




D11.1

**Dissemination,
Communication and
Exploitation Plans**

Project number:	833683
Project acronym:	CyberSANE
Project title:	Cyber Security Incident Handling, Warning and Response System for the European Critical Infrastructures
Start date of the project:	1 st September, 2019
Duration:	36 months
Programme:	H2020-SU-ICT-2018

Deliverable type:	Report
Deliverable reference number:	DS-01-833683 / D11.1/ Final 0.9 2020_CSN_RP_04_Deliverable 11.1_Dissemination Communication and Exploitation Plans_v1
Work package contributing to the deliverable:	WP 11
Due date:	01/03/2020 – M6
Actual submission date:	02/03/2020

Responsible organisation:	ATOS
Editor:	Ana María Morales (ATOS)
Dissemination level:	CO
Revision:	Final 0.9

<p>Abstract:</p>	<p>This deliverable presents the communication and dissemination strategy defined for CyberSANE project considering the key audiences targeted through the different communication and dissemination activities, as well as the objectives, channels, actions, and Key Performance Indicators to measure the success of the strategy. This is a live document that will be updated on D11.2, D11.4, and D11.6 with the results reporting of each action. In addition, it presents a general overview of the CyberSANE Partners' Exploitation Plans and Standardisation activities which will be detailed in-depth on D11.3 and D11.5.</p>
<p>Keywords:</p>	<p>Communication, dissemination, exploitation, strategy, plan, KPIs, website, social media, positioning, impact, visibility.</p>
	<p>The project CyberSANE has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833683.</p>

Editor

Ana María Morales (ATOS)

Contributors (ordered according to beneficiary numbers)

Luis Miguel Campos (PDMFC)

Nathalie Milton, Valerie Loscri (INRIA)

Armend Duzha (MAG)

Sophia Karagiorgou (UBI)

Matej Kovacic (JSI)

Manos Athanatos (FORTH)

Plixavra Vogiatzoglou (KUL)

Ilaria Buri (KUL)

Paris-Alexandros Karypidis (SID)

Konstantinos Kontakis (STS)

Haris Mouratidis (UoB)

Pablo Gimenez (VPF)

Diarmuid OConnor (LSE)

Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author’s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

Executive Summary

The present deliverable aims at presenting the comprehensive plan for the communication and dissemination strategy within WP11, involving more specifically T11.1 led by ATOS and T11.2 led by INRIA, with the main objective of positioning the CyberSANE project among the identified key stakeholders and maximise its impact during its life through the execution of different activities involving the offline and online world.

This document describes the main phases of the dissemination and communication strategy in line with the definition of the stakeholders and their potential relationship with the project, taking into account the technical development expected from other work packages and the achievement of milestones for the definition of the phases, integrated in the communication and dissemination strategy. Each one of the phases has a general aim and also specific activities to be executed towards the achievement of both the project objectives, and the objectives set in terms of communication to contribute to CyberSANE's positioning among stakeholders, including general public, media, potential users of the solution, standardisation bodies, policy-makers, and academia and research institutions, during the project lifetime and after its completion.

Furthermore, it describes the list of channels, formats, and tools considered for managing the communications such as digital ecosystem (website and social media), dissemination and communication material (leaflets, videos, roll-up), participation at external conferences and exhibitions, organisation of workshops, development and submission of scientific papers to journals and academic conferences, and development of press releases and project newsletters among others.

The strategy has also taken into consideration the execution of liaison activities with standardisation bodies within T11.4 led by FORTH, and the potential collaboration with other relevant projects and communities for maximising the impact and reach of audiences of CyberSANE-related messages and contents.

In order to measure the success of the strategy, relevant KPIs have been defined to monitor on a regular basis the progress of the strategy and to determine if any additional action should be implemented to achieve the objectives successfully.

Therefore, the strategy presented must be considered as a live document that will be updated and adjusted if necessary, in conjunction with the reporting of activities developed on further deliverables such as D11.2 (M12), D11.4 (M24), and D11.6 (M36).

In addition, the deliverable presents an overview of the objectives and description of the plan for the development of activities related to exploitation, sustainability, and standardisation as part of T11.3, T11.4, and T11.5 led by FORTH and MAG. These

topics and activities will be addressed in the future on deliverables D11.3 (M20) and D11.5 (M36).

