FORESIGHT

ADVANCED CYBER-SECURITY SIMULATION PLATFORM FOR PREPAREDNESS TRAINING IN AVIATION, NAVAL AND POWER-GRID ENVIRONMENTS

Grant Agreement: 833673

D12.1
Outreach & communication plan and dissemination report (I)

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 833673.

Document Information

Deliverable number:	**D12.1**
Deliverable title:	Outreach & communication plan and dissemination report (I)
Deliverable version:	v1.0
Work Package number:	WP12
Work Package title:	Impact sustainability
Due Date of delivery:	31/03/2020
Actual date of delivery:	31/03/2020
Dissemination level:	Public
Type	Report (RE)
Editor(s):	Paraskevi Raftopoulou, Christos Tryfonopoulos (UOP)
Contributor(s):	Panagiotis Papanikolaou, Eleni Darra, Dimitrios Kavallieros, Alexis Koniaris, Athanasios Grigoriadis, Efthimios Lissaris, Georgios-Efthimios Giataganas, Maria Kioumourtzi (KEMEA) Anna Malamou, Alkiviadis Giannakoulias (ED) Christos Iliou (CERTH) Marco Gercke (CRI) Theodoros Rokkas, Vangelis Logothetis (INCITES) Helen Gibson (CENTRIC) Nicholas Kolokotronis, George Lepouras Nikos Platis, Paraskevi Raftopoulou, Spiros Skiadopoulos, Christos Tryfonopoulos, Costas Vassilakis (UOP) Damir Haskovic (M&S) Stefano De Paoli (UAD) Sebastien Peynet, Lorin Mace (ACS) Stavros Stavrou, Adamantini Peratikou, Constantinos Louca (OUC) David Brosset (EN) Aare Reintam (CYB) Nikos Papagiannopoulos, Ioanna Varvitsioti (AIA) Daniel Gracia Pérez (THALES) Iliana Peevska (CERT-BG) Tsvetelin Tsonev, Kristina Ignatova (BDI) Maria Atanasova (IEIT) Krasimir Ivanov, Kostadin Mladenov, Yordanka Ivanova, Hristo Stanevski, Nikolay Milanov (ESO) Yasen Todorov (CEZ) Xavier Bellekens, Elochukwu Ukwandu (USTRAT) Stavros Shiaeles, Peng Zhao (UOPHEC)
Reviewer(s):	Biserka Radeva (CERT-BG) Maria Atanasova (IEIT)
Project name:	Advanced cyber-security simulation platform for preparedness training in Aviation, Naval and Power-grid environments
Project Acronym	FORESIGHT

Project starting date:	1/10/2019
Project duration:	36 months
Rights:	FORESIGHT Consortium

Document history

Version	Date	Beneficiary	Description
0.1	30.01.2020	UOP	Initial ToC proposal
0.2	07.02.2020	All	Partners' comments on ToC
0.3	28.02.2020	All	Partners' input
0.4	06.03.2020	UOP	Input integration
0.5	10.03.2020	UOP	Submit for review
0.7	17.03.2020		Ethics review
0.8	20.03.2020	UOP	Address ethics review comments
0.9	27.03.2020	CERT-BG, IEIT	Final review
1.0	31.03.2020	UOP	Address review comments & submission

Acknowledgement: This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 833673.

Executive Summary

Global cyber-attacks are increasing in both sophistication and scale; such incidents reveal the extent of threat to which our critical information infrastructures (CIIs) and information and communication technology (ICT) systems are exposed to. Since CIIs provide vital functions that our societies depend upon, cyber-attacks are expected to have a growing negative economic and societal impact in the next decade and should therefore be considered as global risks. A review report recently published by ENISA estimates that the average annual losses due to cyber-crime among European Union (EU) countries is about 0.41% of their gross domestic product (GDP), whereas in some countries the losses exceed 1.5% of their GDP (Germany and Netherlands being amongst them), leading to annual costs in the range of €425K – €20M per company. Among the CII sectors in the EU, those significantly affected are the energy, transportation, financial, health, ICT, and public administration sectors. The economic losses from cyber-criminal activities are now exceeding security investments in IT, made by companies worldwide to protect their assets. This situation is amplified by the technological evolution brought about by the Internet of Things (IoT), which establishes new ecosystems of heterogeneous networked devices that are highly complex to analyse, maintain, and secure.

The FORESIGHT project was established as part of a European Union funded endeavour to develop a federated cyber-range solution in order to enhance the preparedness (prevention, detection, reaction and mitigation) of cyber-security professionals at all levels (from junior to senior) by delivering a realistic training and simulation platform that brings together unique cyber-security aspects from the aviation, power grid and naval ecosystems. Hybrid scenarios will also be implemented by introducing IoT simulated devices (e.g., sensors) to the aforementioned ecosystems.

This document constitutes a stated deliverable of this project, where the FORESIGHT Consortium presents the planned dissemination activities to (i) ensure the visibility and awareness of the project, (ii) promote the project amongst stakeholders, (iii) engage the target audience, and finally (iv) maximise the uptake of project results in industry and research. More specifically, this document provides a detailed description of the information the Consortium aims to communicate, the stakeholders and the targeted audience of the FORESIGHT outcomes, the ways the Consortium plans to demonstrate this information, and the individual communication plans intended by the Consortium Partners.

Contents

Figures

Tables

Acronyms

Term	Description
ACI	Airport Council International
AOC	Airlines Operation Committee
BPM	Business Process Management
CII	Critical Information Infrastructures
DOC	Dissemination, outreach, and communication
EAB	External Advisory Board
EARTO	European Association of Research and Technology Organisations
ECSO	European Cyber Security Organisation
EENA	European Emergency Number Association
ENISA	European Union Agency for Cybersecurity
ENLETS	European Network of Law Enforcement Technology Services
EOS	European Organisation for Security
ERP	Enterprise Resource Planning
ESRIF	European Security Research and Innovation Forum
EuAB	European Association for Biometrics
FTZ	Free-Trade Zone
GDP	Gross Domestic Product
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
ICT	Information and Communication Technology
IDEB	Innovation Dissemination and Exploitation Board
IoT	Internet of Things
IP	Intellectual Property
PSCE	Public Safety Communication Europe Forum
RTD	Research and (Technological) Development
WP	Work Package

1. Introduction

The vision of FORESIGHT is to enhance the preparedness of cyber-security professionals at all levels and eventually to put forward a new era for cyber-range domain by providing a holistic approach to cyber-threat management. Bearing this in mind, the communication activities will be overseen by M&S (as the leader of WP12), an organisation that focuses on improving sustainability of research and innovation outcomes, especially of public funded projects, to ensure that spent resources lead to enduring positive impacts for the society as a whole. Along with M&S, UOP, KEMEA and CENTRIC will form the core of the project's communication team, working together to succeed the planned impact sustainability of the FORESIGHT project. More specifically, M&S is responsible for maintaining the consistency of project communications, therefore having the lead of the clustering with other related projects and with all individual partners, and for the market analysis and the plan regarding the long-term sustainability of the FORESIGHT project; UOP is responsible for promoting and disseminating as broadly as possible the project's activities and accomplishments; KEMEA is responsible for the design and the delivery of the project's website, the creation of the social media accounts, and for the timing of blog posts in FORESIGHT's website, the creation of podcasts, LinkedIn posts, Facebook posts, maintaining the FORESIGHT's twitter feed, etc.; CENTRIC is responsible for the standardisation roadmap envisaged in this project.

In this report, the Consortium documents the planned dissemination activities to ensure the visibility and awareness of FORESIGHT, promote the project amongst stakeholders, engage the target audience, and finally maximise the uptake of project results in industry and research.

When planning the outreach and communication activities, the dissemination process can be split into three major phases:

1. **Make FORESIGHT known among the general public** by using means of online visibility (e.g., create the official FORESIGHT website) and to the research and development (RTD) community and industry by using certain offline activities (e.g., present the project on conferences, organising workshops, etc.).
2. **Use the first convincing results** as a point from which the Consortium can approach a wider set of groups, also with valuable industrial prospects, and undertake aimed dissemination processes.
3. As the project starts delivering its final results, move over to a strategic phase, where the Consortium will put efforts to **let the widest audience benefit from FORESIGHT results**, establishing a fruitful afterlife of the project.

More specifically, this document provides a detailed description of the information the Consortium aims to communicate, the stakeholders and the targeted audience of the FORESIGHT outcomes, the ways the Consortium plans to demonstrate this information, and the individual communication plans intended by the Consortium Partners.

1.1 Purpose of this document

Through the planned dissemination activities, the FORESIGHT Consortium targets the scientific community, industrial stakeholders, the public sector, and other groups who might be interested in

the achievements of the project. This report contains detailed information on potentially interested stakeholders (Section 2.3), methods of communication (Sections 3 and 4), individual partner communication plans (Section 5), and any restrictions to dissemination due to commercially sensitive information (Section 6.1); all the provided information will be then used as a reference to evaluate the progress of the project during its lifecycle. Of course, every year we will refine and undertake the dissemination activities throughout the evolvement of the project according to the given high-level plan (Section 2) aligned with the project objectives (Section 6.1) and thus, extend and improve our ways to reach the targeted groups effectively. Additionally, this report provides Key Performance Indicators (KPIs) (Section 6.2) for each outreach and communication activity to set an initial goal for partners, ensuring that FORESIGHT will achieve the widest adoption of its results.

1.2 Target audience

The main objective of the planned dissemination activities is the external awareness of the FORESIGHT project, i.e. the communication of the project's outputs and benefits to all the potentially interested stakeholders. To that end, this report presents both an overview (in this section) and an extended analysis (in Section 2.3) of the targeted audience.

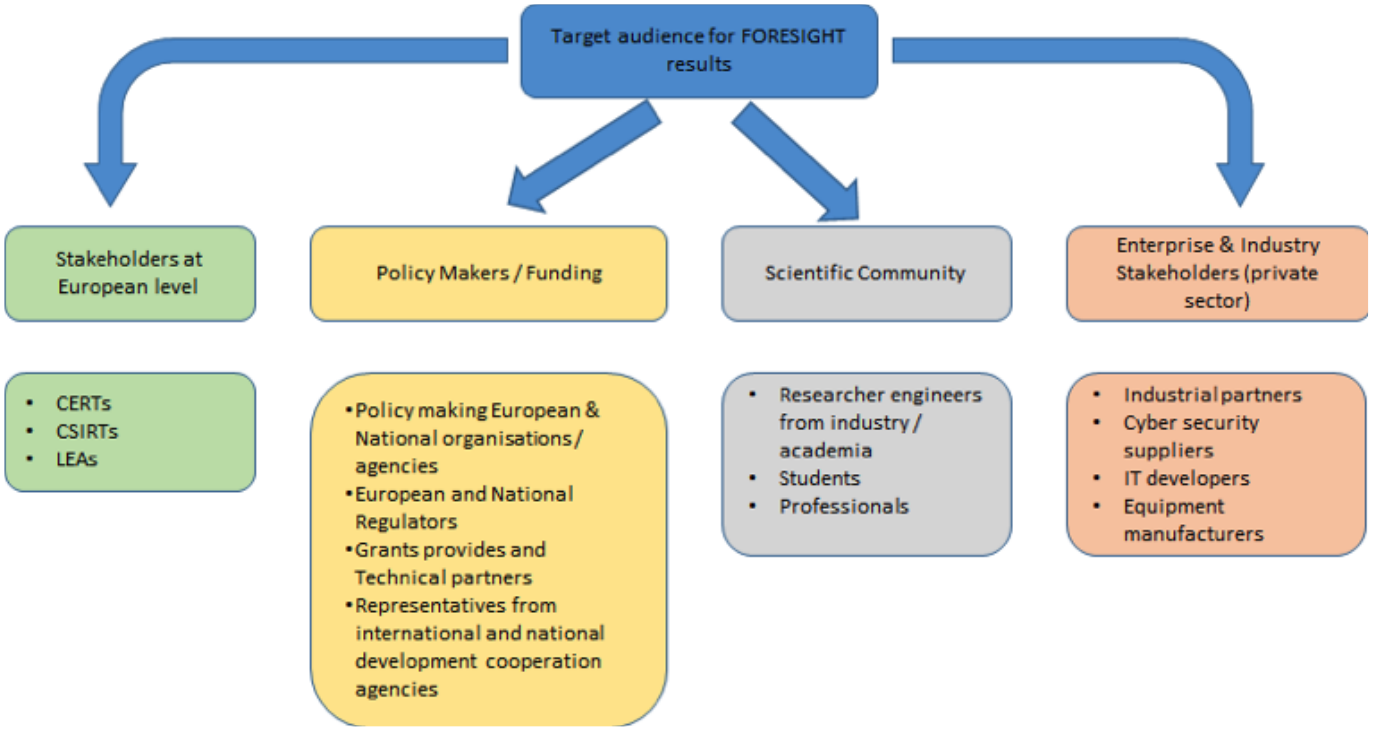

Figure 1. FORESIGHT targeted audience

As also shown in **Error! Reference source not found.**, the targeted audience of the project's results can be classified into the following broad categories.

Scientific community. Scientific community include researcher engineers from industry and academia, (PhD) students, and professionals; to reach this audience the Consortium will use means such as release of demo work packages via mass media channels, scientific publications in European and international venues and in press releases for popular and sectorial magazines and newspapers, as well as presentations and participations in academic events and/or conferences for cyber-security.

Enterprise & industry stakeholders. The dissemination activities targeting commercial and industrial experts aim to raise awareness and inspire interest and market demand concerning the FORESIGHT output. Towards this end, companies and organisations (including manufacturers of cyber-security products and services, as well as associations, regulators and policy makers in the cyber-security industry, the standardisation community, and the aviation, energy and maritime market communities) will become aware of the platform developed in the project and the final outcomes, and have by this multimodal benefits towards facing security and privacy challenges; business decision makers can adopt project results in the IT (cloud) computing infrastructures or in the system architectures used at the enterprises, IT specialists can integrate the provided software solutions into systems developed by companies, equipment manufacturers, and/or cyber-security suppliers can deliver products that may deal with highly sophisticated attacks, etc. The Consortium intends to organise a number of outreach activities in order to interact with the eventual beneficiaries of the FORESIGHT technology.

EU citizens and customers. The topics of future cyber-range technologies, architectures and business models and the future structure of the cyber-security market are attracting more attention across Europe. Already billions of devices (both personal and industrial) are interconnected across the globe in a phenomenon known as the Internet of Things (IoT). Therefore, FORESIGHT's results shall be available to the wider public/end customer via attractive and user-friendly techniques such as press releases in popular culture e-zones and papers, infographics, white board animations, technical videos, technical papers available on its website, and regular updates via social media (i.e., Twitter, LinkedIn, etc.). FORESIGHT Consortium will ensure that the results of the project will become available across Europe in both technical and media focused formats, to allow the general public be aware of and use the project's outcomes.

Policy makers. The federated solution proposed by FORESIGHT is expected to change the current state-of-the-art in cyber-range by advancing the skills of cyber-security professionals via an in-depth domain-specific and cross-domain training and by providing a series of unique features and services that will be incorporated in the resulting platform (like threat forecasting, risk evaluation, econometric models, etc.). Because of the FORESIGHT outcomes, policy makers will be able to focus on novel methods and tools for training cyber-security practitioners to deal with highly sophisticated attacks. Furthermore, the given solution is also expected to impact the whole aviation, energy and naval sector value chain. Towards this end, the Consortium will promote the results of this project into technical deliberations and in the EU cyber-security certification framework in conjunction with the European Union Agency for Cybersecurity (ENISA) and National Regulatory bodies by organising regular formal meetings with all the involved agencies in the European Commission, including also any interested national regulators who may use FORESIGHT results to feed into future market designs and regulatory frameworks.

1.3 Relation to other tasks and deliverables

The inter-dependencies among the FORESIGHT work packages are shown in the following Pert diagram (**Error! Reference source not found.**).

