverables will be available on the project web site and will serve as the official documentation for the project achievements. As public items, they will be indexed by the search engines and therefore appear in searches related to the project objectives.

Major relevant results that interest the scientific and industrial communities will be published as papers in conferences, journals, and magazines, hence reaching out people involved in R&D for security, networking, and cloud computing. The consortium will follow an open access self-archiving policy via its web site for accepted papers.

The project will also use various social media channels to disseminate information about the project's publications (both deliverables and papers) and public presentations. Social media will also be used for discussions and to stir interest in the fields targeted by SHIELD. The following channels have already been activated:

- the web site https://www.shield-h2020.eu/

Figure 1. Home page of the SHIELD web site.

- the LinkedIn page https://www.linkedin.com/company/shield-eu-project
- the Twitter account https://twitter.com/shield_h2020

Moreover, SHIELD will engage the general audience through newsletters that will be used to announce the project, give regular updates and develop and promote the profile of the project. The newsletters will be periodic and utilize the social media channels in order to promote the achievements of SHIELD.

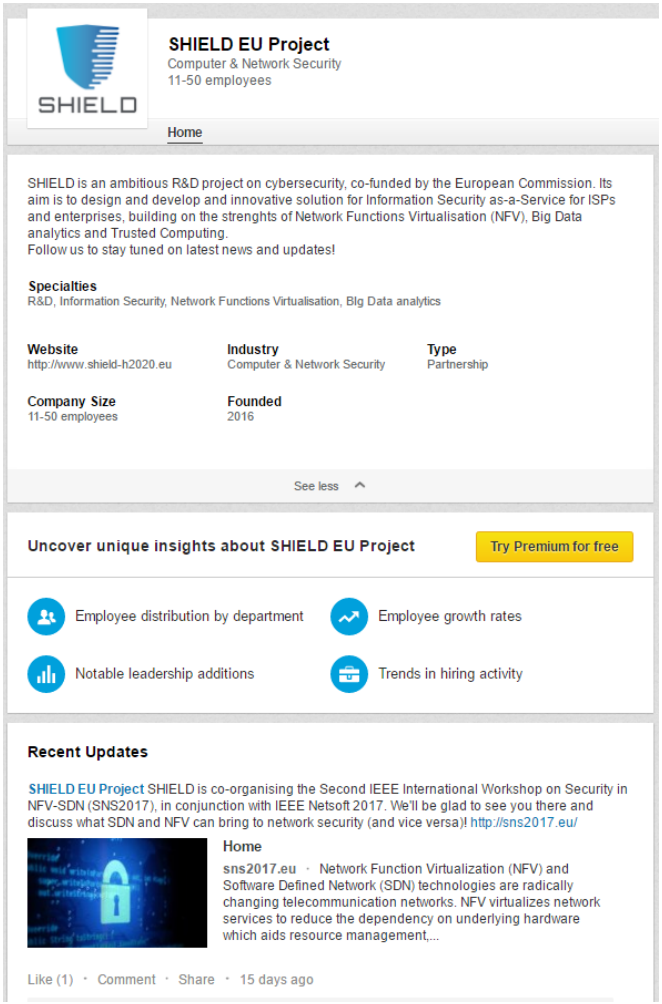

Figure 2. The LinkedIn page of SHIELD.

Figure 3. Twitter account of SHIELD

SHIELD will participate to the **concertation activities** organized by the EC, in order to keep links with other EC-funded projects and explore possible synergies.

In-presence channels will include not only participation (with presentations and booths) to major scientific and industrial events (such as the ICT series of events organized by the EC, as well as other major industrial fairs) but especially two events organized for the project itself:

- one **summer school** (for the academic and research community), and
- a final **workshop** (aiming to the industrial world).

The summer school will present the results of SHIELD with reference to the bigger framework of advanced networking and cybersecurity, while the workshop will focus more on the practical results of the project in terms of service offer and reusable components.

The current program of the summer school includes the state-of-the-art and the advances generated by SHIELD in the following fields:

- hardware-based attestation of the software integrity of a network node;
- virtual security functions and their orchestration;

- use of big data analytics for detection and reaction to threats.
- the digital security market.

We foresee also the organization of hands-on sessions, to allow participants to test the platform developed in SHIELD. In order to promote the participation to the school, we will offer the option to participate in a final evaluation, which may be of interest for those students that need ECTS credits for their respective universities.

