Secure and PrivatE smArt gRid

(Grant Agreement No 787011)

D8.2 Plans for Dissemination and Communication

Date: 2019-08-31

Version 2.0

Published by the SPEAR Consortium

Dissemination Level: Public

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 787011

Document Control Page

Document Details

Document Version:	2.0
Document Owner:	Public Power Company (PPC)
Contributors:	All partners
Work Package:	WP 8 – Dissemination and Exploitation
Task:	Task 8.1 – Dissemination and Communication
Deliverable Type:	PU
Document Status:	Final
Dissemination Level:	Public

Document History

Version	Author(s)	Date	Summary of changes made
0.1	Michael Angelopoulos (PPC)	2018-10-09	Initial version - ToC
0.2	Iheanyi Sam Nwankwo (LUH)	2018-10-09	Input from LUH, ED
0.3	Georgios Boultadakis (ED)	2018-10-10	Input from ED
0.4	Theodoros Rokkas (INC) Manos Panaousis (SURREY)	2018-10-16	Inputs from INC and SURREY
0.5	Michael Angelopoulos (PPC)	2018-10-23	Incorporated contributions from partners, first draft
0.6	Solon Athanasopoulos (PPC) Santiago Otero Peña (ENEL)	2018-10-31	Final draft, after revision from PPC Input from ENEL
0.7	Michael Angelopoulos (PPC)	2018-11-14	Final input from SCH
0.8	Michael Angelopoulos (PPC)	2018-11-19	Revision according to PO comments and DoA amendment.
1.0	Michael Angelopoulos (PPC)	2018-11-19	Final version submitted to the European Commission
1.2	Michael Angelopoulos (PPC) Efstathios Papadopoulos (PPC)	2019-05-22	Final version submitted to the European Commission following the PO comment about the 'Summary of the intended exploitable results of the project'
1.3	Solon Athanasopoulos (PPC) Konstantinos Stamatakis (PPC)	2019-07-10	Section 3.1 was revised based on the 1st review comments, by including all the new features of the updated SPEAR website
1.4	Michael Angelopoulos (PPC) Nikolaos Papadimitriou (PPC)	2019-07-20	Section 5.2 was revised based on the 1st review comments, by including more scientific publications and participation in events.
1.6	Michael Angelopoulos (PPC) Solon Athanasopoulos (PPC)	2019-07-28	Section 5.3 was revised to include more industrial dissemination events following the

			1st SPEAR review results recommendations.
1.7	Michael Angelopoulos (PPC) Solon Athanasopoulos (PPC) Anastasios Papadopoulos (PPC)	2019-08-10	Section 7 was revised by including early exploitable results following the 1st SPEAR review results recommendation.
1.9	Michael Angelopoulos (PPC) Solon Athanasopoulos (PPC) Aglaia Karagianni (PPC)	2019-08-12	Section3 was revised to include the mailing list for allowing visitors to subscribe and get the news from the SPEAR results following the 1st SPEAR review resiults recommendation.
2.0	Michael Angelopoulos (PPC) Solon Athanasopoulos (PPC) Athanasios Kourapas (PPC)	2019-08-20	Final corrections on report. Report formatting. Finalization of Document: Acronyms and References

Internal Review History

Reviewed by	Date	Summary of Comments
Pablo Gómez-Calvente Moreno (ENEL)	2018-11-05	Minor language revisions
Anton Hristov (VETS)	2018-11-12	Minor refined sections
Dimosthenis Ioannidis (CERTH)	2019-08-24	The deliverable is acceptable. Typographical errors should be corrected. An update on the SPEAR consortium publications and event participation is needed.
Panagiotis Sarigiannidis (UOWM)	2019-08-30	The deliverable is acceptable. Some comments attached inside the deliverable should be taken into account.

Legal Notice

Acronyms

Acronym	Explanation
UOWM	University of Western Macedonia
ED	European Dynamics
REAL	Realaiz DOO
TEC	Fundación Tecnalia Research & Innovation
SCHN	Schneider Electric France SAS
EE-ISAC	European Energy - Information Sharing & Analysis Centre
ENEL	ENEL IBERIA S.R. L
CERTH	Centre for Research and Technology Hellas CERTH
SURREY	University of Surrey
PPC	Public Power Corporation S. A
8BL	Eight Bells LTD
INC	Incites Consulting SARL
PIMEE	G.E. Pukhov Institute for Modeling in Energy Engineering of the National Academy of Sciences of Ukraine
LUH	Gottfried Wilhelm Leibniz Universität Hannover
SH	Sidroco Holdings Limited
0INF	0 INFINITY Limited
BSU	Belarus State Economic University
TUS	Technical University of Sofia
VETS	VETS Lenishta OOD
KPI	Key Performance Indicator
EU	European Union
CERT	Computer Emergency Response Team
DCP	Document Control Page
URL	Uniform Resource Locator
RSS	Rich Site Summary
TSO	Transmission System Operator
IEEE	Institution of Electric and Electronics Engineers
ACM	Association for Computer Machinery
CCS	Computer and Communications Security
CeBIT	Centre for Automation, Information technologies and Telecommunications
IPR	Intellectual Property
R&D	Research and Development
CAGR	Compound Annual Growth Rate
CIP	Critical Infrastructure Protection
IT	Information Technology
SWOT	Strengths, Weaknesses, Opportunities and Threats
CAPEX	Capital Expenditures
OPEX	Operational Expenditures
CTTE	Conference of Telecommunication, Media and Internet Techno-Economics
DoA	Description of Action

ENISA	European Union Agency for Network and Information Security
CIRED	International Conference on Electricity Distribution
S&P	Security and Privacy
SEPR	Scholarly Electronic Publishing Resources
CA	Consortium Agreement
TRSC	Testing Research & Standards Centre
ICT	Information and Communication Technology
UK	United Kingdom
WP	Work Package
SAS	Substation Automation System
IED	Intellgent Electronic Device
RTU	Remote Terminal Unit
SCADA	Supervisory control and data acquisition

Executive Summary

This document is the second deliverable of Work Package 8 and defines the dissemination and communication plan that SPEAR will follow through the project's lifetime.

The objective of the dissemination and communication strategy is to create strong awareness of the project and its results, as well as to ensure that the knowledge and information gained can be made available to multiple target audiences. SPEAR defines as its main target groups the producer's community, the scientific community, policy makers and national Computer Emergency Response Teams, as well as the general public.

SPEAR utilises a variety of mediums to disseminate the project's accomplishments and activities. The main dissemination portal is the SPEAR website, where public deliverables, leaflets, latest news and information about the project are available. As a secondary means, LinkedIn and YouTube are employed to enhance the dissemination process.

Dissemination branding and material are also part of the dissemination and communication strategy and include well-designed templates, leaflets and a logo that reflects the project's content. All those materials aim to form the public image of SPEAR and make it recognizable on the Internet and mass media.

All SPEAR partners are engaged in the dissemination process. Partners will interact with other projects to organize special events, workshops and symposiums, as well as they, will organize their own events, individually or in cooperation with each other. Academic and industrial partners will regularly publish scientific papers in journals and conferences in order to widespread the SPEAR outcomes or just initial steps that include extensive surveys and research on literature. Dissemination activities also include standardization efforts and publish of open-sourced parts of the SPEAR platform through the Bitbucket platform.

The monitoring of dissemination and communication activities is an essential process to evaluate the success and efficiency of the plan. SPEAR defines a set of Key Performance Indicators (KPIs) that monitor the progress and impact of the dissemination and communication activities and act as guidance to take proper actions. KPIs include numerous indications like participation in events, number of publications, promotional material produced, as well as traffic statistics of the website, YouTube channel and LinkedIn page. Google Analytics, YouTube Analytics, and LinkedIn Analytics are utilized to obtain useful statistics that will be used to confirm compliance with the minimum KPIs.

An initial exploitation plan is also defined in this document. The exploitation plan results are composed of individual exploitation plans as well as the joint exploitation of the identified exploitable products. By exploiting the results, Industrial partners will enhance their portfolio of products and solutions that they offer, thus their position in the market. Also, academic partners will strengthen their positions in academia and their personnel will take unique hands-on experience. Expected outcomes of the exploitation strategy are methodologies, tools, models, and guidelines.

Introduction

The present document is a deliverable of the SPEAR project, funded by the European Commission's Directorate-General for Research and Innovation, under its Horizon 2020 Research and innovation programme (H2020).

This document is the second deliverable of the Work Package 8 and describes the detailed dissemination and communication strategy that the SPEAR consortium will follow throughout the project's lifespan.

More specifically, the document defines the dissemination strategy and the target groups that dissemination is addressed to, gathers the communication tools and social media accounts that are employed to inform the public opinion about the SPEAR project, as well as summarizes all the material (e.g. logos, templates) that form the public image of the SPEAR project.

In addition, in this deliverable, all the dissemination activities of the SPEAR consortium are being recorded and a set of Key Performance Indicators is being defined that will help SPEAR consortium to evaluate and even alter the dissemination strategy that is being followed.

Finally, the initial exploitation plan of the project's outcomes is being described.

1. Content and Structure of this deliverable

The rest of this deliverable consists of the following sections:

- Section 2 – Describes the dissemination strategy that is defined by its objectives and the target groups.
- Section 3 – Lists the main communication tools that are used by the SPEAR consortium to communicate with the target groups, disseminate the project's achievements and any information that is relative to the project.
- Section 4 – Gathers the dissemination and branding materials of the SPEAR, meaning logos, templates, and leaflets that form the public image of the SPEAR project.
- Section 5 – Lists all the dissemination activities that have or are going to take place throughout the project lifetime.
- Section 6 – Lists the Key Performance Indicators as well as the tools that will be employed to evaluate the dissemination strategy.
- Section 7 – Describes the initial plan to exploit the results of the SPEAR project.

2. Dissemination strategy

This section provides the detailed dissemination plan that the SPEAR consortium is committed to. The strategy is defined by answering two critical questions; what are the objectives of the dissemination process and what are the target groups, meaning to whom the communication campaign is addressed.

2.1 Objectives of dissemination

The aim of the SPEAR dissemination and communication plan is to create strong awareness of the project and its results, as well as to ensure that the knowledge and information gained can be made available to multiple target audiences at national, European and global level. Partners are committed to use their industrial partnerships, standardisation activities and long-standing experience in EU funded projects, to contribute to the communication and dissemination activities, over the project duration. Considering the consortium's experience, it is believed that the project as a whole will have the critical mass to create a large dissemination impact.

2.2 Target groups

The major focus of the SPEAR dissemination and communication plan is to ensure that the project activities and outcomes are widely spread among the appropriate target communities, at appropriate times, via appropriate methods. The first step to this direction is the identification of target groups and key stakeholders, to which the project could offer an added value. Main target groups of the SPEAR project are:

- **Producers community.** An open dialogue will be established via the project's website as well as through the organisation of focused-group meetings in order for the SPEAR project to better address their needs and demands and to integrate their feedback at key points of the project.
- **Scientific community**, in the field of smart grid security. Partners will reach this community using their contacts and cooperation with other research projects, by participating in scientific conferences and publishing in scientific journals.
- **Policymakers** and **national Computer Emergency Response Teams** (CERTs), with whom an open dialogue will be launched to highlight major aspects of SPEAR implementation and receive feedback for further investigation.
- The **general public**, for which 'lighter' versions of project newsletters, leaflets, flyers, etc., will be available at the project's website.

Encouraging the participation of the abovementioned target groups on a systematic and regular basis is a significant component of the project's dissemination plan. Table 1 lists key stakeholders for the development, evaluation, uptake, and exploitation of SPEAR outcomes.

Table 1: Target groups

Producer's community	Scientific community	Policy makers	General public
• Electric power utilities (energy producers, energy distributors, operators). • Software industries and smart grid equipment manufacturers	• Scientific communities of software engineering, security and privacy methods.	• EU Institutions (EU Commission, EU science foundation). • The ENISA. • National public authorities (industrial committees, ministry	

• Industrial associations.	• Related EU-funded projects	and regional councils, regulatory authorities).	

3. Dissemination and Communication tools

The SPEAR project utilises a number of communication tools to disseminate project achievements, publications and documents, events, interviews and other relevant material to the SPEAR project. Those communication tools include a public website that acts as the main information portal as well as secondary social media accounts that act as alternative means of communication and dissemination.

3.1 Website

The SPEAR website is the central information portal to communicate SPEAR to the target groups. The website provides public information, including public documents and updates about the progress of the project, scientific publications, and important upcoming events. The website is located at the following URL:

https://www.spear2020.eu

The website consists of the following six sections:

- **Overview**: The main page of the SPEAR website that gathers a welcome message and short description of the project identity, the latest posts in the News section, the Use Cases and the Objectives of the project **Objectives:** Includes an overview, in bullet points, of the SPEAR objectives.
- **Outcomes** which consists of the following subsections:
  - **Deliverables**: Includes a list of non-classified published deliverables, ordered by work package. Once these documents are made available, one could download them from the same page by clicking the PDF logo.
  - **Publications**: Gathers all original publications, such as open access articles, conference reports and book chapters, that are produced by SPEAR.
- **Use cases**: Provides a summary as well as an interactive map of the four SPEAR use cases.
- **Consortium**: Gives a brief summary of the 18 members of SPEAR and what benefits will be provided to the project by each of them. In addition, this page includes amn interactive map that shows the location of each partner in EU.
- **News**: Includes announcements and notifications about events or public results in the field of cyber security related to SPEAR. This page also provides a dedicated RSS feed to keep the audience up-to-date about new posts.
- **Contact & Mailing List**: Includes contact details of the project's coordinator and the technical support of the website as well as a contact form that forwards messages to the SPEAR consortium. In addition, this page provides a form that allows visitors to subscribe to our newsletter.

