a cyberSecurity Platform for vIrtualiseD 5G cybEr Range services

Deliverable D8.1

Plans for dissemination, communication, standardisation and exploitation

Grant Agreement number:	833685
Project acronym:	SPIDER
Project title:	a cyberSecurity Platform for vIrtualiseD 5G cybEr Range services
Start date of the project:	01/07/2019
Duration of the project:	36 months
Type of Action:	Innovation Action (IA)
Project Coordinator:	Name: Pier Luigi Polvanesi Phone: +39 010 600 2662 e-mail: pierluigi.polvanesi@ericsson.com

Due Date of Delivery:	30/9/2019
Actual Date of Delivery:	25/10/2019
Work Package:	WP8
Type of the Deliverable:	Report (R)
Dissemination level:	Public (PU)
Main Editors:	Neofytos Gerosavva (EIGHT BELLS)
Version:	1.0

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685.

Executive Summary

The current document outlines the SPIDER project's communication, dissemination, standardization and exploitation strategies, which represent a plan of activities and selection of appropriate channels for promoting the project and its expected results. Moreover the current document, presents the individual partners' dissemination and exploitation plans and provides an insight to other H2020 projects, those which are more closely related to the SPIDER concept and some initial thoughts for participating to the established 5GPPP and cPPP-ECSO working groups.

Version History

Version	Date	Comments, Changes, Status	Authors, contributors, reviewers
0.1	5.09.2019	First Draft	Neofytos Gerosavva-8BELLS Ioannis Giannoulakis- 8BELLS Vasilis Machamint –8BELLS
0.2	11.09.2019	Second Draft	Neofytos Gerosavva -8BELLS
0.3	16.09.2019	Third Draft	Filippo Rebecchi –THALES Martin Barmann –SGI Matthias Ghering -CLS Cristina COSTA –FBK Razvan Pucarea- SLGRO Manos Athanatos-FORTH Angela Brignone –ERICSSON Neofytos Gerosavva- 8BELLS
0.4	23.09.2019	Fourth Draft	Jeronimo Mendoza –TID Alberto Mozo –UPM Ioannis Tsampoulatidis –INF Anastasios Lytos- K3Y Christos Xenakis -UPRC Christoforos Ntantogian-UPRC Michalis Chronopoulos- CITY Maurizio Giribaldi-INFO Nuria Rodriguez -ATOS Maria Crociani – STS Franco Davoli –CNIT Anastasios Zafeiropoulos- UBITECH
0.5	25.09.2019	Pre-Final Draft	Neofytos Gerosavva- 8BELLS
0.6	27.09.2017	Reviewed by THALES and ERICSSON	Filippo Rebecchi –THALES Pierluigi Polvanesi-ERICSSON Orazio Toscano-ERICSSON Angela Brignone- ERICSSON

Version	Date	Comments, Changes, Status	Authors, contributors, reviewers
0.7	10.10.2019	Pre-Final Draft	Neofytos Gerosavva- 8BELLS
0.8	16.10.2019	Final Full editorial and contextual review by the Project Coordinator	Pierluigi Polvanesi - ERICSSON
1.0	25.10.2019	Document ready for submission to the European Commission	Pierluigi Polvanesi– ERICSSON Neofytos Gerosavva- 8BELLS

List of Authors

Contributors	Company full name
NEOFYTOS GEROSAVVA, IOANNIS GIANNOULAKIS, ILIAS SKOULAXINOS, VASILIS MACHAMINT	EIGHT BELLS LTD
FILIPPO REBECCHI	THALES SIX GTS FRANCE
MARTIN BARMANN	SERIOUS GAMES INTERACTIVE APS
MATTHIAS GHERING	CYBERLENS LTD
CRISTINA COSTA	FONDAZIONE BRUNO KESSLER
RAZVAN PUCAREA	SINGULAR LOGIC ROMANIA COMPUTER APPLICATIONS SRL
MANOS ATHANATOS	FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS
ANGELA BRIGNONE, ORAZIO TOSCANO, PIERLUIGI POLVANESI	ERICSSON TELECOMUNICAZIONI
JERONIMO NUNEZ, DIEGO LOPEZ, ANTONIO PASTOR	TELEFONICA I+D S.A.U.
ALBERTO MOZO	UNIVERSIDAD POLITECNICA DE MADRID
IOANNIS TSAMPOULATIDIS	INFALIA PRIVATE COMPANY
ANASTASIOS LYTOS	K3Y LTD
CHRISTOFOROS NTANTOGIAN, CHRISTOS XENAKIS	UNIVERSITY OF PIRAEUS RESEARCH CENTRE
MICHALIS CHRONOPOULOS	CITY UNIVERSITY OF LONDON
MAURIZIO GIRIBALDI	INFOCOM S.R.L
NURIA RODRIGUEZ	ATOS SPAIN SA
MARIA CROCIANI	SPHYNX TECHNOLOGY SOLUTIONS AG
FRANCO DAVOLI	CONSORZIO NAZIONALE INTERUNIVERSITARIO PER LE TELECOMUNICAZIONI
ANASTASIOS ZAFEIROPOULOS	UBITECH LIMITED

Glossary

Acronym	Explanation
2G	2th Generation of Mobile Communications
3G	3th Generation of Mobile Communications
4G	4th Generation of Mobile Communications
5G	5th Generation of Mobile Communications
5G-PPP	5th Generation-Public Private Partnership
ACM	Association for Computing Machinery
BSS	Business support system
CA	Consortium Agreement
CCNC	Consumer Communications & Networking Conference
CERTs	Computer Emergency Response Teams
cPPP	Contractual Public Private Partnership
CSIRTs	Computer Security Incident Response Teams
CTF	Capture-The-Flag
Distributed DoS	DDoS
Dos	Denial of Service
DoW	Description of Work
ECSO	European Cyber Security Organisation
ENI	Experiential Networked Intelligence
ENISA	European Union Agency for Cybersecurity
EU	European Union
EuCNC	European Conference on Networks and Communication
GBU	Global Business unit
HW	Hardware
ICT	Information and Communications Technology
IEEE	Institute of Electrical and Electronic Engineers
IH	Innovation Hub
IM	Innovation Manager
IoT	Internet of Things
IPRs	Intellectual property Rights
KPI	Key Performance Indicator
LTE	Long Term Evolution
MANO	Management and Orchestration
MOOCs	Massive Open Online Courses
MPLS	Multiprotocol Label Switching
NFV	Network Functions Virtualization
NGMN	Next Generation Mobile Networks
NoF	Network of the Future
OSS	Operations support system
OTT	Over-The-Top
OPNFV	Open Platform for NFV
PaaS	Platform-as-a-Service
PMI	Project Management Institute

PPP	Public Private Partnership
PR	Public Relations
R&D	Research and Development
SaaS	Software as a Service
SDN	Software-Defined Networking
SM	Standardization Manager
SME	Small Medium Enterprise
TM	Technical Manager
TSP	Telecommunication service providers
VIM	Virtualized Infrastructure Manager
VNF	Virtualized Network Functions
VSOC	Virtual Security Operations Centre (VSOC)
WG	Working Group
WP	Work Package

CONTENTS

List of Tables

List of Figures

1. INTRODUCTION

This deliverable lies under the Task 8.1: Dissemination and Communication and under the WP8 "Dissemination, Communication and Exploitation of Results" that is the work package that encloses and is responsible for undertaking and managing all the project dissemination and communication activities. The WP8 will ensure that the generated know-how and relevant project results are properly promoted in order to reach a broad audience to foster a high impact beyond the project itself.

The SPIDER Dissemination Plan (DP) as described in SPIDER DoA**[1]** identifies three high level objectives:

1) Build awareness: ensure that SPIDER becomes known to all potential stakeholders who can further extend and improve it with new capabilities. A number of communication activities are thus oriented to building awareness, including participation to conferences, publication of research results, newsletters etc.

2) Position SPIDER as providing a solution: explain SPIDER benefits as a single platform and as an ensemble of complementary cybersecurity preparedness capabilities.

3) Generate active interest: encourage potential users to experience SPIDER via active participation in live demonstrations as well as in SPIDER workshops/conferences and other events.

Following the SPIDER DP will allow stakeholders to share their thoughts on the usability and effectiveness of the platform, as well as the likelihood of uptake. In turn, this will enable SPIDER to incorporate stakeholder impressions on a rolling basis.

This document describes how the SPIDER consortium can establish and follow highly effective dissemination and communication activities in order to promote the project and record how the results are being exploited. It will provide both a general overview of the activities together with the individual partners' plans, where each consortium member briefly describe how they intend promote the project results to selected stakeholders throughout the project lifecycle.

This document is written primarily as a guide for the project participants, covering four main aspects:

- **The SPIDER dissemination and communication/promotion goals;**
- **The SPIDER strategy: i.e., how the project will disseminate and promote project activities and work;**
- **A plan of the specific promotional activities that will evolve in line with the progress of the project;**
- **A description of how the project can measure the effectiveness of its dissemination and communication.**

Due to the complex nature of the project, a decentralization of the dissemination activities is expected, with each partner (based on its own specific characteristics) undertaking specific activities in relation to its reach potentials and established networks.

The experienced SPIDER industrial partners will focus on the industrial dissemination of the SPIDER results, while the academic partners will handle the scientific dissemination activities through the publication of results in international peer reviewed journals and technical conferences.

The dissemination leader (EIGHT BELLS) will ensure that the dissemination and communication strategy plan will be followed exactly as described in the current document and that the project dissemination and communication activities will be documented regularly, monitored and evaluated via the provided KPIs and other tools and revised in the course of the project duration.

Within the WP1 and WP8 frameworks, all the necessary communication tools will be created: the web platform, social media, collaterals (e.g. banners, brochures, leaflets, gadgets, posters), market insights (e.g. white papers), practical guides, policy briefs, PR outputs (press releases, press conference material), videos, infographics, in-house newsletters and success stories flyers.
Of course, internal dissemination tasks will be largely performed by all the participating organizations, utilizing their dedicated websites, existing mailing lists, projects and related activities announcement channels, throughout the project's 36 month project lifecycle. Considering that dissemination will play a pivotal role to the project, the planning of the relevant activities has begun with the project kick-off event (held in M1- July 2019)

2. OBJECTIVES

The current document intends to describe the dissemination and communication strategy plan that will elaborate in depth the activities and the dissemination channels needed for carrying out all the necessary work for succeeding the desirable exposure of the project results. Depending on the project's progress, the dissemination of content will be constantly updated and enriched in order to provide a clear representation of the project's objectives by taking into account the various identified stakeholders who will constitute the target audiences and shall benefit from the advances of the project.

The main objectives of this deliverable are to:

- Identify key stakeholders and select appropriate mechanisms for engaging them;
- Define a consistent strategy that will be carried out through the project duration for disseminating the project results;
- Identify the communication channels (documents, research papers, reports, videos, workshops, meetings, promotional material, conferences, etc.);
- Define the rules and procedures that will be applied to implement, monitor and evaluate all the communication and engagement activities;
- Depict the methods, tools and promotional materials (e.g. project logo, website, printable dissemination material, events, publications) that will be used for the project's dissemination and communication;
- Identify relevant publication means for the wider dissemination of research results;
- Provide a complete overview of the planned communication activities, as well as a list of other potential dissemination opportunities to be exploited in the project;
- Define measurable objectives for the dissemination plan and the activities and events described on it along with a purposely defined set of success indicators;
- Provide project partners' insights on their initial dissemination and exploitation plans.

The present report will be updated through the 3 reports expected as separate deliverables (D8.2 D8.3 D8.4) throughout the project duration according to DoA

The Dissemination Manager partner (EIGHT BELLS) will be responsible for steering, coordinate and document all dissemination and communication activities & summarize and present all the related outcomes. The Dissemination Manager will moreover continuously revise and maintain this document during the project lifetime.

3. DISSEMINATION: STAKEHOLDER'S STRATEGY, TARGET AND PLANS

According to the Project Management Institute (PMI) **[2][3]** stakeholders are defined as: "*individuals and organizations who are actively involved in the project, or whose interests may be positively or negatively affected as a result of project execution or successful project completion*". Thus, stakeholders are key to a project's success or failure because they can also affect, the project's objectives and outcomes depending on their own personal interests. As it is easily understood each partner should make a careful stakeholder selection and classification (based on their power, interest, influence, impact, etc.), select appropriate dissemination channels and provide information accordingly.