In order to evaluate the success of each dissemination action, a brief report is going to be prepared after each such event (e.g., conference, exhibition, workshop, etc.) by the leading partner of the activity. This brief report will include the key messages conveyed to the target audience and most importantly the feedback received. In this way SHIELD is going to document and assess the success of the dissemination activities. All this information is going to be included in the dissemination/communication report (as part of the project periodic reports)

The following **KPIs** (from the DoW), related to the dissemination/communication campaign, are confirmed:

Table 1. SHIELD KPIs

Activity	*Description*	*Target group*	*KPI*	*Success indicator*
industry-related publications	publication of white papers, technology roadmaps, articles on magazines, and industry-led journals	industry	no. of publications	>= 5
scientific publications	publication of scientific results to leading journals and conferences	scientific community	no. of publications	>= 3
workshops, symposia, training events	organization of industry-focused events to disseminate information and results of the project	industry	no. of events	>= 1
EU events	Talk about the SHIELD results and innovation	industry and R&D community	no. of presentations	>= 1

3. INDIVIDUAL PLANS OF THE PROJECT PARTNERS

This section describes the initial dissemination and communication plans of each partner and how they are aligned with the general plan for the first (2016/09-2017/08) and the second (2017/09-2019/02) period of the project.

3.1. AgID

The Agency for Digital Italy is in charge of the development and the exploitation of digital technologies within the Italian public administration, mainly for the delivery of digital services to citizens and business.

AgID is committed to the development of the Italian Digital Agenda and the modernization of public administration. The Agency supervises the ICT projects developed by the public administrations and the services that they deliver to citizens and businesses. The Agency directly manages some particularly important projects and monitors the main ICT services that are provided to the public administrations. For this reason, it maintains ongoing relationships with leading ICT vendors and providers operating in Italy.

3.1.1. Target audience and channels

According to its role, the AgID dissemination plan aims to spread the knowledge on the network security technologies developed by the project within the Italian public administrations and their providers.

AgID organizes regular meetings with the CIOs of central and local public administrations. These meetings will be the main dissemination channel for the project achievements and results.

On the other hand, AgID, with the CERT-PA (the Italian Computer Emergency Response Team for the Public Administration), regularly participates to major events on cyber security that are organized in Italy, e.g. ICT Security Forum, Cyber Crime Conference, Security Summit, Cybersec Summit. On such occasions, the main results of the project will be presented to the Italian cyber community.

3.1.2. Plan

In October 2017, AgID will present the status of the project at the end of the first period at the Forum ICT Security 2017. A more extensive presentation will be inserted in the CLUSIT security report 2017 (CLUSIT is an Italian association of OIT security experts).

At the end of the project, AgID will organize a general meeting, with the CIOs of both the public administrations and the providers, to present results and products in a detailed and complete way.

3.2. HPELB

3.2.1. Target audience and channels

Hewlett Packard Labs (HPELB) is the research branch of Hewlett Packard Enterprise (HPE): its charter is to research new technologies, prototype them and then transfer them to the different business units responsible for developing the customer products. Thus, the main targets for HPELB dissemination and communication are:

- the different business units of HPE, particularly the ones responsible for NFV and networking equipment and services.
- the different industries relevant to SHIELD, particularly NFV and network;
- cyber-security community, such as government-led forum with major companies;
- the NFV and network security research communities.

HPELB plans to present SHIELD through different channel such as:

- TechCon, the HPE company-wide technologist conference, which is held every year;
- direct presentation to the relevant HPE chief technologist offices for internal dissemination and through them potentially reaching out to selected customers – such as ISPs and mobile providers;
- presentation at industry consortia, such as ETSI NFV, IETF/IRTF, TCG;
- publication in research conferences and journals such as IEEE SDN-NFV, IEEE NetSoft, ACM SDN-NFV Security, IEEE S&P, Usenix Security, Usenix NSDI, C&ESAR.

3.2.2. Plan

During the first period, HPELB plans to raise awareness in the different communities around the SHIELD concepts and overall architecture, for example:

- Publication and presentation at C&ESAR (conference organized by the French Ministry of Defence, focusing on security).
- Internal presentation to chief technologists.
- Publication of a chapter in the book “Guide to Security in SDN and NFV: Challenges, Opportunities and Applications”.
- Edition of the book “Guide to Security in SDN and NFV: Challenges, Opportunities and Applications” to raise awareness of security of SDN and NFV in general.

In the second period, HPELB will focus its dissemination and communication towards presenting the results of the project and reach out to the different communities and demonstrate the prototype, especially in the relevant consortium such as ETSI NFV.