Figure 1 and Figure 2 illustrate screenshots from the SPEAR website.

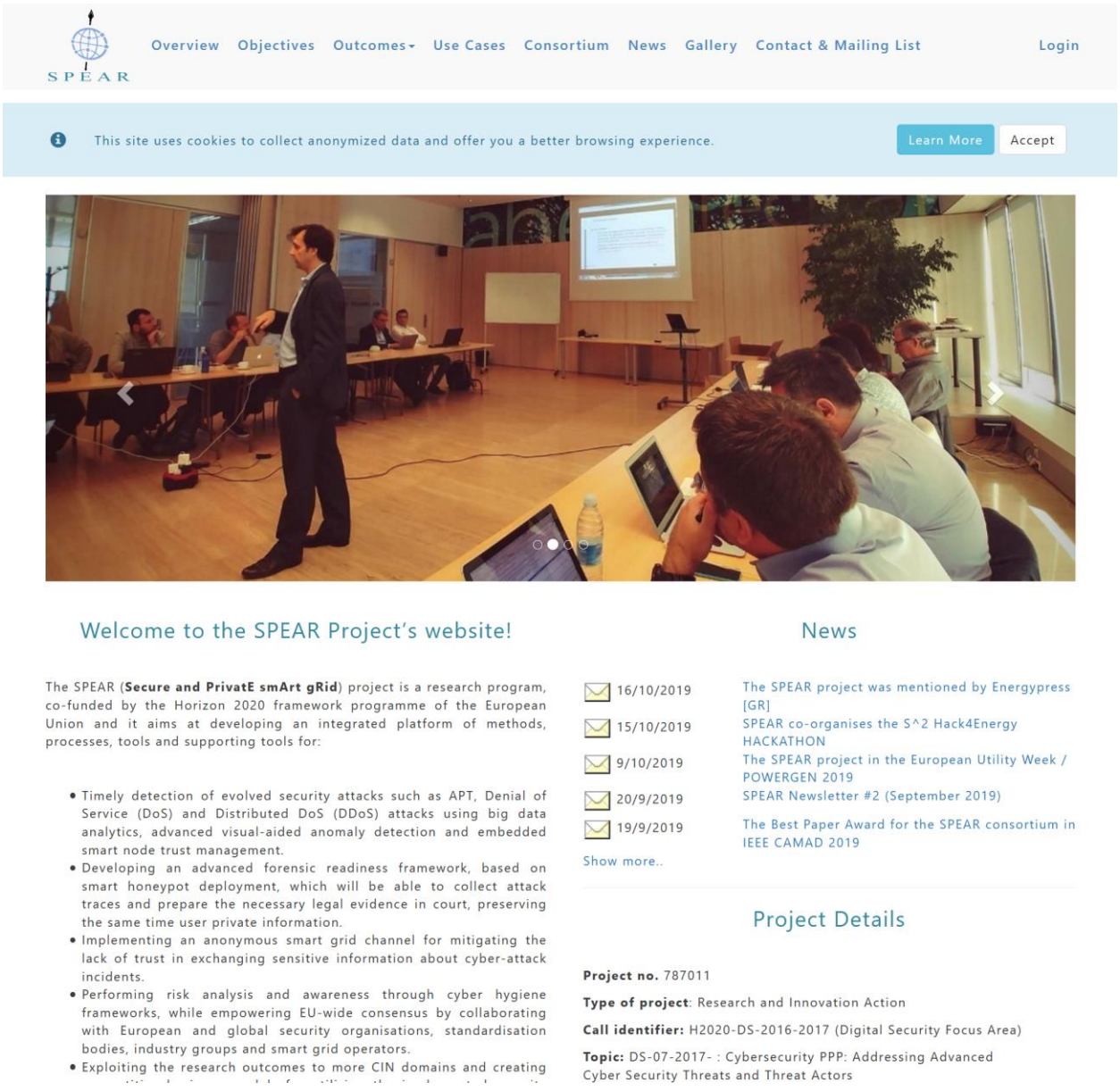

Figure 1: SPEAR's website home page

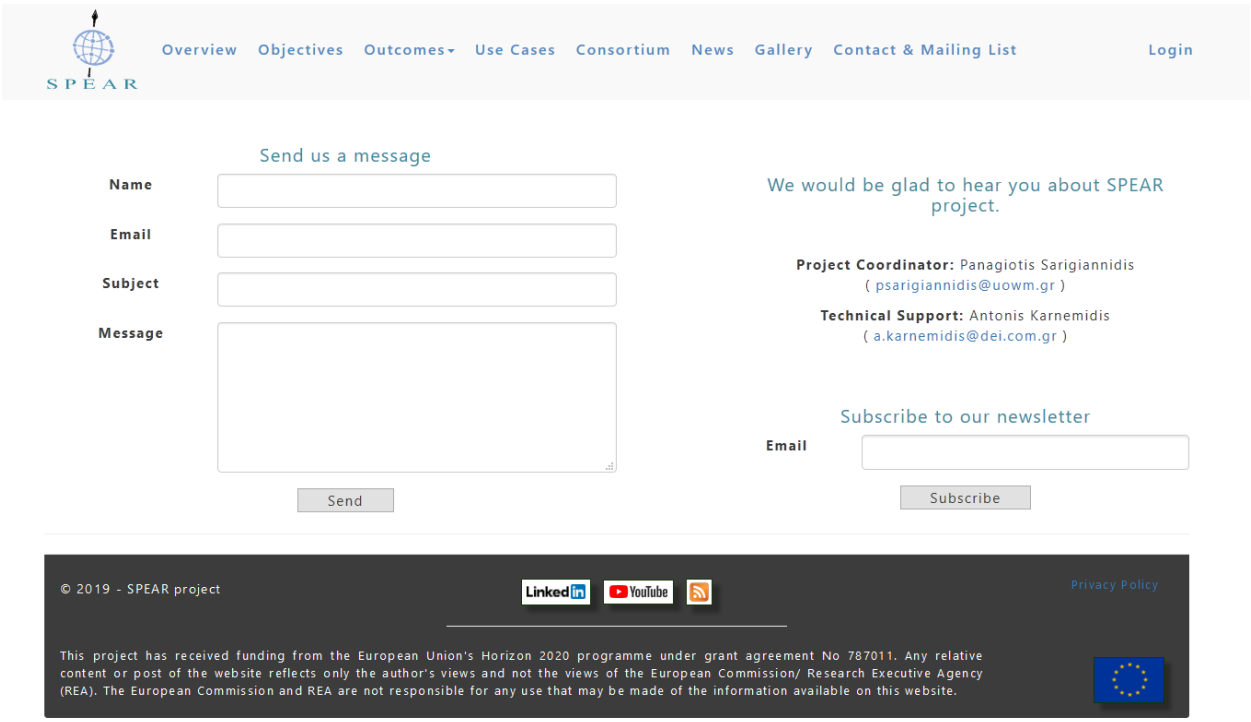

Figure 2: Contact & Mailing List page of the SPEAR web site

3.2 LinkedIn page

A company page has been created in LinkedIn for the SPEAR project, in order to serve the needs of an alternative communication and dissemination channel that supports direct contact with target groups and sharing of multimedia content. A company page has been created instead of a normal LinkedIn account, because LinkedIn offers advanced tools to measure the impact and the performance of the page, tools that are not available for normal accounts. The LinkedIn page can be found under the following link:

https://www.linkedin.com/company/spear2020

Figure 3 is a preview of SPEAR's LinkedIn page.

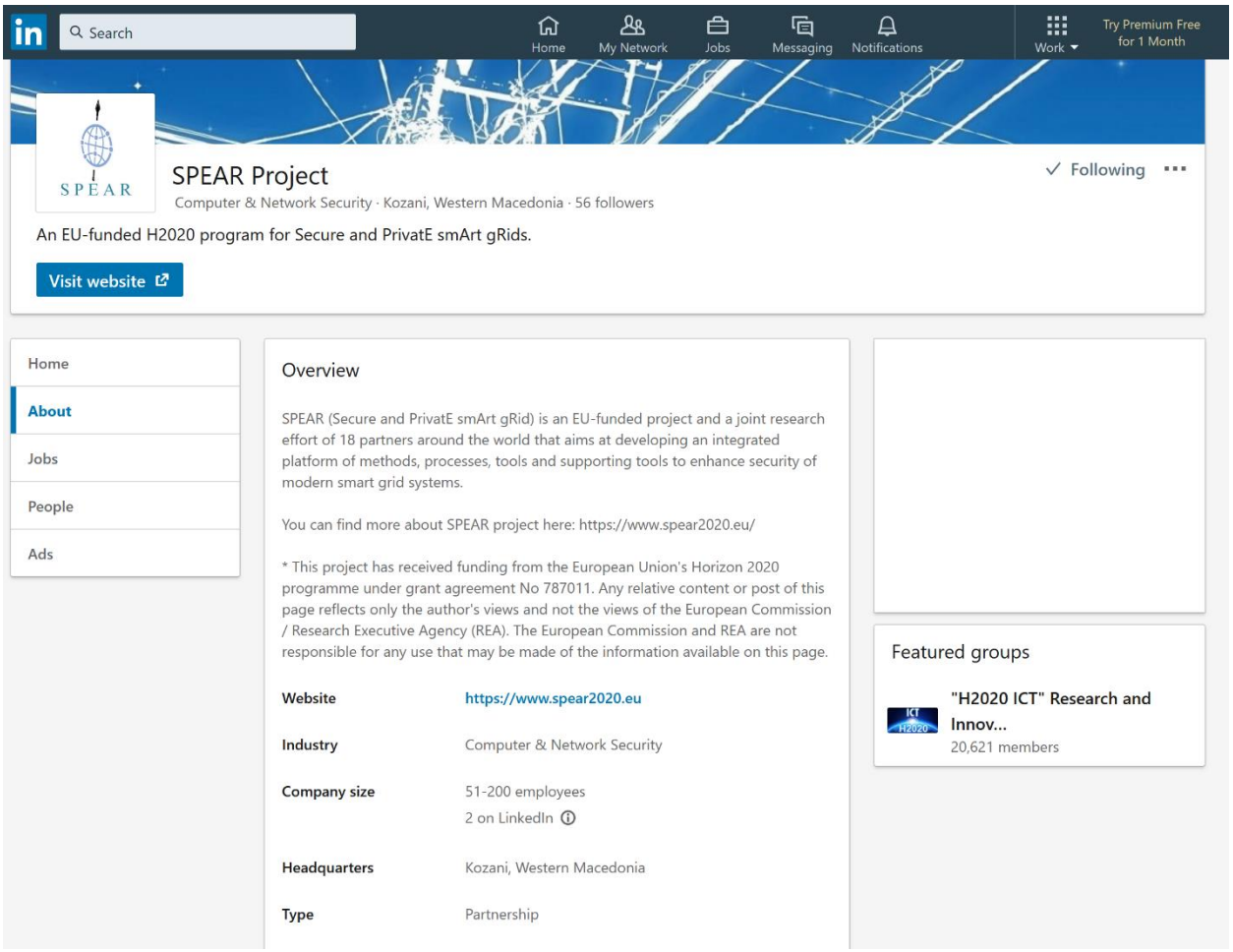

Figure 3: Preview of SPEAR's LinkedIn page

3.3 YouTube channel

YouTube is one additional dissemination channel that allows the SPEAR consortium to share lengthy multimedia content that may include, but not limited to, interviews, public statements relevant to the SPEAR project, as well as videos that share the technological and academic expertise that is being acquired by the SPEAR project. The YouTube channel is available under the following link:

https://www.youtube.com/channel/UCw6-d5G01ToBhCmaUnHIcpw

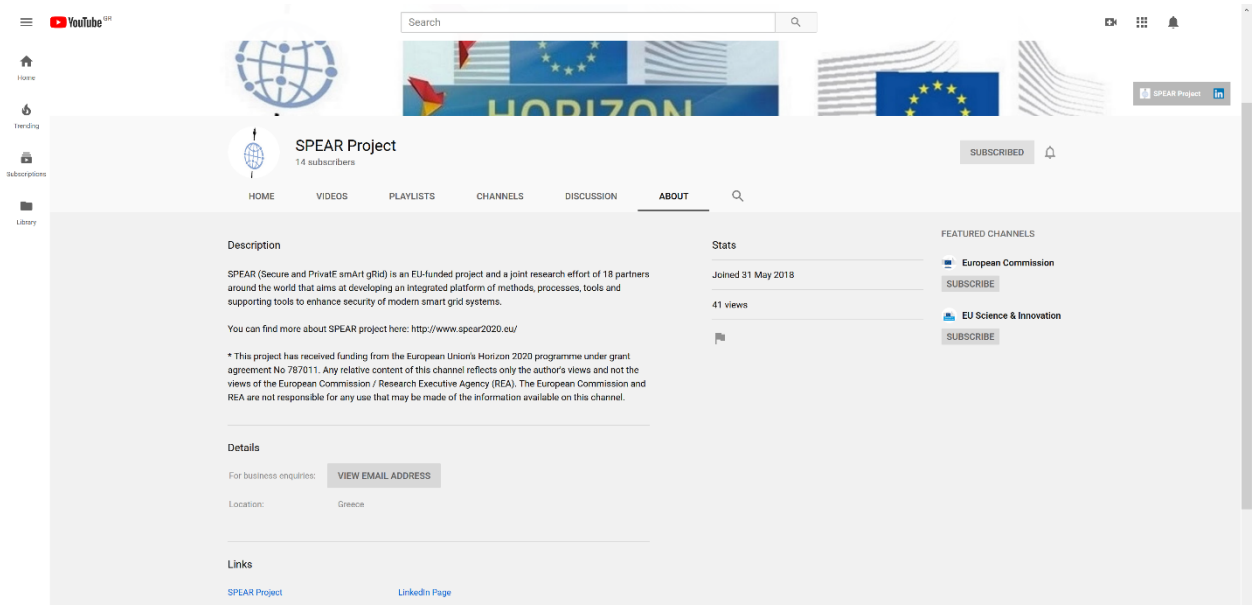

Figure **4** is a preview of SPEAR's YouTube channel.