Contents

Executive Summary	2
Contents	4
List of Figures	6
List of Tables	6
Chapter 1 Introduction	7
1.1 Purpose and objectives	8
1.2 Structure of the document	8
Chapter 2 Communication and Dissemination Strategy	9
2.1 Communication Impact	9
2.2 Communication and Dissemination Objectives	11
2.3 Communication and Dissemination Key Audiences	12
2.4 Communication and Dissemination Channels and Activities	13
2.5 Milestones and messages	14
2.6 Individual Communication and Dissemination Plans	15
2.6.1 PDMFC	15
2.6.2 ATOS	15
2.6.3 CNR	16
2.6.4 S2	16
2.6.5 INRIA	16
2.6.6 MAG	16
2.6.7 UBI	16
2.6.8 JSI	17
2.6.9 FORTH	17
2.6.10 STS	18
2.6.11 KU LEUVEN	18
2.6.12 SID	18
2.6.13 UoB	19
2.6.14 VPF	19
2.6.15 LSE	19
2.6.16 KN	20
Chapter 3 Communication and Dissemination Activities	21
3.1 CyberSANE Website	23
3.2 CyberSANE Social Media Strategy	25
3.3 Communication Material	28
3.4 Journal Publications and Scientific Papers	29
3.5 Media and PR strategy	31
3.6 Newsletter	34
3.7 Events	34
Chapter 4 Dissemination and Communication Reporting	37
4.1 Key Performance Indicators (KPIs)	37

4.2	Reporting Templates	41
Chapter 5	Standardisation and Liaison Activities	42
5.1	Introduction	42
5.2	Individual Standardisation Activities	42
5.3	Standardisation and Liaison Activities in CyberSANE	43
5.3.1	External stakeholders	43
5.3.2	Plan & Potential Liaisons	45
Chapter 6	Exploitation Strategy and Approach	48
6.1	Overview	48
6.1.1	Exploitation Models	48
6.1.2	Exploitation Stakeholders	49
6.2	Joint Exploitation Plan	49
6.3	Initial Individual Exploitation Plans	50
6.3.1	PDMFC	50
6.3.2	ATOS	50
6.3.3	CNR	51
6.3.4	S2	51
6.3.5	INRIA	51
6.3.6	MAG	52
6.3.7	UBI	52
6.3.8	JSI	52
6.3.9	FORTH	52
6.3.10	STS	53
6.3.11	KUL	53
6.3.12	SID	53
6.3.13	UoB	53
6.3.14	VPF	53
6.3.15	LSE	53
6.3.16	KN	54
Chapter 7	Summary and Conclusion	52
Chapter 8	Bibliography	53

List of Figures

Figure 1: CyberSANE - Communication and Dissemination target groups	12
Figure 2: Communication and Dissemination Channels.....	13
Figure 3: Communication Messages.....	14
Figure 4: CyberSANE Logo	21
Figure 5: CyberSANE Logo in White.....	21
Figure 6: CyberSANE Logo with background	21
Figure 7: CyberSANE Symbol	21
Figure 8: Colour Palette	22
Figure 9: CyberSANE Imagery.....	23
Figure 10: CyberSANE Website - Home Page / Project Page / Communication Page	24
Figure 11: CyberSANE Twitter Account.....	25
Figure 12: CyberSANE LinkedIn Account.....	26
Figure 13: CyberSANE Social Media Calendar	28
Figure 14: CyberSANE Word Template.....	28
Figure 15: CyberSANE PPT Template	29
Figure 16: CyberSANE Call for Papers Radar	31
Figure 17: CyberSANE 1st Press Release	31
Figure 18: CyberSANE Newsletter.....	34
Figure 19: CyberSANE Events Radar	36
Figure 20: CyberSANE Reporting	41

List of Tables

Table 1: Related research projects	9
Table 2: Shared Social Media accounts	27
Table 3: Journals targeted for papers publications.....	30
Table 4: Scientific conferences targeted for papers publications	30
Table 5: Website Publications / Press Clippings	34
Table 6: Conferences and Exhibitions targeted	35
Table 7: Communication and dissemination KPI's	40
Table 8: External Stakeholders list	45
Table 9: List of events for standardisation liaison activities.....	46
Table 10: Exploitation Stakeholders	49

Chapter 1 Introduction

CyberSANE's goal is to develop a state-of-the-art solution that improves the detection and analysis of cyber-attacks and threats on Critical Information Infrastructures (CIIs) and increases the knowledge of the current cyber threat landscape. Additionally, CyberSANE will allow human operators to dynamically increase preparedness, improve cooperation among CIIs operators, and adopt appropriate steps to manage security risks, report and handle security incidents. Fully in-line with relevant regulations (e.g. GDPR and NIS directive), CyberSANE will contribute to enhancing the preparedness of organisations against cyber threats.