Depending on the early feedback from the business units and chief technologists, HPELB may also demonstrate to selected customer and internally to the business units.

3.3. I2CAT

i2CAT, as a research and innovation centre, aims to fill the gap between the research and the industrial worlds. i2CAT is an active player in the innovation forums like the Big Data Value Association (BDVA) and the 5G-PPP. i2CAT has direct interaction with the market, through its Business Units, in the fields of Industry 4.0, Smarticities & IoT and iHealth.

During the last years i2CAT has moved from the triple Helix to the quadruple Helix model; embracing the Open Innovation approach while exploiting the outcomes from R&D initiatives. Hence, i2CAT organizes several hackathons, ideathons, co-creation activities and other kind of knowledge-transferring events like summer schools, workshops, hands-on or specific conferences.

3.3.1. Target audience and channels

The KPIs to measure the dissemination activities of i2CAT comprehend two periods: the first year of the project, where the SHIELD vision is explained; and the last year and a half, where the results of the project will be disseminated.

Table 2. Objective and Target Audience (I2CAT)

Period	*Objective*	*Target audience*
09/2016 – 08/2017	Present SHIELD in the telco subgroup of the BDVA	Industrial community
	Publication of SHIELD results in a whitepaper about Big Data	European innovation ecosystem
	Participation in a book chapter publication	Scientific & Industrial community
	Present the project expectations to CESICAT (Catalan cybersecurity agency)	Industrial community
09/2017 – 02/2019	Organization of one summer school	Academic community
	Participation in three publications	Scientific community
	Presentation in an industrial conference like the MWC	Industrial community
	Present the results to CESICAT	Industrial community
	Alignment and collaboration with other projects (CHARISMA, SONATA)	Scientific community

3.3.2. Plan

During the first period, the dissemination plan of i2CAT is to promote the awareness of the industrial, innovation and scientific community about the SHIELD vision and expected advances. To this end, i2CAT will:

- be in direct contact with CESICAT, the Catalan cybersecurity agency, under the department of ICT of the Catalan government
- present the results in the Big Data Value Association (PPP of Big Data), where i2CAT is actively collaborating;
- participate in two publications: a book chapter dedicated to SHIELD, to promote its vision among the SDN community, and publishing the results of SHIELD as part of the whitepaper that I2CAT will elaborate around the topic of Big Data, to be published on September 2017.

During the second period, more dissemination activity is expected. i2CAT will:

- co-organize a summer school that aims to involve university students as well as academic and industrial researchers;
- schedule periodical meetings with CESICAT agency to present the latest outcomes of SHIELD;
- participate in at least three publications during this period;
- present in a big industrial event like the Mobile World Congress (MWC), where i2CAT is a usual presenter as part of the Catalan innovation booth organized by the Catalan Government;
- communicate development and results from the SHIELD project to projects like CHARISMA and SONATA, where i2CAT coordinates and collaborates; and identify susceptible outcomes for integration.

3.4. INCITES

3.4.1. Target audience and channels

INCITES Consulting SARL is the WP6 Leader therefore will lead and work in the exploitation, dissemination and standardisation activities within the work package.

The dissemination of the results from INCITES will be clear and simple, expressed in language understandable by its target audience:

- business actors,
- regulators,
- government agencies,
- telecommunications providers and associations
- Researchers in telecommunications systems and techno-economics.

The goal is to address possible market adopters and stakeholders but also to detect and attract new stakeholders. INCITES will be involved in various dissemination activities such as participating in relevant conferences and networking events including the publication of dissemination material addressing its target audience.

INCITES plans to present SHIELD through different channel such as:

- Conference of Telecommunication, Media and Internet Techno-Economics (CTTE), specialized conference in techno economics, which takes place every two years;
- EC newsletter on “Cybersecurity and digital privacy”;
- Summer school organised by SHIELD;
- Fair exhibitions or other industrial relevant events;
- Publication in relevant research conferences and journals.