Some well-known tools for stakeholders classification are the following ones [4]:

- **Power and Interest grid**
  In this type of classification, the stakeholders are being grouped according to their power and level of interest in the project or its outcome.
  Among all the models, the power/interest model is the most well-known. In this model, you draw a chart that consists of vertical and horizontal lines as shown in the figure below. The horizontal line denotes interest, and the vertical line represents power.

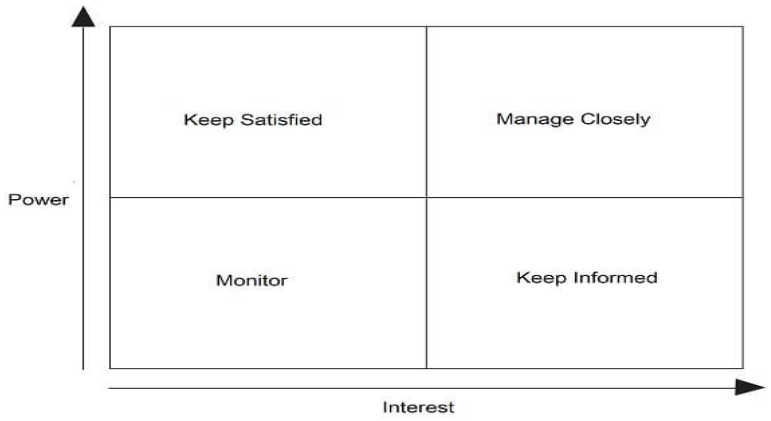


Figure 1: Power and interest grid

- **Power and Influence grid**
  In this type of classification, stakeholders are being grouped according to their power and level of influence on the project or its outcome.
- **Influence and Impact grid**
  This classification is based on the influence and impact of the stakeholders on the project or its outcome.
- **Power, Urgency, and Legitimacy grid -Salience model**
  This model is also known as the **Salience Model**. In this model, stakeholders are classified as per their power, urgency, and legitimacy.

The project partners can select any of the above classification tools for helping them select and classify the appropriate stakeholders

Different targets for the dissemination will be considered, as discussed in the following:

- **Specialised audience:** SPIDER intends to inform potential stakeholders on how they can contribute to SPIDER architecture and to incorporate the feedback obtained during SPIDER demonstrations.

- **Economic Multipliers:** SMEs/groups accessing or affecting stakeholders, such as consulting organisations will be targeted by SPIDER as one of the major sources of citations in their future reports, or other ongoing activities; similar EU funded projects will also be targeted.

- **Non-specialised audience:** SPIDER will communicate the derived results to wider audiences so to increase citizens' acceptance of European research activities and calm down their fears for new technologies.

Table 1 provides a non-exhaustive list of the target audiences and activities that will be further refined in SPIDER's dissemination strategy. It can also be seen as a preliminary stakeholder analysis for SPIDER's proposed approach.

Table 1: Targeted Audience

TARGET AUDIENCE	ENGAGING ACTIVITIES
5G infrastructure providers and operators	**Liaison with industrial associations.** • Key articles in the trade press • Participation in relevant conferences/workshops with large audience among industrial organisations • Organisation of workshops and demo events • Individual presentations / discussions with key organisations
Technology suppliers	**Liaison with telecommunications suppliers and partners.** • Articles in trade press • Participation in relevant conferences/workshops • Organisation of workshops and demo events at pilot sites
Research, Academia & Open Source Communities	**Source Communities** • Liaison and collaboration with researchers and academics from universities • Peer reviewed publications in scientific journals • Participation in conf./workshops with large audience among the scientific community
General public	• Communications through social media (via twitter) • Press releases on project outcomes in national media • Creation of easy to understand video, which will be visible online via website

Dissemination Channels

<u>Main dissemination channels to be used for disseminating the project results are the following ones:</u>

- A **dedicated website to the project** will be created as a communication platform in order to spread project objectives and results to the related stakeholders containing of all the essential information

concerning the project. The objective will be that this platform will be constantly **updated with material such as upcoming meetings, participations in events, dissemination actions, conferences, publications, whitepapers, newsletters, news, photos, etc**. It will also be a key enabler for communications between project partners, stakeholders and the wider public to share project outcomes. All the appropriate internet technologies will be used in order to provide additionally a space for collaborative work to facilitate and enhance the activity of the consortium and create a meeting point for stakeholders interested in the project, creating active knowledge community groups. The main goal will be to create and maintain a website **that will be professional, market facing, crawlable, responsive and regularly updated using different formats** (e.g. webinars, video clips, practical guides, white papers, collaterals, banners, brochures, etc.).

Project has prepared an internal first iteration-internal prototype of the project website[5] in Month 2 and the project is working on the online version that is expected to go online on Month 4. Regarding the selection of the domain name, the one initially selected ('spiderproject.eu') was very similar to other already registered domain names referring to existing products. In order to avoid any confusion, and to highlight the collaborative character of the project, we replaced the domain name with 'spider-h2020.eu'. Moreover, for similar reasons, and to avoid incurring in trademark issues, it was decided that a longer name will be used for other activities, that is the: “SPIDER 5G Cyber Range” plus “project” if needed.

Summarizing the final decision regarding this issue was:

- That the short name (spider-h2020) will be used for website (public and private), and social media.
- That the longer name will be used inside the website, in our leaflets and brochures, and any other generated communication material

The project consortium will take all appropriate measures in order to ensure that the results will be widely available and accessible to the public after the project end through additional mediums for a considerable length of time. The project website will be available and remain online for at least three years after the project end.

- **Press releases –newsletters:** Press releases and newsletters are expected to be produced regularly (**e.g. every three or six months**), posted on websites, and circulated to the relevant stakeholders. This material should be in line and up to date with key project achievements (e.g. participation in events, a significant technical update, etc.) and will be also posted among popular news portals, business related media outlets, and shared with European/international press contacts. General information concerning SPIDER (objectives, foreseen results, planned/on-going activities and outcomes) will be periodically sent out to several points of related interest such as academic networks and organizations, award schemes, professional networks and stakeholders.
- Information illustrating the project’s results and success stories will be distributed among all the related stakeholders.
- Strong and continuing appearance to **popular Social** Media: The project’s online presence will be complemented via a strong **social media** presence. Social media channels, such as **Twitter**, can be effective in communicating project announcements using the easy approach based on the usage of hashtags (in order to target specific audiences as well) while

LinkedIn and Facebook can be effective in promoting discussion, spurring debate and generating awareness of the project and its associated activities. All social media channels will be created and updated regularly by the dissemination leader partner (EIGHT BELLS) in order to ensure the content is consistent and relevant.

- **Creation of short length videos** that will present project news and results. **A YouTube channel page will be created for posting up these videos or any other visually relevant material might** come up during the project's implementation (e.g. participation in events, conferences, etc.).
- An **informational brochure** in electronic and printed form concerning the project's scope, strategic objectives, foreseen goals, expected impact and key activities will be created. This brochure will be utilized for communication purposes towards the general public, relevant stakeholders and potentially collaborative authorities. It will include all necessary logos and identifications (EU logo, H2020 Funding Programme, etc.) as well as the logos of all participating organizations.
- **Articles, papers, publications, whitepapers, and concept notes:** Key preliminary and final research results will be **published** by the project. More specifically, papers or posters will be prepared for targeted top-tier peer-reviewed workshops, conferences, and scientific journals. In addition, the consortium will produce whitepapers that will inform the public about the project achievements as the project evolves. The whitepapers will be uploaded to the project website. Their presentation will facilitate the collection of valuable feedback from researchers and experts in the fields of **study which will be valuable for coordinating and directing future research activities. SPIDER consortium will comply with the open access policy of Horizon 2020 providing on-line access to scientific information that is free of charge to the end-user**. The WP8 leader will keep track of all publications and will ensure that authors do not publish data that may harm patenting and exploitation prospects. Moreover according to Horizon 2020 guidelines, each participant must ensure open access that is online access which is free of charge for any user, to all peer-reviewed scientific publications relating to the project's results. This does not mean that the participants have the obligation to publish their results, nor does this affect their plans for exploitation. In fact, firstly participants must decide on the protection of their results and, once the decision is taken, consider if and when dissemination should be done through scientific publication.

Some journals of interest are the following ones:

-ACM Transactions on Information and Systems Security,

-ACM Transactions on Networking, Entertainment Computing (Elsevier) and

-International Journal of Serious Games.

- Participation of SPIDER in scientific and industrial exhibitions and scientific conferences.

The consortium has identified a list of possible conferences that scientific results can be presented; the list is not exhaustive and will be continuously updated

Table 2: Main conferences targeted by the SPIDER consortium

EuCNC (European Conference on Networks and Communications)
IEEE Conference on Network Softwarization (NetSoft)

The International Conference on Entertainment Computing, USENIX NSDI
ACM Technical Symposium on Computer Science Education
ACM SIGCOMM
USENIX Security
ACM CCS
IEEE S&P
Advances in Computers in Entertainment (ACE)
Games and Learning Alliance (GALA) conference
IEEE GLOBECOM (Global Telecommunications)
IEEE NoF (Network of the Future)
IEEE International Conference on Network Softwarization (NetSoft) 2020
IEEE International 5G Summits
IEEE CCNC Consumer Communications & Networking Conference
IEEE INFOCOM International Conference on Computer Communications
ICT Future Network summit
ACM CONEXT (Conference on emerging Networking Experiments and Technologies)
IEEE ICCCN (International Conference on Computer Communications and Networks)
TERENA Networking Conference (Trans-European Research and Education Networking Association)
CTTE (Conference of Telecommunication, Media and Internet Techno-Economics)
IEEE COMSNETS (International Conference on Communication Systems and Networks)
IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (IEEE Mobile Cloud)
IEEE International Conference on Cloud Networking (IEEE CloudNet)
IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)

- **Logo**

  After various discussions and modification rounds, the consortium decided that the SPIDER logo to be the following one. It has been especially designed so that it can also be used in Social Media. Moreover, the chosen logo will be used in the website, presentation templates, deliverables and all other promotional material such as leaflets, brochures, flyers etc. The current SPIDER project logo and its different variants are being illustrated in Figures 2,3,4

Figure 2: SPIDER LOGO version #1

Figure 3: SPIDER LOGO version #2

Figure 4: SPIDER LOGO version #3

- **Templates**

The PowerPoint presentation, the deliverable and the agenda templates have been created in order to be used by the partners for deliverables and presentations for all external and internal events, meetings, etc.

SPIDER presentations and deliverables templates are presented below:

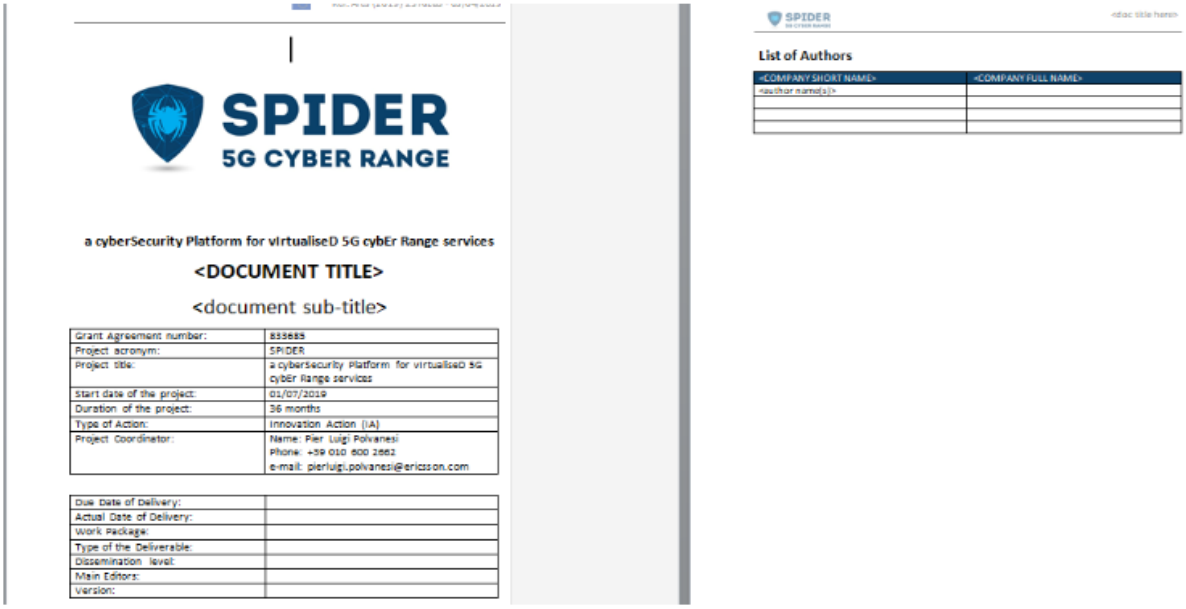


Figure 5: The Spider Deliverable template

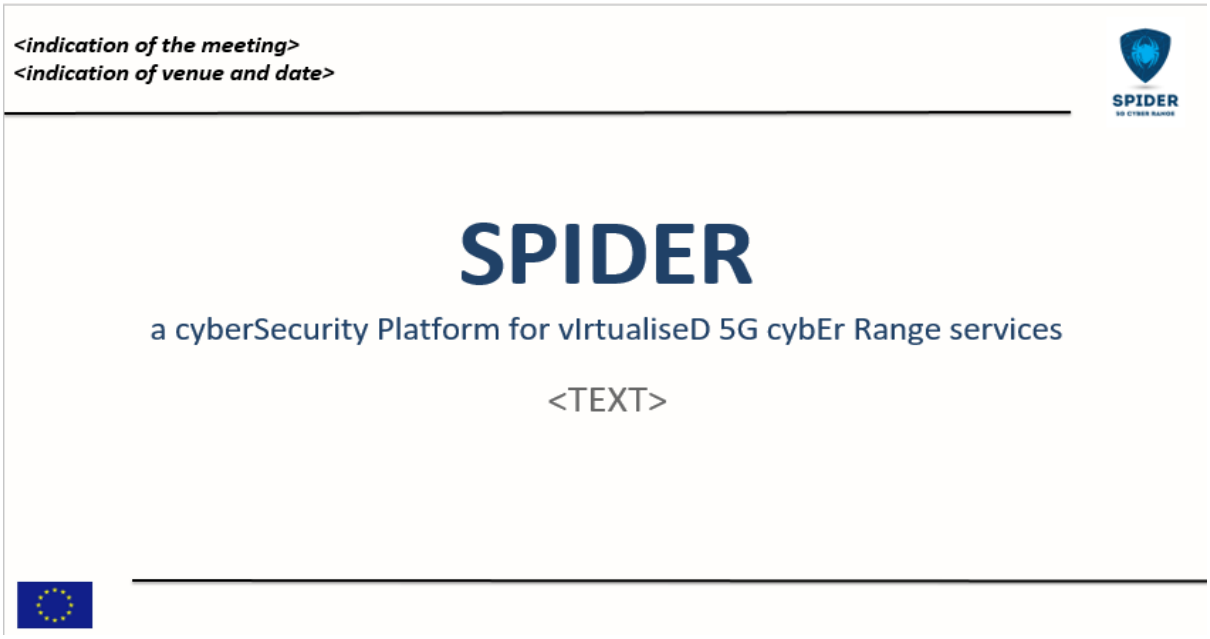
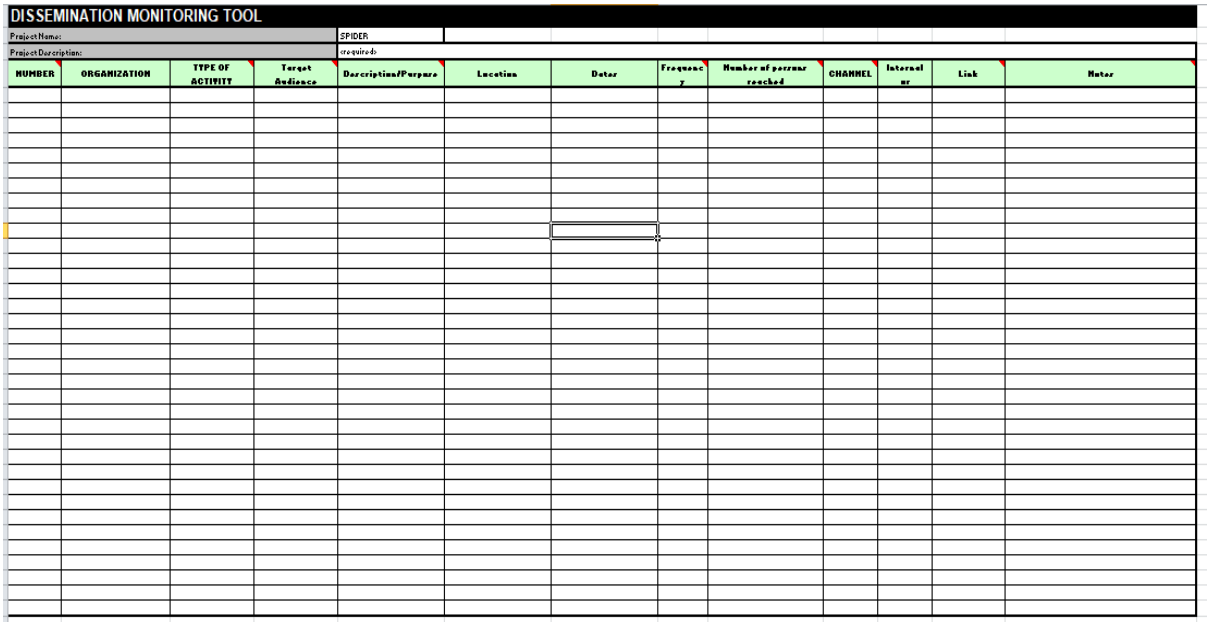


Figure 6: The SPIDER PowerPoint template

4. MONITORING AND EVALUATION OF DISSEMINATION AND COMMUNICATION ACTIVITIES

A monitoring process will be established within the consortium in order to assess the various dissemination and communication activities implemented in the project. This is based on a set of KPIs that covers all the aspects of the dissemination and communication. An efficient monitoring process will **ensure that all partners regularly indicate all dissemination and communication activities they have been participating to**. The process involves creating, making available online and updating a dedicated spreadsheet (see Figure 7: The communication monitoring tool) on the SPIDER's private project area Partners will be required to indicate their "Organization name", the "type of dissemination/ communication activity", "Target Audience" a short "Description of activity", "Dates", "Location", "Impact", as well as the type and number of audiences reached, and evidence of the activity (e.g. photos, web link, newspaper, article screenshots, etc.)**. The evaluation of the dissemination and communication strategy concerns both qualitative and quantitative indicators** and the dissemination plan will be continuously monitored and evaluated in terms of its initial targets (using the dedicated spread sheet and statistics generated from it). **The evaluation will involve examining the progress of the strategy's implementation and will refer to an outreach activity that is quantifiable through the attendance (number) of persons present from the audiences, quantity of material distributed, number of events participated, the development and dissemination of messages and materials, media presence and traffic created in social media. From time to time this process will be assessed from the WP8 leader and the rest of the partners and corrective actions will take place if necessary. The way to monitor this, will be through** the comparison of the on-going project dissemination activities against the dissemination plan and the baseline KPIs that are defined (comparison of baseline KPIs vs current state. This can be accomplished through the collection of data per partner, online meetings, calculation of KPIs and statistics based on the dissemination monitoring tool and the collection of data etc.



DISSEMINATION MONITORING TOOL

Project Name: SPIDER

Project Description: <required>

NUMBER	ORGANIZATION	TYPE OF ACTIVITY	Target Audience	Description/Purpose	Location	Date	Frequency	Number of persons reached	CHANNEL	Internet	Link	Notes

Figure 7: The communication monitoring tool

The communication strategy of the project comprises a set of activities that aim to communicate the project results to relevant target audiences and attract interest in the project. It is recognised that there are three main communication channels: person-to-person (workshops, presentations, etc.); written channels (newsletters, posters, etc.); and technology-based channels (Internet, social media, etc.). The SPIDER consortium will engage in communication activities across all these channels. The target groups and specific key performance indicators (as well as concrete targets) for each communication approach are summarised in the following tables.

Table 3: SPIDER communication activities along with KPIs

Activity	Description	Target group	KPI
Website	Project's website acting as the centrepiece of the project's online presence	Industry, general public, scientific & research community, public sector	Number of distinct Visitors >=4000 (throughout project lifetime)
Social media	Establishing a social network footprint for the promotion of the project	Industry, general public, scientific & research community, public sector	Twitter followers >= 150 LinkedIn Group Members >=100 Facebook followers >= 100 YouTube channel followers >=40
Mailing lists	Two mailing lists will be created: An internal list for the consortium and an external for registered users	Internal: Consortium External: Industry, general public, research community, public sector	Frequency of communication>= once per month Number of external mailing list subscribers >= 800 for the full project lifecycle
Technical forums	Project presentation in technical forums	Industry, scientific & research community, public sector	Number of technical forums SPIDER will be featured >= 2
Communication events	Project participation and presentation in events for face-to-face promotion of the project	Industry, scientific & research community, public sector	Number of events >= 4
Traditional media opportunities	TV, newspapers, radio and other media opportunities to disseminate results of the project and emphasise on the benefits to 5G players,	industry, general public, scientific & research community, public sector	Number of traditional media appearances >=3

Activity	Description	Target group	KPI
	industries, users, as well as the general public.		
Marketing material	Flyers, brochures and leaflets, press releases with easy-to-digest summaries of the project's results, as well as posters in conferences, workshops and exhibitions.	Industry, general public, scientific & research community, public sector	Number of brochures or leaflets produced >=2 Number of posters produced & presented in conferences >= 3

Table 4: SPIDER dissemination activities along KPIs

ACTIVITY	DESCRIPTION	KPI AND SUCCESS INDEX
Industry-led publications	Publication of white papers, articles on magazines, technology roadmaps, and industry-led journals	Number of Publications ≥ 3
International events and conferences	All SPIDER partners will participate in European and international conferences. Academic partners will organise special sessions and workshops in EU and Int. conferences	Number of conference (not necessarily implying physical presence) papers ≥ 12 Number of workshops ≥ 2 (contributes to the KPI of Table 3 -Communication Events)
CTF challenges	Capture-the-Flag (CTF) challenges organised using the SPIDER Cyber Range as a Service platform	Number of CTFs organised ≥ 2
Publications in scientific journals	The scientific publications of SPIDER will facilitate the efforts of professionals and researchers. The journals include but are not limited to ACM Tran. on Information and System Security, IEEE Tran. on Dependable and Secure Computing, IEEE Security & Privacy Journal, Int. Journal of Computer Networks & Security, Information Management & Computer Security.	Number of Open Access publications ≥ 5
Industry focused events	Organisation of industry focused events (i.e., workshops, symposiums, demonstrations, trainings, etc.) to disseminate project outcomes.	Organisation of industry focused event ≥ 2
EU events	SPIDER partners will actively participate in the EC activities organised at programme	Number of participations in EU events ≥ 1

ACTIVITY	DESCRIPTION	KPI AND SUCCESS INDEX
	level relating to cybersecurity training with the objective of providing input towards common activities and receiving feedback, offering advice and guidance and receiving information relating to standards, policy and regulatory activities, national and international initiatives.	
Online seminars	Seminars related to cyber range solutions as well as SPIDER achievements will be developed using appropriate tools. By organising these seminars instead of schools, a significant cost reduction will be achieved.	Number of seminars ≥ 2 Number of participants ≥ 15 per seminar
Liaison with other projects	The SPIDER consortium will collaborate as much as possible with other ongoing projects accepted in the call to exploit opportunities for knowledge exchange and for improving dissemination among the target audience.	Number of collaborations with other projects ≥ 2
Liaison with CERTs/CSIRTs network across the EU	The SPIDER consortium will strive to ensure collaboration and knowledge interchange with CERTs/CSIRTs. The communication will be achieved either via the creation of direct channels between projects or via the participation and collaboration of mandated SPIDER representatives to ECSO technical Working Groups (e.g., WG1, WG3, WG5 and WG6) and ENISA meetings.	Number of collaborations with CERTs/CSIRTs networks across the EU ≥ 3

Post-Project Dissemination: SPIDER will cater for the dissemination of results even beyond the project lifespan, using some of the activities employed during its development, testing and deployment stages. In particular, the Post-Project Dissemination illustrates the actions that will be adopted after the end of the project.

Table 5: Sustainable post-project dissemination channels and their content

Channel	Sustainable dissemination content
Open Access Publications	Research papers will be available in open-access repositories, in addition to the final published versions available at **IEEE Xplore, ACM Digital Library, Springer, Elsevier, etc**. The academic partners will additionally host the publications in the form of green open access in their institutional research repositories. Together with a copyright notice, research papers and whitepapers will be made available on social media platforms and the project's website.
Website	▪ Live up to three years after the project's end ▪ Information about the project's objectives, WP structure and consortium. ▪ Links to SPIDER's social media channels such as Twitter, LinkedIn Group, Facebook Page and YouTube channel.
Social media	▪ LinkedIn Group will provide a look-up tool for cyber range relevant conversations related to SPIDER's R&D work and cyber range vision in general. • Facebook page will provide historical news feed for the project's public relations activities. • A YouTube channel will offer a variety of cyber range related how-to and showcase videos of developed SPIDER's solutions generated by the consortium.