In this context, communication and dissemination activities of the project will aim, in general, at:

- Showing to EU CII operators, the importance, and advantages of the adoption of a security and privacy incident handling system such as CyberSANE;
- Involving relevant stakeholders to foster the implementation of the CyberSANE system in order to promote cooperation and preparedness among CIIs;
- Positioning CyberSANE at EU level as a flagship project and innovative solution among key stakeholders.

The communication actions will focus on the initial phase of the project in order to present the consortium, the projects, its objectives, and expected outcomes, as well as to raise awareness among stakeholders. The generation of research output dissemination will focus on reaching the scientific and research communities, standardisation organisations (T11.4), and key industry representatives. In line with the technical development and progress, both communication and dissemination activities will focus on presenting the results of the CyberSANE system (the system as a whole and its five components) through specific outreach activities to all audiences. At the end of the project, focus will be oriented towards the development and results of the pilots, the system, and the generation of engaging opportunities to support the exploitation and sustainability activities (T11.3 and T11.5).

All the activities will be detailed and broken down in this Communication and Dissemination Plan which constitutes the first deliverable from the WP11 – Dissemination, Exploitation, Sustainability, and Market Take up. The deliverable also describes the activities foreseen in relation to T11.3, T11.4, and T11.5, which will be detailed in-depth on D11.3 (M20) and D11.5 (M36).

The development of activities and any change or adaptation made on the Communication and Dissemination plan will be outlined in D11.2 (M12), D11.4 (M24), and D11.6 (M36). This plan was prepared by Atos within T11.1 (Dissemination and Communication Planning) and will be executed and monitored by INRIA as part of the T11.2 (Dissemination and Communication Activities).

1.1 Purpose and objectives

The purpose of this deliverable is to present the Communication and Dissemination strategy that will guide the development of activities contemplated for the whole project, to maximise the impact of the project on target audiences, and to present the KPIs defined for the project which will allow to monitor and evaluate the success of the work performed on T11.1 and T11.2.

The plan included in this deliverable is based on Atos Research and Innovation methodology and strategy for communication and dissemination activities, but it has been adapted in order to fit CyberSANE and its stakeholders' needs.

The document aims to fulfil the following objectives:

- Define a clear and creative strategy for CyberSANE communication and dissemination activities;
- Define the roles of the partners involved in this task;
- Identify the channels and tools which will be used throughout the duration of the project;
- Set the methodology for the evaluation of the activities defined.

Moreover, the deliverable includes a description and brief plan of the activities related to other tasks included in WP11 such as IPR management, Exploitation, Sustainability, and Standardisation.

1.2 Structure of the document

The deliverable will follow this structure:

- Chapter 2 presents the communication impact and strategy for the CyberSANE project, and the individual communication and dissemination plans of the partners.
- Chapter 3 presents the detailed channels defined in Chapter 2.
- Chapter 4 describes the KPIs established for the whole project and the monitoring process which shall be followed to determine the success of the strategy.
- Chapter 4 describes the standardisation and liaison activities foreseen within industrial partners and the consortium in general.
- Chapter 6 presents an overview of the exploitation strategy, its approach to exploitation models and stakeholders, and the individual exploitation plans of CyberSANE partners.

2.1 Communication Impact

As stated in the project proposal, the communication and dissemination activities are fundamental to contribute to the impact of the project in several areas and overcome major challenges related to the cybersecurity arena in the EU, such as limited consumer awareness, lack of understanding of cybersecurity and privacy issues and processes, and low usability of cybersecurity solutions. By doing so, we will also contribute to boosting the competitiveness of the European ICT security industry in the advent of digital transformations involving key infrastructures for sectors such as Healthcare, Energy and Transportation.

The execution of diverse activities targeting key stakeholders, will be also essential to contribute to the EU Digital Market, and the strategic and research priorities of ECSO, especially in relation to the compliance with and implementation of legal requirements towards the improvement of both existing and future cybersecurity policies.