3.4.2. Plan

Analytically, INCITES will contribute to the newsletter of the project especially when it comes to the surveys topics, business modelling, road mapping and the techno-economic results. (First P1 and second P2 period)

INCITES will also contribute to the EC newsletter on “Cybersecurity and digital privacy”. (P1 and P2)

INCITES will prepare a course for techno economic activities to be used in SHIELD’s summer school emphasizing on the proposed technologies within the project. The course will be available online, to enable future free online courses in order to minimize costs. INCITES will participate to the SHIELD workshop and summer school and will act as a contributor. In addition INCITES will act as a TPC in scientific activities organised by SHIELD (P2)

INCITES will contribute to the dissemination of SHIELD achievements through workshops, conferences such as the CTTE (Conference of Telecommunication, Media and Internet Techno-Economics) conference and our publications (INCITES Consulting SARL newsletter and mailing list). In addition, the publication and the presentation in conferences co-organized by the EC are of the main interests of INCITES. (P1 and P2)

INCITES will participate and support to fair exhibitions or other industrial relevant events in order to promote product dissemination on behalf of SHIELD. (P2)

INCITES is willing to announce the main results of SHIELD project through its website as well as its accounts on Facebook and LinkedIn. INCITES will also be the administrator of SHIELD’s Twitter account. (P1 and P2)

INCITES will create multimedia material for specific audiences described in the research objectives, challenges, tangible results and benefits. (P2)

In addition, INCITES will actively contribute to the creation of scientific papers and publications in international Journals and Magazines like IEEE magazines and Elsevier Journals (mainly on Telecommunication Policy or Telematics and Informatics) concerning the business prospects and techno-economic results from the project. (P1 and P2)

3.5. INFILI

INFILI, as a private company, will undertake dissemination activities towards potential early adopters and commercial legal entities, so that it establishes communication channels mainly with the industry. INFILI will be involved in various dissemination activities such as participating

in exhibitions, fairs and large conferences with industrial outreach. INFILI plans also to be involved in dissemination activities such as creation of technical whitepapers and jointly co-authored publications in prestigious international journals, books and magazines.

3.5.1. Target audience and channels

The following table gives an overview of INFILI's dissemination and communication strategy with respect to the target audience.

Table 3. Objective and Target Audience (INFILI)

Dissemination channel	Dissemination item	Target audience	Estimated Benefits
Scientific Journals, magazines & Conferences *(mainly in the area of cybersecurity and big data analytics)*	Scientific and technical results	Scientific & Research community, Early adopters from the industry.	Greater visibility of results, scientific citations, disseminating of knowledge
Press releases (in newspapers, technical press, and TV)	Major exploitable results of the project	Public audience, Policy makers.	Strengthening public relations and trust with the industry and policy makers.
Exhibitions, For a	Overview of the technical attributes of the SHIELD system	Technical audience, Early adopters	New market opportunities, Meetings with decision makers from the ISP industry.
Communication activities to Public Authorities and other industry stakeholders	Exploitable results	Industry and Public Authorities as potential clients	New opportunities for exploitation.

The project results will also be presented in form of papers and presentations in various conferences and industrial/commercial exhibitions with the purpose of commercial exploitation in the international market. To further amplify the potential of the initiative the following options will be considered: (i) joint organization with other relevant EU projects, (ii) co-hosting in the framework of other well-established events, (iii) organization of a dialogue session with organizations of the private/public sector. Below are some key events that the INFILI plans to monitor and possibly participate during the lifecycle of the project.

Table 4. Targeted events and exhibitions

Name of event/exhibition	URL
INTERPOL World 2016	https://www.interpol-world.com/safe-cities
Safe and Smart Cities Conference	http://safeandsmartcities.com/
IFSEC International	http://www.ifsec.co.uk/?cid=globaleventtab
Secured Cities	http://securedcities.com/
Munich Security Conference	https://www.securityconference.de/

International Conference on Availability, Reliability and Security (ARES)	http://www.ares-conference.eu/conference/
Berlin Security Conference	http://www.european-defence.com/Home/
The IEEE International Conference on Multimedia & Expo (ICME)	http://www.ieee-icme.org/sc/upcoming_conference.php

3.5.2. Plan

Within the immediate plans is the participation of INFILI in some major international events. INFILI plans to attend the following two events and present the project through conference publications:

- For the first period International Conference on Cryptography, Cyber-Security, and Information Warfare (3rd CryCybIW) – Hellenic Military Academy (May 2017). The specific event attracts an international community from stakeholders in the Cryptography and Cybersecurity domain. Among others, the participants include reputable researchers, public authorities and Law Enforcement personnel.
- For the second period: 2017's International Conference: Next Generation Community Policing: a major dissemination and scientific event under the FCT-14 clustering action. The Conference will take place in the last week of October, between 25th – 26th and the 27th of October (as the Demo Day). The conference concentrates in the best practice procedures that law enforcement agencies and communities can adopt in order to promote effective community policing guiding the developments and to the use of social media technologies aiming to increase the security level of citizens in large cities. The Conference will include keynote speakers, experts in community policing from the EU and overseas (USA, Canada, S. America), as well as the EU officials and high-ranking LEAs officers. The specific event is very relevant to SHIELD as law enforcement agencies experts in the field of cybersecurity attend the event and INFILI will have a chance to present the interim results and concept of the project while getting insights of the user requirements.