As expected, WP12 is inter-related with all other WPs of the project, as is the main vehicle to transfer the impact of FORESIGHT. During the whole lifecycle of the project, as project evolves and its outcomes

are produced, the Consortium will take all the required actions to ensure that the FORESIGHT technology and overall results are properly disseminated and communicated to all interested stakeholders. By the time the first outputs are generated [i.e., platform architecture (WP2), framework modelling (WP4, D4.3), risk-analysis and assessment models (WP5, D5.3)], they will be used as a point from which the Consortium can approach a wide set of stakeholders, also with valuable industrial prospects, and undertake aimed dissemination processes. As the project will start delivering its final results [e.g., FORESIGHT toolkit (WP9, D9.1)], the outreach and communication strategy will move over to a strategic phase, where efforts will put to let the widest audience benefit from FORESIGHT results, eventually establishing a fruitful afterlife of the project.

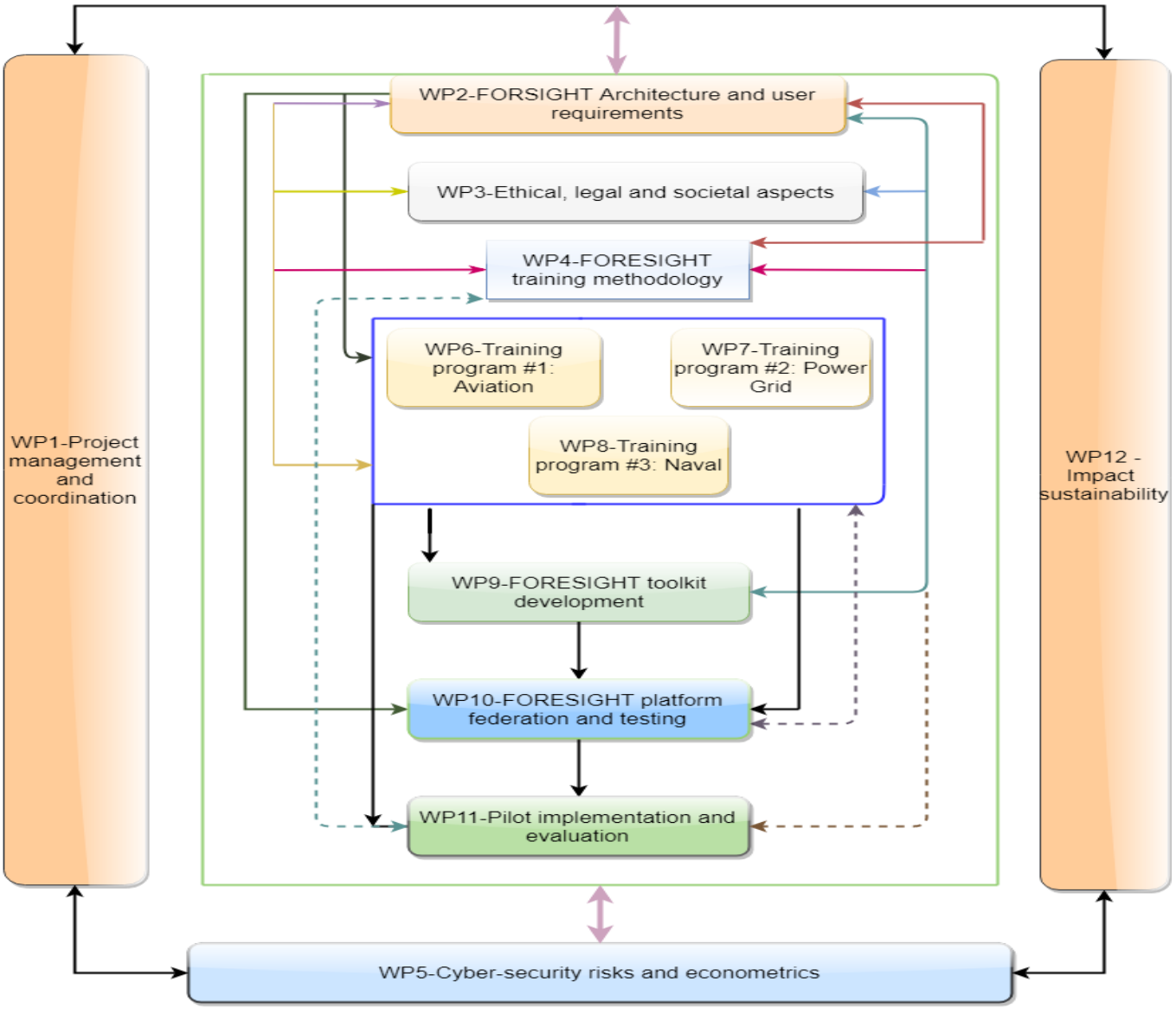

Figure 2. Pert chart illustrating inter-dependencies among the work packages

1.4 Structure of this document

This report is divided broadly into four parts. The first part gives the high-level outreach and communication strategy of the FORESIGHT project; it describes the vision of the Consortium concerning the communication of the FORESIGHT's outputs, presents the objectives of the planned dissemination activities, and provides a detailed analysis of the potentially interested stakeholders (Section 2). The second part presents in detail what type of information will be communicated and the (offline, online, short-term, and long-term) activities used by the FORESIGHT Consortium to disseminate this information (Sections 3 and 4). The third part describes the individual partners' plans intended to disseminate the achievements of the FORESIGHT project to the scientific community and to other interested stakeholders (Section 5). The fourth part discusses the alignment of the proposed communication plan with the project objectives, including the restrictions to dissemination due to commercially sensitive information and the planned Key Performance Indicators (KPIs) (Section 6). We will conclude this report by presenting a final overview of our outreach and communication plan, summing up the information that the FORESIGHT Consortium aims to communicate, the targeted audience of the FORESIGHT outcomes, the planned communication and dissemination activities, and the individual communication plans (Section 7).

2 High-level plan and strategy

FORESIGHT's dissemination high-level strategy consists of the following three successive phases.

1. **Initial awareness phase.** Targets the general public, the RTD community, and the industry in order to gain visibility by presenting the concept, the objectives and the expected results of FORESIGHT.
2. **Targeted awareness market phase.** Uses the first convincing results to approach potentially interested stakeholders and inform them about the technological benefits of the FORESIGHT outputs.
3. **Strategic phase.** Establishes a fruitful afterlife of the project.

Each of the above, abstractly given, phases have different orientation, different target groups, and specific particularities, thus discrete approaches (i.e., methods and activities) must be undertaken in order to achieve the specific goals of each phase. In what follows, we describe the particularities of each one of the above phases.

Initial awareness phase

In order for the FORESIGHT Consortium to raise the public awareness for the project, means for online visibility (e.g., create the official FORESIGHT website) along with certain offline activities (e.g., present the project on conferences / workshops / exhibitions / other events) will be used. More specifically, the intended activities are the following.

- Setting up a common project design used in all (marketing) material (i.e., logo, documents, presentations, social networks, etc.) in order to establish the FORESIGHT brand name in common consciousness.
- Creating and maintaining the official FORESIGHT website, which introduces the project and the Consortium to the public, describes the vision of the project, and gives FORESIGHT's goals.
- Designing and creating FORESIGHT's information materials (i.e., leaflets, brochures, etc.) to be distributed when Consortium members participate to related events.
- Using communication means such as press releases in popular culture e-zones and papers, infographics, white board animations, technical videos, and technical papers available on the website, and regular updates via blogs and social networks (i.e., Twitter, LinkedIn, etc.) to produce and disseminate materials easily accessible to the general public.
- Giving presentations at European and international venues, such as conferences, workshops, and other academic events, concerning the challenges and the goals of FORESIGHT in order to raise the awareness of the project among the academic and the industrial communities.
- Organising workshops held along with known events, exhibitions, and/or conferences in order to establish FORESIGHT brand name among the scientific and industrial stakeholders.

Targeted awareness market phase

The FORESIGHT partners will use the first convincing results as a point from which the Consortium can approach a wider set of groups and stakeholders with valuable industrial prospects, and promote the results, the technological benefits, and the long-term vision of the FORESIGHT project. The planned activities are the following.

- Uploading and promoting latest concrete results and project news through the project's website to keep interested stakeholders up-to-date.
- Sharing news and project updates through social communication channels in order to demonstrate the live spirit and the progress of the project.
- Publishing and disseminating press releases after having reached important milestones; these releases will be circulated to representatives of the European press focusing on security and privacy issues providing cyber-security professionals with advanced preparedness (prevention, detection, reaction and mitigation) skills.
- Submitting high-quality papers and articles, which will thoroughly present the findings and the outputs of the project, to scientific and industrial venues concerning cyber-security.
- Presenting the technical and scientific findings of the FORESIGHT project at related European and international venues in order to promote both its outputs and its prospects dealing with cyber-security in the aviation, power grid and naval ecosystems.
- Promoting FORESIGHT's results into technical deliberations and the EU cyber-security certification.
- Building awareness of innovation opportunities using online platforms (e.g., ProductHunt).

Strategic phase

The dissemination activities targeting commercial and industrial experts aim to inspire interest and market demand concerning the FORESIGHT final outputs. Specifically, the planned activities of this phase are the following.

- Upgrading the project website, including optimisations for search engines and optional registration for specific keywords in order to ensure a long-term awareness of the FORESIGHT brand name.
- Demonstrating FORESIGHT's final outputs at scientific and industrial venues as the new high-quality suggestion for facing security and privacy challenges and enhancing the preparedness (prevention, detection, reaction and mitigation) of cyber-security professionals at all levels (from junior to senior).
- Organising outreach activities in order to interact with the eventual beneficiaries of the FORESIGHT technology and communicate the findings of the project.
- Disseminating the results via in house presentations and/or newsletters to industrial partners and interested parties (including manufacturers of cyber-security products and services, associations, regulators, policy makers and the standardisation community); business decision makers can then adopt project results in the IT (cloud) computing infrastructures or in the system architectures used at the enterprises, IT specialists can integrate the provided software solutions into systems developed by companies, etc.
- Feeding EU cyber-security certification framework in conjunction with the European Union Agency for Cybersecurity (ENISA) and National Regulatory bodies framework with the final outputs of the project will provide the policy makers with a different perspective, novel

methods, and tools for training cyber-security practitioners to deal with highly sophisticated attacks, changing by this the current state-of-the-art in cyber-range and advancing the skills of cyber-security professionals.

- Promoting FORESIGHT by using communication channels (e.g., Twitter, Facebook, etc.) and electronic newsletters, and by creating YouTube videos showcasing the system in trials and users' opinion.

2.1 Vision

The FORESIGHT project aims to develop a federated cyber-range solution in order to enhance the preparedness (prevention, detection, reaction and mitigation) of cyber-security professionals at all levels (from junior to senior) by delivering a realistic training and simulation platform that brings together unique cyber-security aspects from the aviation, power grid and naval ecosystems. Hybrid scenarios will also be implemented by introducing IoT simulated devices (e.g., sensors) to the aforementioned ecosystems. The long-term vision of FORESIGHT is to empower organisations to protect themselves both legally and economically by reducing cyberattacks. The adoption and use of the FORESIGHT outputs by organisations will lead to increased marketing opportunities, which would dramatically increase its user base. Hitting that milestone will, in turn, generally increase the resilience of society to cyberattacks. Towards this end, the vision of the dissemination strategy is to communicate and promote the FORESIGHT's outputs concerning research and development (i.e., research on advanced cyber-threats, experimentation, development of novel ideas and tools) as the key to impact how future guidelines are formed across a range of critical infrastructure and community sectors and feed into a new, robust, resilience certification mechanism that will promote a set of common procedures and testing criteria across the EU.

2.2 Objectives

The proposed dissemination plan consists of several objectives to be met over the lifetime of the project.

- **DO1** Raise awareness on the FORESIGHT project and its achievements by employing a diverse range of dissemination and communication outreach (DCO) strategy.
- **DO2** Develop and maintain communication channels, such as the project website, social media channels and newsletters, to produce and disseminate easily accessible material.
- **DO3** Offset the mechanisms for the FORESIGHT Consortium to communicate with the potentially interested stakeholders, using social media and other collaboration tools.
- **DO4** Clustering with other relevant projects and related networks.
- **DO5** Impact on the technology roadmap and future research on cyber-security by participating in expert forums, publishing in conferences/journals, and contributing to policymaking.
- **DO6** Monitor, support and track the dissemination and communication activities by the partners, and provide a regular report to the commission, the consortium and the EC.
- **DO7** Perform a detailed market analysis and evaluate selected business models and commercialisation practices to improve the awareness of the European industry and the EU cyber-security certification framework.
- **DO8** Set up a business-model-driven exploitation plan as a guideline that presents several

scenarios for bringing the solution to the market and make better use of the project results.

2.3 Stakeholder analysis

Thoroughly aligned with the project's objectives, the dissemination activities targeting commercial and industrial experts consist of several policies intended to transfer FORESIGHT achievements and lessons learned, and aim to inspire interest and market demand concerning the FORESIGHT final outputs. Towards this end, the Consortium has carefully considered the stakeholders and the targeted audience of the FORESIGHT outcomes.

Table 1 highlights a broad cross section of the type of audience FORESIGHT expects to engage with and the added value FORESIGHT will provide to them and vice versa.

Table 1. FORESIGHT target groups and added value

Target group	FORESIGHT added value
European industry	Marketing campaigns and in-house presentations to increase public awareness and commercialise the results of FORESIGHT
Scientific and academic community	The researchers can contribute on advanced cyber-threats, experimentation, development of novel ideas and tools as the key to increase the dynamics of training and awareness methods in order to match or even exceed the rate of evolution of cyber-attackers
EU citizens and customers	Users of cyber-security products and services and cyber-security professionals are key players in the cyber-security transformation; FORESIGHT ensures that the results of the work are available across Europe in both technical and media focused formats and the wider public uses the results and creates opportunities
IT organisations and professionals	Business decision makers can adopt project results in the IT (cloud) computing infrastructures or in the system architectures used at the enterprises, IT specialists can integrate the provided software solutions into systems developed by companies, equipment manufacturers and/or cyber-security suppliers can deliver products that may deal with highly sophisticated attacks, etc.
Policy makers and reform	The integrated, interconnected approach of the project will be complemented by an interconnected dissemination approach towards policy makers
Other running projects	FORESIGHT outputs will be disseminated through other networks in order to influence the future game-changers in the cyber security industry; academic debates and discussions may provide new direction for the project results which will allow for innovation and result in job creation across Europe

In addition, the following table (Table 1) provides a more detailed plan of the activities per target group to be undertaken as part of the project's communication strategy. For each target group, the main partners involved along with the envisaged instruments are presented; this is accompanied by a brief explanation of the activities, identifying indicative events, groups etc., where appropriate.

Table 2. FORESIGHT communication strategy

Target group	Involved partners	Communication instruments	Comments and indicative details about FORESIGHT'S plans
» EU citizens and customers	all	» Press/media » EC magazines » Website » Social media » Social hack day	Marketing campaigns to increase public awareness and promote the project's approach, e.g. set different themes and release specific challenges within those themes to help refine ideas
» Academic institutes » Research centres » Security researchers » MSc/PhD students	KEMEA, UOP, OUC, CERTH, CENTRIC, UAD, THALES, USTRAT, UOPHEC	» Publications » Conferences » Workshops » Targeted lectures	Apart from publications in high-quality journals and conferences (given in Section 4.2), plans have been made for » organising events » incorporating research material in class lectures
» Academic institutes » Research centres » Security researchers » MSc/PhD students » IT organisations » IT professionals » European industry » Policy makers and reform	KEMEA, UOP, OUC, CERH, CENTRIC, ED, CRI, INCITES, UAD, CYB, THALES, USTRAT, UOPHEC	» Training sessions » Seminars » Open days » In-house presentations	Organise standalone seminars, training sessions and open days, and perform marketing campaigns and in-house presentations to increase public awareness and commercialise the results of FORESIGHT
» European industry » IT professionals » IT organisations » FORESIGHT domains	ACS, BDI, IEIT, ESO, INCITES, ED, EN, CYB, CEZ	» Seminars » Training sessions » Focused groups » Exhibitions » Mailing lists » F2F meetings	» IMG-S meetings, www.imgs-eu.org » EU-VRI meetings, www.eu-vri.eu » European cybersecurity forum » International Energy Forum 2020 » Online magazine Energetika
» Clients' network » Collaborations' network » Partners' network	ACS, BDI, CEZ, IEIT, ESO, EN, AIA, CYB	» F2F meetings » Own social media » Own website » Mailing lists	The industrial partners will use their well-established networks of European and national contacts to communicate the results of FORESIGHT project, draw their attention and increase its visibility
» External bodies » H2020 projects	M&S, all	» Website » Social media » Conferences » Workshops » F2F meetings » Working groups » Open days	Present sister projects on the website and promote them through social media; FORESIGHT partners will get in contact with potential external cooperation partners and other projects, ensuring that any result and approach from FORESIGHT in terms of interoperability, standards, and security, together with business validation and sustainability, can be clustered horizontally

3 Outreach and communication plan

This section outlines the activities and tools to present the project to the general public.