As part of the topic SU-ICT-01-2018 “Dynamic countering of cyber-attacks”, CyberSANE envisions the collaborative work and knowledge exchange with other research and innovation activities both from the same call and topic, and from the previous one, in order to maximise the impact and create synergies in the communication and dissemination activities. The identified projects mentioned in the following table will be considered for the development of joint activities for sharing information, and even as a reference for implementing best practices in this field:

Table 1: Related research projects

Project	Description ¹	Website	Social Media
DEFEND	Platform to empower organisations in different sectors to assess and comply to the European Union’s General Data Protection Regulation (GDPR).	https://www.defendproject.eu/	Twitter: @DefendProject LinkedIn: DEFENDProject YouTube: DEFENDProject
CIPSEC	Unified security framework that orchestrates state-of-the-art heterogeneous security products to offer high levels of protection in IT (information technology) and OT (operational technology) departments of CIs.	https://www.cipsec.eu/	Twitter: @CIPSECproject LinkedIn: CIPSECproject
STOP-IT	Strategic, tactical and operational protection of critical water infrastructures against physical and cyber threats.	https://stop-it-project.eu/	Twitter: @STOPIT_Project LinkedIn: STOP-ITProject Facebook: Stop-ItProject

¹ Description taken from each project website

D11.1 – Dissemination, Communication and Exploitation Plans

SPEAR	Timely detection of evolved security attacks such as APT, Denial of Service (DoS) and Distributed DoS (DDoS) attacks using big data analytics, advanced visual-aided anomaly detection and embedded smart node trust management, in energy and smart grids scenarios.	https://www.spear2020.eu/	LinkedIn: SPEAR Project YouTube: SPEAR Project
GUARD	GUARD develops a cybersecurity framework for complex business chains, composed by public services that exchange data and commands through open APIs. GUARD targets concrete technologies and architectures (i.e., FIWARE, IDS).	https://guard-project.eu/	Twitter: @Guard_Project
nIoVe	Detect cyber-attacks in real-time while simultaneously preventing them. Regarding the automotive market, nIoVe purpose to uptake the innovative cybersecurity solutions for the protection of all CAVs and infrastructure in the IoV network against complex cyber-attacks.	https://www.niove.eu/	Twitter: @NioveProject
CARAM EL	Address modern vehicle cybersecurity challenges applying advanced Artificial Intelligence (AI) and Machine Learning (ML) techniques and also to continuously seek methods to mitigate associated safety risks.	https://www.h2020caramel.eu/	Twitter: @caramel_project LinkedIn: H2020 Caramel Project YouTube: Caramel Project
C4IIoT	Design, build and demonstrate a novel and unified Cybersecurity 4.0 framework that implements an innovative IoT architecture paradigm to provide an end-to-end holistic and disruptive security-enabling solution for minimizing the attack surfaces in Industrial IoT systems.	https://www.c4iiot.eu/	Twitter: @c4iiot LinkedIn: C4IIoT Facebook: C4IIoT.eu
CONCORDIA	Provides excellence and leadership in technology, processes and services to establish a user-centric EU-integrated cyber security ecosystem for digital sovereignty in Europe.	https://www.concordia-h2020.eu/	Twitter: @concordiah2020 LinkedIn: CONCORDIA Project Facebook: Concordia-h2020.eu
CyberSec4Europe	Designing, testing and demonstrating potential governance structures for a future European Cybersecurity Competence Network using best practice examples derived from concepts like CERN, as well the expertise and experience of partners.	https://cybersec4europe.eu/	Twitter: @CyberSec4Europe LinkedIn: CyberSec4Europe

D11.1 – Dissemination, Communication and Exploitation Plans

ECHO	Delivers an organized and coordinated approach to strengthen proactive cyber defence of the European Union, through effective and efficient multi-sector collaboration.	https://ec-honetwork.eu/	Twitter: @ECHOcybersec LinkedIn: ECHO Cybersecurity YouTube: ECHO Cybersecurity
OPENQKD	Raise awareness of the maturity of QKD and its seamless integration into existing security solutions and networks for a wide range of use-cases.	https://openqkd.eu/	Twitter: @openqkd
SIMARGL	Integrated and validated toolkit improving European cybersecurity.	https://simargl.eu/	Twitter: @SIMARGL8 Facebook: Simargl
SAPPAN	Aims to a cyber threat intelligence platform to enable privacy preserving and efficient response and recovery utilizing advanced data analysis and machine learning.	https://sappan-project.eu/	Twitter: @SAPPAN_H2020
SPARTA	Long-lasting community capable of collaboration to define, develop, share, and evolve solutions that will help practitioners prevent cybercrime and enhance cybersecurity.	https://www.sparta.eu/	Twitter: @sparta_eu

The objective of the CyberSANE communication and dissemination policy is to coordinate the activities and tasks among the project partners according to the timeline proposed and to ensure the success of the strategy.