The research and innovation carried out SPIDER has a significant potential to attract the 5G and other community stakeholders. The table 6 provides a quantification of the project's dissemination activities and sets a basis for verifying whether the project dissemination objectives will be met.

Table 6: Quantification of general SPIDER dissemination activities and related objectives

General dissemination activities	KPIs for dissemination objectives
Whitepapers (technical and technical/business- business oriented), Newsletters	Number of whitepapers & technical/business-oriented publications >=2 Newsletters >= 2 per year
Scientific knowledge transfer	Number of technology and scientific transfer events >=2
Website	Active participation of project partners as evidenced by number of website content updates per week >=1
Social media engagement	Active participation of project partners as evidenced by number of social media posts per week >=1
Summer school, training	One summer school cyber security training event

SPIDER clustering activities

Apart from the standard dissemination and communication activities analysed before, the SPIDER consortium will additionally conduct dedicated stakeholders clustering, engagement and awareness raising activities (see Table 7).These activities will target mainly the industrial communities, namely the communities that hold more potential in commercially exploiting the results and applying them in daily practice. The SPIDER consortium through its business portfolio holds the potential to engage various stakeholders thus generating hype around the SPIDER approach.
This portfolio, which comprises the initial industrial ecosystem of 5G / ICT vendors, cloud computing and software engineers as well as cybersecurity professionals, will be enhanced by identifying additional 5G stakeholders. These may include organisations focused on entrepreneurship, and business support services, e.g. incubators or accelerators programmes. By initiating discussions about business cases/models and implementation pathways, the consortium will raise awareness regarding SPIDER objectives and results, and through them will promote the project results and bring the project one step closer to the market, ensuring dialogue with potential funders and/or customers. **In order to facilitate this, the SPIDER consortium in the context of Task 8.1 is planning to organise two (2) SPIDER industrial and stakeholders clustering workshops**. These workshops will be held at during the second half of the project duration. These workshops will give emphasis on presenting the more mature industrial results and will present the integrated SPIDER cyber range platform, the demonstrators, the lessons learnt, and the adoption methodologies.
These workshops will aim at informing the key stakeholders identified, and at generating early interest. These workshops will include representatives from the telecommunications community, including members of the EC, representatives from the industry (software engineers, software houses, start-ups), and more specifically from the domains of interest (cybersecurity, 5G, cloud computing and software engineering, etc.), investors etc.

Table 7: SPIDER clustering activities with target groups and values

Key Performance Indicators	Stakeholders Targeted	Target Value
Number of industrial and stakeholders clustering workshops organised	Industry/Companies (mainly ICT), Investors	2
Number of invited persons in a position to push SPIDER to the market (e.g. investors)		>=10

5. TIME PLAN FOR DISSEMINATION AND COMMUNICATION ACTIVITIES

In the Gantt Chart below (see Figure 8: SPIDER Dissemination activities GANTT CHART), a tentative timeline for the implementation of the project's various dissemination activities is being presented. Of course, depending on the project progress and the availability of the project results that justify any update or content publication this plan can be reviewed and some activities may be shifted in an earlier or later stage. However, the project partners will take all the appropriate measure for meeting the proposed timeline with the main objective of ensuring the various target values for the KPIs as these have been specified in the above tables (Table 3,Table 4,Table 6) Depending on the individual consortium partners' initiative a level of flexibility is reasonable that each individual consortium member may search for the best opportunity to organize an event or release an article, paper, etc.

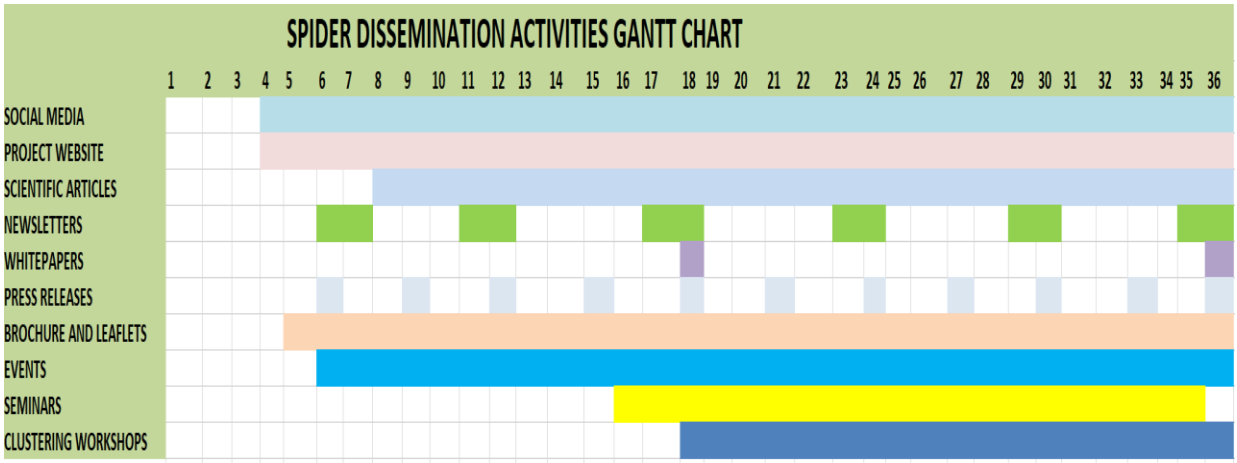


Figure 8: SPIDER Dissemination activities GANTT CHART

6. PARTNERS INDIVIDUAL DISSEMINATION PLANS

Below the consortium partners' individual dissemination plans are being presented:

- **ERICSSON**

"Dissemination is essential for take-up and take-up is crucial for the success of the project and for the sustainability of outputs in the long term." Ericsson endorses this sentence from the European Commission and strongly believes in the importance of communication and dissemination to raise awareness, inform, engage, promote and make project outputs sustainable.

Ericsson will pursue communication of the SPIDER results and will therefore regularly give updates about SPIDER progress, events, results, press releases etc. through corporate webpages, newsletters, social media accounts, and press with the aim to reach: (i) the scientific community, which would benefit for novel tools and platforms, (ii) telecommunication service providers (TSP), mobile network operators, small cell operators and Over-The-Top (OTT) players, which would benefit from achieving a complete solution for an effective cybersecurity preparedness and for solutions assessments and investments planning, and (iii) vendors of Network Elements (PNF/VNF) and Network Solutions which would benefit from a complete solution for threat and vulnerability assessment."

In the context of WP8, Ericsson will leverage on its articulate and worldwide communication activities to take care of the project promotional tasks. **In the following it is proposed a short list of some of most interesting events suggested by Ericsson:**

- Conferences: European Conference on Networks and Communication(EuCNC), IEEE Conference on Network Softwarization (NetSoft), IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)
- Workshops: International Workshop on Computing, Networking and Communications, 5G World Event

- **Consorzio Nazionale Interuniversitario per le Telecomunicazioni**

CNIT's main dissemination activities include: (i) publications in international journals, (ii) presentations at international scientific conferences, (iii) seminars/lectures for university students, particularly at the graduate level and with specific reference to the partner university (University of Genoa) directly involved in the project activities.

More in detail, an initial list of targeted journals and conferences is the following:

- Journals: IEEE Communications Magazine, Computer Networks, IEEE Journal on Selected Areas in Communications, Transactions on Emerging Telecommunications Technologies, Future Generation Computer Systems, IEEE Cloud Computing, IEEE/ACM Transactions on Networking, IEEE Network, IEEE Internet Computing, IEEE Pervasive Computing, IEEE Transactions on Network and Service Management, IEEE Transactions on Dependable and Secure Computing, IEEE Proceedings, Elsevier Computer Networks, IEEE Transactions on Information Forensics and Security, IEEE Security & Privacy, ACM Transactions on Privacy and Security, Computer and Communications Security.

- Conferences: ACM SIGCOMM (Flagship annual conference of the ACM Special Interest Group on Data Communication), IEEE INFOCOM (International Conference on Computer Communications), IEEE GLOBECOM (Global Communications Conference), IEEE ICC (International Conference on Communications), IFIP/IEEE IM (International Symposium on Integrated Network Management), IEEE/IFIP NOMS (Network Operations and Management Symposium), USENIX NSDI (Symposium on Networked Systems Design and Implementation) and OSDI, ACM CoNEXT (International Conference on emerging Networking Experiments and Technologies), European Conference on Networks and Communications, USENIX Security: USENIX Security Symposium, IEEE Symposium on Security and Privacy, Network and Distributed System Security Symposium (NDSS), IEEE International Workshop on Information Forensics and Security, ACM European Conference on Research in Computer Security, Italian Conference on Cybersecutiy (ITASEC).

- **TELEFONICA I+D S.A.U. (TID**)

TID, as the branch of the Telefónica Group dedicated to innovation and strategic vision, will share the SPIDER 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;
- GCTIO Councils in the Network and Core Virtualisation, Radio and Mobile access and Security areas;
- TID demonstration rooms;
- Presentation of the main innovations to the entrepreneurship initiatives of Telefonica (Wayra, Amerigo and Telefonica Open Future),
- Internal security knowledge communities in the Telefónica Group.

In addition, TID will raise awareness about SPIDER 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 SPIDER with several publication activities in corporate magazines and social media.
TID regularly participates to industry events related with virtualization technologies and security and has the aim to represent SPIDER at venues such as the Layer123 SDN & NFV World Congress, or the MPLS + SDN + NFV World Congress.
TID will actively build awareness about SPIDER services and technology in bodies and PPPs where Telefónica is present, such as the 5GPPP or the cPPP. This will be achieved by meeting participation and formal presentations there, information sharing, or direct discussions. Moreover 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, and cybersecurity services.
To maximize the impact of SPIDER 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 or ETSI workshop) in order to arrange at least one workshop on the concepts and results developed by SPIDER. In order to make the message as close as possible to the final outcome of the project, we intend to organize the workshop during 2022. Currently, as part of this activity, a SPIDER presentation has been already made in ETSI Security Week 2019 in June. Another presentation was made to introduce the project in a workshop during the ETSI ENI (Experiential Networked Intelligence) meeting #11, at Aveiro in July.
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 SPIDER results on the 5TONIC testbed.

- **THALES SIX GTS FRANCE (THALES)**

THALES dissemination strategy includes internal and external stakeholders' communication, participation in industry exhibitions, and scientific dissemination.
Internal communication will include the organization of seminars, and regular advancement points with relevant internal stakeholders to orientate the research and innovation work. The already identified actors for internal communication are the members of the Critical Information Systems and Cyber Security Business Line that are in charge of the Cybels range product development.
Also, THALES will disseminate the advancements of the projects to its network of cyber training operation centres (Belgium, Netherlands, Dubai and Hong Kong) built around the world.
Finally, the team in charge of the work on SPIDER will benefit from regular exchange with members of the French CERT-IST that is operated by THALES. THALES will also leverage on its presence in exhibitions and trade shows for showcasing and demonstrating SPIDER achievements. Finally, the company will also contribute to the production of scientific literature published in relevant conferences, journals or books. Also THALES will make liaisons with the 5G PPP Security WG project

- **ATOS SPAIN S.A. (ATOS)**

ATOS has a large expertise in communicating and disseminating results from its research projects. Through the Innovation Hub, a group of communication and design experts provides all methods and tools for an effective communication. In the context of SPIDER, ATOS will explore through them how to maximize the potential impact of SPIDER in the cybersecurity domain.
ATOS would disseminate SPIDER results at international level (presentations in cybersecurity-related conferences and events, publications in relevant general media and journals, etc) as well in the Industrial Spanish Stakeholder arena. ATOS is also committed to support all dissemination and communication activities via on-line communication (Atos Spain and ARI social networks, press media, web site, etc), exploiting synergies with already running research projects and networks (ENISA, ECSO) and support all dissemination activities carried out by the project.

- **UBITECH LIMITED (UBITECH)**

UBITECH plans to disseminate the project results to relevant actors and stakeholders in the 5G, digital security, information and communication technologies, virtualized infrastructures and software engineering scientific community and market, as well as in vertical industrial sectors, communities, markets and domains with high interest in end to end 5G services engineering and lifecycle management, as well as in security, certification and trust - focusing its first dissemination

efforts and activities on its long list of industrial, telecom and software partners, business associates and customers.
The major dissemination channel will be research publications at top-quality international journals (e.g., IEEE Networks, IEEE Communications, Ad-hoc Networks) and conferences (e.g. ACM conferences, EUCNC, Globecom) in the broad area of cyber security in 5G, and any relevant forums (e.g., European Commission Cyber Security & Privacy Innovation Forum) as opportunities arise.