3.1 Communication tools

3.1.1 Visual identity and project logo

A full visual identity kit has been provided to the consortium. It includes visual aspects, such as logo variations, colour codes, fonts, picture language, as well as print materials (leaflet / factsheet, rollup, stickers) and screen designs (banners, avatars, PowerPoint elements). The project's visual identity has been developed in order to provide a uniform and consistent communication strategy for the project. As such, it guarantees a visual synergy with the FORESIGHT brand and a recognisable image, which can help in capturing the audience's attention and interest.

The main project logo has been voted by all consortium partners. The final version represents a clear, coherent, distinct, professional and high-quality branding. It consists from a logotype, made from the word FORESIGHT with all capital letters. The first four letters "FORE" are marked in blue colour, and the subsequent 5 letters "SIGHT" are marked in red colour. This represents the red (attackers, bad guys, danger) and blue (defenders, good guys, solution) teams. The isotype is incorporated in the letter "O" and is represented by a "watching eye". Additionally, the isotype is surrounded by three red dots, which represent attention areas, searching, analysing etc. The FORESIGHT logo, with its two variations shown in Figure 3, is used throughout the communication and dissemination material.

Figure 3. FORESIGHT logo (colour, solid black, clear space)

Furthermore, the primary colours used in the logo variations and the dissemination and communication material, as well as the fonts used, are listed in Table 3.

Table 3. FORESIGHT main colour scheme, body and headline font (Google Free Font)

	RGB 0/49/132 HEX #003184 CMYK 100/85/15/10	Barlow Light 1234567890#"!? Barlow Regular 1234567890#"!? Barlow Medium 1234567890#"!? Barlow Semibold 1234567890#"!? Barlow Bold 1234567890#"!? Barlow Extrabold 1234567890#"!?
	RGB 224/0/19 HEX #E00013 CMYK 0/100/100/0	

3.1.2 Project website

The project website ( ) functions as the official source of available information regarding consortium partners, planned work and events. It will contain access to the FORESIGHT on-line collaboration among the consortium, and public documents produced by FORESIGHT. The web portal will promote dissemination activities by featuring press releases, publications and conference presentations. It also serves as a gate to FORESIGHT social media channels by providing the necessary links to them making the visitor aware of the existence of these channels and in the same time giving the visitor easy access to them. The main page of the FORESIGHT's webpage is shown in Figure 4.

Figure 4. FORESIGHT Home page

3.1.3 Social media

FORESIGHT project will have a strong social media presence and actively engage in social networking in order to reach the relevant audiences and to further enhance the scope and outreach of the project. To this end, Twitter™ (*@FORESIGHT_H2020*) and LinkedIn™ Group (*FORESIGHT Project*) have been set up, are also linked from the FORESIGHT website, and will serve both as communication and dissemination platforms; they will offer quick updates, reposts of news content related to the project, such as links to opportunities to engage with the project, forthcoming events, and related news from other sources that impact the project.

In order to create a more engaging content for both the Twitter™ and LinkedIn™ Group, a more visually oriented approach is favourable. This includes images, that are free for reuse (under Creative Commons License), or when using pictures from project events (with consent from participants) or FORESIGHT materials. All FORESIGHT consortium partners are required to contribute to the growth of the social media channels by either sharing, liking, subscribing, following, engaging or posting regularly.

Twitter™, as an open platform that allows access to the contained information without restricting the end-user (e.g., by requiring to register and log-in into the platform to access content), will be used to disseminate current information about the project scope, open feedback channels, and establish two-way dialogues with the wider public. When posting on Twitter™, it is recommended to use the project's Twitter™ handle *@FORESIGHT_H2020*, along with *@EU_H2020* and the *#H2020* as well as with further relevant hashtags to give tweets more visibility. The project's Twitter™ feed is shown in Figure 5.

According to the provided guidelines from the Guidance Social media guide for EU funded R&I projects [1], and since Twitter™ has a 160-character limit for profile information, the following sentence is pinned as the profile bio:

"*This project receives funding from the @EU_H2020 Research & Innovation Programme. Any related tweets reflect only the views of the project owner*."

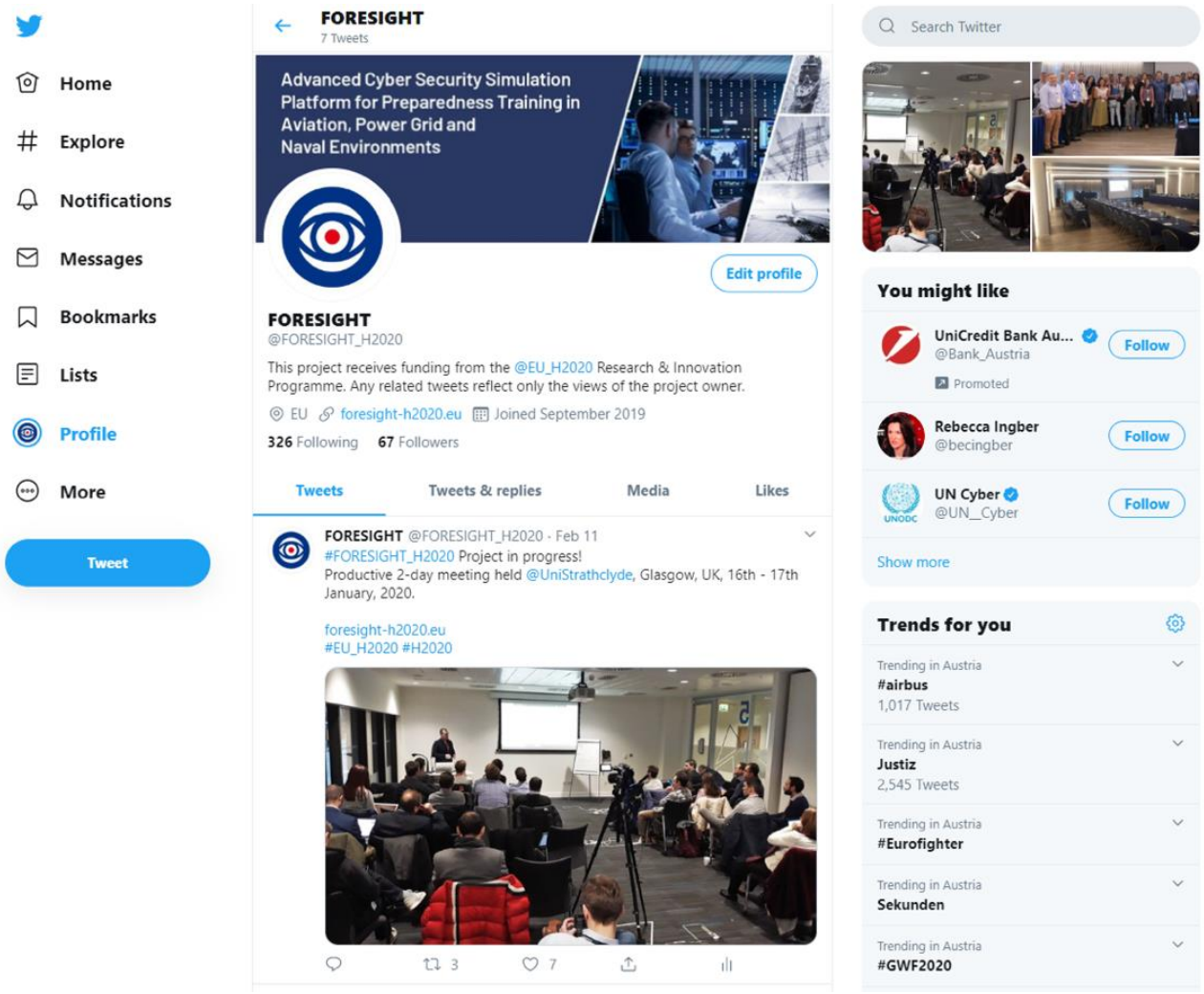

Figure 5. FORESIGHT Twitter Profile

LinkedIn™ is, on the other side, a professionally focused social media platform which provides value to the project. The main aim is to provide a live feed and concise information about the main ongoing activities, outcomes, future plans, and also a universal platform for communication between various stakeholders and professionals in the field of cyber security, cyber ranges and preparedness training. The project's LinkedIn™ Group is shown in Figure 6.

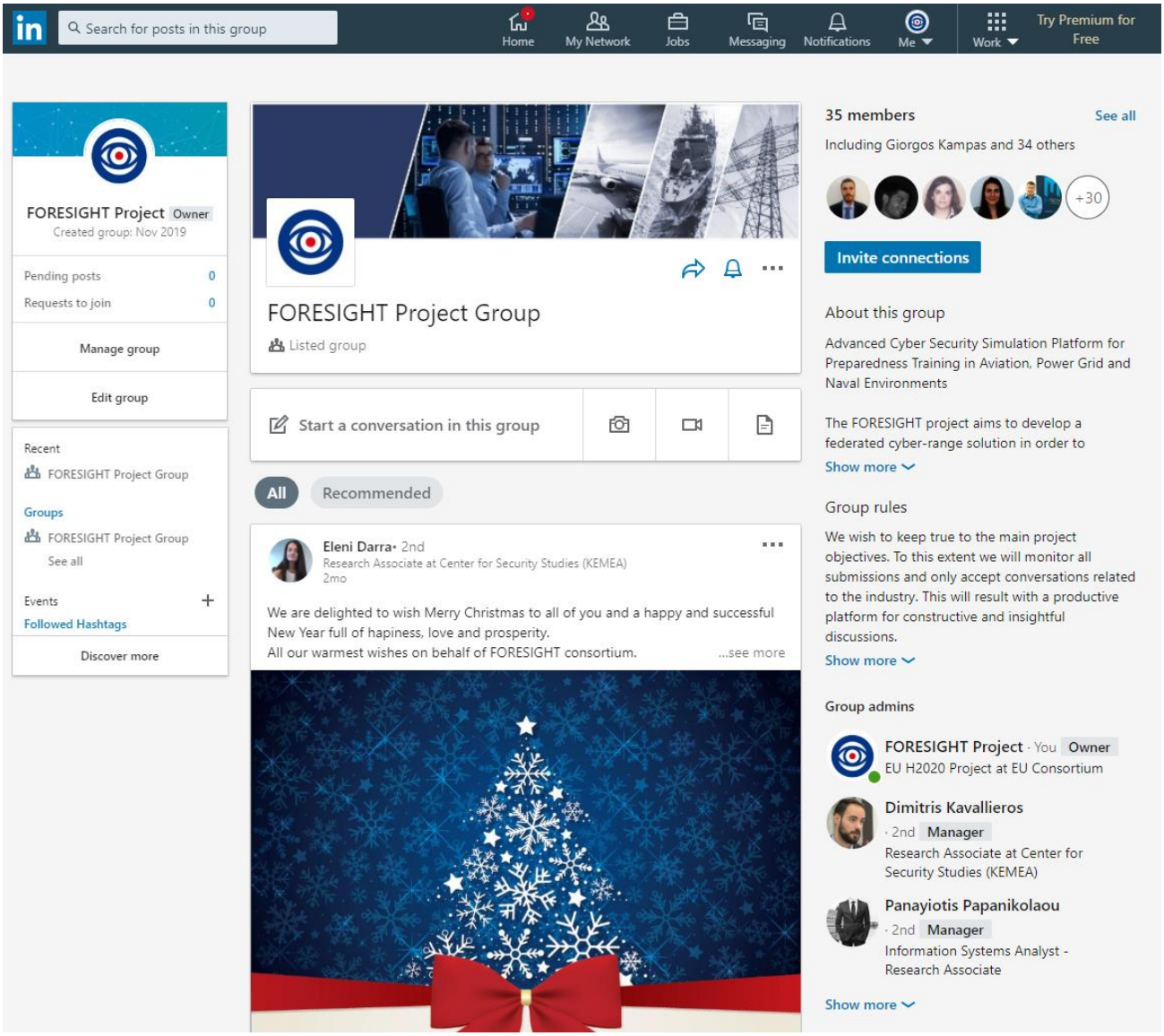

Figure 6. FORESIGHT LinkedIn Group Page

3.1.4 Newsletters

Newsletters (an example is shown in Figure 7) are another communication channel which aims at providing the project stakeholders and the general audience with information related to the project activities. Disseminating the project results using Newsletters will further raise the awareness of the audiences and in the same time will increase the communication impact. Newsletter will be made available both in printed and electronic form.

NEWSLETTER

FORESIGHT

Advanced Cyber Security Simulation Platform for Preparedness Training in Aviation, Power Grid and Naval Environments

Issue #1 - January 2020

FORESIGHT Project Kick off Meeting

KEMEA being the Coordinator of the Horizon 2020 Foresight Project, successfully organized between 1 – 2 October 2019, the project Kick off Meeting in Athens, Greece. The meeting was attended by 50 representatives of FORESIGHT Consortium. During the KoM the project partners discussed the planned work and decided about the near future actions taken within the framework of the project.

FORESIGHT is a research project funded by Horizon2020 EU's new research and innovation programme, with the aim to develop a federated cyber-range solution to enhance the preparedness of cybersecurity professionals at all levels and advance their skills towards preventing, detecting, reacting and mitigating sophisticated cyber-attacks.

The project with duration of 36 months (1 October 2019 – 30 September 2021) and a total budget of 7.3 Million Euros brings together leading European research/academic institutions, governmental organisations, industrial partners and legal partners.

The FORESIGHT project's scope is to deliver an ecosystem of networked realistic training and simulation platforms that collaboratively bring unique cybersecurity aspects from the aviation, smart grid and naval domains.

The proposed platform will extend the capabilities of existing cyber-ranges and will allow the creation of complex cross-domain/hybrid scenarios to be built jointly with the IoT domain. Emphasis is given on the design and implementation of realistic and dynamic scenarios that are based on identified and forecasted trends of cyberattacks and vulnerabilities extracted from cyber-threat intelligence gathered from the dark web; this will enable cybersecurity professionals to rapidly adapt to an evolving threat landscape.

The development of advanced risk analysis and econometric models will prove to be valuable in estimating the impact of cyber-risks, selecting the most appropriate and affordable security measures, and minimising the cost and time to recover from cyber-attacks. Innovative training curricula, guiding cyber-security professionals to implement and combine security measures using new technologies and established learning methodologies, will be created and employed for training needs; they will be linked to professional certification programs and be supported by learning platforms. Aside from the development of skills, the project aims at a holistic approach to cyber-threat management with the ultimate goal of cultivating a strong security culture. As such, the project puts considerable emphasis on research and development (i.e. research on cyber-threats, development of novel ideas, etc) as the key to increasing training dynamics and awareness methods for exceeding the rate of evolution of cyber-attackers.

Figure 7. FORESIGHT Newsletter

3.1.5 Press releases

Press releases and news briefings (see an example in Figure 8 provides the website visitor to the respective webpage where news briefings regarding FORESIGHT project activities along with the relevant photos are presented. There, the visitor will be able to find out more about the posted news and press releases in terms of disseminating the project achievements and communicating the project activities.