2.2 Communication and Dissemination Objectives

As outlined in the proposal, information to be communicated about CyberSANE has a twofold goal: 1) to raise awareness about the project in order to attract potential users and other stakeholders in the ecosystem, and 2) to spread the results obtained to boost the impact of the project after its completion.

The main objective on the communication side is the following:

To position CyberSANE among its stakeholders as a state-of-the-art cybersecurity solution for the efficient detection and analysis of threats and attacks, while providing support to professionals to increase preparedness, improve cooperation, develop and execute a communication and dissemination plan involving relevant and creative actions to generate visibility, improve awareness and maximise the impact of the project.

In order to achieve such goal, some specific objectives related to awareness, visibility and engagement, have been defined:

1. Raise awareness about the project and its impact in the cybersecurity arena through the implementation of a digital strategy considering the development of the project website and the setup of social media channels targeting key audiences and related projects to generate brand recognition and engagement.

D11.1 – Dissemination, Communication and Exploitation Plans

2. Boost online and offline visibility of the project by creating and developing valuable, diverse and relevant content in different formats, regarding the project activity and results, to be shared through several channels (website, social media, partners websites, media outlets, scientific journals etc).
3. Maximize interest among key target audiences to generate engagement, interaction and feedback through the active presence and participation in events, and the organization of CyberSANE workshops.

On the dissemination side, the objectives targeting scientific audiences to support the exploitation of CyberSANE outcomes are the following:

1. Raise awareness about the CyberSANE system and its components to attract entities in the academic and research ecosystem and foster interaction;
2. Transfer knowledge among partners and boost the further development of components and technologies on other research and innovation activities;
3. Ensure broad applicability of the project results taking into consideration regulations and standards.

2.3 Communication and Dissemination Key Audiences

The project focuses on the development of a Security and Privacy Incident Handling system offering multiple features to improve, intensify and coordinate the overall security efforts against multi-dimensional attacks within the interconnected web of cyber assets on CII's, aimed mainly at the Energy, Transport and Healthcare sectors. These sectors will be the main targets of our communication plan as the technology developed within the technical WPs of CyberSANE will be tested in these scenarios.

Moreover, the target audiences will be defined by a full range of stakeholders, contributing to the project communication and dissemination objectives achievements, such as CII's, sectorial industry clusters, European Networks and programmes, standardisation bodies, regional governments, academic and research organisations, research projects, media, the general public, among others. The following image represents the ecosystem of audiences targeted by CyberSANE:

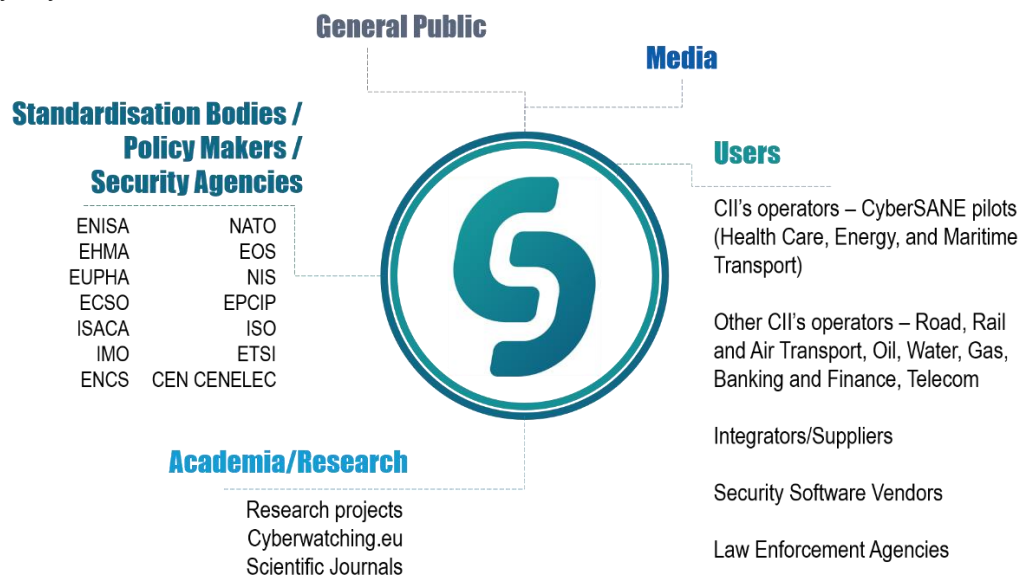


Figure 1: CyberSANE - Communication and Dissemination target groups

D11.1 – Dissemination, Communication and Exploitation Plans

In order to reach key audiences defined in European countries involved in CyberSANE, the project will use a combination of channels, including:

- Partners' ecosystems: Companies and organisations linked to partners, or communities which usually cooperate with partners
- Partners' networks: National or European networks in which partners are directly represented

The use of these contacts will be fundamental to maximise the impact of the communication and dissemination activities.