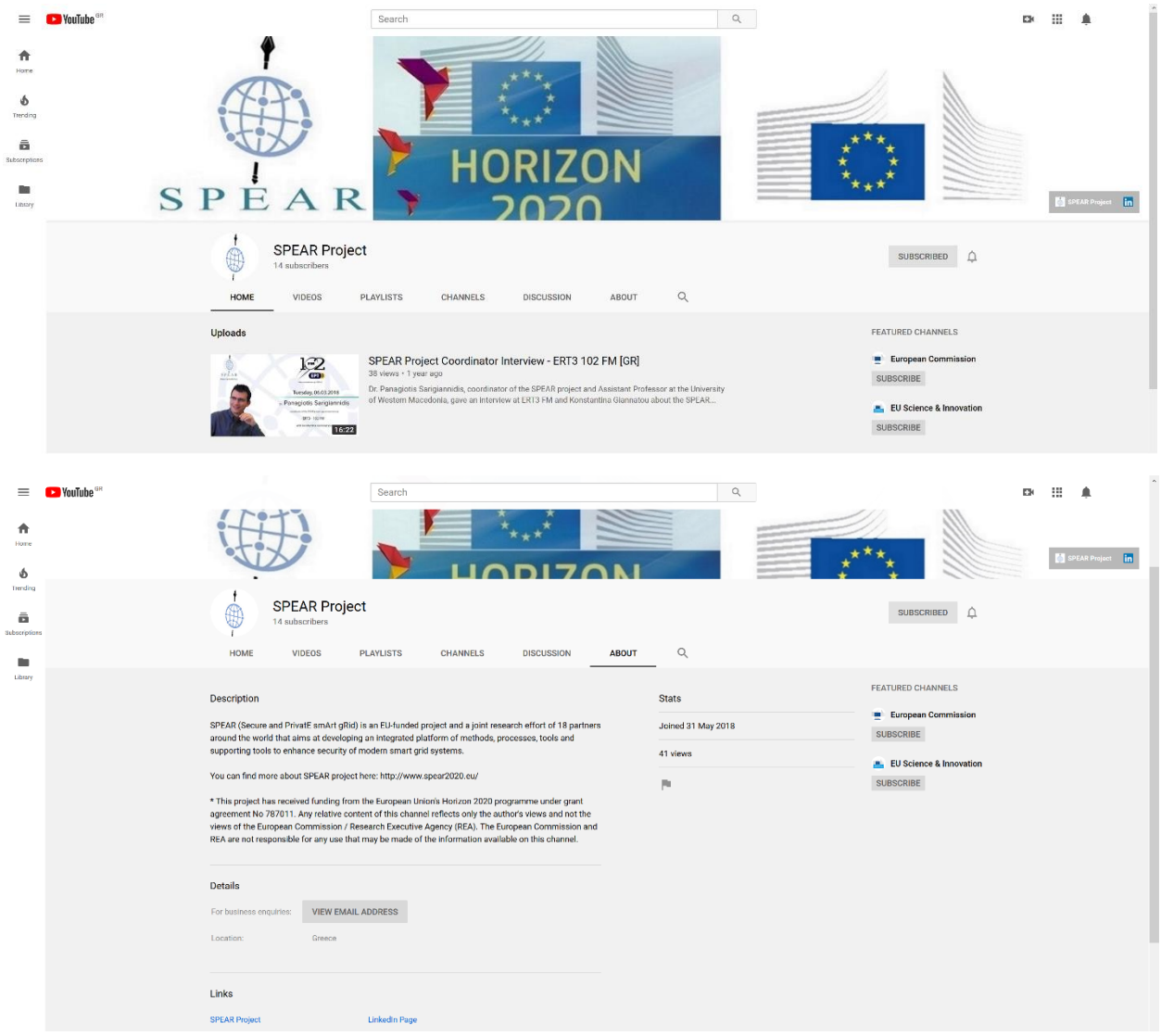

Figure 4: SPEAR's YouTube channel

3.4 Media relations

The SPEAR consortium realises the importance of communication with the target groups also by traditional media, like TV/radio shows and newspapers. Upcoming public appearances on TV and radio will be announced from the LinkedIn page and its content will be shared through SPEAR's social media, YouTube channel and LinkedIn page.

4. Dissemination branding and material

A toolkit of dissemination branding and material has been designed in order to foster and enhance the dissemination process. This toolkit includes document templates, the project's logo, leaflets, and a complete multimedia presentation.

4.1 Templates

A set of Word and PowerPoint templates have been created by UOWM in order to facilitate the consistent format of each deliverable, public, restricted or confidential, as well as the presentations that are performed by the SPEAR consortium during dissemination events.

As for the deliverable template, the front page contains the most important information about the document, meaning the project's identity (name and logo), the title and deliverable number, the submission date, the document's version as well as the dissemination level. The Document Control Page (DCP) is followed by the frontpage and summarizes detailed information about the document, the document history, the internal review history and some legal notices that are identical for each document. The document style uses Arial 10pt and justification for the body text as well as Arial 16pt and bold for section headings and Arial 14pt for subsection headings. Caption titles are Arial 9pt centred.

The PowerPoint template combines grey and blue colours and uses the logos of the SPEAR project and that of the European Commission. The front page describes the task or the deliverable that the presentation is about and its title. Alternately, only a title would be present if the presentation is addressed to people not involved in the project procedures.

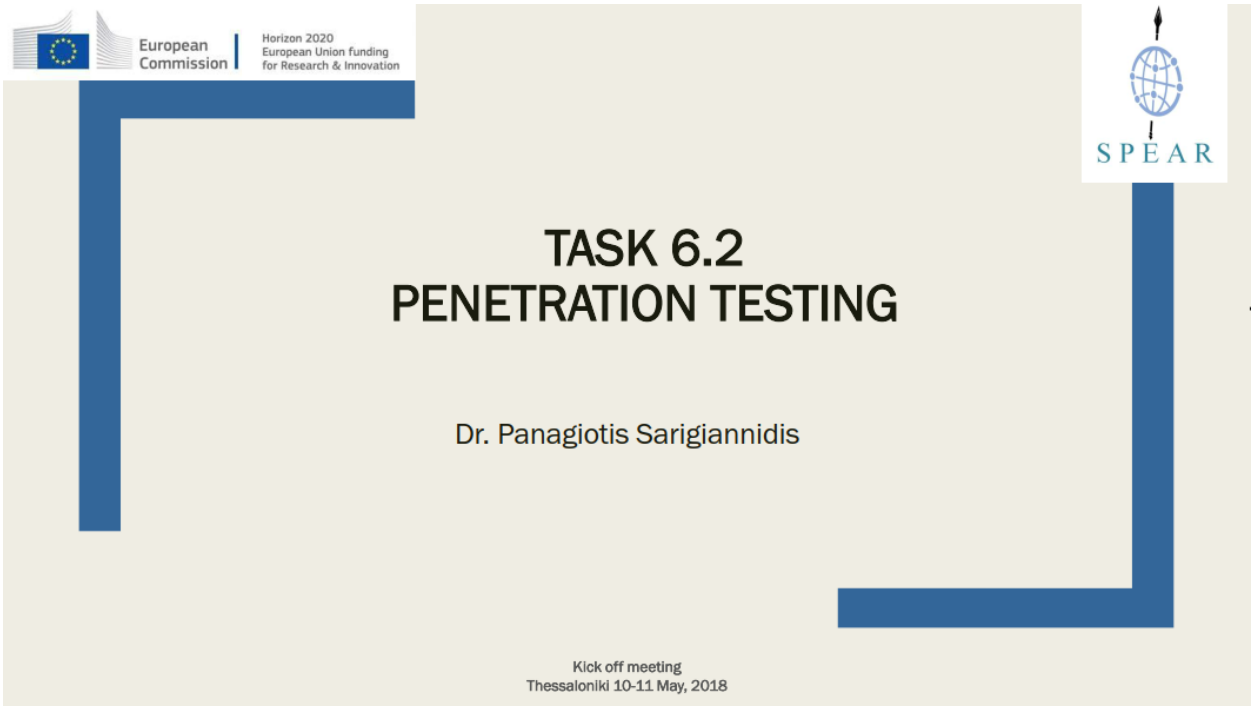

Figure 5: The front page of the PowerPoint template.

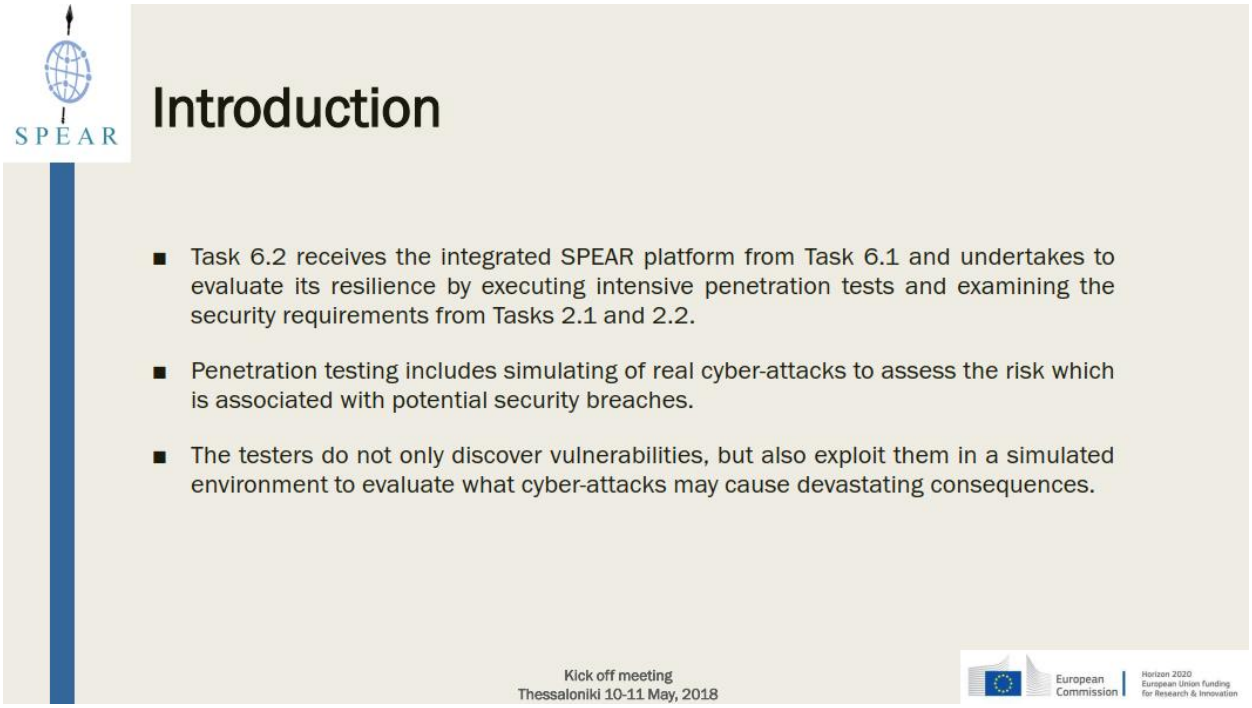

Figure 6: The body of the PowerPoint presentation template

4.2 Logos

In order to foster successful dissemination with high visibility, an easy-to-recognise logo has been created, to be used in both online and printed material. The logo is illustrated in Figure 7 and consists of a globe with nodes, that reflect both the Internet and an interconnected smart grid, and a spear that goes through the globe and associated with the project's acronym. Under the logo, the emerald coloured project's acronym takes place (SPEAR).

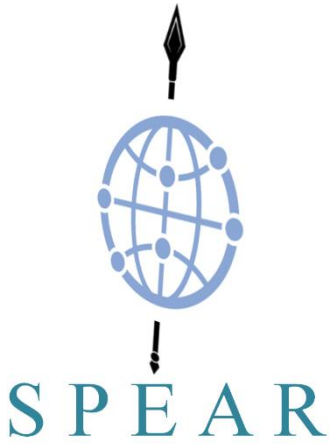

Figure 7: The SPEAR logo

4.3 Leaflets

SPEAR plans to publish a three-monthly leaflet that will inform SPEAR's target groups about the project's achievements and important events that have been taken or will take place. Leaflets will be posted in the News section of the website and the audience will automatically be notified through RSS. Relevant posts on LinkedIn will also follow the publication of each leaflet.

4.4 Multimedia presentations

Under the dissemination activities, multimedia material (video clips, interviews, short demos, etc.) will be prepared and distributed in order to describe the research objectives, challenges, tangible results and benefits deriving from the SPEAR project. This material will be delivered on the Internet via the dedicated YouTube channel and it is expected to serve as a mean for mobilising targeted communities in different countries.

5. Dissemination activities

SPEAR will carry out project communication activities to facilitate the targeted communities to assess, accept and adopt the new knowledge generated by SPEAR. Communication activities are based on primary and secondary communication channels to spread new knowledge and results and they aim at reaching the dissemination objectives.