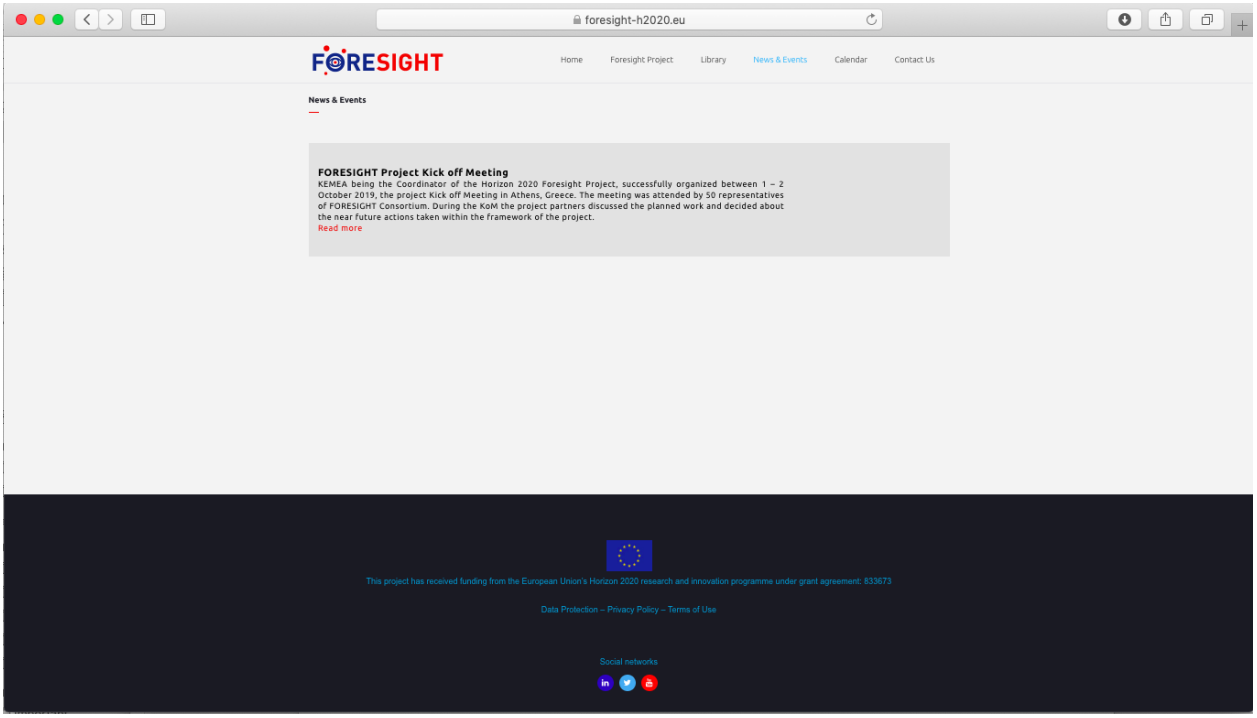

Figure 8. FORESIGHT news through its website

3.1.6 Leaflets and brochures

A first project leaflet (Figure 9) has been voted by all consortium partners and has been prepared for the project kick off meeting. It describes the project and its main features, timeline, contact information and expected outcomes to the general public in an easily understandable way. The flyers are intended for distribution, during aviation, energy and naval sector events, where FORESIGHT core partners are involved as organisers or co-organisers, as well as online and to communicate the project concept in a comprehensible manner.

Figure 9. FORESIGHT Leaflet: Front and Back side

3.2 Special innovation/lesson

Powering innovation is of high importance for FORESIGHT. A “Special innovation/lesson” action will start the second year of the project (M13) focusing on innovation capacity building. The aim of this action is to present the innovations coming out of FORESIGHT to a broader audience, to open up the ecosystem and include new actors from other areas except the three training thematic areas of FORESIGHT. This action will target stakeholders from industry, consulting, research, technology that can use the innovations from FORESIGHT.

The communication and dissemination channels of the project will be used to build up an external innovation community. In coordination with all WP leaders selected highlights and outcomes coming from FORESIGHT (beyond deliverables) will be presented and promoted on the website under a section especially designed for this purpose, and by selected dissemination channels, such as target audience related press distribution lists, blogs, local promotional events, social media etc. Furthermore, we will examine the possibility of liaison with other initiatives that nurture innovation, be it innovation forums hubs or clusters, incubators, or hackathon organizers. The Cyberwatching.eu Project Hub will be used to facilitate information transfer and communication with other projects and experts in the area of cyber-security. Furthermore, the "Technology Radar" methodology developed by Cyberwatching.eu will be used to establish FORESIGHT position among the European Cybersecurity research landscape.

Collaboration with other RTD projects in the same research area will be established as a mean to promote the innovation potential of FORESIGHT.

3.3 Code repository

To enable and ensure the replicability and traceability of the FORESIGHT results, it is essential that the project results are disseminated through scientific publications. The same applies for the software developed in the framework of the project that should be either carefully documented or if possible, openly shared and directly accessible to other interested parties. The rise of openly available software and source code is facilitated by several code repository services such as SourceForge, Bitbucket, GitLab, and GitHub, among others [2]. In the FORESIGHT project, the GitHub repository is a great option that can be used for hosting the source code, documentation, and project-related content. GitHub provides a dynamic and collaborative environment that supports peer review, commenting, and discussion among developers' teams and researchers. Some of this content can be made open to the public in order to attract visibility. An option is to use a private GitHub repository at first with access granted only to the project's developer's teams and at a later stage this repository or part of it can then be made public, for example, upon submission, acceptance, or publication of corresponding journal articles.

GitHub features that can boost visibility, include help pages, manuals, tutorials and content related to specific projects. Furthermore, GitHub enables developers to exchange ideas and issues, share aspects of their work and report bugs or get support through real-time communication platforms. Within a chat functionality, members can reference issues, comments, and pull requests. Another GitHub service is Gist [3], which represents a unique way to share code snippets, single files, parts of files, or full applications. Gists can be generated in two different ways: public gists that can be browsed and searched and secret gists that are hidden from search engines. One of the main features of Gist is the possibility of embedding code snippets in other applications, enabling users to embed gists in any text field that supports JavaScript [4].

It should be noted that the availability of a public repository containing the source code does not make the software open-source per se. An Open Source Initiative (OSI)-approved license (https://opensource.org/licenses/alphabetical) should be used that defines how the software can be freely used, modified, and shared.

Concluding, popular social coding sites like GitHub are changing software development and the dissemination possibilities of research projects. Users have the ability to follow some interesting developers, listen to their activities, find and follow new projects. In this way GitHub can be a useful tool to disseminate projects, attract stakeholders and increase the popularity of a project. A deep understanding of project dissemination on social coding sites can provide important insights into the project diffusion characteristics and into improvement of popularity [5]. In the same way researchers are following developments in their field through publications in scientific journals, scientific programmers can follow publicly available projects that might benefit their research. GitHub enables this functionality by allowing users to follow other GitHub users and monitor the activity and progress of projects, as it is the case in many social media platforms. This is envisaged for the FORESIGHT project.

3.4 Other channels

Promo videos, webcasts, podcasts, and presentations will be developed to present the FORESIGHT project to the general public in an easily understandable way. A YouTube channel will be created, where the Consortium will plan short series of white board videos/animations to explain the role and the goals of the FORESIGHT project in a focused and digestible way for all targeted stakeholder groups. Furthermore, presentations will be offered at local level (aiming at all target groups) during the project lifetime and towards the end of the project to present the project results to policy makers and potential investors. Research-active partners will create awareness of FORESIGHT at research level, presenting the project findings to the engineers and scientists of the future through lectures and seminars for undergraduate and postgraduate students and academics. Finally, the project will identify channels to promote its objectives, results and opportunities to promote inclusion of minority groups and gender equality. Special focus will be made in identifying and promoting opportunities for innovation and entrepreneurship that encourage uptake by groups that are under-represented in the cyber-security sector across Europe. The Consortium will use innovative platforms such as ProductHunt to promote business ideas in a way that encourages engagement. Special features promoting product opportunities, with a focus on equality and diversity will be produced each year, and the project team will identify speaker opportunities that support this objective.

4 Dissemination plan

This section outlines the activities and tools to present the project to the scientific community.

4.1 Deliverables

The dissemination, outreach and communication (DOC) plan is under WP12 and concerns T12.1; a dissemination report will be delivered on months 6 (D12.1) , 18 (D12.8), and 36 (D12.13) of the project, aka this document is the first deliverable of the FORESIGHT's planned outreach and communication activities, and two more deliverables will follow during the life-time of the project. Deliverable D12.1 is a detailed DOC plan that describes the related (first) activities, defines the target audience, presents the communication levels and the responsibilities attributed to each partner, and gives the indicators to measure the dissemination actions and the methods for monitoring and reporting these actions. Throughout the evolvement of the project, we will refine and undertake the dissemination activities based on the high-level dissemination plan (Section 2) and aligned with the project objectives (Section 6.1), in an effort to extend and improve our ways to reach the targeted groups effectively; the evolvement of the DOC plan will be reported in the next Deliverable D12.8 of T12.1. In the Deliverable D12.13, that comes in with the end of the project, the Consortium will highlight where, when, how and for whom the FORESIGHT project was presented, whether and in which ways the project outputs were demonstrated in dedicated events; these might include scientific conferences, developer workshops or symposia as well as large cybersecurity fairs and exhibitions.

4.2 Scientific publications

Since FORESIGHT has also a research dimension, the consortium plans the publication of the project's development and outputs in high-quality journals and conferences. The tables that follow (Table 4, Table 5, and Table 6) present an indicative list of journals and conferences that are relevant to the FORESIGHT research areas. Please notice that the following list is non-exhaustive and the submission of articles will be based on whether journals' or conferences' specific topics (or call for papers in special issues) match those of the particular work carried out in the context of FORESIGHT.

Table 4. Indicative list of scientific journals

ID	Title of Journal	Aim	Web-site	Acronym	Publisher
1	ACM Transactions on Information Systems	Information Systems (TOIS) is a scholarly journal that publishes previously unpublished high-quality scholarly articles in all areas of information retrieval	https://tois.acm.org/	TOIS	ACM
2	IEEE Transactions on Knowledge and	The scope includes the knowledge and data engineering aspects of computer science, artificial intelligence, electrical	https://ieeexplore.ieee.org/xpl/aboutJournal.jsp?punumber=69	TKDE	IEEE

ID	Title of Journal	Aim	Web-site	Acronym	Publisher
	Data Engineering	engineering, computer engineering, and other appropriate fields			
3	Large-Scale Data- and Knowledge-Centered Systems	The objective of the international journal on Large Scale Data and Knowledge Centered Systems is to provide an opportunity to disseminate original research contributions and a high-quality communication platform for researchers and practitioners	https://www.irit.fr/tldks/		Springer
4	The VLDB Journal	The VLDB Endowment journal contains scholarly contributions that examine information system architectures, the impact of technological advancements on information systems, and the development of novel database applications	https://link.springer.com/journal/778	VLDBJ	Springer
5	Information Processing and Management	Information Processing and Management is a leading international journal focusing on publishing peer-reviewed original research concerning theory, methods, or application in the field of information science	https://www.journals.elsevier.com/information-processing-and-management	IPM	Elsevier
6	ACM Transactions on Privacy and Security	Publishes high-quality research results in the fields of information and system security and privacy. Studies addressing all aspects of these fields are welcomed, ranging from technologies, to systems and applications, to the crafting of policies. Topics of interest include Security Technologies, Fundamentals, Secure Systems, Privacy Methods, Security and	https://dl.acm.org/citation.cfm?id=J789	ACM	TOPS

ID	Title of Journal	Aim	Web-site	Acronym	Publisher
		Privacy Applications, Privacy and Security Policies			
7	International Journal of Human-Computer Studies	Publishes original research over the whole spectrum of work relevant to the theory and practice of innovative interactive systems	https://www.journals.elsevier.com/international-journal-of-human-computer-studies	Elsevier	IJHCS
8	International Journal of Learning Technology	An international, refereed, scholarly journal providing an interdisciplinary forum for the presentation and discussion of important ideas, concepts, and exemplars that can deeply influence the role of learning technologies in learning and instruction. This unique and dynamic journal focuses on the epistemological thrust of learning vis-à-vis instruction and the technologies and tools that support the process. IJLT publishes papers related to theoretical foundations, design and implementation, and effectiveness and impact issues related to learning technologies	https://www.inderscience.com/jhome.php?jcode=ijlt	InderScience	IJLT
9	International Journal of Serious Games	The IJSG publishes original, peer-reviewed, scientific articles addressing theoretical, experimental and operational aspects in the areas related to design, development, engineering, deployment and assessment of digital Serious Games (SGs); IJSG aims at being a high-level reference point for a growing academic and industrial community, providing innovative research ideas and	http://journal.seriousgamessociety.org/index.php/IJSG	Open Journal	IJSG

ID	Title of Journal	Aim	Web-site	Acronym	Publisher
		application results, reporting on pressing challenges and leading-edge research			
10	IEEE Transactions on Visualization and Computer Graphics	Publishes papers on subjects related to computer graphics, information and scientific visualization, visual analytics, virtual and augmented reality, focusing on theory, algorithms, methodologies, human-computer interaction techniques, systems, software, hardware, and applications in these areas	https://www.computer.org/csdl/journal/tg	IEEE	TVCG
11	IEEE Transactions on Dependable and Secure Computing	The purpose of TDSC is to publish papers in dependability and security, including the joint consideration of these issues and their interplay with system performance	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8858	IEEE	TDSC
12	IEEE Transactions on Information Forensics and Security	The IEEE Transactions on Information Forensics and Security covers the sciences, technologies, and applications relating to information forensics, information security, biometrics, surveillance and systems applications that incorporate these features	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10206	IEEE	TIFS
13	IEEE Security & Privacy	IEEE Security & Privacy's primary objective is to stimulate and track advances in security, privacy, and dependability and present these advances in a form that can be useful to a broad cross-section of the professional community-ranging from academic	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8013	IEEE SECUR PRIV	IEEE

ID	Title of Journal	Aim	Web-site	Acronym	Publisher
		researchers to industry practitioners			
14	Computers & Security	Computers & Security is the most respected technical journal in the IT security field. With its high-profile editorial board and informative regular features and columns, the journal is essential reading for IT security professionals around the world	www.journals.elsevier.com/computers-and-security	COSE	Elsevier
15	IET Information Security	IET Information Security publishes original research papers in the following areas of information security and cryptography	https://digital-library.theiet.org/content/journals/iet-ifs	IET	IFS
16	International Journal of Information Security	The Journal offers prompt publication of high quality research on system security (intrusion detection, operating system security, database security), network security (Internet security, firewalls, mobile security, security protocols, anti-virus), foundations (privacy, access control, authentication, identification, applied cryptography, and formal security methods)	https://link.springer.com/journal/10207	Springer	IJIS
17	Network Security	Network Security is devoted to solving your network security issues in detail, now with even more news, information and solutions to your network security problems	www.journals.elsevier.com/network-security	Elsevier	

ID	Title of Journal	Aim	Web-site	Acronym	Publisher
18	Future Generation of Computer Systems	The journal aims to lead the way in advances in distributed systems, collaborative environments, high performance and high performance computing, Big Data on such infrastructures as grids, clouds and the Internet of Things (IoT)	https://www.journals.elsevier.com/future-generation-computer-systems	Elsevier	FGCS
19	Journal of Network and Computer Applications	The Journal of Network and Computer Applications welcomes research contributions, surveys and notes in all areas relating to computer networks and applications thereof; among others, the paper topics include applications of security in computer and networks	https://www.journals.elsevier.com/journal-of-network-and-computer-applications	Elsevier	JNCA
20	IEEE Access	The scope of this journal comprises all of IEEE's fields of interest, emphasizing applications-oriented and interdisciplinary articles	https://ieeeaccess.ieee.org/	IEEE ACCESS	IEEE
21	ACM Computing Surveys	These comprehensive, readable surveys and tutorial papers give guided tours through the literature and explain topics to those who seek to learn the basics of areas outside their specialties in an accessible way. The carefully planned and presented introductions in Computing Surveys (CSUR) are also an excellent way for researchers and professionals to develop perspectives on, and identify trends in complex technologies	https://dl.acm.org/journal/csur	ACM COMPUT SURV	ACM