2.4 Communication and Dissemination Channels and Activities

The communication and dissemination channels and activities have been selected considering the aim to cover both online and offline scenarios, creating a 360° strategy that targets the multiple audiences selected with specific messages, while raising awareness in general regarding the project and its progress. The communication channels to achieve our communication and dissemination goals are the following:

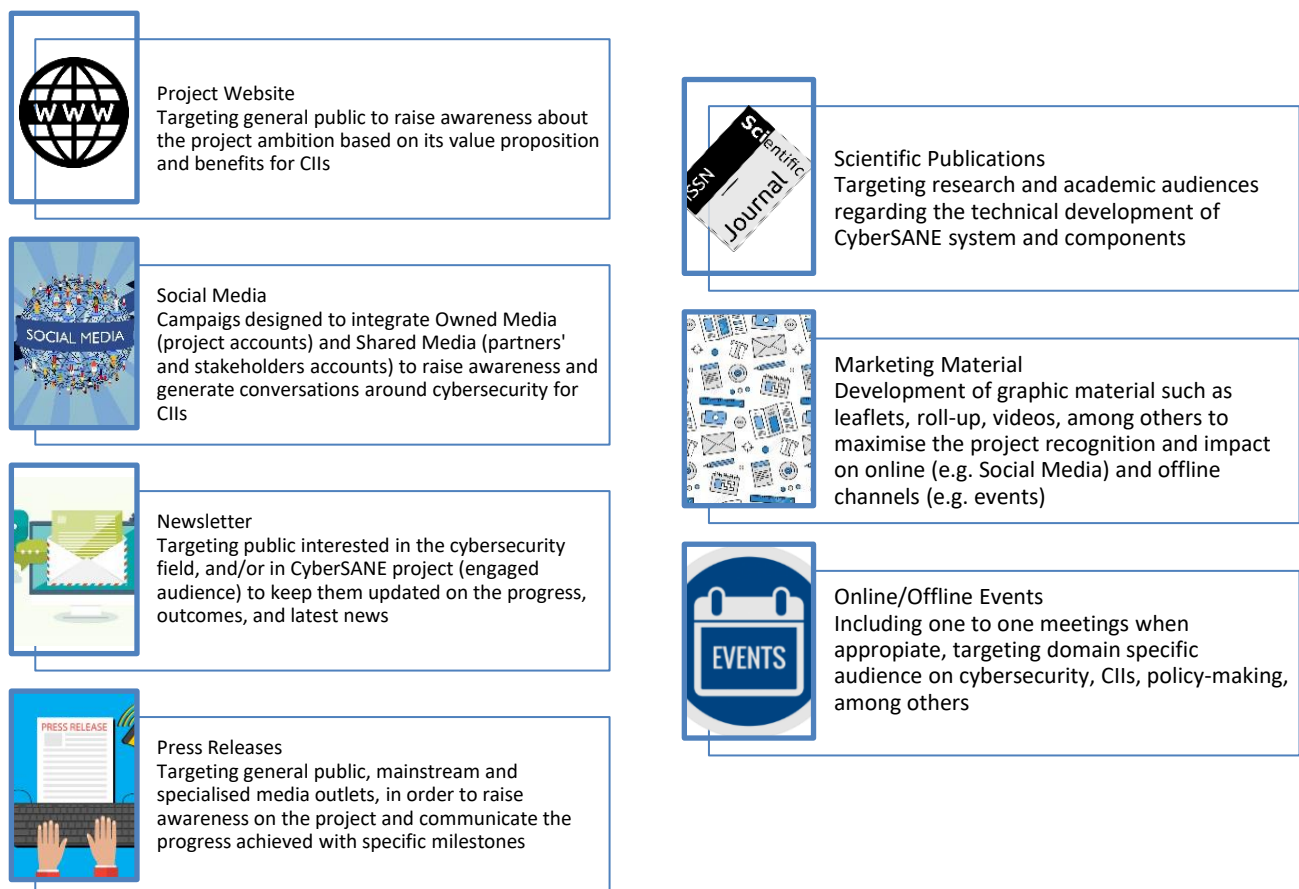


Figure 2: Communication and Dissemination Channels

We will also rely on partners' internal and external communication channels to communicate and multiply the audience reach, by possibly activating several cross-communication actions

D11.1 – Dissemination, Communication and Exploitation Plans

with entities identified through a community mapping based on the stakeholders and standardisation plans. At the same time, we will work on boosting the possibility of reaching earned media with interesting and relevant content we will develop, making those entities interested enough to spontaneously like or share CyberSANE information.