The ambition of SPEAR is mainly based on a robust interaction among the scientific and technological communities of electric and cybersecurity sectors. Security represents a consolidated research and innovation area, as well as in cybersecurity. Meanwhile, the scientific conceptual approaches, the references framework, the methodological approaches, are different in the cybersecurity field. Scientific communities share different conceptual frameworks and specialised Conferences and Journals are separated and, in a word, the specific "language" used in the two sectors is different. To reduce such a distance and to allow a concrete and effective synergy is one of the main goals of SPEAR. This lack of systematic integration reduces the potential of both sectors and represents a constraint against the possibility to develop strong and effective new cyber-secure solutions.

The novelty of the proposed approach is to overcome the conceptual separation of the two above mentioned scientific communities, to develop and consolidate a new area of cybersecurity.

The participation in the consortium of partners with a significant international role and experience in cybersecurity sectors will allow, along with the whole project development, to consolidate such an integration. The participation of partners with significant international role and experience in cybersecurity sectors will allow the SPEAR consortium to integration the results of the project in an efficient and effective way.

The whole activity of SPEAR will enable a systematic integration of research activities in such a sector, allowing the definition and consolidation of a common reference framework. This reference framework will allow the development and consolidation of a shared conceptual framework where research, industry, and service can easily cooperate. So, dissemination activities will represent a strategic step to reach the scientific ambition and contribute to the creation of a new specific area.

The strategy to reach such an ambitious goal is articulated with a progressive introduction of a secure point of view on the cybersecurity scientific community and, on the other side, to introduce cyber security. Such strategy will be implemented according to an incremental approach, that will start with the project and will be designed step by step according to the activities.

In order to demonstrate the technical and scientific results achieved within the SPEAR project, the following examples are provided:

- Assessed vulnerabilities and general cyber and privacy threats;
- Envisioned cybersecurity measures – mainly concerning design and architecture, to ensure cyber-secure critical systems and devices;
- Technical solutions implemented to test and show evidence of the effectiveness of cyber resilience improvements in primary substations.

The proposed actions comprise open international dissemination in tradeshows, exhibitions for the industry in scientific and technology conferences, where the disclosure of the project results can have great interest and technical impact.

5.1 Interaction with other projects

ED is the coordinator of the H2020 FLEXITRANSTORE and INTERRFACE projects that deal with the enhancement of the flexibility services and the coordination of the TSO-DSO-customers of the European power system. In both projects, large scale experiments are taking place at a pan-European level, bringing the digitisation of the energy grid in Europe. ED will pursue to coordinate the work being conducted in SPEAR with both projects, and more specifically with National Regulator Authorities, the ENTSO-E (European Association of TSOs), the DSO organisations and other stakeholders and consider the experience from SPEAR to the BRIDGE initiative works, where other Digitisation of Energy projects are participating.

ENEL is the coordinator of the H2020 Coordinate project that deals with the enhancement of the flexibility services and the coordination of the TSO-DSO-customers of the European power system. Large scale experiments are taking place at a pan-European level, bringing the digitisation of the energy grid in Europe. Enel will pursue to coordinate the work being conducted in SPEAR with this project, and more specifically with National Regulator Authorities, EDSO (European Association of DSOs), and other stakeholders and consider the experience from SPEAR to the BRIDGE initiative works, where other Digitisation of Energy projects are participating.

As **SURREY** is also a partner in the ASTRID project (funded under the same call DS-07-2017 with SPEAR), SURREY will collaborate with ASTRID partners towards the organisation of a workshop in the IEEE NetSoft 2019 conference. Synergies with other H2020 projects of SURREY, such as CUREX (seCUre and pRivate hEalth data eXchange) project, that was recently awarded under the SC1-FA-DTS-2018-1 call, will be explored.

5.2 Scientific publications and participation in events

UOWM's research team actively plans and delivers high-quality research papers and publications in cooperation with other partners of the project. Following the 1st SPEAR review results (M12), where the reviewers kindly suggested that high impact factor (IF) journals and A-level conferences are much more preferred instead of quantitative targets, the SPEAR consortium will aim to publishing scientific publications in high-impact results, such as the IEEE Access, the IEEE Communications Surveys and Tutorials, and the IEEE Transactions on Dependable and Secure Computing, and in A-level conferences such as the IEEE International Conference on Communication, the IEEE Globecom, and the IEEE Symposium on Security and Privacy. It is worth mentioning that the SPEAR consortium succeeded to win the Best Paper Award in the 2019 IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), by submitting a paper which was developed by a synergy of industrial, academic, and SME partners of the SPEAR consortium.

The following publications from UOWM aim to support the development of various SPEAR's WPs, to contribute to the dissemination of the project's progress / achievements and to have a significant scientific impact:

- An extensive investigation and comparison about the latest industrial honeypot technologies as well as the initial deployment efforts of the Smart Home use case scenario was presented to the IEEE NetSoft 2019: **C. Dalamagkas, P. Sarigiannidis, D. Ioannidis, E. Iturbe, O. Nikolis, F. Ramos, E. Rios, A. Sarigiannidis and D. Tzovaras, "A Survey On Honeypots, Honeynets And Their Applications On Smart Grid", in 2019 IEEE Conference on Network Softwarization (NetSoft), 2019**
- A scientific publication about the proposed Anonymous Incident Communication Channel that will be exploited for the SPEAR project was presented in the PCI 2018 conference (http://pci2018.uniwa.gr/): **A. Triantafyllou, P. Sarigiannidis, A. Sarigiannidis, E. Rios, and E. Iturbe, "Towards an anonymous incident communication channel for electric smart grids," in Proceedings of the 22nd Pan-Hellenic Conference on Informatics - PCI '18, 2018, pp. 34–39.**
- A survey about all ICS/SCADA protocols that are used on smart grids is also planned by UOWM. This publication mainly aims to increase the consortium's knowledge and expertise about the industrial protocols that should properly be engaged to SPEAR's use case scenarios.
- A new IDS for the Advanced Metering Infrastructure (AMI) utilizing machine learning capabilities based on a decision tree was presented to the Global Information Infrastructure and Networking Symposium (GIIS 2018): **P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, "An Anomaly-Based Intrusion Detection System for the Smart Grid Based on CART Decision Tree," in 2018 Global Information Infrastructure and Networking Symposium (GIIS), 2018, no. October, pp. 1–5**
- An overview study of the various firewall systems in the smart grid paradigm, while providing new research directions in this field was presented to the Global Information Infrastructure and Networking Symposium (GIIS 2018): **P. Radoglou-Grammatikis, P. Sarigiannidis, T. Liatifis, T. Apostolakos, and S. Oikonomou, "An Overview of the Firewall Systems in the Smart Grid Paradigm," in 2018 Global Information Infrastructure and Networking Symposium (GIIS), 2018, October, pp. 1–4.**
- A paper examining the contribution of Intrusion Detection and Prevention Systems (IDPS) in smart grids, while providing an analysis of 20 cases by comparing their methodologies and technological elements that they utilize was published in the prestigious IEEE Access journal. The 20 cases are focused on the Advanced Metering Infrastructure (AMI), synchrophasor systems and substations. Based on the comparative analysis, the limitations of the current IDPS systems are identified, while appropriate recommendations are provided for better empowering the security layer of smart grids. In addition, important challenges and directions for future research efforts are discussed: **P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, "Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems," IEEE Access, vol. 7, pp. 46595–46620, 2019.**
- A SCADA threat model based on a Coloured Petri Net was presented in the IEEE Services 2019 conference, where four different types of cyber attacks against IEC-104 were emulated, while the AlienVault's risk assessment model was used to evaluate the risk level that each of these cyber attacks: **P. Radoglou-Grammatikis, P. Sarigiannidis, I. Giannoulakis, E. Kafetzakis, and E. Panaousis, "Attacking IEC-60870-5-104 SCADA Systems," in 2019 IEEE World Congress on Services (SERVICES), 2019.**
- An anomaly-based IDS for smart grid applications utilising operational data from a real power plant was presented to the IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD) 2019. In particular, many machine learning and

deep learning models were deployed, introducing novel parameters and feature representations in a comparative study. The evaluation analysis demonstrated the efficacy of the proposed IDS due to the suggested complex data representation: **G. Efstathopoulos, P. Radoglou-Grammatikis, P. Sarigiannidis, V. Argyriou, A. Sarigiannidis, K. Stamatakis, M. Angelopoulos, and S. Athanasopoulos, "Operational Data Based Intrusion Detection System for Smart Grid", in 2019 IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks. This paper won the best paper award of the conference.**

- An interactive, proof-of-concept ICS honeypot, which is based on Conpot, that is able to emulate a physical ICS device, by replicating realistic traffic from the real device was presented to the IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD) 2019. A real-life demonstration scenario was designed, which involves a hydro power plant. The honeypot architecture is also provided, while the structural components are presented in detail: **D. Pliatsos, P. Sarigiannidis, T. Liatifis, K. Rompolos, and I. Siniosoglou, "A Novel and Interactive Industrial Control System Honeypot for Critical Smart Grid Infrastructure," in 2019 IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks.**
- A work focusing on the requirements of establishment an anonymous channel of cybersecurity incidents, the possible obstacles, and the proposed data protection techniques to be applied in the SPEAR anonymous channel was published to the Azerbaijan Journal of High Performance Computing following an invitation coming from this journal: **A. Triantafyllou, P. Sarigiannidis, A. Sarigiannidis, E. Rios, and E. Iturbe "TOWARDS AN ANONYMOUS INCIDENT COMMUNICATION CHANNEL FOR ELECTRIC SMART GRIDS," Azerbaijan Journal of High Performance Computing, vol. 2, no. 1, pp. 7–28, Jun. 2019**.
- An extensive overview of the related work on big data-enabled IDS mechanisms and the most efficient classification methods in detecting anomalies in the smart grid systems are proposed in the submitted paper entitled 'Revisiting the Arsenal of Smart Grid Against Security Threats: Big Data, Analytics, Anomaly Detection and Requirements', which was submitted in the prestigious IEEE Access journal and currently it is under major revision: **D. Pliatsios, P. Sarigiannidis, A. Sarigiannidis, G. Sakellari, E. Panaousis, "Revisiting the Arsenal of Smart Grid Against Security Threats: Big Data, Analytics, Anomaly Detection and Requirements", IEEE Access, under major revision**.
- An extensive survey providing an overview of the general SCADA architecture along with a detailed description of the SCADA communication protocols was submitted in the highest impact factor journal according to the Guide2research (http://www.guide2research.com/journals/), which is currently under minor revision: **D. Pliatsios, P. Sarigiannidis, T. Lagkas, A. Sarigiannidis, "A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics", IEEE Communications Surveys and Tutorials, under minor revision.**
- A novel anomaly-based IDS, called DOSMA, capable of protecting efficiently the smart grid communications was submitted to one of the most high-impact journals in cybersecurity: **P. Radoglou-Grammatikis, P. Sarigiannidis, G. Efstathopoulos, W. Rao, HN Dai and E. Panaousis, "Detecting Cyber Attacks and Operational Anomalies in Smart Grid", IEEE Transactions on Dependable and Secure Computing, 2019, submitted**. DOSMA combines three detection layers that are devoted to identifying possible cyberattacks and anomalies against Transmission Control Protocol/Internet Protocol (TCP/IP) network flows, Modbus packets and operational data respectively. Each detection layer tests a set of machine learning models that were trained utilising data coming from a real power plant in Greece.

ED attended to SGTech Europe conference in March 2019, which illustrating the latest practical implementation experiences and advice, whilst networking beyond functional boundaries, to support

the industry's drive towards IT, OT & Telecom convergence in delivering the smart grid (**http://www.sgtech-europe.com/**). ED also attended to EDSO events on Smart Grid Cyber Security.

Additional possible opportunities for scientific publications and presentations are gathered in Table 2:

Table 2: Conferences and forums for possible participation

Potential opportunities for dissemination (Scientific dissemination events)	**Relevant publications for dissemination project results**
International Conference on Electricity Distribution – CIRED (2020 onwards)	PSCC - Power Systems Computation Conference or CIGRÉ Session (Conseil International des Grands Réseaux Électriques)
European Utility Week (2019 onwards)	IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)
International Council on Large Electric Systems – CIGRÉ Symposia	IEEE International Forum on Smart Grids for Smart Cities (SG4SC)
Protection, Automation & Control World Conference – PAC World (2019 onwards)	2019 IEEE PES Innovative Smart Grid Technologies Conference
International Conference on Availability, Reliability, and Security (ARES) (2019 onwards)	Intern. Journal of Electrical Power and Energy Systems (Elsevier)
2019 Symposium on Security and Privacy.	IEEE Transactions on Industrial Informatics: https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=9424
IEEE Conference on Decision and Control (CDC) 2019	IEEE Transactions on Power Systems: https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=59
European Control Conference (ECC) 2019	IEEE Transactions on Emerging Topics in Computing https://www.computer.org/web/tetc
2019 IEEE PES Innovative Smart Grid Technologies Conference (ISGT 2019)	IEEE Transactions on Dependable and Secure Computing
European Cybersecurity Forum	ACM Transactions on Information and System Security

5.3 Industrial Dissemination

Considering the innovation aspect of this project, the need to maintain active communication with the market as well as the need to reach stakeholders and future customer segments, the SPEAR consortium plans to participate in industrial events that can communicate the vision and the benefits of the SPEAR platform as a market product that can provide solutions of critical infrastructure protection and privacy enhancement in the smart grid environment. To this end, the following actions are planned to be implemented by the consortium members:

- **PPC**, realising its role in the Greek and European energy market, plans to participate in industrial events in the energy sector, in order to disseminate the project's vision and results. In particular, PPC plans to participate in the prestigious POWERGEN Europe event, one of the largest conference and exhibition events in Europe focusing on distributed generation,

smart grids and lifecycle management. In the same event, the European Utility Week will be also co-located and PPC plans to participate in the EU Project Zone of this event by exhibiting the SPEAR project.