ID	Title of Journal	Aim	Web-site	Acronym	Publisher
22	IEEE Communications Surveys & Tutorials	IEEE Communications Surveys and Tutorials focuses on integrating and adding understanding to the existing literature on communications, putting results in context. Whether searching for in-depth information about a familiar area or an introduction into a new area, IEEE Communications Surveys & Tutorials aims to be the premier source of peer-reviewed, comprehensive tutorials and surveys, and pointers to further sources	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=9739	IEEE COMMUN SURV TUT	IEEE
23	Journal of Information Security and Applications	Provides a common linkage between a vibrant scientific and research community and industry professionals by offering a clear view on modern problems and challenges in information security, as well as identifying promising scientific and "best-practice" solutions. JISA issues offer a balance between original research work and innovative industrial approaches by internationally renowned information security experts and researchers	https://www.journals.elsevier.com/journal-of-information-security-and-applications	JISA	Elsevier

Table 5. Indicative list of scientific conferences

ID	Title of Conference	Aim	Website	Acronym	Frequency
1	ACM International Conference on Web Search and Data Mining	WSDM publishes original, high-quality papers related to search and data mining on the Web and the Social Web, with an emphasis on practical yet principled novel models of	http://www.wsdm-conference.org/2020/	WSDM	Annual

ID	Title of Conference	Aim	Website	Acronym	Frequency
		search and data mining, algorithm design and analysis, economic implications, and in-depth experimental analysis of accuracy and performance			
2	ACM International Conference on Management of Data	The annual ACM SIGMOD conference is a leading international forum for database researchers, practitioners, developers, and users to explore cutting-edge ideas and results, and to exchange techniques, tools, and experiences. We invite the submission of original research contributions relating to all aspects of data management defined broadly, and particularly encourage submissions on topics of emerging interest in the research and development communities	http://sigmod2019.org/sigmodcfp	SIGMOD	Annual
3	Conference on Innovative Data Systems Research	CIDR encourages papers about innovative and risky data management system architecture ideas, systems-building experience and insight, resourceful experimental studies, and provocative position statements. Papers are encouraged to present novel approaches to data systems architecture and usage, to inspire discussions on the latest innovative and visionary ideas in the field	http://cidrdb.org/cidr2020/	CIDR	Biennial

ID	Title of Conference	Aim	Website	Acronym	Frequency
4	ACM Conference on Research and Development in Information Retrieval	SIGIR is the premier international forum for the presentation of new research results and for the demonstration of new systems and techniques in information retrieval	http://sigir.org	SIGIR	Annual
5	IEEE International Conference on Data Mining	ICDM has established itself as the world's premier research conference in data mining. It provides an international forum for presentation of original research results, as well as exchange and dissemination of innovative, practical development experiences; the conference covers all aspects of data mining, including algorithms, software and systems, and applications. In addition, ICDM draws researchers and application developers from a wide range of data mining related areas such as statistics, machine learning, pattern recognition, databases and data warehousing, data visualization, knowledge-based systems, and high performance computing	http://icdm.bigke.org	ICDM	Annual
6	International Conference on Data Science, Technology and Applications	The purpose of the International Conference on Data Science, Technology and Applications (DATA) is to bring together researchers, engineers and practitioners interested on databases, big data, data mining, data management, data security and other aspects of information systems and	http://www.dataconference.org	DATA	Annual

ID	Title of Conference	Aim	Website	Acronym	Frequency
		technology involving advanced applications of data			
7	European Conference on Research in Computer Security	The aim of ESORICS is to further the progress of research in computer security by establishing a European forum for bringing together researchers in this area, by promoting the exchange of ideas with system developers and by encouraging links with researchers in related areas	http://conf.laas.fr/esorics/	ESORICS	Annual
8	ACM Conference on Computer and Communications Security	The ACM Conference on Computer and Communications Security (CCS) is the flagship annual conference of the Special Interest Group on Security, Audit and Control (SIGSAC) of the Association for Computing Machinery (ACM). The conference brings together information security researchers, practitioners, developers, and users from all over the world to explore cutting-edge ideas and results	http://www.sigsac.org	CCS	Annual
9	Games and Learning Alliance	The Games and Learning Alliance conference is an international conference dedicated to the science and application of serious games. The conference aims at bringing together researchers, developers, practitioners and stakeholders; the goal is to	https://conf.seriousgamessociety.org	GALA	Annual

ID	Title of Conference	Aim	Website	Acronym	Frequency
		share the state of the art of research, analysing the most significant trends and discussing visions on the future of serious games. The conference also includes an exhibition, where developers can showcase their latest products			
10	International Conference in Information Visualization	The IV conference includes a wide variety of topics in the areas of information visualisation including theory & practice, evaluation, applications, visualization and storytelling, visual analytics & data science, social media analytics, and others	http://www.wikicfp.com/cfp/program?id=1803	IV	Annual
11	ACM Dependable, Adaptive, and Trustworthy Distributed Systems	The Symposium on Applied Computing has been a primary gathering forum for applied computer scientists, computer engineers, software engineers, and application developers from around the world. SAC 2020 is sponsored by the ACM Special Interest Group on Applied Computing and the SRC Program is sponsored by Microsoft Research	http://www.dedisys.org/sac20/	DADS/SAC	Annual
12	USENIX Security Symposium	USENIX Security brings together researchers, practitioners, system administrators, system programmers, and others to share and explore the latest advances in the security and privacy of computer systems and networks	https://www.usenix.org/conference/usenixsecurity20	USENIX	Annual

ID	Title of Conference	Aim	Website	Acronym	Frequency
13	IEEE Symposium on Security and Privacy	IEEE SP has been the premier forum for presenting developments in computer security and electronic privacy, and for bringing together researchers and practitioners in the field	https://www.ieee-security.org/TC/SP2020/	SP	Annual
14	IEEE European Symposium on Security and Privacy	IEEE SP has been the premier forum for presenting developments in computer security and electronic privacy, and for bringing together researchers and practitioners in the field	https://www.ieee-security.org/TC/EuroSP2020/	EuroSP	Annual
15	ACM Asia Conference on Computer and Communications Security	Presentation of novel research from academia, government, and industry on all theoretical and practical aspects of computer and network security	https://asiaccs2020.cs.nthu.edu.tw	AsiaCCS	Annual
16	ARES: International Conference on Availability, Reliability and Security	ARES aims at a full and detailed discussion of the research issues of security as an integrative concept that covers amongst others availability, safety, confidentiality, integrity, maintainability and security in the different fields of applications.	https://www.ares-conference.eu	ARES	Annual
17	R3: Resilience, Response & Recovery Summit	R3 is the leading Summit focusing on how you grow your organisation's resilience to cyber-attack, and best-practice in crisis management and incident response to ensure a full recovery	https://www.teiss.co.uk/r3/	R3	Annual
18	European Interdisciplinary Cybersecurity Conference	The conference is devoted to exploring and presenting original innovative applications, scientific and	https://www.fvv.um.si/eicc2020/	EICC	Annual

ID	Title of Conference	Aim	Website	Acronym	Frequency
		technological advancements in the field of cybersecurity			
19	IEEE Symposium on Visualization for Cyber Security	VizSec is a forum that brings together researchers and practitioners from academia, government, and industry to address the needs of the cyber security community through new and insightful visualization and analysis techniques; VizSec provides an excellent venue for fostering greater exchange and new collaborations on a broad range of security- and privacy-related topics	https://vizsec.org/	VizSec	Annual
20	Graphical Models for Security	The GraMSec workshop seeks submissions from academia, industry, and government presenting novel research on all theoretical and practical aspects of graphical models for security	https://www.gramsec.uni.lu/	GraMSec	Annual
21	International Conference on Next Generation Wired/Wireless Advanced Networks and Systems	The conference goal is in the identification, investigation and integration of new algorithms, approaches, architectures, methods and mechanisms to enable proper and efficient operation of a next-generation IP-based wireless network; therefore, wireless networks and their interaction with wired networks shall be widely examined and addressed throughout the conference. The proceedings will be published in LNCS, Springer	http://www.new2an.org	NEW2AN	Annual

ID	Title of Conference	Aim	Website	Acronym	Frequency
		(confirmed) and indexed by relevant databases			
22	Conference on Internet of Things and Smart Spaces ruSMART 2020	The wireless solutions have moved beyond their traditional areas of application and today we can talk about a space where users can access a number of wireless technologies and interact with various services; also, the Internet of Things disrupts limitations of Internet that use based on human-entered data. New technologies for short-range and low-power wireless communications, real-time localization and sensor networks allow computers to perceive the world. Support of the future commercial success of IoT solutions require efficient and scalable infrastructures for managing, sharing and processing collected data. We can see that research on interlinking of the physical and cyber worlds is becoming more and more relevant. This conference is targeted to bring together top specialist in the field to discuss ongoing studies and obtained results.	https://rusmart.e-werest.org/2020.html	ruSMART	Annual

ID	Title of Conference	Aim	Website	Acronym	Frequency
23	IEEE World Congress on Services	Covers all aspects of services computing and applications, current or emerging; SERVICES 2020 event topics include various systems and networking research pertaining to cloud, edge and Internet-of-Things (IoT), as well as technologies for intelligent computing, learning, big data and blockchain applications, while addressing critical issues such as high performance, security, privacy, dependability, trustworthiness, and cost-effectiveness	https://conferences.computer.org/services/2020/	IEEE Services	Annual
24	IEEE Conference on Network Softwarization	Software-Defined Networking (SDN), Network Function Virtualization (NFV) and Cloud-Edge-Fog Computing are driving an unprecedented techno-economic shift in the Telecom and ICT industries. Network softwarization and programmability promise to reduce operational costs, provide better flexibility and bring new service paradigms. In particular, they are enabling the deployment of 5G infrastructures, spanning from high data rate fixed-mobile services to the Internet of Things, which is expected to accelerate the digital transformation that all the industry is witnessing. As a result, new service models and new value chains will emerge, leading to novel business	https://netsoft2020.ieee-netsoft.org/	IEEE Netsoft	Annual

ID	Title of Conference	Aim	Website	Acronym	Frequency
		models and significant socio-economic impact.			
25	IFIP International Conference on New Technologies, Mobility and Security	Aims at fostering advances in the areas of New Technologies, Wireless Networks, Mobile Computing, Ad hoc and Ambient Networks, QoS, Network Security and E-commerce, to mention a few, and provides a dynamic forum for researchers, students and professionals to present their state-of-the-art research and development in these interesting areas	http://www.ntms-conf.org/ntms2020/	NTMS	Annual
26	IEEE International conference on cyber security and resilience	The conference focuses on both the theoretical & practical aspects of the security, privacy, trust and resilience of networks, devices, applications, and services as well as novel ways of dealing with their vulnerabilities and mitigating sophisticated cyber-attacks (to share results/promote work carried out in the project/train professionals)	https://www.ieee-csr.org/	CSR	Annual

Table 6. Indicative list of workshops

ID	Title of Conference	Aim	Website	Acronym	Frequency
1	2020 IEEE SERVICES Workshop on Cyber-Security and Resilience in the Internet of Things	The workshop focuses on both the theoretical & practical aspects of the security, privacy, trust and resilience of IoT networks, devices, applications, and services as well as novel ways of dealing with their vulnerabilities and mitigating	https://conferences.computer.org/services/2020/workshops/csriot2020.html	CSRIOT	Annual

ID	Title of Conference	Aim	Website	Acronym	Frequency
		sophisticated cyber-attacks (to share results/promote work carried out in the project/train professionals).			
2	2020 International Workshop on Cyber-Security Threats, Trust and Privacy management in Software-defined and Virtualized Infrastructures	Aim to gather together novel approaches for providing organizations the appropriate situational awareness in relation to cyber security threats allowing them to quickly detect and effectively respond to sophisticated cyber-attacks (to share results/promote work carried out in the project/train professionals).	https://cyber-trust.eu/secsoft-2020/	SECSOFT	Annual

4.3 Conferences, workshops and other events

The FORESIGHT consortium will be proactive in putting forward proposals for themed workshops and symposia addressing priorities of H2020 programme and bringing together key industrial sectors represented within the targeted value chains and public sector to present FORESIGHT, look at integration opportunities and best practice examples, and allow communication of FORESIGHT outputs to a wide audience. Additionally, in Tasks 12.2 and 12.4 stakeholders will be invited at workshops organised by FORESIGHT to learn about the outcomes of the project, explore synergies and cooperation possibilities. All partners will be involved in the aforementioned activities in order workshops to be organised. To this end, the FORESIGHT Consortium plans the organisation of a number of special sessions (an indicative list of events is presented in Table 7).

Table 7. Indicative list of events organised by FORESIGHT

ID	Event type	Aim	Outreach impact	Partners leading the effort
1	2019 Mediterranean Security Event	Strengthen the interaction among actors of security innovation and provide a venue for discussing challenges and demonstrating capabilities and solutions to address emerging security threats	The conference addressed a wide audience of 200+ cyber-security stakeholders including academics, research engineers from industry and academia, and security professionals	KEMEA
2	2020 International Workshop on Cyber-Security Threats, Trust and Privacy management in Software-defined and Virtualized Infrastructures (SECSOFT)	Aims to gather together novel approaches for providing organisations the appropriate situational awareness in relation to cyber security threats allowing them to quickly detect and effectively respond to sophisticated cyber-attacks (to share results/promote work carried out in the project/train professionals)	The workshop is co-located with IEEE NetSoft 2020 and addresses a wider audience of 100+ cyber-security stakeholders	UOPHEC, UOP
3	2020 IEEE SERVICES Workshop on Cyber-Security and Resilience in the Internet of Things (CSRIoT)	Focus on both the theoretical and practical aspects of the security, privacy, trust and resilience of IoT networks, devices, applications, and services as well as novel ways of dealing with their vulnerabilities and mitigating sophisticated cyber-attacks	The workshop is conducted under the umbrella of the IEEE World Congress on Services; it will address an audience of 30+ cyber-security stakeholders including academics, research engineers from industry and academia, (PhD) students, and security professionals	UOP, UOPHEC

ID	Event type	Aim	Outreach impact	Partners leading the effort
4	2020 International Workshop on Electrical Power and Energy Systems Safety, Security and Resilience (EPESec)	Focus on next-generation smart power and energy ecosystem that promises self-healing, resilience, sustainability and efficiency to the critical energy infrastructure	The workshop is conducted under the umbrella of the 15th International Conference on Availability, Reliability and Security (ARES); it will address an audience of 30+ cyber-security stakeholders including academics, research engineers from industry and academia, (PhD) students, and security professionals	INCITES, UOP, KEMEA
5	2021 IEEE International Conference on Cyber-Security and Resilience (IEEE CSR)	Focus on theoretical and practical aspects of the security, privacy, trust and resilience of networks and devices with applications in complex cyber-physical systems (CCPS) and use of contemporary techniques for thwarting sophisticated multi-step cyber-attacks	The conference is expected to address a wide audience of 100+ cyber-security stakeholders including academics, research engineers from industry and academia, (PhD) students, and security professionals	UOP, UOPHEC
6	IEEE Cyber Situational Awareness	International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA 2019), is an international refereed conference dedicated to the advancement of the principles, methods and applications of situation awareness on Cyber Systems, Business Information Systems (BIS), Computer Network Defence (CND), Critical National Infrastructures (CNI), Cyber Physical Systems (CPS) and Internet of Things (IoTs)	The conference is expected to address a wide audience of 200+ cyber-security stakeholders including academics, research engineers from industry and academia, (PhD) students, and security professionals	USTRAT

ID	Event type	Aim	Outreach impact	Partners leading the effort
7	IEEE Cyber Security	IEEE is the Technical Co-Sponsor (TCS) of the International Conference on Cyber Security and Protection of Digital Services (Cyber Security 2019), an international refereed conference dedicated to the advancement of Cyber Security, information security, network security, application security and business transformation of digital services, and the protection of public digital services, especially high value bearing online services	The conference is expected to address a wide audience of 200+ cyber-security stakeholders including academics, research engineers from industry and academia, (PhD) students, and security professionals	USTRAT
8	IEEE Cyber Incident	EE is the Technical Co-Sponsor (TCS) of the International Conference on Cyber Incident Response, Coordination, Containment & Control (Cyber Incident 2019) is an international refereed conference dedicated to the advancement of Cyber Incident Response, Coordination, Containment and Control	The conference is expected to address a wide audience of 200+ cyber-security stakeholders including academics, research engineers from industry and academia, (PhD) students, and security professionals	USTRAT

4.3.1 Technical factsheets

Each of the three pilots planned in FORESIGHT (i.e., aviation, naval, and power grid) will develop factsheets with information about successful application and implementation of the project solutions. The factsheets, provided in English and in native language of the demonstration host country, will be updated every six months and will be used to demonstrate the project's progress and to promote the technological benefits of the FORESIGHT platform to the interested/involved stakeholders. Technical factsheets will be available on the project's website and will also be promoted through the social media, online trade news sites, and relevant information portals.