A detailed description of the aforementioned channels along with the specific use that shall take place from our party is included in the following section of this document.

2.5 Milestones and messages

Given the duration of the project, it is important to define the major phases of the implementation of the overall communication strategy. The messages for each one of these phases will be aligned with the technical progress and the main project milestones achieved, as it follows:

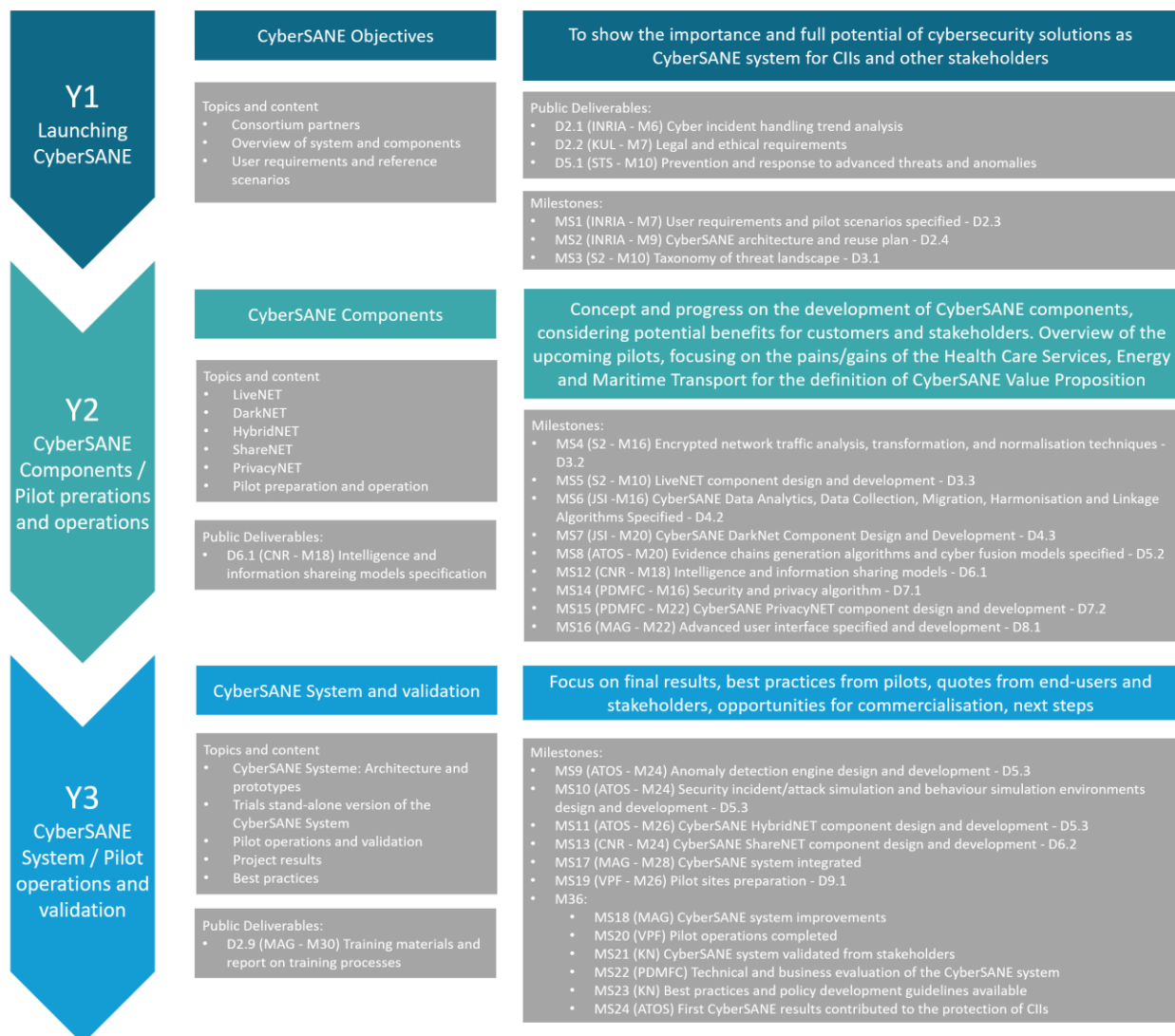


Figure 3: Communication Messages

The timeline of the communication messages will follow the development phases achieved in the technical WPs and will be transmitted to the stakeholders defined on different channels according to the content developed.