- **UNIVERSIDAD POLITECNICA DE MADRID (UPM)**

Along the project, UPM will be mainly involved in the preparation and publication of articles in scientific journals and peer-reviewed conferences, which are very valuable in terms of project results visibility. Additionally, UPM will participate in conferences, workshops and demos in major international events. Specifically, the development of machine learning algorithms threat detection and mitigation will be one of the main focuses of UPM's research.

In terms of education, UPM will use the knowledge obtained from the collaboration in SPIDER for teaching, training, and research purposes, using them as a platform for the education of undergraduate, graduate and PhD students. The results will be used for updating and introducing innovative topics into the course programs, seminars, master's theses and also as cornerstones for further scientific research activities. UPM plans to adapt some of the SPIDER outputs to prepare PhD candidates to work in technologically and scientifically advanced cybersecurity and machine learning for network and cloud environments. UPM will also leverage these outputs to design advanced undergraduate courses.

- **FONDAZIONE BRUNO KESSLER (FBK)**

FBK as an academic partner, will contribute to SPIDER dissemination by submitting high-quality scientific publications to top-notch venues. These include high quality (Q1) journals and conferences (indicatively; conferences: IEEE NOMS/IM, IEEE CNSM, IEEE NetSoft, and journals: IEEE TNSM, IEEE JSAC, IEEE Communication Magazine). Contribution to the organization of workshops and panels is also being considered.

- **SINGULAR LOGIC ROMANIA COMPUTER APPLICATIONS SRL (SLGRO)**

As also stated in the SPIDER description of work, SingularLogic Romania (SLGRO) will undertake to disseminate the SPIDER project results at the best possible level. The company is one of the leading integrators, IT services providers, and enterprise application systems vendors in the Balkan market and active in various sectors (Telecommunication, Health and the public sector). SLGRO intends to disseminate the project results to its wide customer base as well as to its authorized business partners' network, numbering more than 400 partners in the Balkan market. Main goal of our dissemination activities will be to create awareness in the communities of stakeholders addressed by the project and attracting customers. Therefore, we will undertake pre-marketing activities, such as creating lists of potential customers and organizing targeted demonstrations to interested parties.

- **EIGHT BELLS LTD (8BELLS)**

8BELLS will disseminate project results through its social network pages (Facebook and Twitter) as well as on its website. Also, it will broker project relevant information to stakeholders in Cyprus and across Europe. 8BELLS will actively contribute to the creation of scientific papers and publications in

international Journals and Magazines, while knowledge will be widely disseminated through the participation in conferences and demonstrations. 8BELLS regularly publishes results as contributions in relevant international journals/magazines and conferences.

Furthermore, results will be published in form of studies and white papers directly by the company. IEEE and other conferences and events shall be also addressed and included into the individual dissemination plan. EIGHT BELLS will furthermore organize informational campaigns over local media and institutions and will seek to present SPIDER in relevant national events like for instance «European Researchers' Night» organized by the Research and Innovation Foundation (RIF) in collaboration with academic and research institutions as well as other organisations in Cyprus. EIGHT BELLS will design related material such as leaflets, brochures etc and distribute them during the aforementioned campaigns and will moreover promote the project through regular press releases and news releases at key project milestones.

8BELLS will pursue moreover participation and co-writing in articles, papers, whitepapers and concept notes with other consortium members.

Moreover, 8BELLS will incorporate the results regarding cybersecurity into its commercial and research activities, thus providing the results to its customers. Finally, 8BELLS through its participation in the H2020 SPEAR cybersecurity project and other projects will work on building liaisons with 5G-PPP, cPPP and other similar initiatives that may use results of the SPIDER project.

- **FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS (FORTH)**

FORTH as an academic partner will disseminate in the scientific community the research achievements obtained within the project. They will target very high-profile publication venues (see below) for the security, security training and awareness, 5G and system engineering domains. FORTH will also incorporate the project results within their advanced educational activities, disseminate the knowledge and expertise gained through SPIDER project to a large number of MSc and PhD candidates. Integration of results in advanced studies is known to have the capability of filling the gap between classical technical disciplines and interdisciplinary socio-technical domains like systems' security, cellular technologies and communication applications.

Some list of events to participate, and publish results:

- **Journals:** International Journal of Internet of Things; Advances in Internet of things (Scientific Research open ac-cess); ACM Transactions on Software Engineering and Methodology; ACM Transactions on Information and Systems Security; IEEE Transactions on Secure and Dependable Computing, IEEE Transactions on Information Forensics and Security; Computers and Security; IEEE/ACM Transactions on Networking; Springer International Journal of Information Security; Springer Wireless Personal Communications; Elsevier Network Security;
- **Magazines:** IEEE Security and Privacy; IEEE Cloud Computing; and IEEE Internet Computing.
- **Conferences**: ACM Conference on Computer and Communications Security; ESORICS – European Symposium on Research in Computer Security; ACM/IEEE International Conference on Cyber-Physical Systems; IEEE International Conference on Pervasive Computing and Communications; IFIP International Information Security and Privacy

Conference; IEEE Symposium on Security and Privacy; ACM Conference on Computer and Communications Security; ACM Conference on Data and Application Security and Privacy; IEEE International Conference on Internet of Things; and European Conference on Smart Objects, Systems and Technologies.

- **Special Issues in Scientific Journals:** The partners will take the initiative of jointly creating special issues in the area of IoT in scientific journals, and invite top international colleagues to be part of the initiatives.
- **Other Events**: ENISA NIS Summer School, ICT: Imagine Digital - Connect Europe, FIRST.org Annual Conference, Researcher's Night

- **SERIOUS GAMES INTERACTIVE APS (SGI)**

SGI aims to reach groups that cut across the domains of training, serious games and gamification.

- **Fellow Professionals:** We will focus on disseminating the project as a case study that highlights different aspects of the project development and learning depending on the specific domain. Preferable we will identify events and channels that are cross-domain.
- **Researchers**: This is not our primary network but we will provide a lightweight article that will share the results from the pilots. The focus will be on providing evidence where such intervention work or just as important doesn't work to make sure future investments in 5G security training is solid.
- **Companies**: We will showcase the results of the intervention to raise skills and awareness to make companies consider investing in cybersecurity. We will focus on companies that are more at risk with the 5G e.g., manufacturing companies that will be reliant on IoT to run critical business processes.
- **Social media:** The project hashtags of the generated social media channels will be used for all national and European level social media dissemination. We would like to reach the right level of level dissemination with regular postings being conducted. Social media will be used for awareness-raising towards the target groups using our main channels such as LinkedIn and Facebook.
- **Events/Conferences**: SGI will also attend several events (looking also for other opportunities as the event space is fluid) including the following:
  - CeBit: Historically the event has featured serious games, and with its affinity to IoT and Security, this would be a good venue.
  - LearnTec: One of Europe's strongest sites for corporate digital learning that could be a good window to showcase results from the project.
  - Online Educa: One of Europe's best event for training and education in the inter-section between companies and research.

- **UNIVERSITY OF PIRAEUS RESEARCH CENTRE (UPRC)**

UPRC, as an academic partner, plans to disseminate the results of SPIDER primarily through scientific publications in high-impact, both national and international conferences, workshops, and journals.

Additionally, the active participation of UPRC in several national and European research projects and collaboration groups, will be leveraged to further communicate the results of SPIDER to the research community, as well as build new collaboration channels in the field.
However, UPRC will not only act as a pure academic and research unit. Due to its close and strong collaboration with commercial, industrial and public organizations such as the General Secretariat of Research & Technology, the National Documentation Centre (NDC), and the Technical Chamber of Greece, UPRC will disseminate the results of SPIDER at a national level towards the general public and the industrial community being represented in the aforementioned groups.
Through a series of well attended, annual events that the UPRC researchers participate to every year (e.g., Infocom Security conference, eCommerce & Digital Marketing Expo, and more), the solutions offered by SPIDER will be introduced to key players in the industry, such as telecommunication service providers and cybersecurity companies.
The team of UPRC will also pursue participation to industrial workshops, scientific seminars and public events such as the Researchers' Night, the European Cyber Security Month, and the European Cyber Security Challenge, which are European initiatives aiming at bringing awareness to the public.
Specifically, regarding the European Cyber Security Challenge, due to the well-established communication channels with ENISA and the leading role of UPRC for the Greek participation in the contest, SPIDER platform is planned to be leveraged for the training of the Hellenic Cyber Security Team. To further support the dissemination of SPIDER, UPRC's Systems Security Laboratory (SSL) which maintains its own website and social media (i.e., Facebook, Twitter and LinkedIn), will promote the project along with any communication activities taking place within its framework. Finally, the SPIDER results will be demonstrated in dedicated lectures and training sessions for the undergraduate and postgraduate students of the university.
To summarize, the UPRC members will actively disseminate project results through different means: (i) scientific publications in high-impact journals and conferences, (ii) participation in both national and European events / exhibitions, (iii) organization of targeted sessions (e.g., workshops) with respect to SPIDER research focus, and (iv) training sessions/lectures in undergraduate and postgraduate programs

- **City University London**

As an academic partner, City, University of London will handle the scientific dissemination activities through the publication of results in international peer-reviewed journals and technical conferences. **Specifically, dissemination of the insights will be achieved via:**

(i) Technology transfer,
(ii) Courses, advanced workshops and seminars organised by City University London, and
(iii) Participation in events to communicate the research findings and the modelling methodology that are derived as key outputs from the SPIDER project.

City, University of London will be leading WP5 and is in charge of deliverables D5.3 and D5.4. These are briefly described below:

- **D5.3: Asset pricing and impact loss analysis: an empirical framework.**

This deliverable will report on the system's risk exposure under different scenarios as well as the interdependences and correlations between asset vulnerabilities.

- **D5.4: An empirical decision-support framework for econometric analysis of cyber risk and investment.**

This deliverable will report on the empirical framework that supports the CIC Component of SPIDER. We expect to deliver peer-reviewed academic papers for publication in journals such as Annals of Operations Research, European Journal of Operational Research, Management Science or Operations Research. In order to receive feedback at intermediate stages of the work, we will also endeavour to present this work at major international conferences, such as the Annual Meeting of the Institute for Operations Research and the Management Sciences (INFORMS) and the annual Real Options conference

- **CyberLens LTD**

CLS will actively participate in the dissemination activities of SPIDER through publication in areas related to technical outputs in which CLS is responsible for in the project, such as decision-support approaches for cyber security investments and the effective management of cyber security risks. The major dissemination channel will be research publications at top-quality international journals (e.g., ACM Decision Support Systems Journal, IEEE Intelligent Systems Magazine) and conferences (e.g. ESORICS, Workshop on the Economics of Information Security - WEIS) in the broad area of cyber security investment decision support, and any relevant forums (e.g., European Commission Cyber Security & Privacy Innovation Forum) as opportunities arise.
CLS will also contribute to the production and wide circulation of marketing material like leaflets and posters specifically adapted to professionals and technical communities. Market assessments and reviews in areas relevant to SPIDER will also be provided through the CLS website and on its blog with regard to project-specific outputs.

- **INFALIA PRIVATE COMPANY (INFALIA)**

In the following Table 7, INFALIA's planned dissemination activities are estimated in the project's timescale (i.e. in terms of semesters).

Table 8: INFALIA's planned dissemination activities

	SPIDER					
	Year 1		Year 2		Year 3	
	Semester I	Semester II	Semester III	Semester IV	Semester V	Semester VI
Social media posts	1	2	3	3	6	6
News posts	1	2	3	3	4	4
Publications in conferences / journals						2
Networking and clustering activities		1		1		1
Communication with potential clients						2

The table provides a set of measurable indicators for a list of dissemination activities ranging from blog posts and social media posts to scientific publications and communication with clients.