4.3.2 Aviation pilot

Airports are equipped with traditional as well as more specialised IT systems, which consist of databases, BPM solutions (Business Process Management), ERP solutions (Enterprise Resource

Planning), building monitoring systems, access control systems and fire detection systems. Some of these systems are used to manage airport operations, whereas some other are used to monitor activities in the Free-Trade Zone (FTZ). ACS will develop an Airport's digital twin on the FORESIGHT cyber range platform by mapping the network and the systems of Airports' critical IT services and will perform penetration tests to determine an impact and vulnerability assessment of existing architecture and determine required enhancements. Indicative scenarios that will be tested are the following:

- Detection and prevention of cyber-attacks
- Network operations and management
- Cyber-attack countermeasures
- Cyber protection policies, procedures, skills and methodologies
- Automation of cyber-attack responses

The aviation range is focused on performing a gap analysis of the current versus the proposed cyber security architecture, assessing the impact propagation of cyber-attacks and performing a risk assessment of current architecture, performing cyber-attack scenarios with no operational risks, gaining experience and insight on detecting and mitigating cyber-attacks, experimenting with automated cyber-attack responses and impact on Airport's critical IT services operations, training of cyber-attack response teams to detect and mitigate a cyber-attack, deciding on most appropriate monitoring methods and building an automated notification and alerting procedure, and eventually, performing and assessing alternative information security architectures for the Airport to decide on most efficient and effective ones, creating this way a roadmap for implementation.

4.3.3 Naval pilot

The French Naval Academy is building a realistic Naval Cyber Range simulating a ship within different contexts. This Cyber Range reproduces all the main functions of a ship with the four main systems found on a merchant ship of medium size:

- Ship Management System / Power management system:

  On a merchant ship, the power management system provides the high voltage power generation on board, according to the requirements in voltage and intensity. Whatever the sources are (turbine, generating sets, batteries…), the energy is converted and distributed through switchboards. The system also transforms high voltage to low voltage and provides required lighting on board.

- Ship Management System / Utilities management system

  On a merchant ship, the utilities management system manages the fuel, pneumatic and hydraulic distribution onboard. It also controls drinkable water production, greywater and blackwater treatment as well as food refrigeration.

- Ship Management System / Utilities management system

  On a merchant ship, the utilities management system manages the fuel, pneumatic and hydraulic distribution onboard. It also controls drinkable water production, greywater and blackwater treatment as well as food refrigeration.

- Ship Management System / Safety management system

On a merchant ship, the safety management system handles the detection and fight against fire and floods, the opening and closing of valves, doors and watertight doors, ventilation and cool water production.

The network architecture of the naval cyber range is similar to the one found on real ships. Some points considering the network topology could be modified to improve to improve cyber resiliency but the aim of the cyber range is to be the more realistic possible and even reproducing vulnerabilities.

4.3.4 Power-grid pilot

CybExer Technologies, in cooperation with energy sector partners of the project, will build the power grid module for the FORESIGHT federated platform. The power grid range is focused on providing training to power grid operators and security practitioners from different grid operators, raising the security awareness of the power grid operators, optimising cybersecurity tactics of power grid defenders and enabling advanced training to develop defense skills against attacks on office and power grid components. To enhance learning experience and assessment, CybExer will employ its Dynamic e-Learning and Risk Assessment Platform which provides a structured way of learning, testing and developing a holistic view of trainees' skill levels. The development of the power grid module is spread over more than two years consisting of infrastructure modelling and simulation and development of training use cases.

4.4 Seminars, lectures and technical presentations

The FORESIGHT partners' dissemination strategy is to exploit all possible opportunities to maximise the impact of dissemination. This, among others, includes the organisation of seminars, lectures and technical presentations; during the FORESIGHT project, at least 4 workshops and 4 regional promotional events will be organised.

For the workshops, the action leaders will be UOP and KEMEA, also with all academic partners. Action partners will be ALL partners that can support this action by providing the respective inputs (slides, contribution material, etc.). The success of the seminars will be based on the number of participants attending.

The lectures will take place at the premises of the universities and research centres of FORESIGHT partners that will lead these actions and they will demonstrate the current research and innovations of the FORESIGHT project as well as teach participants about the novel technologies that are used in FORESIGHT. These will be split throughout the duration of the project. The success of the lectures will be based on the number of participants attending.

Finally, the technical presentations will take place at the premises of the FORESIGHT partners that will organise these presentations as well as at other events where FORESIGHT partners are invited (for more details, please look at the tentative plan of the activities to be undertaken as part of the project's communication strategy in **Error! Reference source not found.**). During the presentations, technical details, novel aspects and innovations will be presented to all interested parties. The success of the presentations will be based on the number of participants attending.

4.5 Project synergies and other targeted initiatives

FORESIGHT will identify European projects related to cyber security, cyber ranges, simulations and preparedness training (please find an indicative list in Table 8. For clustering with other project and stakeholders, the reference point of communication will be the project website and the social media channels, which will drive the clustering activities. This will allow finding synergies with other sister projects to establish cluster participation in events and publications, as well as to multiply the dissemination potential of the public website and social media by sharing news and links. These synergies are empowered by the commitment of the partners to disseminate FORESIGHT in other H2020 projects.

Research on similar and relevant projects which have been funded under H2020 program leads to a preliminary list of projects FORESIGHT can potentially start a collaboration with.

Table 8. Related European projects

Project Acronym	Project name	Website	Short Description	Coordinator
SPIDER	A cyberSecurity Platform for vIrtualiseD 5G cybEr Range services	Link	The SPIDER cyber-range virtual environment will be used to help train information security professionals to deal with real-world incidents, test new security technologies, and support companies in making optimal cybersecurity investment decisions.	ERICSSON TELECOMUNICAZIONI SPA
Cyber-MAR	Cyber preparedness actions for a holistic approach and awareness raising in the MARitime logistics supply chain	Link	Cyber-MAR platform is not only a knowledge-based platform but more importantly a decision support tool to cybersecurity measures, by deploying novel risk analysis and econometric models.	INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS
CYBERWISER.EU	Civil Cyber Range Platform for a novel approach to cybersecurity threats simulation and professional training	Link	CYBERWISER.EU will be an educational, collaborative, real-time civil cyber range platform where cybersecurity competitions will take place, making it the EU's reference, authoritative, independent cybersecurity platform for professional training.	ATOS SPAIN SA
EnergyShield	Integrated Cybersecurity Solution for the Vulnerability	Link	The EnergyShield toolkit will combine the latest technologies for vulnerability assessment (automated threat modelling and	SIVECO ROMANIA SA

Project Acronym	Project name	Website	Short Description	Coordinator
	Assessment, Monitoring and Protection of Critical Energy Infrastructures		security behaviour analysis), monitoring & protection (anomaly detection and DDoS mitigation) and learning & sharing (security information and event management).	
SOTER	cyberSecurity Optimization and Training for Enhanced Resilience in finance	Link	SOTER project will create tools to tackle future cyberattacks and vulnerabilities. These tools will improve the interconnections between different service providers and users and help identify the level of cybersecurity that exists.	EVERIS SPAIN SL
PHOENIX	Electrical Power System's Shield against complex incidents and extensive cyber and privacy attacks	Link	PHOENIX aims to offer a cyber-shield armour to European EPES infrastructure enabling cooperative detection of large scale, cyber-human security and privacy incidents and attacks, guarantee the continuity of operations and minimize cascading effects in the infrastructure itself, the environment, the citizens and the end-users at reasonable cost.	CAPGEMINI TECHNOLOGY SERVICES
SDN-microSENSE	SDN - microgrid reSilient Electrical eNergy SystEm	Link	SDN-microSENSE project intends to provide a set of secure, privacy-enabled and resilient to cyberattacks tools, thus ensuring the normal operation of EPES as well as the integrity and the confidentiality of communications.	AYESA ADVANCED TECHNOLOGIES SA
THREAT-ARREST	Cyber Security Threats and Threat Actors Training - Assurance Driven Multi-Layer, end-to-end Simulation and Training	Link	THREAT-ARREST will develop an advanced training platform incorporating emulation, simulation, serious gaming and visualization capabilities to adequately prepare stakeholders with different types of responsibility and levels of expertise in defending high-risk	IDRYMA TECHNOLOGIAS KAI EREVNAS

Project Acronym	Project name	Website	Short Description	Coordinator
			cyber systems and organisations to counter advanced, known and new cyber-attacks.	

4.6 Standardisation activities

An important part of FORESIGHT is to make a wider contribution to the cybersecurity landscape, beyond the platform, and deliver roadmap that aims to establish a wider set of certifications and standards. Such standardization activities will involve engaging with organisations and events relevant to establishing standards for cyber-resilience across Europe. This may involve contacting and working with organisations such as ENISA and CEN-CENELEC as well as current providers specific to the aviation, naval and power grid domains. FORESIGHT will specifically monitor, engage and incorporate cyber security standards from across the critical infrastructure domains and sectors and seek input and feedback on the roadmap throughout its development.

4.7 Project boards

The communication and dissemination of FORESIGHT objectives, achievements and results throughout the duration of the project, is important for the project's success and impact creation. For effective communication and dissemination, it is imperative to promote the project outcomes promptly to the right audiences while it is essential to recognize the different communication tools and activities that are appropriate in different project lifecycle phases. Towards this direction, the Innovation, Dissemination & Exploitation Board (IDEB) and the External Advisory Board (EAB) of the project can provide useful guidance and input for the communication and dissemination materials and activities.

More specifically, the IDEB in collaboration with the Steering Committee will be responsible and will deal with all matters related to the dissemination and communication of the project results, the management of the knowledge acquired in the course of the project, the innovation aspects and the quality of provided services. The IDEB will be also responsible to:

- identify new opportunities for the participation of FORESIGHT in events, workshops and conferences,
- identify new media channels,
- explore possible publication opportunities in scientific journals and online means,
- maintain the project's visual identity,
- pursue synergies with other related projects and initiatives,
- update frequently the project's social media and website,
- keep the target audiences engaged through frequent newsletters and press releases,
- identify the types of stakeholders to be targeted and their impact with regards to the project aims and objectives,
- formulate, monitor and update the outreach and communication plan

Based on the above, the main role of the IDEB is to promote engagement through communication, consultation and collaboration. Moreover, the IDEB in collaboration with the Security Advisory Board (SAB) will safeguard that the dissemination material can be disclosed and that it does not contain any

confidential information that would compromise: (i) the commercial interests of involved partners and (ii) insights related to critical infrastructures.

On the other hand, the EAB consists of industrial and scientific experts who, although, not directly involved with the technical activities of the project, have significant technical expertise and business activities in the subjects related to the project. Consequently, EAB members will be invited to review project results, dissemination and communication material, propose ideas to further enhance the visibility of the project and provide feedback to ensure that the project results address business problems related to the scope of the project. In addition, these experts will directly support the project implementation by giving feedback or providing their expertise while participating in different activities, including workshops, meetings and pilot activities. More specifically, the EAB members will:

- consult and provide valuable feedback on consortium activities related to communication, dissemination and exploitation,
- participate in project workshops and conferences to directly discuss the progress and influence the implementation of work packages, work and tasks,
- collaborate with FORESIGHT consortium and relevant stakeholders (industry, practitioners, policy makers etc.) in order promote the project's results in the most efficient way

The engagement plan envisages a two-way activities roadmap between the EAB and the IDEB in order to maintain and encourage engagement throughout the duration of the project and after its closure for accurate and effective dissemination of the project's results.

5 Individual partner plans

This section presents in detail the individual partners' communications plans; each plan is in-line with the related partner's expertise, capability, and commitment to the project. M&S, being the leader of WP12, overseas all communication activities; the focus and the expertise of the M&S organisation provides the Consortium members with the reassurance that communications will benefit the Consortium project as a whole and that the individual plans will be treated in respect.

5.1 KEMEA

KEMEA is highly involved in Horizon 2020 European research projects in the security sector. KEMEA is a member of a number of European associations and organisations including the "European Security Research and Innovation Forum (ESRIF)", the European Cyber Security Organisation (ECSO), the "European Organisation for Security (EOS)", the "Public Safety Communication Europe Forum (PSCE)", the "European Association of Research and Technology Organisations (EARTO)", "the European Emergency Number Association (EENA)", the European Association for Biometrics (EuAB) and has established links to the ENLETS community (European Network of Law Enforcement Technology Services). KEMEA also closely cooperates with the RAN Centre of Excellence and since 2016, it is a Framework Partner of CEPOL.

Addressing to a vast pool of policy makers KEMEA will raise awareness to FORESIGHT stakeholders with a targeted campaign raising high in the agendas the objectives of FORESIGHT project. The latter will be realized through the communication of the project identity and the dissemination of the project results to international fora.

Following, through the participation of KEMEA to international conferences, FORESIGHT will increase its communication and dissemination impact to its interested parties as well as to the general audiences.

Being the Think Tank of the Hellenic Ministry of Citizen Protection, which is the supervising ministry of the Hellenic Police, KEMEA is in direct communication with ranking officers and the Hellenic Police scientific personnel. In this way, through targeted campaign, FORESIGHT objectives and results will be disseminated accordingly.

KEMEA has great experience in organizing large-scale Conferences such as the "Border Surveillance and Search and Rescue Technologies" (2014), "Next Generation Community Policing" (2017), "Mediterranean Security Research Event" (2019) attracting the interest of hundreds of participants and most of all of the Policy Makers in EU level.

KEMEA showcase a constant presence in major EU conferences, exhibitions and workshops in which FORESIGHT project will found a fertile ground for its proper promotion.

5.2 ED

ED is very active in the provision of IT and commercial solutions in the private and public sector offering –among others– services for the professional community of Governments services and Security, thus participating in related events, conferences, fairs, and workshops. ED will disseminate the project results through its channels/ networks with its extensive expertise in disseminating project results.

FORESIGHT, through these channels, will be presented to both commercial as well as research stakeholders thus creating a more "adapted awareness" regarding the functionalities and technologies the solution offers. ED plans to participate in conferences, exhibitions, events and workshops relevant to FORESIGHT and 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, and the project as a whole. Furthermore, ED plans to pursue connections with other relevant projects to identify and set up any potential synergy with the aim to increase impact. For example, ED is participating in the H2020 research project SPEAR (https://www.spear2020.eu/) also in the topic of Cyber Security. Dissemination to related Business Interest Groups namely ICT applications suppliers and Industrial Community (Technological domain) will be produced by means of the following demonstrating that FORESIGHT can easily be the basis for many other applications for other target groups and even other application domains.