- **ENEL, ED, UOWM,** and **CERTH,** towards creating synergies in the threat intelligence sharing domain with other industries, plan to participate in the 12th European Energy - Information Sharing & Analysis Centre (EE-ISAC) Plenary meeting that concerns trust-based data and information sharing technologies to help utilities to improve the cybersecurity and resilience of their grids.
- An energy-related workshop destined for energy stakeholders is planned to be organised in January 2020 by CERTH and UOWM in the CERTH premises. Energy stakeholders across Europe will be invited to participate in discussing on cybersecurity issues in the energy domain and in providing feedback on the SPEAR solution.
- **SCHN** and **ENEL** are exploring more dissemination activities to be organised in the context of SPEAR up to December 2019.
- **CERTH** and **UOWM** plan to create synergies with other projects by co-organising hackathons with other EU projects in the smart grid domain. Aim of those events is, on the one hand, to create usable software at the end of each contest and, on the other hand, to communicate and advance the technologies that the SPEAR consortium applies to develop the SPEAR platform.
- **0INF** plans to prepare a video that presents and visualises the key aspects and benefits of the SPEAR solution.
- Towards intending the industrial dissemination as the project matures, the Project Coordinator requested from all industrial partners to fill a form that indicates their planned industrial dissemination activities.

5.4 Bitbucket repositories

The Bitbucket software has been deployed to facilitate code development and collaboration, as well as to disseminate important open-source elements of the SPEAR platform. Bitbucket offers a cloud-based and self-hosted service that allows users to create an unlimited number of projects, both private and public, and collaborate on them. Developers can pull requests to edit code, publish reviews and discuss specific projects or pulls. Furthermore, Bitbucket has been chosen because it integrates with Confluence, the main collaboration software of the consortium.

Figure 8 offers an overview of Bitbucket repositories.

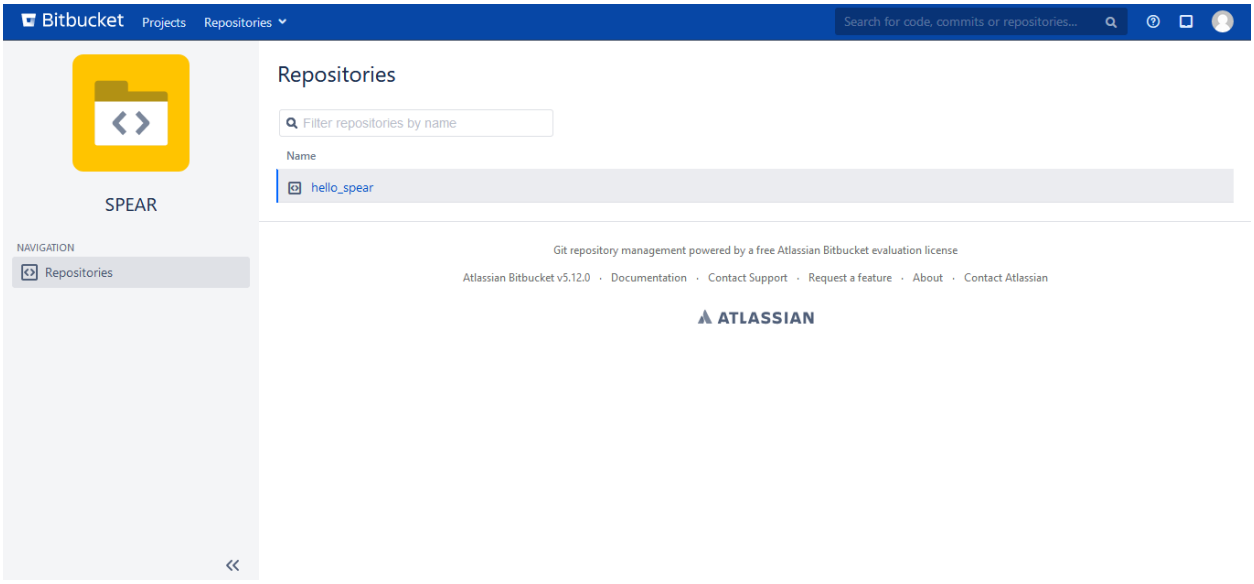

Figure 8: Bitbucket repositories

5.5 Individual dissemination plans

UOWM will contribute to publishing high-quality research papers, chapter books, and technical reports in high-quality international journals (IEEE Security and Privacy, IEEE Transactions on Communications, IEEE Transactions on Wireless Communications, IEEE Transactions on Vehicular Technology etc) and international conferences (IEEE Globecom, IEEE ICC, IEEE ISCC, IEEE ICOCN, SecureCom and IEEE Infocom).

ED has extensive expertise in disseminating project results and will complement the dissemination activities of the project, given its worldwide presence in 45 countries. ED is commercially active offering –among others- services for the professional community of Governments services and Security, thus participating in related events, conferences, fairs and workshops; SPEAR, through these channels, will be presented to both the commercial as well as research stakeholders thus creating a more “targeted awareness” regarding the functionalities and technologies it offers. ED plans to participate in conferences, exhibitions, events and workshops relevant to SPEAR and cybersecurity, as well as to author articles and journal publications presenting the outcomes of the project and the innovations related to the development of the modules that ED is responsible for. Furthermore, ED intends to pursue connections with other relevant projects to identify and set up any potential synergy with the aim to increase impact, as described above in the relevant section.

REAL will focus its dissemination activities on the presentation of project objectives and the demonstration of its results in conferences on a national and European basis. REAL is offering services for the public domain, which channels will be used to further disseminate the project achievements.

TEC will be focused on the presentation of both project objectives and results at conferences, seminars and workshops, to exchange knowledge with other cybersecurity experts as well as to collect feedback both from industry and academia. TEC will also work on the research network building through exchanging knowledge gained in the project with other stakeholders from European research projects on cybersecurity. Additionally, internal dissemination channels within TEC will also be used.

SCHN plans to contribute to the dissemination of the project’s results by collaborating in conferences and workshops and other relevant dissemination events (European Utility Week, CIRED, etc.).

SCHN ES will focus the dissemination on the National Technical Platform PLANETIC, the Spanish Technological Platform in the area of embedded systems and it will provide its powerful channels to deploy project results at international level.

ENEL will contribute to the diffusion of SPEAR results mostly in joint publications with the rest of the consortium, particularly on the requirements, methodology and results of the smart grid use case. In addition, ENEL plans to collaborate in the best dissemination message and channel selection for describing project results and getting feedback from external utilities.

CERTH has a strong collaboration with SMEs and industrial partners in National and European level for promoting SPEAR's scientific achievements to the market. With the project, CERTH will make contacts with key stakeholders and the opportunity to link the activities and achievements of SPEAR and CERTH exploitable foreground. Moreover, CERTH will organize at least two events to communicate the SPEAR project to several citizens and other relevant stakeholders, in order to inform them about the cyber security issues in smart grids (SPEAR's concept aiming at providing a secure and privacy-enabled smart grid solution against cyber-attacks using advanced and cutting-edge logging and defence solutions).

SURREY will contribute to the dissemination of the SPEAR achievements through publications in conferences (ACM CCS, IEEE S&P) and high impact factor journals (IEEE Transactions on Information Forensics and Security). Finally, SURREY will use social media, such as Twitter, and the Department of Computer Science website, to promote the results of the project.

PPC will use all its industrial contacts and partnerships as well its public channels to promote the project to the public and stakeholders as well. Moreover, PPC will communicate SPEAR's results to practitioners via publication in Conferences and international journals and participations in seminars, fairs, and workshops related to smart grid security.

8BL will incorporate the results regarding cybersecurity into its commercial and research activities, thus providing the results to its customers. 8BL regularly publishes results as contributions in relevant international journals/magazines and conferences. Furthermore, results will be published in the form of studies and white papers directly by the company. In addition, 8BL will disseminate project results through its social network pages (Facebook and Twitter) as well as on its website. The company will communicate the project relevant information to stakeholders in Cyprus and across Europe. Finally, 8BL will work on building liaisons with 5G Infrastructure Public Private Partnership (5G PPP) and cybersecurity initiatives that may use the results of the project.

INC will contribute to the dissemination of the SPEAR achievements through workshops conferences such as the CTTE conference and its own publications (INCITES newsletter). In addition, INCITES will actively contribute to the creation of scientific papers and publications in international Journals and Magazines. Finally, INCITES is willing to announce the main results of the project through its business website as well as the social media accounts it retains on Facebook and LinkedIn.

PIMEE will promote SPEAR's through publications at high quality conferences and journals, in the field of cybersecurity, as well as by organising parallel sessions in conferences, held in their premises 4 times per year, involving all stakeholders within industry.

LUH has a number of different ways of spreading its activities, and these will be utilized them in the dissemination of the SPEAR project, such as the LUH website and the LUH Newsletter that is accessed from all over the world. There are also series of lectures and forums such as the "IT Forum Recht" organized 3 times per year by LUH members of staff and the alumni association. LUH equally disseminates its activities through participation in numerous lectures and conferences at national and international levels. Furthermore, LUH publishes in national and international law and other journals on topics related to data protection, data security and IT-law and will disseminate the results of SPEAR through this medium, among others.

SH intends to enhance SPEAR dissemination plans in a) publishing scientific articles in international, peer-reviewed journals and conference, b) preparing public material and c) establishing communication channels in Cyprus and southern Europe. In particular, SH 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, SH 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. SH 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, SPEAR information material, and initial research findings. SH will establish dissemination strategies in Cyprus by disseminating the scopus and the results of the SPEAR project in networks of start-ups in Cyprus and in ICT companies such as the Start-up Cyprus (http://startupcyprus.org/), Start-up Catalyst (http://www.startupcatalyst.com.au/) and European Start-ups (http://www.europeanstartups.org/).

TUS will spread the results of the tasks in which it is involved. This will be achieved via scientific joint publications in international journals, presentation of the project outcomes in international and national conferences and events, as well as organizing a workshop in Bulgaria.

VETS will promote SPEAR's results by participating in a joint publication in scientific journals and conferences, in the field of smart grid security. Additionally, it will exploit its industrial partnerships, contacts as well as its consumers to widely spread the project's achievements.

5.6 Standardisation

The substation automation systems (SASs) such as supervisory control and data acquisition (SCADA), remote terminal unit (RTU), and intelligent electronic device (IED) are considered as core components of the smart grid at transmission and distribution level. Substation automation is a mission-critical task, and in addition, those systems are working under real-time conditions. SASs provide a reliable bedrock for future smart grid developments in electric facilities, where the Substation is the backbone of the electric system and key element of Smart Grid.

Electric grids are considered critical infrastructure as they are essential for the well-being of the citizens. Attacks on this infrastructure are not limited to office computers and networks. They can also directly impact the citizen's lives and the economy as a whole. For instance, in December 2015, Ukraine's electric grid got hacked. The attackers managed to remotely access and manipulate the grid's industrial control system by stealing user credentials. Because of this attack, over 225.000 customers experienced a service outage for three hours.

The list of the most significant standards that are currently used, or could be used, to support the security in Smart Grids and therefore in the substations:

- ISO/IEC 27001 and ISO/IEC 27019: ISO/IEC 27001 is a standard that provides requirements that should be fulfilled for information security management systems. In the context of Smart Grids, the requirements collected in this standard can be used to certify policies and procedures in an organization for developing, producing, building or operating smart grid systems and/or components.
  In addition, based on ISO/IEC 27002, ISO/IEC 27019 provides guidelines for information security management in process control systems. Those principles could be applicable to the process control systems deployed for Smart Grids. However, the information published in this standard

consists only of recommendations, which do not object to certification as ISO/IEC 27001 requirements are.

- IEC 62443: The IEC 62443 series of standards, which is considered as the evolution of the ISA.99 standard, is built on established standards for the security of general purpose IT systems but identifying and addressing the differences and peculiarities of Industrial Automation and Control Systems (IACS).
  The 62443 series focuses on functional security to be applied to the system and components of an IACS to improve the safety, availability, integrity, and confidentiality of the system and their components. This involves that the IEC 62443 does not provide specific details about the technical implementation of a secure IACS, but the functionalities and/or behaviours that need to be fulfilled.
- IEC 62351 Power systems management and associated information exchange - Data and communications security. As it can be deduced by the title, this set of standards is focused on the security of information to be exchanged to perform operations on power systems. It was developed to evaluate the security of the communication protocols defined by the IEC TC 57, including IEC 61850, IEC 60870-5, IEC 60870-6, IEC 61970 and IEC 61968 series.
  Among the security aspects addressed by IEC 62351, we can find information exchange authentication with digital signature, listening prevention, identity theft prevention, and intrusion detection.
- IEEE 1686 IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities: The scope of this standard is to define functions and features that should be provided in intelligent electronic devices to suit the protection program for critical infrastructure.
  Security functions such as access, operation, configuration, firmware revision and data retrieval from the IED. What is missing in this standard are the aspects related to communications of power system protection, such as encryption of data within and out of the substation.

Within Smart Grid standardisation, Schneider Electric is one of the most active companies in: IEC SG3: Smart grids standardisation strategy, IEC TC57: Power utility automation, IEC TC8: System approach, Schneider Electric is also leading the European Smart Grid standardisation roadmap (as part of the mandate M/490), holding many positions in IEC such as IEC TC95 secretary (electrical protection), IEC TC64 secretary (electrical installation), IEC TC17/SC17C chairmanship, IEC PC118: co-convenor on Smart Equipment to serve Demand-Response, IEC TC65 secretary (industrial automation) and many others.