More specifically, for social media posts and for news posts, INFALIA counts both posts to be uploaded to the SPIDER website and social media accounts, as well as posts that will be uploaded to the company's website and social media accounts.
INFALIA plans to perform social media and news posts when there is a significant scientific progress in the project, or a newsworthy outcome is arising.
INFALIA envisages contributing to at least two publication in the final semester where most subsystems will be finalised, and the SPIDER platform will mature.
INFALIA will target prestigious journals, such as Data & Knowledge Eng., Data Mining & Knowledge Discovery, Knowledge & Inf. Systems, and Information Sciences, as well as security-oriented conferences, such as Security & Policing Event, ARES Conference, Annual Privacy Forum, and EISIC.
In addition, INFALIA aims to participate in three networking and clustering activities (one per year) that will emphasize the outcomes of SPIDER. Near the end of SPIDER's lifetime, INFALIA will pitch the project and its services and solutions to at least two clients, stemming from the public sector where most customers of INFALIA are derived.

- **INFOCOM S.R.L. (INFOCOM)**

INFOCOM will support major SPIDER partners in the production of scientific literature published in relevant conferences, journals or books and will contribute to the set-up of exhibitions and trade shows for showcasing and demonstrating SPIDER achievements.

- **SPHYNX TECHNOLOGY SOLUTIONS AG (STS)**

STS will participate in joint publication initiatives along with other consortium partners. They will also participate in major EU events, such as meetings and workshops organized by ENISA and SANS (https://www.sans.org/) information security events and will present enhancements of its products, based on the ongoing work during the project, to key industry centric events such as the INFO SEC.

- **K3Y LTD (K3Y)**

K3Y intends to enhance SPIDER dissemination plans in a) publishing scientific articles in international, peer-reviewed journals and conference, b) preparing public material and c) establishing communication channels in Bulgaria and in the south-east Europe.

In particular, will carry out high-level research, the results of which will be published in popular IEEE, ACM, Elsevier and Springer journals such as:

a) IEEE Security and Privacy,

b) IEEE Transactions on Cybernetics,

c) IEEE Transactions on Information Forensics and Security,

d) IEEE Systems journal,

e) Computers and Security,

f) ACM Transactions on Information and System Security and

g) International Journal of Information Security.

Similarly, K3Y aims at publishing cutting-edge results in well-known International Conferences such as:

a) ACM Symposium on Computer and Communication Security,

b) IEEE Symposium on Security and Privacy,

c) USENIX Security Symposium and

d) IEEE Computer Security Applications Conference. K3Y will undertake the preparation of public multimedia material such as videos published in the YouTube channel and the presentations hosted in SlideShare, containing educational material, SPIDER information material and initial research findings. K3Y will establish dissemination strategies in Bulgaria by disseminate the Scopus and the results of the SPIDER project in networks of start-ups in Bulgaria and in ICT companies such as the Bulgaria Startups (http://www.bulgarianstartups.org), Start-up Catalyst (http://www.startupcatalyst.com.au/) and European Start-ups (http://www.europeanstartups.org/).

7. PARTNERS INDIVIDUAL EXPLOITATION PLANS

Below the consortium partners individual exploitation plans are being presented

- **ERICSSON**

ERICSSON is one of the leading providers of Information and Communication Technology (ICT) with a complete offering that comprises services, software and infrastructure for telecommunication operators, traditional telecommunication and Internet Protocol (IP) networking equipment, mobile and fixed broadband, operations and business support services, and an extensive services operation.

Its main Business Unit, the Networks one, has been considered among the strategic drivers in the development of 2G, 3G, 4G/LTE technologies and it is now proposing itself as a world leader for the incoming 5G implementations.

The network infrastructure development is tackled from a 360 degree perspective spanning from 5G Access to 5G Transport, from Network Services and Automation to Cellular IoT, from fixed wireless access to mission critical and private networks and embraces all the network domains and technologies, from the radio access domain to the transport one, from the distributed cloud and NFV to the centralized data centres.

With 5G we see the transition to a mostly all-software network, and considering the cyber vulnerabilities of software, the tougher part of the real 5G “race” is about the hardening of the most important network of the 21st century and developing stronger protection of the ecosystem of devices and applications that originated from that network.

In this overall landscape the Cyber-Security context represents a crucial aspect that is being addressed with great efforts by Ericsson to face the increasingly stringent customers’ needs and expectations.

To support this view, it is strategic for Ericsson to increase its scientific collaborations with qualified partners in an excellent enlarged industry and research teamwork.

In this perspective the innovative SPIDER framework is an opportunity for Ericsson to extend portfolio proposal creating opportunity for its Customers to validate their networks, upskill their telco security professionals and drive their networks investments in order to face the 5G technology challenges.

- **Consorzio Nazionale Interuniversitario per le Telecomunicazioni**

With the participation in the SPIDER project, CNIT wants to reinforce its position in cutting-edge research topics concerning cybersecurity and spread the knowledge through its MSc and PhD sponsored programs.
CNIT will also internally exploit the results to offer solutions and expertise to its partner universities and to use the SPIDER platform in education and training.
Besides, SPIDER generated results and know-how will be used for future research and involvement in similar projects, enhancing hardware and software tools that can constitute platforms and resources to be exposed in new proposals.

This is the case of the test bed that CNIT is building in the framework of the SPIDER project; as a general-purpose test bed, it can serve to support other future research projects. Additionally, CNIT plans to exploit the results obtained in the SPIDER project either letting other partners use them on a royalty-free basis or, on the contrary, on fair and reasonable conditions, depending on the specific agreement to be reached.
Though it is a non-profit organization, CNIT may have a part of commercial activity, consisting of consulting services or of engineering part of the solution for inclusion of the jointly owned results in the other partner's production line. Indeed, CNIT is strongly committed to technological transfer, especially to start-ups and spinoffs that create new market and job opportunities, and this activity is fed by the results CNIT obtains in this kind of projects.

- **TELEFONICA I+D S.A.U. (TID)**

TID will disseminate and exploit the project results in Telefonica, with the goal of promoting them within the group's strategic 5G roadmap. The practical orientation of this proposal, with validations on different scenarios related to new services and vertical sectors 5G technology, and additional results of high interest, will foster its application in several trials and tests in the relevant Telefonica business units in Europe and the world.
Knowledge and results transfer is in active progress within Telefonica Data unit (LUCA) and Telefonica cybersecurity Unit (11Paths). TID's expectations to leverage the SPIDER results as part of the variety of security services in design or already in production to enhance their capacity. Some examples are Managed Security Operations service or Clean Pipes product. Also, the long-term plans will focus in rollout a SPIDER model integrated with 5G network evolution services.
TID is also interested in possible patents for the services and system pieces derived from the SPIDER model.

- **THALES SIX GTS FRANCE (THALES)**

THALES proposes the Cybels Range platform as the foundation of its cyber training offer, from the delivery of the platform itself up to the services to assist its customers in the platform usage and to increase their experience. The Cybels Range platform allows creating complex network topologies that reproduce the behaviour of real-life systems.
The Cybels Range platform's architecture consists of the following elements:

(1) a virtualization platform that supports the virtualization of typical network topologies and their assets;
(2) the virtualization of hosts and information systems;
3) a traffic generator;
4) an administration platform.

The exploitation of the innovations brought by the SPIDER project are expected to allow better flexibility in the deployment of the Cybels range platform on top of softwarised assets, such as OpenStack VIM and cloud resources representing a market advantage. Also, the specific 5G industry targeted in SPIDER represents a novel market segment for THALES both in cyber range deployments and in cyber security products.

- **ATOS SPAIN S.A. (ATOS)**

Atos is a global leader in digital transformation with 120,000 employees in 73 countries and annual revenue of € 13 billion. European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions through its Digital Transformation Factory, as well as transactional services through Worldline, the European leader in the payment industry. With its cutting-edge technologies and industry knowledge, Atos supports the digital transformation of its clients across all business sectors. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos Syntel, Unify and Worldline. Atos is listed on the CAC40 Paris stock index.

Atos Research & Innovation (ARI) is the R&D hub for emerging technologies and a key reference for the whole Atos group. With almost 30 years of experience in running Research, Development and Innovation projects, we have become a well-known player in the EU context.

In recent years, ARI has been characterized by a wider strategic integration of research and innovation activities with Atos approach to business. As a result, Innovation Hub (IH) unit is born in 2018 to foster and facilitate the innovation at ARI.

In order to achieve such mission, about twenty business consultants and communication experts work in collaboration with researchers, technicians and managers in innovation projects to support them in finding the best way to communicate and approach their technological results to the market; to envisage the impact of future research may have in the market; and to facilitate the transfer of generated innovative results to the Atos business units.

The main objectives of the IH are:

- Maximize the impact of the ongoing research projects in and out of Atos. Thanks to the large and extensive experience of Atos in this kind of projects, we apply an own and proven methodology based on latest marketing and business development techniques, and a catalogue of good practices and examples for plans and reports, which have entailed satisfactory results in numerous projects.
- Transfer those solutions we consider relevant to generate new business in Atos, carried out then the research results closer to the market and demonstrating the innovative capacity of Atos. This requires establishing a permanent link and close to the business units and communicate internally in an efficient and constant manner our results to such units.
- To ensure a proper transfer, we provide some incubation units for the most promising and aligned solutions with the company's strategy. The idea is to transform the ARI solutions in solutions for the market reusables in commercial projects. Each incubator is in charge of mature and evolve the seed solution, by fostering the development of pilots with customers or internal proof of concepts, where to show the business feasibility of the solution. Besides, each incubator (called shuttle) supports the elaboration of commercial bids and tenders which include the use of such solutions; provides training to the business units; and offers technical support to delivery projects born from the transferred solution.

The activities that ATOS will develop in SPIDER will allow not only preserve the current business but also extend and provide our clients with the cutting-edge technology that impulses their business. SPIDER purposes connect perfectly with the ATOS commitment in the cybersecurity arena and will entail new business opportunities increasing our solutions and services portfolio. For this purpose,

the first step is to approach the market through the ATOS sales team communicating internally across all Atos business units and GBUs the ARI assets and results (innovation workshops, digital show, etc.) and to promote the adoption of innovative solutions and emerging technologies bringing R&D project results closer to market.
There is a systematic and permanent process in place to detect promising assets from R&D projects; to present them to the Innovation Board where most promising are evaluated by business units and experts; and to set up a commercialization roadmap for the winners after evaluation. Other exploitation activities will be establishing partnerships with the rest of Europe increasing our competitiveness, having the opportunity of exchange know-how with research institutions, public administrations and industrial partners.
This project will be carried out by the R&D team who will ensure a continuous research in that area after the project. In this sense, the exploitation of SPIDER project results in current and future R&D projects is also of key importance for the company.

- **UBITECH LIMITED (UBITECH)**

UBITECH aspires to reinforce its solutions portfolio through the offering of innovative and specialised applications and services not yet present in the market or through the expansion and optimization of its current services and prototypes (in particular, exploiting the outcomes of the ARCADIA H2020, SPIDER H2020 and ASTRID H2020 projects) exploiting the acquired know how and the technological results of the proposed project in order to proceed to the implementation of integrated vertical solution in the field of optimized deployment, security, certification and trust of end-to-end 5G services in vertical industries. This way it will increase its competitiveness, targeting in both the public and private sectors and especially the industry.
Thus, UBITECH aspires to include the proposed project' exploitable outcomes to the overall corporate offerings and promote, exploit and commercialize the developed framework and mechanisms to its existing clients list as well as to the Spanish-speaking countries of Central and Latin America wherein UBITECH operates through its subsidiary in Buenos Aires (Argentina) and its business partner in Guayaquil (Ecuador).

- **UNIVERSIDAD POLITECNICA DE MADRID (UPM)**

As an academic institution, UPM focuses on non-profit exploitation activities. In accordance with this profile, these consist primarily in leveraging SPIDER innovation results and the knowledge and experience acquired from them in future R&D projects.
The knowledge obtained in the project will be exploited through the following activities:

- Publication and dissemination of project results. Publication and presentation of project achievements and innovation results in technical journals and conferences. (time schedule: 36 months).
- Postgraduate courses. The results of SPIDER will be used in Master and PhD courses and seminars. (time schedule: 36 months)
- Master and PhD theses. We will propose master theses related to SPIDER and attract students to these in the next years. (time schedule :36 months).

Regarding further research and development, we will investigate new research areas extending project results and finding synergies and collaboration opportunities in future projects and applications, both at the regional and the international level (time schedule: 3-5 years).
In addition, we will explore options to secure IP generated within the project and launch and incubate spin-offs or license the IP, all with the ultimate goal of introducing innovative services and/or products into the market. UPM created the Centre for Support for Technological Innovation (CAIT – its initials in Spanish) in 2010 with the fundamental objective of promoting the exploitation of the results of R&D activities as well as serving as a stimulus to the innovation process in the business ecosystem close to the UPM.
In this context, CAIT will explore options to secure IP generated within the project and launch and incubate spin-offs or license the IP.