Especially, for the second period INFILI will mainly strengthen its focus its on dissemination activities in joint journal publications and participation in events such as the ones described in the table above.

3.6. NCSRD

3.6.1. Target audience and channels

Being a research centre, NCSRD's main dissemination and communication target audience of the projects' results is the research community, encompassing the scientists with similar interests to the SHIELD research topics, with special interest in enhancing security using NFV and SDN technologies. However, the communication of the projects' results and distribution of information will aim at a wider audience, the broader scientific R&D community and the European/world Industry, who are interested and will benefit from the project's outcomes.

3.6.2. Plan

During the first period of the project, the planned dissemination activities of NCSRD aim to foster collaboration opportunities, exchange knowledge, and raise awareness of SHIELD's research areas. Specifically, NCSRD will be involved in the following dissemination and communication activities:

- Co-organisation of the Second International Workshop on Security in NFV-SDN (SNS2017[1]) in conjunction with the 3rd IEEE Conference on Network Softwarization (IEEE NetSoft 2017[2]). The workshop is related to security in SDN and NFV and is co-organized by SHIELD, CHARISMA, 5G-ESNURE projects and security experts from University of Derby.
- Co-authoring of a book chapter that presents SHIELD's vision for the book "Guide to Security in SDN and NFV – Challenges, Opportunities, and Applications" (GSSNOA2016[3]). The aim of the book is to explore various security challenges and benefits of NFV and SDN and provide novel methods and approaches to assure security in NFV and SDN-based networks.
- Participation to events organized by the EC, such as the European Conference on Communications and Networks (EuCNC[4]) and clustering events for better dissemination across EU activities and other EU funded projects with similar research interests.
- Establishment of links with other projects that investigate similar research topics, such as CHARISMA 5G project, in which NCSRD is contributing.

Dissemination activities will intensify during the second period of the project, since it is expected that the project will have achieved more mature results than in the first phase. Tangible technical results are expected to be available, which will offer a better ground basis for a wider dissemination of SHIELD in the scientific community, as well as in the industry. During the second year of SHIELD, NCSRD will:

- Seek to publish project results in the NFV and SDN domains in high-quality conferences and international scientific journals and present the project outcomes at a major academic conference, discussing the project ideas and results with the academic and industrial community attending the event. Possible targets for publication are the IEEE Conference on Network Function Virtualization & Software Defined Networks (IEEE SDN-NFV), the European Conference on Networks and Communications (EuCNC), the IEEE Network of the Future (IEEE NoF) and the IEEE INFOCOM Workshop on Software-Driven Flexible and Agile Networking (IEEE SWFAN).
- Participate in a major ICT-related event, such as the European Future Internet Assembly (FIA) or the European Conference on Communications and Networks (EuCNC), to increase the collaboration with other European Commission funded projects with common interests to those of the SHIELD project.
- Participate in working groups related to SDN/NFV (e.g. the 5G-PPP Software Networks WG) and exchange of technical knowledge, experiences and know-how on topics related to SDN/NFV implementation and experimentation.

[1] http://sns2017.eu/
[2] http://sites.ieee.org/netsoft/
[3] http://computing.derby.ac.uk/gssnoa2016/index.html
[4] http://www.eucnc.eu/

- Aim at disseminating SHIELD results in the form of demonstrations and raise awareness about the key outputs and planned activities of the project among a large group of stakeholders and players, including actors from the research community, the industry and SMEs.

Additionally, the development efforts of NCSRD will be become available to the Open Source community, actively supporting new contributions and developments, exceeding the SHIELD project duration.

3.7. ORION

3.7.1. Target audience and channels

ORION will incorporate the results regarding cybersecurity into its commercial and research activities, thus providing the results to its customers. ORION regularly publishes results as contributions in relevant journals and on conferences. Furthermore, results from the project will be incorporated into research efforts and published in form of studies and white papers directly by the company. Awareness for cybersecurity issues as well as for possible solutions can thereby be disseminated through an efficient path.