SCHN, as an active participant in TC57 WG15 IEC62351, will contribute to standardising the SPEAR solution to the energy community.

6. Impact reporting

6.1 Key Performance Indicators

The monitoring of dissemination and communication activities is an important and essential process to evaluate the success and efficiency of the plan. The monitoring activities will help the consortium to remain in focus on the strategy and if needed to react and make the necessary changes to the strategy to provide high quality results.

To that purpose, a set of Key Performance Indicators (KPIs) will be used, to measure the progress in the dissemination and communication activities. Special emphasis will be put on the quality of the attainted results rather than the quantity. All partners within SPEAR share the idea that the dissemination strategy is a preliminary activity towards the exploitation and commercialization of the results achieved in SPEAR after the end of the project, and as such, each partner will participate in these activities in a dynamic and interactive manner.

The monitored KPIs include statistics for the website and social media accounts, active participation in events, number of publications and promotional material produced, etc. KPI analysis will drive SPEAR towards the most effective dissemination tools and strategies in order to obtain the highest possible impact.

In the following table, the KPIs associated with each tool and activity are presented. Furthermore, in Annex A of the DoA, there are several tables in which all the activities will be tracked and reported. These tables will be used for the next deliverables of WP8 and also for the reporting of the project.

Table 3: KPIs associated with each tool and activity

Product	Audience	Objective (min value)
Organization and/or Attendance to exhibitions	Strategic stakeholders, Industry	200 visitors
Workshops co-located with major conferences	Research community, Strategic stakeholders, Industry, Other Projects	1-2 workshops per year
On-site demonstrations	Research community, Strategic stakeholders, Industry	3 demonstrations
Publications in workshops, conferences and journals	Research community	Workshop papers (1-3 per year) Conference papers (1-2 per year) Journal papers (1-2 per year)
Online publications (magazines, newspapers, blogs)	Research community, Strategic stakeholders, Industry, Public	10 publications per year 500 views
Posts to social networks	Research community, Strategic stakeholders, Industry, Public	10 posts 100 contacts 50 likes/share 5 comments
Participation in CeBIT	Research community, Strategic stakeholders, Industry, Public	5 brochure copies delivered
Project website	Research community, Strategic stakeholders, Industry, Other Projects, Public	Top 5 SEPR
Inclusion of light content for non-specialized audience in the project website, blog, social media, as well as publishing “lighter” versions of project newsletters, leaflets, flyers, etc.	Public	5 material 100 reads
Summer schools / open events with free access, where visitors will realize in a lively way the SPEAR benefits.	Research community, Strategic stakeholders, Industry, Other Projects, Public	1 summer school 50 attendees 1 open event
Participation in media (TV, newspapers, radio) events	Public	10 media appearances

6.2 Evaluation of dissemination process

SPEAR consortium takes advantage of dedicated tools to measure the impact of each dissemination and communication mean that possesses, meaning the website, the LinkedIn page, and the YouTube channel.

6.2.1 Google Analytics

Google Analytics is a freemium service that has been installed on the website and is being used to measure the impact and popularity of the website. Google Analytics analyses web traffic and is capable of indicating how close the SPEAR is to get the aforementioned goals. Figure 9 illustrates the home page of Google Analytics.

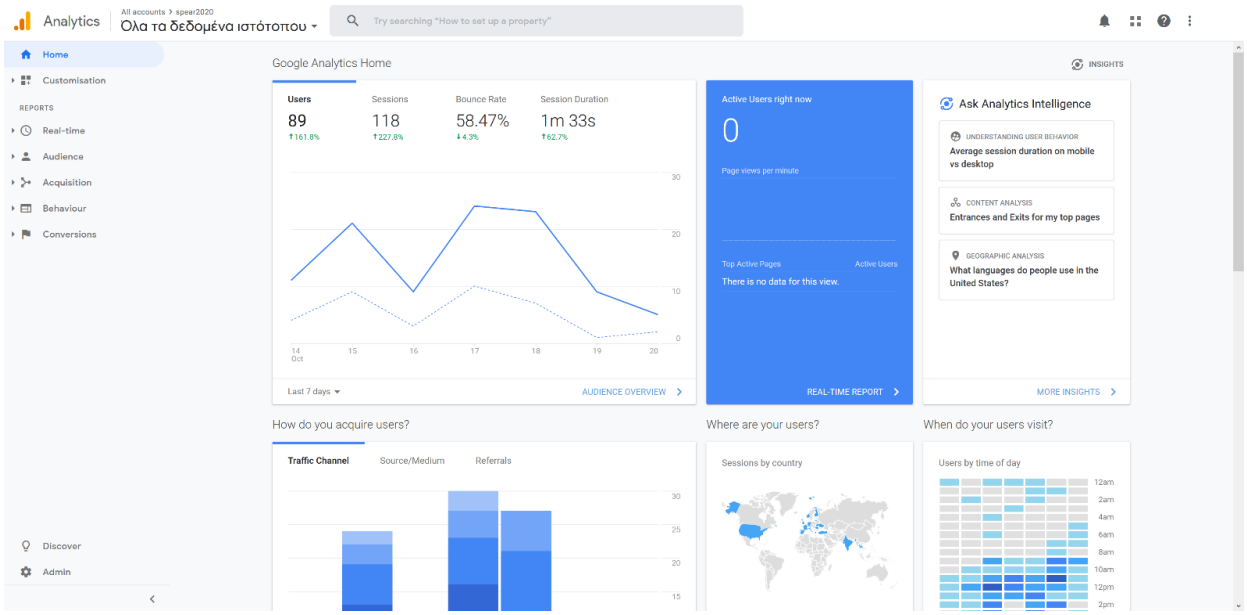

Figure 9: A preview of Google Analytics

6.2.2 LinkedIn Analytics

The main reason that the SPEAR consortium decided to go with a company page instead of a personal profile on LinkedIn was LinkedIn Analytics. This service offers the ability to analyse the impact and efficiency of the communication strategy as well as how intensively the audience reacts to specific posts or campaigns. Figure 10 is a screenshot from the LinkedIn Analytics homepage. The peak that is observed in the main graph was due to reactions that were caused during the second plenary meeting of the SPEAR consortium.

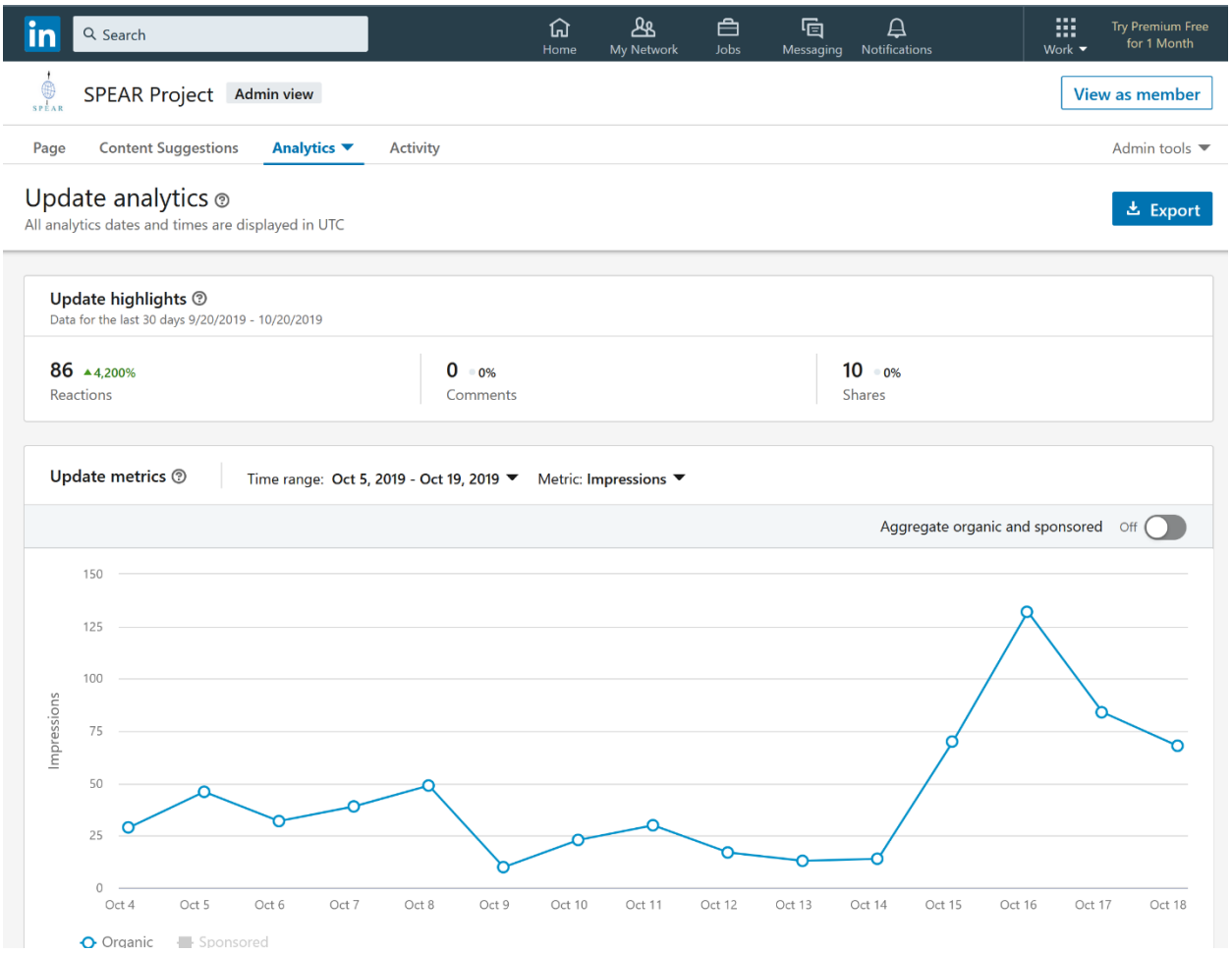

Figure 10: The LinkedIn Analytics homepage

6.2.3 YouTube Analytics

YouTube also offers a service similar to Google and LinkedIn Analytics, for measuring the impact that each uploaded video has. Figure 11 illustrates the homepage of the YouTube Analytics homepage.

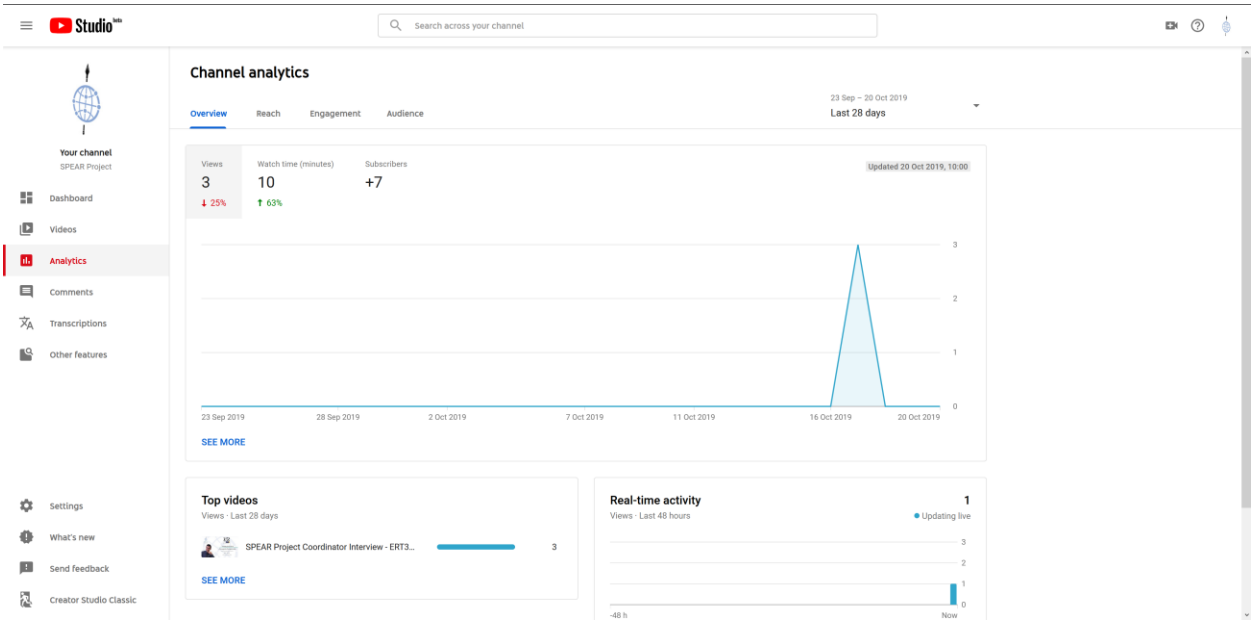

Figure 11: YouTube Analytics homepage

7. Initial exploitation strategy

SPEAR brings together key players of the smart grid cybersecurity value chain: from distribution system operators, providers, and integrators to research centres, academia, and high-tech SMEs. The complementary skills of the partners offer a key exploitation opportunity for the innovations that will be achieved at the project. The main aim of the SPEAR project exploitation activities is to explore innovative products and services and identify the perspectives to turn them into commercially viable offers in targeted markets, throughout Europe.

The initial exploitation plan of SPEAR project results is composed of the individual exploitation plans as well as the joint exploitation of the identified exploitable products. Industrial partners will be the main responsible regarding the exploitation strategy. By incorporating the developed components, partners will enhance their portfolio of products and solutions and will strengthen their position in the market.