5.3 CERTH

CERTH aims to disseminate the results of the project through (i) publishing the outcomes of its research activities within FORESIGHT to top cybersecurity scientific journals and conferences, (ii) participating in and organising related events, conferences, fairs, and workshops, and (iii) participating in demonstrations and talks at symposiums aimed at the cyber security industry. Furthermore, CERTH will contribute to the overall dissemination of the project's aims, vision, and results to the aforementioned venues. Finally, through its participation to the ECHO (European network of Cybersecurity centers and competence Hub for innovation and Operations) project, CERTH will do its utmost to raise awareness of the FORESIGHT project and disseminate its results to the ECHO network.

5.4 CRI

CRI, though it's associated experts, is involved in various high-level forums. CRI experts for example serve as scientific advisors to international organisations and Europol, they are chairmen of working groups on UN level, are involved in the work of international organisations such as the UN and ITU and various academic forums. In addition, CRI experts are frequently publishing scientific articles and contribute to publications. Furthermore, CRI publishes a book series. CRI will leverage on its unique experience and position to disseminate projects results. This includes:

- Presenting the FORESIGHT project and non-classified research results at international conference and workshops targeting the government community, critical infrastructure provider, international organisations and academia
- Establishing synergies to other related projects and initiatives CRI is involved in
- Publishing non-classified results in scientific publications
- Including non-classified results in the advisory work carried out for international organisations

5.5 INCITES

INCITES will contribute to dissemination activities of FORESIGHT achievements through participation in workshops and conferences such as the CTTE conference. In addition, INCITES will actively contribute in the creation of scientific papers and publications in international Journals and Magazines. INCITES will announce the main results of the project through the corporate website as well as its accounts on social media (Facebook, Twitter and LinkedIn). It will also use its own publications (INCITES

newsletter) to promote the project. INCITES is participating in two other H2020 projects SPEAR (https://www.spear2020.eu/) and SDN-microSENSE (https://www.sdnmicrosense.eu/) in the same thematic area of Cyber Security. These connections will be used to examine possible synergies such as organisation of workshops to share results and ideas between the researchers in these projects.

5.6 CENTRIC

As a research centre within Sheffield Hallam University and a prominent member of the security community, CENTRIC will target opportunities within both the academic community and the security domain. CENTRIC will aim to publish the results of its research in academic journals, conferences and trade magazines as well as participate in relevant workshops and expositions relevant to the domain. CENTRIC will communicate aspects of the project the project through its website, Twitter account and Knowledge Byte online series as well as including the project in its printed media and promoting the goals of the project during various meetings and activities. CENTRIC will also be to disseminate the results of the project through its large stakeholder network and through its membership of the European Organisation for Security (EOS). Additionally, the results may also feed into the taught post-graduate programmes on International Security Management, PhD programmes and other training and teaching activity carried out within the remit of the centre.

5.7 UOP

As a higher education establishment, UOP aims primarily at communication and dissemination activities targeting the RTD community and the academia at large. The main dissemination and communication target audience for the project and its results is mainly the cyber-security research community, encompassing researchers, scientists and students with interests similar to the FORESIGHT research topics. However, the communication of the projects' results and distribution of information will also aim at wider audiences such as the broader scientific RTD community, European commercial and industrial stakeholders, as well as other EU-funded and national projects, that will be interested in and benefit from the project's outcomes.

More specifically, the new intellectual property (IP) generated by the work carried out in the FORESIGHT project will allow UOP to: (a) get a return on investment from royalties generated from the project results and background IP; (b) reuse the knowledge acquired to increase their academic and industrial collaborations; (c) provide state-of-the-art international professional training courses and accreditation programs (jointly or individually with other partners) on cyber-security, forensics, privacy and data protection, and other emerging topics; (d) foster innovation and the generation of spin-off companies that specialise in cyber-security training, as well as, on the detection and mitigation of sophisticated cyber-attacks; (e) exploit by various complementary activities the visibility gained by contributing to the federated FORESIGHT solution.

To do so, all appropriate channels will be utilized; communication of the project itself will be facilitated to the target audiences mainly through invited talks in partner institutions, invited publications in relevant venues, training sessions, etc. (indicatively, see Table 9)

Table 9. FORESIGHT target groups and communication instruments

Target group	Communication instruments
Cyber Security researchers Academia and RTD centres	Scientific publications Seminars/training sessions
IT professionals Commercial and Industrial stakeholders	Open days/summit/events Seminars/training sessions
Other research projects	Joint dissemination activities

To maximize the penetration and impact of the dissemination activities, communication of the project and its results will be adapted (e.g., in terms of terminology, presentation of details, potential benefits etc.) to fit the background and interests of its target audience. Communication of the project's results will be mainly achieved through publications in high-impact journals and magazines, conferences, and specialized workshops pertaining the project's research topics.

In particular, during the first period of the project, the planned dissemination activities of UOP aim to foster research collaboration opportunities along with clustering activities with other projects, exchange knowledge, and raise awareness of the FORESIGHT's research areas: in cyber-security, forensics, gamification and cyber-security visualisation, privacy and data protection, and other security mechanisms for privacy. Hence, the target audiences (Table 9) will mainly be cyber-security researchers, researchers at large, academic institutions and RTD centres. The main goal is to achieve at least three publications during the first half of the project, and at least two invited talks to be given at academia/RTD centres or other events. In addition, the organisation of two special sessions or workshops are envisioned that are related to the above areas.

Dissemination activities are expected to be more intense during the second period of the project, since it is expected that the project will have achieved more mature results than in the first phase. As tangible technical results are expected to be available, this will provide the ground to offer a wider dissemination of FORESIGHT in the scientific community, but to also include IT professionals as well as European commercial and industrial stakeholders. During the second half of FORESIGHT, UOP will seek to publish FORESIGHT results in high-quality conferences and international scientific journals and present the project outcomes at a major academic conference, discussing the project ideas and results with the academic and industrial community attending the event; continue seeking clustering opportunities with other EU-funded projects to increase collaboration and organise joint workshops at major cyber-security related events.

Overall, throughout the project, based on the progress and achievements, UOP will seek suitable venues for publishing the scientific results of the project, with special emphasis on its major areas of expertise: security, privacy and trust, information retrieval, data management, game theory, visualisation, and distributed systems.

5.8 M&S

Within first three months of the project, M&S focused on developing the first communication outputs including the FORESIGHT project logo, promotional stickers, general designs, templates and the overall

project identity which were agreed among all partners. Furthermore, social media accounts (Twitter and LinkedIn) were launched and the first leaflet was designed and distributed.

In order to maximize the impact of the FORESIGHT project, M&S will develop a clear definition of target values, target audiences, key messages, channels and communication tools. M&S will draw on its networks consisting of current and former proposal and project partners for creating awareness for the FORESIGHT project. Due to performing the duty of a dissemination and communication lead in several other projects, M&S will create networks between the projects by connecting the social media channels and promote the exchange and setting up of links between websites of sister projects. In addition to highlighting the project on the company website, M&S will furthermore present the FORESIGHT project in internal meetings of other projects in order to explore potential synergies. One such possibility is another cybersecurity H2020 project GUARD (https://guard-project.eu/) in which M&S is participating. M&S will also highlight FORESIGHT project during national and European events, where the company is represented – such as the ICT Proposers Days, the Security Research Event in Brussels or national events by the FFG.

5.9 UAD

As an academic partner of the project, Abertay intends to use the its results from Foresight in two main ways: (1) research publications in the form of conference papers and (2) in research-lead teaching at the University. The input of Abertay to the Foresight research sits largely within the 6 months of the project with the main input included in WP2. To this end we will endeavour to collaborate in particular with the WP2 leader (University of Strathclyde) on a joint publication. We will discuss with the University of Strathclyde for the appropriate conference/venue for the joint publication among those presented in the University of Strathclyde dissemination plan. The publication will contribute to the next cycle of the Research Assessment Framework for the Abertay staff involved in the project. The publication will increase Abertay University capacity to bid for funding in the area of cybercrime. Additionally, the results of the project will be used by Abertay staff in their teaching. Abertay runs successful degrees in Ethical Hacking and Criminology and the staff involved all teach in relevant modules where there could be wide dissemination of the results to students in particular the module CRM303 “The social construction of surveillance and cybercrime” in the Criminology degree and in the module CMP416 Digital Forensics 2 of the Ethical Hacking Degree.

5.10 ACS

In the FORESIGHT project ACS intends to enhance its expertise and maturity to be able to address future airport security challenges and incoming Cyber Ranges federation needs.

ACS contribution to dissemination will be done through its Cyber Range events and surrounding eco-system. Airbus Cyber Range is widely used for various events like Security Training, Cyber Challenges or cyber security technological research.

On short-term plans: ACS will promote the expertise built in attack modelling and security monitoring targeted towards the airport industry and airport authorities.

The main objective would be to develop consulting services and audits in that particular domain. This includes advanced training of airport staff, validation of new equipment, etc.

To achieve that and most-importantly, deliver high-quality consultancy services, ACS needs to avail state-of-the-art knowledge in domain of airport security.

ACS aims to improve its Cyber Range platform, by adding some features to support scoring and training capabilities, as well as its capability to be interconnected to other platforms in a federation.

On mid-term plans: Those plans amount to the transformation of the techniques developed in the context of FORESIGHT into demonstrable innovations (i.e., to provide proofs of involved concepts in cooperation with airport suppliers and manufacturers).

ACS will (re-)use the attack modelling and vulnerability analysis methodology developed in FORESIGHT to help its customers satisfy their security needs during the design stages of their projects.

Along this line, further ACS plans include the improvement of their methodology to perform certified technical audits (i.e., security testing) relying on the FORESIGHT achievements.

This will enable ACS to address future airport challenges and provide cyber-security guarantees to airport industry actors.

ACS will also use the feedback of training that will be used for Airports to improve training methodologies.

5.11 OUC

OUC, and more specifically the Cybersecurity and Telecommunications Research Laboratory (CTRL) of OUC, will contribute to the communication and dissemination activities through scientific publications at relevant conferences and journals. The OUC team will also aim to participate to relevant cyber security workshops in order to present the work OUC leads in WP10 on the federation gateways. Also, since OUC is a distance learning university with relevant postgraduate security degrees. It will also disseminate the results of the project through its distance learning classes and use the case studies demonstrated in FORESIGHT in order to enhance its own Cyber Range and develop virtual and remotely accessible labs to be used by its geographically distributed pool of students. OUC will also organise through its synchronous platforms an online seminar to present various aspects of cross domain cyber scenarios examined in the course of the FORESIGHT project.

5.12 EN

The French Naval Academy (EN) is the only French school providing higher education and training for all future naval officers.

The science education program is directly connected to the research conducted at the Naval Academy Research Institute. The aim of the Academic education is to graduate engineers capable of technical skills to maintain, operate and improve naval systems.

This institute is composed of:

- 2 research domains oriented to Maritime Information Modeling and Processing (Motim) and Mechanics and Energy in the Maritime Environment (M2EN)
- 1 innovative dept
- 1 sea test base
- 1 industrial chair on cyber-defense of naval systems

The institute contributes to the recognition of the French Naval Academy as an international reference in maritime engineering by publishing scientific papers in the main international conferences and journals and by attending and organising international scientific conferences.

Several national events and interactions occurred per year at the academy such as:

- Several symposiums open to the public
- Conferences to enhance the social, political and cultural dimensions of the nation
- Official meetings and international visits of the academy

All these events are used to promote and disseminate FORESIGHT results. The French Naval Academy uses the French Navy media to communicate information and achievements about FORESIGHT. The French Naval Academy has a strong community on social media (We are present on Facebook, Instagram, LinkedIn and Twitter) with a great engagement rate. We share and relay the information released by FORESIGHT on our different pages, in order to highlight the major events.

EN promotes the Foresight project in the French Naval Academy campus using roll-up, which present the project. The academy also created a custom door at the entry of the naval cyber-range containing the FORESIGHT logo.

5.13 CYB

CYB will contribute to dissemination activities of FORESIGHT achievements through participation in workshops, conferences, CybExer organised live-fire exercises, seminars and fairs in the field of cyber security. For example, presenting Power Grid environment modules and design components of the training environment to cyber security and power grid operators with the aim to collect information about power grid security incidents and bring in more area specific professional knowledge. In addition, CYB will actively contribute in the creation of dissemination papers and publications when applicable. Furthermore, CYB will announce the main results of the project through the corporate website as well as its accounts on social media (Facebook, Twitter and LinkedIn). The dissemination activities will take place through the project.

5.14 AIA

As Greece's biggest international Airport, Athens International Airport (AIA) aims primarily at communication and dissemination activities targeting the Airport community, Airport & Aviation industry stakeholders, businesses hosted in the Airport, connected stakeholders and the general public. The main dissemination and communication target audience for the project and its results is mainly the Airport community, encompassing professionals, organisations and connected businesses with interests similar to the Foresight's cybersecurity training methodology, that will benefit from the project's outcomes.

AIA has by nature great exposure to the public, both locally and internationally, and additionally nurtures this exposure with focused channels of communication. Our bilingual (Greek & English) monthly Newsletter which is an account of the business and cultural highlights of the organization's actions is received by more than 20.000 recipients that include the general public, organizations from the tourist sector, airline companies and 250 journalists to name a few among them. Our social media accounts directly reach more than 50.000 Facebook friends and 2.000 followers while our Annual

Report and Corporate Social Responsibility print and web publications are additional channels of communicating the highlights of the year. With more than 8 million visitors last year, our website is a high public exposure area for communication banners to the global public. Last but not least, further exposure and visibility regarding the action can be ensured via targeted press releases to Trade Press.

More specifically AIA aims to disseminate the project outcomes to key scientific journals, such as:

- Journal of Airport Management https://www.henrystewartpublications.com/jam, the leading quarterly journal for airport management, airlines, ground handling companies, advisers and researchers

Moreover, AIA actively participates in major industry conferences such as:

- Passenger Terminal Expo,
- Airport IT Conference,
- Airport Council International (ACI) - ACI Europe Security Committee
- International Air Transport Association (IATA) - IATA security related events https://www.iata.org/events/Pages/index.aspx
- International Civil Aviation Organization (ICAO) - ICAO security related events https://www.icao.int/meetings/Pages/Home.aspx

Furthermore, AIA as the overall orchestrator of Airport activities at the Athens Airport, organizes several stakeholder committees such as the:

- Airlines Operation Committee (AOC),
- Airport Ground Handlers Committee,
- Safety Committee

and participates to Airport's dedicated cybersecurity committees from ACI and EASA, etc.

Finally, AIA is responsible for the safety and security at the Airport and in this context is organizing, producing content, delivering training and certifies AIA and third-party employees for the safe and secure operation at the Airport.

5.15 THALES

Thales Research & Technology (TRT) will publish the results on the modules involved and the project as a whole in journals and participate at conferences/workshops relevant to FORESIGHT. Furthermore, TRT will disseminate to the Thales business units through technical/communication whitepapers and the presentation of the project, its results and demonstrators during company JPAL event at which the Thales product units participate. We expect this external and internal dissemination activities to take place mainly during the second and third year of the project.

5.16 CERT-BG

CERT-BG will contribute to the dissemination activities of FORESIGHT achievements. CERT-BG will participate in workshops and conferences by presenting non-classified research results. Furthermore, CERT- BG is going to publish non-classified results in its monthly bulletins and the official website. The organisation is planning to present these results in the CSIRT Network meetings and on the meetings

with the essential service providers. CERT-BG is going to carry out these dissemination activities throughout the project.

5.17 BDI

The Defense Institute "Professor Tsvetan Lazarov" is established in Bulgaria and internationally recognized scientific organisation that has proved its unique expertise in the field of defense and security.