Table 5. Objective and Target Audience (ORION)

Type of Activity	Target audience	Description
SHIELD project awareness and scientific knowledge transfer	Scientific research and development community	Participation or organization of scientific events, conferences and workshops.
Exhibitions/other events	Industry	Participation to industry interest groups, venues, associations.
Promotion of SHIELD through ORION's website/Social Media accounts	Public audience	Foster project activities and raise awareness of SHIELD among specialized users.

ORION plans to present SHIELD through various channels:

- publication to scientific journals with high impact factor that will comprise submission targets for SHIELD architecture and results (IEEE Transactions on Cloud Computing, IEEE Transactions on Network and Service Management, Computer Networks Elsevier);
- publication of SHIELD results to international conferences (IEEE GLOBECOM, IEEE ICC, ACM CONEXT);
- demonstration of project concepts and findings during events like EUCNC or other relevant conferences (e.g. the ENISA Security Conference).

3.7.2. Plan

During the first period of SHIELD, ORION has been involved in the book chapter "Guide to Security in SDN and NFV: Challenges, Opportunities and Applications" GSSNOA2016. Within the immediate plans is the participation of ORION in the following major international events:

- Cloud Security Expo 2017
- DataCloud Europe 2017
- NetSoft 2017

In the second period of the project, more tangible technical results are expected to be available, which will offer a better ground basis for a wider dissemination of SHIELD in the industry, as well as in the scientific community.

Some of the targeted events are:

- SDN NFV World Congress 2017
- Cloud &DevOps World 2017

3.8. POLITO

3.8.1. Target audience and channels

The target audience for POLITO's dissemination activities is threefold:

- the scientific community (especially that concerned with cybersecurity and networking) for sharing the knowledge about the innovation generated in SHIELD
- the ICT industry (cloud, service, and network providers) as potential adopters of the SHIELD technologies likely with the support of POLITO as a consultant
- the Public Administration and SMEs as the major potential users of the SHIELD services.

To reach this multifaceted audience, POLITO will mainly use three kinds of channel:

- scientific publications to journals, magazines, and conferences (such as those published or organized from IEEE, ACM, and IFIP);
- direct contact at events such as industrial fairs and roundtables;
- electronic media (mainly the web) to disseminate public information about the project's progress.

3.8.2. Plan

POLITO developed the web site of the project, and will maintain it, regularly publishing news and updates (e.g. public deliverables, papers, and presentations).

Throughout the project, based on the progress and achievements, POLITO will seek suitable venues for publishing the scientific results of the project, with special emphasis on the security of the infrastructure as this is the major area of expertise for POLITO.

In the second period of the project, POLITO will be the scientific organizer of the SHIELD summer school, taking care of the global organization, plan of the lectures and hands-on sessions, and final evaluation (for those participants that need it for their curriculum).

3.9. SPH

3.9.1. Target audience and channels

The dissemination and communication activities of Space Hellas will be focused both on the SHIELD system as a whole as well as the subsystem to which SPH is particularly contributing, i.e. the DARE platform. The audiences to be targeted are both from the technical/scientific domain (R&D communities and individuals in the fields of networking and security) as well as from the commercial domain – mostly big enterprises from the banking, industry and telco sector who will be candidate users for the SHIELD results.

3.9.2. Plan

During the first period of the project, SPH will mostly aim at communicating the project endeavour in its whole and "spread the word" about the SHIELD scope and results to all relevant audiences. This will be achieved via:

- the co-organisation of a targeted workshop for security in/through NFV, in conjunction with the 3rd IEEE Conference on Network Softwarization (NetSoft 2017, http://sites.ieee.org/netsoft/). The workshop is titled "Second IEEE International Workshop on Security in NFV-SDN" (http://www.sns2017.eu/) and will be co-organised by SHIELD and other relevant projects dealing with security in software-based networks.
- a featured relevant article in the corporate printed newsletter ("SPACETalk") which is released annually and distributed by mail or courier to hundreds of company customers and partners;
- the project LinkedIn account (https://www.linkedin.com/company/shield-eu-project) which SPH is maintaining and will publish latest news of interest to the professional community.