Academic partners will also benefit from SPEAR results since they will have the opportunity to use the technological achievements of the project. Academic institutes will strengthen their position and can attract more students in the relative areas, providing them with unique cutting-edge hands-on experience in a growing emerging area, and by means of future projects and licensing of developed IPR. Students will also have the possibility to use the developed tools in their courses. The SPEAR integrated exploitation approaches will precise possible scenarios for the further evolution of the developed solution, during or after the end of the project.

The exploitation strategy will be directed according to the spread of expected outcomes such as methodologies, tools, models, and guidelines. Each category will have the potential for adoption and commercialization of results. The general directions are the following:

Research activities are the major exploitation activity within the SPEAR consortium. All partners participating in SPEAR are interested in building on and further developing, existing research activities. Academic partners will benefit from SPEAR results as they will have the opportunity to use the technological achievements of the project in future research activities (applied and theoretical). Additionally, they will be able to enrich and enhance academic curricula with new material and courses inspired by the project's

research results. This will help to further improve teaching activities and to attract more Master and PhD candidates in relative research areas. All partners will also design new follow-up projects and initiatives at both national and international levels.

Products: all partners of the SPEAR consortium are expected to increase their knowledge on the project related technologies and possibly exploit them by, for instance, filing patents. Industrial partners will lead the activities seeking to identify unexplored technological challenges and produce commercially available services and products closely related to the project. For the exploitation of results, different options might be used, such as the commercialization of the overall SPEAR solution or the incorporation of individual research results into existing platforms or solutions of the individual partners.

Consulting and specialized services: are the main focus for partners interested in transferring the acquired knowledge into consulting and specialized technical services for their customers. These partners will focus on the creation of consulting services to the industry such as early adaptors, technology providers, start-ups and SMEs.

Standardisation: academic and industrial partners will extend their networking activities to standardisation bodies and other organisations that can influence the adoption of the results and guidelines developed in SPEAR.

The target of the exploitation strategy is to transform the research results and outcomes of the SPEAR into potential market products and services, which may be followed by a commercialization of selected elements.

During the project d, specific actions that aim to ensure the correct exploitation of the project results will be undertaken. In more detail, the consortium will perform the following activities:

- Identify the exploitable assets coming out of the project.
- Contact a market analysis with the aim to identify the targeted stakeholders and the current status of competitive solutions
- The creation of business models towards commercialization of exploitable assets
- The evaluation of the business models and the feasibility study
- The final development of a business plan

To illustrate these activities a Roadmap of the exploitation strategy, formulated into four stages, has been designed and is depicted in Figure 12. In each stage, certain activities will take place and the required input for each stage is associated with deliverables coming not only from WP8 but from all work packages of the project.

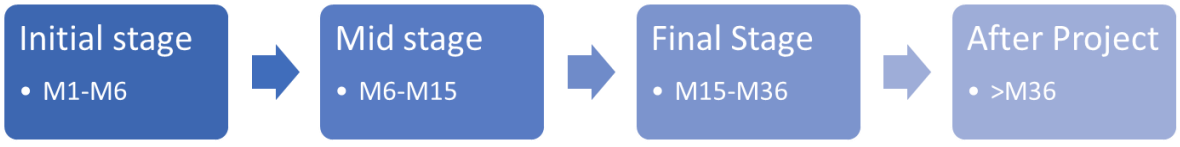

Figure 12: The four stages of the exploitation strategy

The initial exploitation plan that is described in this deliverable will be followed by the market analysis and business modeling report at M15. The final exploitation plan will be delivered at the end of the project and will contain financial and economic analyses along with sensitivity and risk analyses in order to assess technology and market risks. Based on these results, strategic guidelines for the most appropriate exploitable assets will be provided. The timeline of the relative deliverables is illustrated in Figure 13

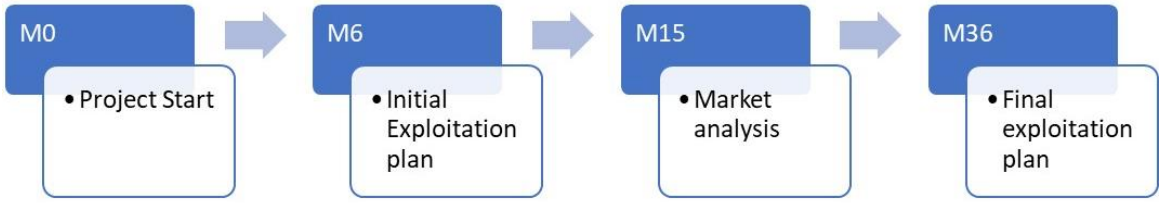

Figure 13: Timeline of deliverables related to the exploitation plan

In addition, Table 4 includes the summary of the intended exploitable rsults of the SPEAR project.

Table 4: Summary of the intended exploitable results of the SPEAR project

IPR holder(s) - Foreground	**Type of exploitation envisaged (C – commercial, S – scientific)**	**Exploitable result**	**Notes**
TEC, UOWM	C	SPEAR Security Information and Event Management (SIEM) basis: the main architetural brick of the SIEM tool, including logs, traces and events monitoring and collecting.	Open access tools will be used, e.g., AlienVault's Open Source Security Information and Event Management (OSSIM) platform.
TEC, UOWM	S	SPEAR SIEM basis in scientific journals and conferences.	Open access tools will be used, e.g., AlienVault's Open Source OSSIM platform.
TEC	C	SPEAR SIEM basis: A highly advanced Industrial Traffic and Data Capturing and Parser module and Event Manager for advanced cyber threats SIEM in Industrial Control Systems.	-
TEC, SCHN	C	A highly advanced RTU Honeypot to enrich cyber threat intelligence in Smart Grids.	-
SURREY, 0INF, UOWM, CERTH, TEC, SH	C	Big Data Analytics Component (BDAC): A modular platform for time series analysis supporting multiple Machine Learning (ML) solutions customized to the end users.	Open access tools will be used, e.g., Python and Spark.
SURREY, 0INF, UOWM, CERTH, TEC, SH	S	BDAC assessment in scientific journals and conferences.	Open access tools will be used, e.g., Python and Spark.
SH, 0INF, TEC,	C	Visual-aided Intrusion Detection System (IDS): A web based application for real	Open access tools will be used, e.g., Django.

CERTH, TEC UOWM		time visualization of alerts and data, using advanced graphs and visual analytics.	
SH, 0INF, TEC, CERTH, TEC UOWM, PPC, SCHN, VETS	S	Visual-aided IDS assessment in scientific journals and conferences.	Open access tools will be used, e.g., Django.
TUS, VETS	C	Mobile application for real time visualization of alerts and data.	Allows for remote monitoring of automated power plants or vacant smart homes.
TUS, VETS	C	A modular option of the detection system, excluding visualization or honeypot usage for the sake of affordability	Data provided by end user. Lower level of security, only detection of incidents.
SURREY, CERTH, UOWM	C	Grid Trusted Module (GTM): the GPM module of the SPEAR SIEM tool.	Open access tools will be used, e.g., Django.
SURREY, CERTH, UOWM, PPC, SCHN, VETS	S	GTM assessment in scientific journals and conferences.	Open access tools will be used, e.g., Django.
ED, UOWM, TEC, PPC, LUH	C	Privacy Preserving, Forensic Ready Smart Grid Network Architecture (Service). Design of smart grid network architecture to enable collection of necessary forensic information, by various smart grid nodes and components that can be used as legal evidence in court, while protecting fundamental rights and privacy of individuals.	• OSCAR methodology for the task of performing network forensics. • DPIA process for identifying what data items can be logged/captured, whether data needs to be pseudonymised or anonymized, the time period data can be stored, etc. including, the purpose for which data is logged. • Network Forensics, including policy development on how monitoring will take place, followed by what will be monitored and what additional data sources besides logs, flow- and packet capture data are needed.

			• Technical threat intelligence, providing Indicators of Compromise (IoC) built around a database which is being fed with information from publicly available threat feeds, and/or Cyber Threat Intelligence (CTI) databases.
ED, UOWM, TEC, PPC, LUH, SCHN, VETS	S	Privacy preserving framework assessment in scientific journals and conferences.	• OSCAR methodology for the task of performing network forensics. • DPIA process for identifying what data items can be logged/captured, whether data needs to be pseudonymised or anonymized, the time period data can be stored, etc. including, the purpose for which data is logged. • Network Forensics, including policy development on how monitoring will take place, followed by what will be monitored and what additional data sources besides logs, flow- and packet capture data are needed. • Technical threat intelligence, providing Indicators of Compromise (IoC) built around a database which is being fed with information from publicly available threat feeds, and/or Cyber Threat Intelligence (CTI) databases.

TEC, UOWM, SURREY	C	Advanced Meter Infrastructure (AMI) Honeypots	Open access tools will be used, e.g., Conpot.
TEC, UOWM, SURREY, PPC, SCHN, VETS, TUS	S	AMI Honeypots	Open access tools will be used, e.g., Conpot.
TEC, 8BL, UOWM	C	Anonymous repository of incidents.	Open access tools will be used, e.g., www.misp-project.org.
TEC, 8BL, UOWM, PPC, VETS, SCHN, CERTH	S	Anonymous repository of incidents assessment in scientific journals and conferences.	Open access tools will be used, e.g., www.misp-project.org.
UOWM, SH, ENEL, PPC	C	Smart grid penetration testing suite.	Open access tools will be used, e.g., Kali Linux.
UOWM, SH, ENEL, PPC, SCHN, VETS	S	Smart grid penetration testing suite: assessment and (filtered) results.	Open access tools will be used, e.g., Kali Linux.
0INF	S	Advanced anomaly detection solutions based on deep architectures.	Open access tools will be used.
0INF	S	Novel visualization techniques of multi-dimensional time series using manifolds.	Open access tools will be used.
SCHN	C	Security Server and Configuration tool new functionalities.	Security server and configuration tool background
8BL	S	A white paper including a market potential report in regards with cybersecurity solutions for the smart grid, report on the results of the demo sites, the success and the potential commercialisation of the SPEAR solution.	Open access tools will be used.
CERTH, UOWM, 8BL	C	Digitized cyber hygiene framework	Open access tools will be used.
TUS, VETS	C	Mobile application for real time visualization of alerts and data	Remote monitoring of automated power plants or vacant smart homes.
TUS, VETS	S	Publications in scientific journals and university journals and others	Bring awareness for the product availability and capabilities to current and future participants in the smart grid.
INC	C	Business model of the SPEAR platform	There are neither foreground nor background IPR. INC will use that knowledge to increase the

			expertise in the area and create new products for its customers.
INC	C	Roadmapping of SPEAR platform	There are neither foreground nor background IPR. INC will use that knowledge to increase the expertise in the area and create new products and services for its customers.
INC	C	Techno-economic analysis of SPEAR	There are neither foreground nor background IPR. INC will use that knowledge to increase the expertise in the area, understand the major costs and thus create new consulting services for its customers.

7.1 Early Exploitable Results

Since some project results have been archieved earlier than planned, the SPEAR consortium explores the commercial exploitation of these results rearlier than envisioned in the workplan, in order to maximise impact for the industry. The table bellow summarises the early exploitable results:

Table 5: Summary of the early exploitable results of the SPEAR project

IPR holder(s) - Foreground	**Type of exploitation envisaged (C – commercial, S – scientific)**	**Exploitable result**	**Notes**
TEC, UOWM	C	ICS Honeypot	Open access tools will be used, e.g., AlienVault's Open Source Security Information and Event Management (OSSIM) platform.
UOWM, PPC	C	ICS Honeypot	
UOWM, VETS	C	ICS Honeypot	
0INF, UOWM, SID, PPC	C	Big Data Analytics software	Developed in the context of the publication "Operational Data Based Intrusion Detection System for Smart Grid" published in 2019 IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks and authored by G. Efstathopoulos, P. Radoglou-Grammatikis,

			P. Sarigiannidis, V. Argyriou, A. Sarigiannidis, K. Stamatakis, M. Angelopoulos, and S. Athanasopoulos.

7.2 Exploitation plans from each partner

UOWM will utilize the innovations in security and privacy fields in both teaching and research activities. A master degree course will be designed based on the SPEAR results. The undergraduate curriculum will be updated and advanced in terms of security and privacy while the IoT experience will be included in new courses. UOWM will be able to pursue more R&D projects at the national and EU levels.

ED is a leading innovative IT company, acting internationally and is always interested to enlarge its current activities. Based on its proven long history, ED can successfully launch new products and services in the international market, and this is demonstrated by the number and the importance of its clients. ED implements commercial products and projects that are in line with this development. ED's management invests annually in R&D (funded internally or by national and European research agencies) around 7% of its turnover, to provide next generation products and services and to continuously gain competitive advantages. ED will enlarge its products and services with innovative solutions for cyber security and, specifically, in terms of the public sector clients addressing the energy domain and solving key challenges of the public sector and the society. Towards that direction, ED will exploit the project results in various ways. ED will enlarge its technical know-how and services within the cyber security sector, which addresses a big market in Europe and internationally and a modern research and application area. The Privacy Preserving Framework and the integration activities to be conducted in the area of the energy power system will be exploited in the future for new research activities and projects and -more importantly- for commercial projects in areas where ED is active in the IT world, such as the public domain service provision.

REAL will exploit the project results, in the effort to widen its portfolio of products and services offered to its clients. REAL will further pursue to enhance its knowledge on cyber security and create new products and technologies complementary to its own. It envisions to create alliances with European players of the consortium in the cyber security market.