- **FONDAZIONE BRUNO KESSLER (FBK)**

FBK is already working on five spin-offs originating from previous FP7/H2020 research projects; local public bodies are encouraging and supporting these initiatives. The innovations from SPIDER will be candidate for further business exploitation within new spin-offs. Moreover, FBK, as an official member of the EIT Digital initiative, will identify exploitation opportunities together with key stakeholders to ensure faster go-to-market opportunities of the SPIDER concepts and technologies. The outcomes of SPIDER will contribute to the overall strategy in the 5G landscape where FBK is heavily involved with its participation to four 5G-PPP projects.

FBK plans to exploit the results of this project by:

(i) Enhancing its know-how in the field of open smart cities and regional infrastructures,
(ii) Connecting with similar initiatives at the EU and global level, and
(iii) Strengthening its position in the development of future infrastructures for research and innovation.

- **SINGULAR LOGIC ROMANIA COMPUTER APPLICATIONS SRL (SLGRO)**

SingularLogic Romania (SLGRO) strongly supports the platform to be implemented by the SPIDER project, as it believes that the methods and tools to be developed through the proposed project are of broad interest towards its extending target. To this end, SLGRO intends to play an active role in this process as a system integrator and a software-as-a-service solution provider, identifying the platform to be developed as an important tool for the future Security and SaaS-based corporate strategy. Overall, the SPIDER project outcomes are expected to deliver impact on the services offered by SLGRO.
The company's internal planning shift concerns the extension of our current product portfolio with security services (e.g. risk assessment). Therefore, as soon as the first outcomes of the project will become available, they will be evaluated to this direction.

- **EIGHT BELLS LTD (8BELLS)**

As a market-oriented company, 8BELLS will take advantage of SPIDER project to enhance future reports and seminars related to cybersecurity testing and assessment, with specific focus on business cases as well as other opportunities that may rise via the proposed environment for

cybersecurity preparedness. Stakeholders involved in the industry will use these market reports to understand better the opportunities and also to manage more easily, more securely, and with greater resiliency the SPIDER cyber range concept.
Furthermore, the SPIDER project will then help strengthen 8BELLS position as reference of international centre of excellence for cyber security and networking modelling. 8BELLS will participate and support all the necessary activities for the commercial exploitation of SPIDER, including the investigation to form a new legal entity (e.g., start-up).

- **FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS (FORTH)**

FORTH: The results of the SPIDER project will be exploited by the established mechanisms of FORTH. Those include the PRAXI network (http://praxinetwork.gr/el), the Science and Technology Park of Crete (STEP-C) (http://www.stepc.gr/) and FORTHcert (http://www.forthcert.gr/). Through PRAXI Network benefits and technologies produced by the project can be exploited by SMEs, especially those involved in 5G technologies. FORTH has a well-established CERT, namely FORTHcert, which collaborates with CERTs/CSIRTs in EU.
Tools produced by SPIDER can be used for training and awareness creating operational links with other CSIRTs or end users. Technological and Cybersecurity knowledge can also be disseminated and exploited through FORTHcert.

- **SERIOUS GAMES INTERACTIVE APS (SGI)**

Overall, SGI aims to build a strong business case for future companies to invest in skills and awareness training. This will extend from our existing expertise in the area where we have already delivered solutions to the Danish Home Office (www.samtaenkning.dk) serving important infrastructure companies in Denmark and one of the biggest banks in Denmark.
SGI has also recently been invited to provide cybersecurity serious games proposals for two global companies. Evidence from the SPIDER pilots will also be used to build a strong business case, so we can attract companies that will invest in their own solution.
The topics/domains SGI aims covering include:

- *Domain analysis:* We will early in the project examine the needs of European companies to make sure the solution developed have broad relevance, and we design a solution that is not just relevant for pilot sites
- *Evidence:* We gather evidence in terms of impact both on awareness, skills, knowledge, perception and behaviour. This evidence is crucial to convince future interested companies
- *Business case:* We construct a business case in the form of a slide deck that shows the potential of the offering, and how much already exist from the research project that commercial companies can build upon
- *Service offering site:* We make a dedicated landing page for offering cybersecurity serious games/gamification service tailored around the solutions developed in this project. This is put on our website that scores among the highest in Google search index for serious games

- **UNIVERSITY OF PIRAEUS RESEARCH CENTRE (UPRC)**

UPRC, as a non-profit academic institution, intends to be involved in challenging, real-life problems that extend its research interests to new areas and thus advance and proliferate scientific knowledge. Nonetheless, UPRC members aim at actually exploiting the outcomes of research and innovation projects, by developing and releasing "products" that meet a set of quality requirements such as software tested, accompanied documentation, installation guidelines and best practices.

The goal of this strategy is twofold:

(i) Showcase through tangible results the expertise of the UPRC team and the added-value that could be brought based on these results in different domains not necessarily relevant to the project scope (e.g., security approaches applicable to healthcare, maritime, smart power grid, and industrial control systems), and

(ii) Provide the ground for spin-off companies that will further exploit these results (based on the outcomes obtained initially through their applicability in different domains as explained previously).

UPRC exploitation will be in the context of UPRC's strategic plans in the areas of:

(i) Education: the SPIDER results will be proliferated among the attendants of the University activities, mainly among postgraduate and continuing education programs due to the advanced nature of the topics,

(ii) Technology transfer to the Greek IT industry that includes a wide portfolio of cyber security and telecom institutions, offering technology transfer services to companies and public bodies through joint projects, and

(iii) Technology promotion in the Greek industry as part of an effort to increase the adoption of SPIDER technologies.

Moreover, UPRC has close and strong collaboration with commercial, industrial and public organizations providing specialized scientific expertise and innovation to improve and enhance products and services. For example, UPRC members are often invited by private and public bodies to evaluate the level of security.

The exploitation plan of UPRC addresses different domains, both in terms of focus and in terms of target groups. With respect to focus, UPRC targets multi-disciplinary domains by developing research outcomes into a form that can be used in different contexts. Lastly, the communication channels between the UPRC and ENISA, and especially the Hellenic Cyber Security Team, which competes annually at the European Cyber Security Challenge, offer a unique opportunity to pursue the exploitation of the SPIDER platform, either during the competition as part of the challenges, or for the purposes of training of the national teams.

- **City University London**

CITY will leverage on both the research and the innovation activities carried within SPIDER since these will offer the basis for novel and advanced academic and entrepreneurship experiences. Moreover, the results and tasks undertaken SPIDER will form a valuable material for CITY's research and training of PhD students, advanced seminars offered to the M.Sc. students, tutorials and training courses at national and international scientific events with emphasis on cyber security economic analysis, policy making, and practical risk assessment.

As CITY, University of London is an academic partner, exploitation plans may involve activities to promote related academic programs and enhance the collaboration between academic departments in view of enhancing research output.

- **CyberLens LTD**

CLS aims to exploit the outcomes of research and innovation projects by developing and releasing "products" that meet a set of quality requirements such as software tested, accompanied documentation, installation guidelines and best practices.

The goal of this strategy is twofold:

(i) Showcase through tangible results the expertise of the CLS team and the added-value that could be brought based on these results in different domains not necessarily relevant to the project scope (e.g. security approaches applicable to healthcare, maritime, smart power grid, and industrial control systems), and

(ii) Provide the ground for the company to further exploit these results (based on the outcomes obtained initially through their applicability in different domains as explained previously).

Overall, CLS will gain significant insights from the results of SPIDER that will reinforce the company's position through the upgrade of its software solutions such as the DEFENDER (DEcision support for efFEctive aNd buDget constrainEd Risk management) tool that addresses the problem of cyber security decision making in 5G ecosystems under increased uncertainty. CLS will aim to identify opportunities for technology transfer into industry, e.g. by transferring technological know-how and/or integrating the software components developed in the SPIDER project in future collaborations with industrial partners, e.g. 5G vendors, cybersecurity consultants, in the Netherlands and in the rest of the EU.

These potential new business collaborations resulting from SPIDER will clearly give CLS the capacity it needs to transform the company's current line of business applications in the field of risk management to solutions relevant to economics of 5G security.

- **INFALIA PRIVATE COMPANY (INFALIA)**

INFALIA will exploit the project results by reinforcing its competencies in collecting 5G network data, providing visual analytics and performing incident detection for the 5G cyber security domain. INFALIA is interested in commercialising components of the developed platform by licensing the developed services to the interested clients. The visual analytics dashboard, and the network data collection toolkit can be further developed by INFALIA after the end of the project, to meet the new market security needs.

INFALIA will also contribute actively to bring the SPIDER solution to the market in cooperation (and by considering the IPR agreement) with the other industrial partners.

INFALIA participates in SPIDER as a technical / industrial partner and its exploitation activities dealing mainly with the commercial exploitation of the project outcomes. INFALIA aims at reaching the 5G market and the telecommunications industry associated with cybersecurity, training, certification,

experimentation and validation of new approaches that will occurred in the project's lifetime. As a spin-off company of CERTH/ITI, INFALIA has also access to both academia and research field, which will further promote the potentiality to further exploit the project's results.
Although the core exploitation of SPIDER will be provided as a PaaS or SaaS solution, there are various type of services that can be created on top of this and offered as a separate service towards potential customers or users of SPIDER. Whereas both PaaS and SaaS are focusing more on the setup, deployment and implementation of the platform, there is room for specific add-on services such as training, customisation and process guidance. INFALIA aims to provide customisations and training focusing mainly in the visualisation of data.

- **INFOCOM S.R.L. (INFOCOM)**

INFO's business activities include the design of tailored ICT solutions for the support of non-safety-critical application in the railway field (spanning network infrastructures for the interconnection of track side sensors and software tools for Supervisory Control And Data Acquisition – SCADA - systems). INFO also aims to extend the reach of such solutions to other similar vertical applicative scenarios, such as Smart Cities, Smart Logistic and Smart Factories, as well as to update them in line with the emergence of 5G technologies.
One of the key issues that all potential vertical clients are increasingly aware of and constitutes a key differentiator for a winning offer is certainly security. In this regard, INFO will exploit SPIDER outcomes so as to:

  - Improve company's awareness about 5G infrastructure and 5G-based services security issues and, consequently, with meaningful design rules to strengthen infrastructures and services;
  - Industrialize tool, derived from SPIDER prototypes, to evaluate and test the resilience of critical 5G infrastructures and services against advanced cyberattacks, which INFO could conveniently exploit in the design and validation phases of tailored 5G-based vertical solutions.

- **SPHYNX TECHNOLOGY SOLUTIONS AG (STS)**

STS will use the outcomes of SPIDER project to strengthen its service and product portfolio. The plan is to augment the security assurance and certification platform in order to support cyber security training programmes, such as providing monitoring and dynamic testing, establishing interoperability with emulation environments etc.
STS's main goal is to deliver new cyber security training programmes after the end of the project

- **K3Y LTD (K3Y)**

K3Y will exploit the results and the products of the SPIDER project by utilizing its capacity in creating, maintaining and improving the gamified cyber exercises that will be developed throughout the project. The K3Y's participation in the creation of serious games for cybersecurity training purposes creates new opportunities to the enterprise as it provides the ability to create new products and aim new markets. Contacts and interactions with companies in the private sector in Bulgaria will be exploited to highlight the benefits of the SPIDER capabilities for training purposes.

8. STANDARDIZATION PLANS

The main objective of the standardisation task of SPIDER is to succeed exposure of the project results on national and international professional societies as well as standardisation bodies.