During the second period, SPH will mostly focus on disseminating the project results, which by then will have become more tangible and mature enough. Special attention will be paid to the DARE platform, which is of high commercial interest to SPH. In this context, specific dissemination actions will be closely related to the company's exploitation plan for SHIELD. Overall, dissemination targets will include:

- Papers in acclaimed scientific conferences, such as IEEE International Conference on Communications (IEEE ICC), European Conference on Communications and Networks (EuCNC), IEEE Symposium on Computer and Communications (IEEE ISCC), IEEE Conference on Network Function Virtualization and Software Defined Networks (IEEE NFV-SDN)
- A paper in a selected journal or magazine, such as IEEE Communications Magazine
- Demos in national and international exhibitions to which SPH participates. The plans include:
    - a demo in EuCNC, to raise awareness in the European research community
    - a demo in a Cisco Live! Global event (SPH is a Cisco Gold Certified partner) - http://www.ciscolive.com/global/

- a demo in the Infocom Security conference (major national event on information security) - http://www.infocomsecurity.gr/

3.10. TID

3.10.1. Target audience and channels

TID, as the branch of the Telefónica Group dedicated to innovation and strategic vision, will share the SHIELD research results in network security technologies to different areas and companies within the Telefónica Group. The following list shows some examples of the most relevant target areas:

- technical areas of Telefónica in Europe (Spain, Germany, and the UK) and in Latin America (all countries within the Telefónica footprint);
- OSS/BSS security units;
- security service units and companies;
- GCTO Councils in the Network Virtualisation and Security areas;
- internal security knowledge communities in the Telefónica Group.

In addition, TID will raise awareness about SHIELD results among the Telefónica provider ecosystem (telco equipment vendors, system integrators, etc.) and selected customers, including those acting as wholesale service brokers

Finally, with relation to the general public, and customers outside of the technical knowledge of the project, TID will promote SHIELD with several publication activities in corporate magazines, blogs[5], and social media.

TID regularly participates to industry events related with virtualization technologies and security, and has the aim to represent SHIELD at venues such as the Layer123 SDN & NFV World Congress, or the MPLS + SDN + NFV World Congress.

TID will actively build awareness about SHIELD services and technology in bodies and PPPs where Telefónica is present, such as the 5GPPP[6] or the cPPP[7]. This will be achieved by meeting participation and formal presentations there, information sharing, or direct discussions.

3.10.2. Plan

In the first period of the project TID will focus in identifying synergies with new cPPP activities and projects, and creating awareness in internal Business units and enterprise clients.

Also, collaboration will be promoted with different projects of the 5GPPP. TID is a relevant industrial partner in 5G infrastructure research, especially in areas related to enabling technologies such as NFV, SDN, machine Learning. As an example, in the COGNET[8] project TID

[5] http://blogthinkbig.com/
[6] The 5G Infrastructure Public Private Partnership. https://5g-ppp.eu/
[7] Cybersecurity Public Private Partnership. https://www.ecs-org.eu/cppp
[8] http://www.cognet.5g-ppp.eu/

is involved in security-related activities, and their results could be adopted or shared with SHIELD, based on potential formal liaisons and mutual awareness.

With respect to the second period of the project, to maximize the impact of SHIELD in the networking industry, TID will contact the organizers of the relevant industry events in which our staff regularly participates (such as the SDN World Conference, the NFV World Conference, Network Virtualization Europe, or the MPLS+SDN+NFV Summit) in order to arrange at least one workshop on the concepts and results developed by SHIELD. In order to make the message as close as possible to the final outcome of the project, we intend to organize the workshop during 2018.

TID is also strongly involved in a global 5G testbed, 5TONIC (5G Telefonica Open Innovation Centre). 5TONIC is located in Madrid (the main site is at the IMDEA Networks Institute) as an open research and innovation ecosystem on 5G for industry and academia, to promote joint project development, joint entrepreneurial ventures, discussion fora, and a site for events and conferences, all in an international environment of the highest impact. TID will seek for opportunities to demonstrate SHIELD results on the 5TONIC testbed.

3.11. UBIWHERE

3.11.1. Target audience and channels

Ubiwhere is a Portuguese industrial SME with special focus on Telecom & Future Internet as well as Smart Cities. Therefore, Ubiwhere has contact with entities that directly map with SHIELD's stakeholders such as network service providers, network regulators as well as service providers. Some partners/clients such as ALTICE, Vodafone, ANACOM, MicroIO or Wavecom, will be direct targets of dissemination of the SHIELD results. Furthermore, Ubiwhere is currently becoming a smart-city provider and thus it is itself a possible user of the SHIELD results concerning security features either by implementing these features in its smart city solution or by providing them as requirements for network connectivity when selecting a given network service provider. All the previously mentioned actors will be targeted by Ubiwhere when disseminating both SHIELD project results and Ubiwhere's achievements in the project.