The **TEC**´s exploitation strategy for developed SPEAR technologies will be mainly related to consultancy services as well as selling the tools and mechanisms developed during the project, but not only, TEC will transfer the knowledge and lessons learned to the companies interested in the deployment of advanced cyber-attacks detection technologies in the smart grids field. TEC Intellectual Property Rights (IPR) will be managed according to the Consortium Agreement (CA) to be signed in the negotiation phase. This will cover the use of foreground and background to ensure fair and open access to results and required components during the project and for exploitation. During the project, TEC will study the need of patenting the implemented detection mechanisms.

SCHN plans to use the SPEAR results to enhance the security of its substations in France. This will allow SCHN to provide a strong new added value to existing or new customers. In addition, thanks to the international presence of the company and its leadership in the sector, SCHN has the intention to exploit the results of the project with an international vision, focused mainly in the Substation Automation area but not restricted only to that, due to the active participation of SCHN in other smart grid markets. This international presence would allow other SPEAR project partners to participate in international opportunities that could be out of reach for them otherwise.

SCHN ES will focus its contribution on the RTU cyber security brick and the integration of the honeypot's technology. Also, SCHN ES intends to use the SPEAR results to enhance the security of its substations

based on the Substation Scenario Use Case experience. As a result, the experience gained from this SCHN ES will be an asset in attracting new customers in Spain.

ENEL aim is to get knowledge and experience on innovative cybersecurity methodologies and solutions developed within the Project. The Company will exploit the network of experts to improve its own risk assessment process and get knowledge from new use and test cases. In particular:

- Insights on the potential cybersecurity risks, requirements to fulfill and possible security solutions, in terms of new architectures, technologies and processes, based on available Cyber Security frameworks and standards (e.g. IEC 62351 series), also aimed to the interoperability of the secure communication among the electricity actors (DSO, TSO, aggregator) and the various controllers (microgrid controllers, individual - generation and consumption - controllers, etc).
- Deployment of standard based available standard based solutions (considering as well beyond the standard possible approaches) will allow Enel to prevent cybersecurity risks in time for the full realization of the smart grids scenario and share these results with the local regulatory authorities (in the countries where Enel GIN operates), though a well proven and open approach.
- Besides the results of the scenario (where Enel is directly involved), Enel will also benefit from the results of the grid operation pilot and the results, in particular from the recommendations for further development of existing standards, providing gap analysis and feedbacks to standardization bodies (e.g. IEC Cyber Security WGs).

Since Cybersecurity is still relatively new to the energy domain, the Project brings knowledge in terms of day-to-day business best practices to adopt and the potential impact cybersecurity could have on internal organizational change. The results of the project will provide also new elements for new editions of Cyber Security guidelines, in the scenario of Electrical Critical Infrastructure protection.

CERTH is a leading European Research Institute in the ICT domain and its contribution to the exploitation strategy for SPEAR project results and advances will be based on a multi-scale approach with central axis the academia, research, and industry. CERTH plans to participate in various spin-off commercial companies capable of exploiting its research. Being responsible for the logging analysis software, as well as of the vision-based solutions for ensuring user privacy combining Computer Vision and Machine Learning within SPEAR project, CERTH plans directly after the end of the project to further develop and commercialize the results and experiences gained regarding these issues through aforementioned spin off companies. CERTH will also communicate SPEAR in relevant events on national and European scale, by presentations in international scientific conferences, workshops and exhibitions, web-based publishing and small seminars and talks organized for special audiences.

SURREY has vast experience in commercialising research ideas. As part of its exploitation strategy, SURREY will attempt to establish an innovative start-up based on unique software created within task 3.4, without neglecting the potential for further exploitation of other SURREY's outcomes.

PPC will use SPEAR results primarily to shield the national power grid and TRSC network from possible cyber-attacks.

As a market research company, **8BL** will take advantage of SPEAR project to enhance future market reports and seminars related to cyber security and smart-grid, with specific a focus on business cases and opportunities via smart energy-as- a-service. Stakeholders involved in the industry will use these market reports to understand better the opportunities and also manage more easily, more securely and with greater resiliency smart energy networks. The SPEAR project will then help strengthen 8BL position as reference international centre of excellence for cyber security and networking modeling. For this purpose, 8BL will participate and support all the necessary activities for the commercial exploitation of SPEAR, including the investigation to form a new legal entity (e.g., start-up).

INC as a market research company will take advantage of the project's results to enhance its future market reports and seminars related to Critical Infrastructure Cybersecurity solutions, with specific focus on business cases and opportunities via advanced innovative services / use cases. These market reports will be used by industry stakeholders to better understand the opportunities in the new era of Smart Grid. SPEAR will thus help INCITES to strengthen its position as a reference international centre of excellence for cybersecurity solutions from the business perspective.

PIMEE intends to further develop and commercialize the results and experiences gained with central axis the academia, research and industry. Additionally, it will participate in EU and other clustering events for better dissemination across EU activities and projects, within ICT and secure society area.

LUH plans to draft an article on the requirements under data protection law as they relate to forensic data analytics employed in tackling cybercrime. The intention is to submit this in due course to a peer reviewed journal in the field of IT law.

SH will exploit the results and the products of the SPEAR project by utilizing its capacity in creating, maintaining and optimizing the usage of honeypots with the aim of efficient forensics. The usage of the honeypots in attracting modern cyber-attacks will be further advanced by SH in delivering more services and applications after the project. SH will combine its experience in handling penetration tests with the SPEAR research findings in order to provide concrete solutions to organisations and companies that seek protection against serious cyber-attacks. Contacts and interactions with companies in the private sector in Cyprus will be exploited to highlight the benefits of the SPEAR capabilities in handling and addressing cyber-attacks.

0INF will continue their continuous work in the local market (UK), in order to address potential clients of the SPEAR solution in the different target sectors, as it is already in contact with energy providers and related private industries. 0INF will work also on the following dissemination activities: project web dissemination through our own website and social media channels and publication of project advances in relevant national online media.

TUS will contribute to the development of the dissemination and exploitation plan with the other partners. The knowledge gained will be exploited in teaching activities.

VETS, as an energy utility will contribute to the development of the SPEAR exploitation plan. This will allow VETS to boost its reputation and provide a new added value to existing or new customers.

7.3 Common exploitation strategy

Partners of the consortium are confident that there are a lot of commercialization opportunities related to SPEAR, thus the business prospects of these should be examined and evaluated. According to the market research firm's critical infrastructure (protection) market is expected to have a significant growth in the next years due to the increase of data, as a result of which the number of cyber-attacks will also increase.

According to "Mordor Intelligence", the critical infrastructure market is estimated to grow from USD 87.34 billion in 2016 to USD 31.33 billion in 2021, at CAGR of 8.50% over the forecast period 2016 – 2021. The global market is driven by the current trend of investment in smart grids, increase in IT spending, growth in the deployment of automation solutions, integrated functioning of cloud and CIP, increase in cyber-attacks and cyber-crimes, and efficient policy regulations and implementations. Lack of technical workforce, a deep understanding of industrial control system and the lack of interoperability between products are some of the factors restricting the market growth'. Moreover, Markets and Markets predicts that the CIP market size is estimated to grow from USD 110.41 Billion in 2017 to USD 153.16 Billion by 2022, at an estimated CAGR of 6.8%. The Global Market for CIP is forecasted by Global Industry Analysts Inc to reach USD 94.8 Billion by 2020 driven by the growing need to protect critical national assets and prevent disruptions to normalcy

due to physical and virtual threats. In the above context, we consider that there is a potential space for the commercialization of the SPEAR solutions.

In order for the market potential to be better identified, market research will be performed in WP8. The cooperation between all partners will be based on shared and strong business interests. The consortium is committed to explore and compare the viability, sustainability and scalability of a large number of different exploitation schemes (e.g., direct exploitation by the partners, creation of new ventures) and take clear go and not go decisions as far as those are concerned, which will be reflected at the end of the project in the business plan. The consortium may also form an entity (e.g., a start-up) offering the developed solution. Before the commercial take-up of SPEAR's innovations, both a solid business plan and model has to be created. These elements are essentially a map to the success for any company, however, it is a daunting task no matter how great innovations a project brings. In the following, a high-level overview of the SPEAR business model is presented using the powerful Business Model Canvas (Figure 14).

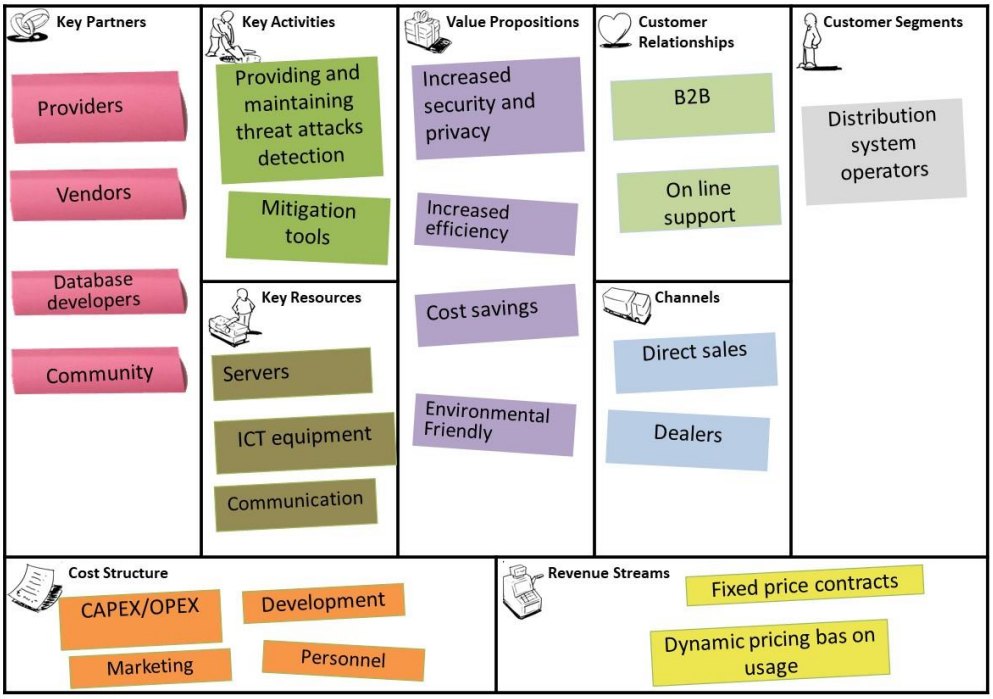

Figure 14: A high-level overview of the SPEAR business model

The approach that will be followed regarding the commercialization of SPEAR solutions is described in the following steps of a tentative business plan:

Step 1 – Vision Statement: SPEAR will develop a secure and privacy-enabled smart grid solution against cyber-attacks using advanced and cutting-edge logging and defence solutions. SPEAR intends to provide more comprehensive SA across both enterprise business systems and operational energy industrial control environments. Distribution system operators, IoT application / service providers, vendors, and third-party companies are the main targets of SPEAR.

Step 2 – Industry Overview – Market and Competitive Analysis: In the last years, there is an explosive growth in terms of critical infrastructures traffic volume, automation systems, number of connected devices and number of threats. However, CIP market is still immature allowing new players and innovative products to enter into it. During the project and before the establishment of the new entity, the overall nature of the

industry, including sales and other statistics will be investigated and described. The area(s) of the market that is targeted will also be described in detail (demographic information on the target group, size, etc.). Another important issue that should be examined is the market growth and trends. Information about SPEAR competitors will be collected. The market segments of competitors will be identified. The benefits of competitor solutions will be investigated and analysed. Data about their products and/or services, pricing, and promotion will also be gathered. This will help us to outline SPEAR's competitive advantage, explaining why and how our entity will be able to compete with these competitors and be established as a successful business. A useful tool in order to analyse a new entity's position in the market is the SWOT analysis. Figure 15 illustrates a preliminary SWOT analysis that will be updated during the project. Factors (barriers to entry) that will affect market adoption and evolution of SPEAR solution will be identified and prioritized.

Figure 15: SPEAR's project SWOT analysis

Step 3 – Product/Services description: Advanced software will be developed. A more efficient and appropriate toolbox as a response to a cyber incident compared to standalone solutions by using a more sophisticated way of logging and trapping cyber traces into contained virtual traps in real, market-based dynamic environments will be offered.

Step 4 – Marketing plan: A detailed explanation of the sales strategy, pricing plan, proposed advertising, and promotion activities will be provided. Marketing of SPEAR solution will also be performed during the lifetime of the project mainly through the industrial partners following the dissemination and communication activities.

Step 5 – Management plan: The management team and the structure of business ownership are very important for the success of a new entity especially when funding is needed. SPEAR consortium consists of experienced partners with management skills able to contribute towards this direction.

Step 6 – Operating plan: Business's physical location, facilities and equipment, kinds of employees needed, inventory requirements and suppliers, and any other applicable operating details, such as a description of the manufacturing process will be provided. The new entity is very likely to be located in a central European country, to facilitate contacts with European network operators and European standardization bodies. New entity's staff will come from the personnel of consortium's companies ensuring high quality human assets. The technical team will be formed from experts from the rest companies and graduates from the involved universities.

Step 7 – Financial plan: After completing the market analysis and set goals for the new entity, the viability of the business idea will be assessed. Although the need to attract any investment in the idea is minimized since SPEAR solution will be developed during the project, potential funding sources are EU-initiated activities, venture capitals, business angels and / or the European Investment bank. SPEAR has included a dedicated for this purpose task where a technoeconomic analysis will be performed. In this analysis, expenses (start-up expenses, CAPital EXpenditure (CAPEX) and OPerating EXpenses (OPEX) will be identified and quantified. The provided services along with their tariffs and demand will be modeled. The combination of these elements will lead to a cash flow projection revealing business evolution and funding needs.

Table of Figures

Table of Tables