The consortium has a strong will and ambition to distribute, transfer and exploit the knowledge, experience and relevant project results to the European community and worldwide and as a research and innovation action, the SPIDER project expects to contribute to related standards as much as possible. Thus, whenever applicable, SPIDER will build on and promote existing or emerging standards of any nature, including specifications from standardization bodies and contributions to open-source communities, and seeking for all kinds of collaboration, from the direct contributions to specifications or code-bases to applicability statements and proof-of-concept demonstrators to assess the viability of proposed solutions. SPIDER holds a dedicated task for standardisation (Task 8.3), aiming at achieving a high level of contribution to current and future standardization efforts, which aim to internationalise the results beyond European borders. Several standardisation bodies and organisations that are relevant to SPIDER have already been identified. It should be noted that this list of bodies will be constantly updated during the lifetime of the project. A preliminary plan of SPIDER's contributions to standards is presented in Table 9:

Table 9: Standardisation fora relevant to SPIDER and foreseen contribution areas

Standardisation Forums & Open Source Initiatives	SPIDER Partners	Expected contributions
Open Platform for NFV (OPNFV)	ERICSSON	Virtualisation and orchestration of the SPIDER network functions; VNF Manager functions for the ENM entity.
OpenStack, OCCI THALES	THALES ATOS	HW acceleration functionalities for the vSOC; Data analytics functions for cyber range's security analytics.
ETSI NFV ISG	TID	NFV applicability in cyber range scenarios; Dataset generation mechanisms and interfaces; Cyber range automation scenarios; Security analytics and dataset characterization.
Internet Engineering Task Force (IETF) groups	TID	Cyber range management interfaces; Dataset generation and applicability; Security analytics and data-driven security management.
3GPP SA5	TID	Applicability and assessment on security analytics for 5G networks.
NGMN Alliance	TID	Define 5G requirements in relation to cyber ranges and corresponding

Standardisation Forums & Open Source Initiatives	SPIDER Partners	Expected contributions
		cybersecurity preparedness offerings in SPIDER.
ETSI OSG OpenSource MANO (OSM)	TID UBITECH	Security orchestration functionalities; Data-driven security management mechanisms.
ISO/IEC 27000	SGI	Alignment of both the 5G cyber security serious games and 5G cyber security gamification game with the ISO/IEC 27000.

The SPIDER project has appointed a dedicated Standardisation Manager (SM), who will be dedicated to promote the standardisation potential of the project results and coordinate the standardisation activities in the project. The main activity of the SM is to monitor and plan the standardisation strategy together with the Innovation Manager (IM) and the Technical Manager (TM), and to periodically monitor and assess the standardisation potential of the scientific results from the project.

A procedure to stimulate, prepare and submit standard contributions is described below:

- The SPIDER consortium led by the SM will constantly assess the standardisation potential of the project's key innovations
- The consortium will be continuously leasing with various standardisation bodies and initiatives in order to ensure that SPIDER is building upon emerging standards.
- After identifying the most important and relevant SPIDER innovative aspects that need to be standardised, then the consortium will map these key exploitable innovations to the most appropriate standardisation objectives in order to prepare a concrete plan for submitting contributions to selected standardisation bodies.
- The SM along the rest partners will establish and follow an appropriate methodology on how to transform these innovative aspects into standards contributions, including the identification of appropriate industrial channels for pushing the SPIDER standard contributions to respective Standardization Bodies
- The SM will coordinate the SPIDER standard contributions across the respective standard developing organizations and other related forums and along with the Project Board will ensure that these contributions follow the initial strategies and aims of the project
- The SPIDER partners (individually or collectively) will put efforts to maximize the chances of success of the project's standardization strategies

9. LIAISON AND INTERACTION WITH 5G-PPP PROGRAM AND CPPP-ECSO

The objectives of the SPIDER dissemination activities include the establishment of connections within the 5G-PPP programme, in an aim to exploit the possibilities for enhancing collaboration and this can be succeeded through the participation in the most relevant of 5G-PPP working groups **[6]** like for instance the 5G- PPP Security Work Group **[7]** leading the contributions coming from the outcomes of the project

5G PPP Security Work Group

This WG was officially launched on 5/4/2016 and results from an initiative created by a Phase 1 Security Project (5G-ENSURE) **[8].** Since its creation this Working Group has been the place where the 5G Security topics and vision were discussed and progressed. By the end of Year 2017 and per decision of the 5G Industry Association Board this WG was moved to 5G IA. As such this WG is not only open to Projects from any of the phases of 5G-PPP but also to 5G IA members interested in joining. The purpose of the group is to drive the 5G Security Vision by working in a coordinated and complementary manner to support a common security architecture able to address the key security areas for 5G and moreover to foster development of the 5G Security Community made of 5G security experts and practitioners who pro-actively discuss and share information to collectively progress and align on the field**.** This while organizing specific communications/events (e.g. Whitepaper, Workshop …), interacting with other WGs whenever Security input is needed nd developing liaisons with other interested/interesting Security communities.

cPPP-ECSO

The European Cyber Security Organisation (ECSO)**[9]** ASBL is a fully self-financed non-for-profit organisation established in 2016 that's represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). The aim of the cPPP[10] partnership is to foster cooperation between public and private actors at early stages of the research and innovation process in order to allow people in Europe to access innovative and trustworthy European solutions (ICT products, services and software) that take into account fundamental rights such as the right for privacy. It also aims to stimulate cybersecurity industry, by helping align the demand and supply sectors to allow industry to elicit future requirements from end-users, as well as sectors that are important customers of cybersecurity solutions). The cPPP will be instrumental in structuring and coordinating digital security industrial resources in Europe. It will include a wide range of actors, from innovative SMEs to producers of components and equipment, critical infrastructure operators and research institutes, brought together under the umbrella of ECSO.

10. 5G-PPP PROJECTS, FORUMS AND SPIDER

This section provides an overview of other H2020 collaborative projects which can be considered as relevant to the SPIDER project. Therefore, the consortium will investigate all the possible ways to liaise and connect with these projects, exchange information on project progresses and when feasible, schedule and organize joint activities that can take the form of joint scientific papers, joint events and technical panels organized in international conferences. Possible joint activities will be explored by the consortium partners and evaluated on a step-by-step basis during the project lifetime

MATILDA

The vision of MATILDA **[11]** is to design and implement a holistic 5G end-to-end services operational framework tackling the lifecycle of design, development and orchestration of 5G-ready applications and 5G network services over programmable infrastructure, following a unified programmability model and a set of control abstractions. It aims to devise and realize a radical shift in the development of software for 5G-ready applications as well as virtual and physical network functions and network services, through the adoption of a unified programmability model, the definition of proper abstractions and the creation of an open development environment that may be used by application as well as network functions developers.

ASTRID

The ASTRID project **[12]** aims at addressing threats for virtualised services using a smart orchestration logic. More specifically, ASTRID wants to address the issue of threats coming from the virtualization layer itself and other security threats that have to be managed from people without enough skills or specific expertise. The ASTRID project aims at shifting the detection and analysis logic outside of the service graph, by leveraging descriptive context models and their usage in ever smarter orchestration logic, hence shifting the responsibility for security, privacy, and trustworthiness from developers or end users to service providers. This approach brings new opportunities for situational awareness in the growing domain of virtualised services: unified access and encryption management, correlation of events and information among different services/applications, support for legal interception and forensics investigation. ASTRID will develop a common approach easily portable to different virtualisation scenarios. In this respect, the technology developed by the Project will be validated in two relevant domains, i.e., plain cloud applications and Network Function Virtualisation, which typically exploits rather different chaining and orchestration models.

CYBERWISER.EU

The CYBERWISER.eu **[13]** aims to provide an educational, collaborative, real-time civil cyber range platform and a web based simulated environment for creating cyber incident and cyber attacks scenarios where both students and IT professionals evolve their skills and continuously evaluate their performance, getting ready for future real attack episodes. Thus, CYBERWISER is an initiative that addresses the need for effective, user-friendly environments dedicated to training of high skilled multidisciplined professionals in the field of cybersecurity. Similarly to the SPIDER concept,

users can play the role of attackers and/or defenders in different scalable and configurable scenarios, composed of a set of virtual resources representing a company ICT infrastructure.
CYBERWISER.EU through the provision of the aforementioned platform where cybersecurity competitions will take place, aims to become the EU's reference, authoritative, independent cybersecurity platform for professional training. CYBERWISER started on September 2018, has a duration of 30 months and builds on a 3-year legacy brought by its predecessor WISER

THREAT-ARREST

The THREAT-ARREST **[14]** is an ongoing project started on September 2018 (having a duration of 3 years) that will develop an advanced training platform incorporating emulation, simulation, serious gaming and visualization capabilities to adequately prepare stakeholders with different types of responsibility and levels of expertise in defending high-risk cyber systems and organizations to counter advanced, known and new cyber-attacks. The THREAT-ARREST platform will deliver security training, based on a model driven approach where cyber threat and training preparation models, specifying the potential attacks, the security controls of cyber systems against them, and the tools that may be used to assess the effectiveness of these controls, will drive the training process, and align it with operational cyber system security assurance mechanisms to ensure the relevance of training. The platform will also support trainee performance evaluation and training program evaluation and adapt training programs based on them.

5G ESSENCE

The 5G ESSENCE **[15]** addresses the paradigms of Edge Cloud computing and Small Cell as a Service by fuelling the drivers and removing the barriers in the Small Cell market, forecasted to grow at an impressive pace up to 2020 and beyond and to play a key-role in the 5G ecosystem. The 5G ESSENCE provides a highly flexible and scalable platform, able to support new business models and revenue streams by creating a neutral host market and reducing operational costs by providing new opportunities for ownership, deployment, operation and amortisation.

SPEAR

The SPEAR **[16]** (Secure and PrivatE smArt gRid) project started on 2018 and will be completed on 2021. SPEAR is a research program, co-funded by the Horizon 2020 it aims at developing an integrated platform of methods, processes, tools and supporting tools for a)Timely detection of evolved security attacks such as APT, Denial of Service (DoS) and Distributed DoS (DDoS) attacks using big data analytics, advanced visual-aided anomaly detection and embedded smart node trust management b)Developing an advanced forensic readiness framework, based on smart honeypot deployment, which will be able to collect attack traces and prepare the necessary legal evidence in court, preserving the same time user private information. c)Implementing an anonymous smart grid channel for mitigating the lack of trust in exchanging sensitive information about cyber-attack incidents. d)Performing risk analysis and awareness through cyber hygiene frameworks, while empowering EU-wide consensus by collaborating with European and global security organisations, standardisation bodies, industry groups and smart grid operators. e) Exploiting the research outcomes to more CIN domains and creating competitive business models for utilising the implemented security tools in smart grid operators and actors across Europe.

11. CONCLUSIONS

This deliverable presented the SPIDER project's dissemination and communication strategy plan, an internal useful tool for providing a consistent framework for all activities needed to disseminate and sustain the concepts, achievements, as well as the technical and knowledge project results.

Moreover, the intention is that this deliverable can be a practical guide, a handbook and a tool for **every consortium member throughout the project lifetime as it summarizes the main stakeholders, appropriate communication channels, key dissemination activities and corresponding key performance indicators**. The consortium partners recognise that the communication activities are an integral part of the project and special attention will be given through the project's three-year duration.

As said, basic "ingredients" of the dissemination & communication strategy are being presented **here such as dissemination channels, stakeholders, tools, key activities, events, etc. that explain the basic rationale behind the strategy for succeeding the desired project promotion**. For instance, online promotion of the project, organization and participation in events, a number of scientific publications in journals and conferences, high-quality promotional material (brochures, leaflets, videos, etc.) as well as cross collaboration with other projects & initiatives and standardisation activities constitute some of the most important activities towards the implementation of the dissemination, exploitation and standardization strategies.

Furthermore, in order to measure the achieved progress and impacts of the proposed strategy and plan, a monitoring and evaluation framework has been defined and a number of indicators have been recognised and reported. **Of course, as this is a dynamic process, the dissemination plan and the respective strategies will be constantly evaluated and revised in the course of the project duration.** Particularly, the report of the achievements and the update of the plans will be provided in M12, M24 and M36 through the deliverables D8.2 "Initial report on dissemination, communication, standardisation and exploitation", D8.3 "Interim report on dissemination, communication" and D8.4 "Final report on dissemination, communication, standardisation and exploitation".

REFERENCES

[1] Grant Agreement NUMBER 833685 — SPIDER

[2] A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Fifth Edition

[3] PMI Institute https://www.pmi.org/learning/library/stakeholder-analysis-pivotal-practice-projects-8905

[4] Stakeholder Classification and Management Strategy https://pmstudycircle.com/2012/06/stakeholder-analysis-stakeholder-management-strategy/

[5] The SPIDER website https://spider-h2020.eu

[6] 5G-PPP web site: https://5g-ppp.eu/

[7] 5G Work Groups https://5g-ppp.eu/5g-ppp-work-groups/

[8] The 5G ENSURE project http://www.5gensure.eu/

[9] The European Cyber Security Organisation https://www.ecs-org.eu/

[10] The cPPP contractual Partnership among the European Commission and the European Cyber Security Organisation (ECSO)https://ecs-org.eu/cppp

[11] The MATILDA project https://www.matilda-5g.eu/

[12] The ASTRID project https://www.astrid-project.eu/

[13] The CYBERWISER project: https://www.cyberwiser.eu/

[14] The THREAT ARREST project https://www.threat-arrest.eu

[15] The 5G ESSENCE project http://www.5g-essence-h2020.eu

[16] The SPEAR project https://www.spear2020.eu