Ubiwhere has also important connections with academic entities such as Universidade de Aveiro, Universidade de Coimbra and Instituto de Telecomunicações de Aveiro to name a few. These academic institutions are also a target audience aimed by Ubiwhere since they also have ongoing research projects concerning security, SDN/NFV or smart city solutions.

Other scientific and industrial communities will also be targeted by the participation in relevant conferences and networking events as well as the publication of dissemination material in relevant venues for each target audience.

Ubiwhere's dissemination channels will consist in the following ones:

- Activity generated using Ubiwhere's communication channels such as Ubiwhere's website, Ubiwhere's news section, Ubiwhere's linkedin and Ubiwhere's mailing list. These channels will highlight intermediary SHIELD milestones or specific contributions to the project by Ubiwhere.

- Leading or contributing to the elaboration of one or more papers to be published in relevant conferences or journals, with special focus on Ubiwhere's main contributions such as the NSF Store, Dashboard or NSF development;
- Participation in both preparation and presentation in the Summer school event with focus on Ubiwhere's main contributions such as the NSF Store, Dashboard or NSF development;
- Participation in both preparation and presentation in the Industry Workshop event with focus on Ubiwhere's main contributions such as the NSF Store, Dashboard or NSF development;
- Participation in SHIELD's dissemination activities at international conferences/events such as MWC or EUCNC;
- Internal presentation of SHIELD's results both to TELECOM & Future Internet as well as Smart cities Ubiwhere product teams;
- Dissemination activities with Ubiwhere's industrial or academic partners in the form of workshops or round table discussions.

3.11.2. Plan

The first period of SHIELD project will see Ubiwhere focusing its dissemination and communication activities on the project's goals and use cases in order to raise awareness and interest on the project's ambitious goals. The following activities are scheduled to occur in the first year:

- Activity generated using Ubiwhere's communication channels such as Ubiwhere's website, Ubiwhere's news section, Ubiwhere's LinkedIn, Ubiwhere's mailing list. This activity will done through the release of Ubiwhere's annual report (to be shared among all Ubiwhere's clients and close partners) containing a reference to SHIELD project as well as SHIELD related articles to be shared in the remaining Ubiwhere's communication channels.
- Dissemination activities with Ubiwhere's industrial or academic partners in the form of workshops or round table discussions.

In the second period of SHIELD project, Ubiwhere aims to concentrate its dissemination and communication activities on the results achieved. The following activities are scheduled to occur in the second year:

- Activity generated using Ubiwhere's communication channels such as Ubiwhere's website, Ubiwhere's news section, Ubiwhere's LinkedIn, Ubiwhere's mailing list. This will consist on blog posts and news releases published focused both on the project achievements as well as on Ubiwhere's contribution.
- Leading or contributing to the elaboration of one or more papers (to be published in relevant conferences or journals) with special focus on Ubiwhere's main contributions such as the NSF Store, Dashboard or NSF development.
- Participation in both preparation and presentation in the Summer school event (focus on Ubiwhere's main contributions such as the NSF Store, Dashboard or NSF development).

- Participation in both preparation and presentation in the Industry Workshop event (focus on Ubiwhere's main contributions such as the NSF Store, Dashboard or NSF development).
- Participation in SHIELD's dissemination activities at international conferences/events such as MWC (Mobile World Congress) or EUCNC (European Conference on Networks and Communications).
- Internal presentation of SHIELD's results both to TELECOM & Future Internet as well as Smart cities Ubiwhere teams.
- Dissemination activities with Ubiwhere's industrial or academic partners in the form of workshops or round table discussions.

4. CONCLUSIONS

SHIELD has created via this deliverable a detailed plan for the dissemination and communication of its achievements. The SHIELD partners are confident that the actions described in the present plan will generate awareness of the problems addressed and the solutions offered by SHIELD, thus paving the way to the successful exploitation and market uptake of the projects' results.

LIST OF ACRONYMS

Acronym	Meaning
ACM	Association for Computing Machinery
ETSI	European Telecommunications Standards Institute
ICT	Information and Communications Technology
IEEE	Institute of Electrical and Electronics Engineers
IFIP	International Federation for Information Processing
IoT	Internet of Things
IPS	Intrusion Prevention System
ISG	Industry Specification Group
ISP	Internet Service Provider
KPI	Key Performance Indicator
NFV	Network Function Virtualisation
NFVI	NFV Infrastructure
NS	Network Service
SDN	Software-Defined Network
SP	Service Provider
TC	Trusted Computing
UC	Use Cases