The Bulgarian Defense Institute will contribute to dissemination activities of FORESIGHT project through participation in:

- **Hemus scientific conference** which is held every two years and it is connected with defence and security fields in couple sections like:
  "Defense and Security Research and Innovation", with subsections: armament, battle systems and technologies; communication and information systems and technologies, cybersecurity; military-political, social and economic aspects of defense.
  "Investing in Technology Innovation", with subsections: research, technologies and systems for defense and security; innovations and cooperation for defense and security.
- **Newspaper Bulgarian Army** is official newspaper of Ministry of Defence in Bulgaria. The newspaper function is always the same - to reflect and promote Bulgarian military affairs, to defend the honour and dignity of the Bulgarian warrior. BDI can contribute to dissemination activities of FORESIGHT project through the newspaper.
- **The series of DIGILIENCE conferences**, the first of which took place in Sofia, 2-4 October 2019, aims to establish the state of the art and future demands in the provision of security and resilience of processes, services and systems that are heavily reliant on information technologies.

BDI takes part in Digilience conference through preparing and presented publications related to cyber security range in front of international audience.

- **The website of the Institute** https://www.di.mod.bg/en could be very helpful for dissemination activities of FORESIGHT project.

5.18 IEIT

Innovative Energy and Information Technologies LTD (IEIT) will participate at conferences and workshops relevant to FORESIGHT project and disseminate the FORESIGHT accomplishments. Links will be developed in IEIT's website (https://www.ieit.eu/). One of the expected means to disseminate the FORESIGHT results is also scientific publication. We expect these dissemination activities to take place mainly during the third year of the project.

5.19 ESO

ESO's communication and dissemination activities are as follows:

- A section for the project on the ESO's website as a part of the cybersecurity project's section http://projects.eso.bg/projects/cyber-security/.
- A general publication about the project in the online magazine ENERGETIKA in Bulgarian language is planned for the end of April – http://eso.bg/
- The project will be presented on the International Energy Forum 2020 which will take place from 23th to 26th of June 2020 at the International Home of Scientists "F. J. Curie", Seaside Resort "St. St. Constantine and Helena" Varna, BULGARIA - http://www.ntse-bg.org/conf-en. We still are not sure about the form of the activity-presentation or information about the project summarized in a leaflet/brochure.

5.20 CEZ

CEZ will contribute to dissemination activities of FORESIGHT project by attending scientific conferences and workshops engaged in cybersecurity in Energy Sector, where the FORESIGHT results will be presented. CEZ will also disseminate the results of the project through the corporate website (http://www.cez.bg/en/home.html). These dissemination acts will take place in the third year of the FORESIGHT project.

5.21 USTRAT

The University of Strathclyde is a leading international technological university, inspired by its founder's vision of a 'place of useful learning', and ambitious to make a positive difference to the lives of its students, the society it is a part of, and the world it shares. In 2019, Strathclyde has been awarded the Times Higher Education UK University of the Year (the only University to be awarded this for a second time, having previously won the award in 2012) & Times Higher Education 2019 Widening participation or Initiative of the Year, The Queen's Anniversary prize for Higher and Further Education award (which is presented to a small selection of UK institutions every two years and is the highest national honour awarded to the sector) and the Sunday Times 2020 Scottish University of the Year. Together, with our partners, we are at the forefront of international research in our strategic theme areas, including: Energy; Health and Wellbeing; Society and Policy; Innovation and Entrepreneurship; Advanced Manufacturing and Materials; Ocean, Air & Space; Measurement Science and Enabling Technologies. The Broadband Networks Group and the Mobile Communications Group have extensive experience in high quality and high impact cyber-security, machine learning and autonomous network research.

Table 10. University of Strathclyde communication and dissemination plan

S/N	Events	Descriptions
1	Journal publications	Computers & Security, Information and Computer Security, Journal of Cryptology, IEEE Transactions on Information Forensics and Security, ACM Transactions on Information and System Security, IEEE Transactions on Dependable and Secure Computing, IEEE Security & Privacy
2	Academic conferences	ACM Symposium on Computer and Communications Security (ACM CCS), USENIX Security Symposium, IEEE Symposium on Security and Privacy , CACOE 2020, SANS 2020, RSA Conference 2020, NATO CCDCOE conference. We are also co-organisers of the IEEE Cyber Science collocated conferences and will promote the FORESIGHT project within at the conference (IEEE Cyber Science).
3	Professional conferences and meetings	6th Big Data in Cyber Security International Conference – The Cyber Academy, Edinburgh Napier 26th-27th May 2020. Securitay, ENUSEC LTDH.
4	Promotion of FORESIGHT	We will promote the FORESIGHT project through conferences we co-organise and co-host as well as through our outreach programs, STEM programs and through the mailing lists we administrate.
5	Social media outreaches	We will promote all activities related to FORESIGHT through the Social media account of the University: on LinkedIn, Twitter, Facebook and Snapchat as well as linking it to official Social Media account of FORESIGHT.

The dissemination and communication activities of the project will be tailored to the background and interests of the target audience. The main dissemination activities will be focused on the publication of high impact conferences and journals.

5.22 UOPHEC

The University of Portsmouth (UOPHEC) is non-profit public higher education institution in the UK. The research outputs from FORESIGHT project, particularly those high quality and high-impact publications contributed by UOPHEC staffs, will be included in the submission made by the University to the UK Research Excellence Framework (REF) in 2020. REF is the evaluation mechanism used by the UK government for allocating research funding to UK research organisations, and as such will contribute to the economic viability of the University.

Throughout the project's life cycle, UOPHEC aims to:

- Publish the scientific work from the project in high-quality and high impact journals such as (*in Acronym*) *COSE, IEEE Access, IEEE SECUR PRIV, ACM COMPUT SURV, IEEE COMMUN SURV TUT,* and *JISA*.

- Publish and present the scientific work from the project in high-quality and major conferences, e.g., (*in Acronym*) *NEW2AN, ruSMART, IEEE Services, IEEE Netsoft, NTMS, CSR* , and discuss the ideas and results with attendees from academic and industry.
- Publish and present the scientific work from the project at workshops, e.g., (*in Acronym*) *CSRIOT* and *SECSOFT*.
- Co-organise, along with the project partner (UOP, Greece), one conference (*CSR)* and two workshops (*CSRIOT* and *SECSOFT*).
- Promote FORESIGHT project at Hack Pompey, a social hack day open to everyone looking to learn, create and meet new people. It is south coast's biggest hackathon, organised by Portsmouth graduates and take place at University.
- Continue clustering with partners from other EU-funded projects (e.g., CYBER-TRUST) and stakeholders to explore the synergies and collaboration possibilities. Meanwhile, explore potential partners through conferences, meetings and workshops for future collaboration.

6 Plan assessment and evaluation

The long-term vision of FORESIGHT is to empower organisations to protect themselves both legally and economically by reducing cyberattacks. The adoption and use of the FORESIGHT outputs by organisations will lead to increased marketing opportunities, which would dramatically increase their user bases. Hitting that milestone will, in turn, generally increase the resilience of society to cyberattacks. The plan for exploitation and dissemination of results is in line with the overall FORESIGHT innovation management approach and consists of several policies intended to transfer FORESIGHT achievements and lessons learned to business, having also as end goal the commercialisation and customer engagement with the project's outcomes. In this section, we present an evaluation of the outreach and communication strategy planned by the FORESIGHT Consortium and explain how the planned dissemination activities target the FORESIGHT vision.

6.1 Alignment with project objectives

The FORESIGHT project aims to develop a federated cyber-range solution in order to enhance the preparedness (prevention, detection, reaction and mitigation) of cyber-security professionals at all levels (from junior to senior) by delivering a realistic training and simulation platform that brings together unique cyber-security aspects from the aviation, power grid and naval ecosystems. Hybrid scenarios will also be implemented by introducing IoT simulated devices (e.g., sensors) to the aforementioned ecosystems. The high-level project objectives are the following.

- **PO1** Delivery of a state-of-the-art platform that considerably extends the capabilities of existing cyber-ranges by allowing them to be part of a cyber-range federation, where current and future cyber-ranges and simulation training environments of varying TRLs contribute by adding domain specificities (apart from those considered during the project's lifetime) and allowing complex cross-domain (i.e., hybrid) scenarios to be built.

- **PO2** Development of realistic and dynamic scenarios based on identified and forecasted trends and needs in terms of cyber-attacks and vulnerabilities (along with their cascading effects), based on cyber-threat intelligence that is gathered from various online sources and the dark web, to enable cyber-security professionals to rapidly adapt to an evolving threat landscape.

- **PO3** Development of advanced risk analysis and econometric models, constantly updated with real-life incidents, that will assist organisations to estimate the impact of cyber-risks, select the most appropriate and affordable security measures to protect valuable assets, and minimise the cost and time to recover from cyber-attacks.

- **PO4** Delivery of innovative training curricula, going far beyond those individual domains considered in the project, guiding cyber-security professionals to implement and combine security measures in innovative ways by using new technologies; established learning methodologies will be employed to maximise the outcome of training, which will be efficiently supported by learning platforms to establish a rich cyber-security FORESIGHT knowledge base.

From the above given objectives is made clear that, besides mere development of skills, the FORESIGHT platform aims at a holistic approach to cyber-threat management; the project puts considerable emphasis on research and development (i.e., research on advanced cyber-threats, experimentation, development of novel ideas and tools) as the key to increase the dynamics of training and awareness methods in order to match or even exceed the rate of evolution of cyber-attackers.

Thoroughly aligned with the project's objectives, the dissemination activities targeting commercial and industrial experts consist of several policies intended to transfer FORESIGHT achievements and lessons learned, and aim to inspire interest and market demand concerning the FORESIGHT final outputs. Towards this end, the Consortium has carefully considered the stakeholders and the targeted audience of the FORESIGHT outcomes and has gingerly planned dissemination activities to ensure the visibility and awareness of FORESIGHT, promote the project amongst stakeholders, engage the target audience, and finally attain commercialisation and customer engagement with the project outcomes. Bearing in mind that the conversion of public funding into socio-economic benefits is a priority for FORESIGHT, the three-phase planned dissemination strategy promotes the vision for a new era in cyber-security; uses the first convincing results to approach the general public, the RTD community, the industry and other potentially interested stakeholders and make them aware about the research and technological benefits of the FORESIGHT outputs; establishes a fruitful afterlife of the project.

The development, the continuous feed, and the afterlife maintenance of communication channels, such as the project website, social media channels and newsletters, will produce and disseminate material easily accessible by the targeted stakeholders. Promoting the FORESIGHT platform when clustering with other relevant projects and related networks, participating in expert forums, publishing in conferences/journals, and contributing to policymaking is expected to have a huge impact on the technology roadmap and future research on cyber-security, as well as on the European industry and the EU cyber-security certification framework.

6.2 Key Performance Indicators

As planned in the FORESIGHT proposal, efficient communication during the project will make use of a variety of dissemination tools and channels, including the ones shown in Table 11.

Table 11. Proposed dissemination tools and channels

ID	Activity	Measurable results	KPI (initialized from DOA)
1	Websites	A dedicated website will be set-up (including an open access and restricted area). One of the website sides, the Project website side, will focus on the description of the project content, objectives and information on the involved partners. The restricted part of the website will enable exchange of documents and information between the partners.	1000 visits year 1, 50% annual increase in visits/year => 5000+ visits year 4

		Links to the websites of the partners and relevant organizations will be featured. On the website the opportunity will be offered for external visitors to subscribe for the magazine and project updates.	
2	Conference workshops	The consortium-members will be proactive in putting forward proposals for themed workshops and symposia addressing priorities of H2020 programme and bringing together key industrial sectors represented within the targeted value chains and public sector to present FORESIGHT, look at integration opportunities and best practice examples. Additionally, in T12.2 & 12.4 stakeholders will be invited (workshops organised by FORESIGHT) to learn about the outcomes of the project and exploring the synergies and cooperation possibilities.	3 workshops participation/year, 4 workshops organised by FORESIGHT
3	Technical factsheets	Each of the three pilots will develop a factsheet with information about successful application and implementation of the project solutions; factsheets will be provided in English and the native language of the demonstration host country. Factsheets will be published electronically and will be promoted through social media, online trade news sites, and relevant information portals. They will be updated every six months as project demonstrations progress.	Technical factsheets produced for each demonstration and available on website. Updated every 6 months
4	Publications	During the course of the project, publications (at least 8) are foreseen in international (peer-reviewed) journals and industrial magazines. These publications will be prepared by the work packages leaders and partners.	>8 publications on peer-reviewed journals

5	Newsletters	After the starting phase of the project (after month 6), FORESIGHT will start issuing a regular subscription-based newsletter distributing website and project updates to interested parties. By this means, FORESIGHT will build a database of dissemination contacts that can be approached with targeted information suiting exactly their needs. Existing networking and media contacts will be used to promote the project wherever possible. The consortium will also look for opportunities to include feature articles in third party newsletters	10 issues of newsletter, 500 subscribers by end of project, 3 articles per year in third party newsletters
6	Press releases	In order to reach also national stakeholders and end-users of results within the partner's countries (including industry and the broader public), press releases will be prepared and sent to the project partners so that they can function as local dissemination hubs by sending the material to their own dissemination networks and by publishing them on their own websites. Relationships will be developed with relevant press officers to allow news to be effectively disseminated via trade journals and news outlets. Press releases will also be released on social media	Press release every 6 months
7	Special innovation / lesson	The action 'Special innovation/lesson' will start at Month 13 of the project. Regular presentation and special promotion of selected FORESIGHT highlights and outcomes (beyond deliverables) will take place on the website under a section especially designed for this purpose, and by selected dissemination channels, such as target audience related press distribution lists, blogs, local promotional events, social media etc.	10 special features, 4 regional promotional events

8	Leaflet, brochures, presentation	Leaflet, brochures, project video, presentations will be developed to present the project to the general public in an easily understandable way. A first project leaflet will be produced within the first three months of the project and will be describing the project and its main features, timeline and expected outcomes. It will also be printed and distributed at events of the aviation, energy and naval sector where FORESIGHT core partners are involved as organisers or co-organisers. One presentation will be offered at local level (targeting all target groups) during the project and at the end of the project to present the project results to policy-makers and potential investors.	1 Leaflet, 3 brochures, 1 video YouTube channel, 12 presentations
9	Social Media	Awareness will be raised using social media (up to bi-weekly updated). Not only about the project itself, but also about the potential benefits and the unique opportunities to address cyber security challenges in CIIs and ICTs across the EU. Social networks channels such as a LinkedIn page, a YouTube page and a project Twitter account will be created and updated regularly. The project team will monitor trends in social media and will identify emerging, suitable channels for dissemination of results. Producing podcast on challenges and on the business models.	400 followers, 100 retweets, 50 comments
10	Standardization activities	FORESIGHT will collaborate with organsations involved in standardisation activities and procedures.	Number standardization organisations / experts consulted >= 5

11	Project synergies and other targeted initiatives	FORESIGHT consortium will collaborate as much as possible with other ongoing related projects to exploit opportunities for knowledge exchange and for improving dissemination among the target audience. Particular emphasis will be placed on project synergies and clustering activities, in collaboration with the other projects accepted in the same call, so as to maximize the impact and minimize the replication of work.	Number of project synergies =>2

7 Conclusions

This deliverable gives all the details for the dissemination and communication strategy as planned by the FORESIGHT Consortium; it will serve as the principle communications guide to how the project will disseminate findings and research to the target audience to raise awareness. The FORESIGHT partners are confident that the activities presented in this document will generate awareness of the issues addressed and the solutions offered by FORESIGHT, thus paving the way (i) to achieve higher visibility and recognition from both industry and academia and (ii) to the successful exploitation and market uptake of the projects' results.

References

[1] https://ec.europa.eu/research/participants/data/ref/h2020/other/grants_manual/amga/soc-med-guide_en.pdf
[2] https://journals.plos.org/ploscompbiol/article?id=10.1371/journal.pcbi.1004947
[3] https://gist.github.com/
[4] https://help.github.com/en/github/writing-on-github/creating-gists
[5] J. Jiang, L. Zhang and L. Li, "Understanding project dissemination on a social coding site," 2013 20th Working Conference on Reverse Engineering (WCRE), Koblenz, 2013, pp. 132-141.