2.6 Individual Communication and Dissemination Plans

The Individual Communication and Dissemination Plans are based on the information presented in the proposal and updated accordingly by some partners. Those that did not update the information, present the same text described in the proposal.²

2.6.1 PDMFC

regarding cybersecurity, into its commercial and research activities, making those exploitable results available to our growing number of CII operators in a continuous manner. PDMFC regularly publishes results as contributions in relevant international journals/magazines and conferences. Furthermore publishable, results will be published in form of studies and white papers directly by the company, often in conjunction with the National Center of CyberSecurity (Portugal) with whom we collaborate closely. The company will communicate the project relevant information to stakeholders in all geographies where we are present.

In addition, PDMFC hosts twice a year a large conference on the topic of cybersecurity, with over 50 C-level participants from the largest companies in Portugal, where we present the latest developments in cybersecurity technologies as well as present the most up-to-date threat landscape in line with the work done by ENISA and NIS.

We also organize 4 cybersecurity workshops / hackathons (one per quarter) where hundreds of cybersecurity professionals and students have the chance to experience with cybersecurity challenges using Capture the Flag environments. PDMFC staff participates in multiple cybersecurity events (summer schools, industry fairs, etc) both as invited speakers as well as regular participants and it is expected that we will disseminate CyberSANE and its results to large audiences.

2.6.2 ATOS

Atos has large expertise in communicating and disseminating results from its research projects. Through the Innovation Hub, a group of communication and design experts, Atos Research and Innovation can provide all methods and tools for effective communication. In the context of the CyberSANE project, Atos will define the communication and dissemination strategy that will be executed by INRIA and will explore how to maximize the potential impact of integrated cybersecurity systems. Atos leads WP11 and T11.1 to guarantee the maximum visibility of the project and the achievement of the KPIs established, by acting proactively in every online and offline communication and dissemination opportunities.

Atos is also committed to support all communication/dissemination activities via on-line communication (social networks, press media, website, etc.), exploiting synergies with already running research projects and support all dissemination activities carried out by the project.

For CyberSANE project, Atos will make use of the following channels to contribute to the visibility and positioning of the project: Atos Research and Innovation monthly internal newsletter (350 recipients), Atos Research and Innovation Booklet (<http://booklet.atosresearch.eu/>) with more than 500 Unique Visitors per month, Atos Iberia

² (CyberSANE Consortium, 2019)

D11.1 – Dissemination, Communication and Exploitation Plans

internal weekly newsletter (1100 recipients), Atos Spain and Global Twitter and LinkedIn accounts, and Atos Research and Innovation Twitter account. In addition, Atos will publish at least one of the CyberSANE press releases on its website.

2.6.3 CNR

CNR dissemination strategy focuses on the publication of scientific results in the main venues, either conference or journals. CNR also manages several PhD schools and the FOSAD summer school (currently at its 18th edition) and the NeCS winter school both devoted also to the techniques for cyber security management. CNR is also heavily involved in the cPPP ECSO, being among the 5 initial coordinators of this initiative. (CyberSANE Consortium, 2019)

2.6.4 S2

S2 Grupo's dissemination strategy focuses on the industrial sector. As a SME, S2 Grupo will participate in cyber security trade shows, industrial dissemination events, workshops and industrial level cyber security publications. In addition, CyberSANE will feature in S2 Grupo's online marketing strategy and will be highly featured in the corporate responsibility activities, such as the company's blog [Security at Work](#). (CyberSANE Consortium, 2019)

2.6.5 INRIA

Inria as an academic partner will contribute to the dissemination of the project results through the publication of scientific articles in international peer reviewed journals and through the presentation of the results at high-level international conferences and workshops. In addition, Inria oversees communication activities of the whole CyberSANE project by maintaining the project website, publishing news regarding the outcomes of the project, and building a social media network with LinkedIn and Twitter CyberSANE accounts. Information about the project will also be disseminated through Inria communication channels (websites, special events, Inria industrial meetings, etc). Relevant journals where scientific publications will be pursued: IEEE transactions on wireless communications, IEEE Communication Magazine, and IEEE Journal of Selective Area. Relevant conferences where dissemination activities will be pursued: IEEE Infocom, IEEE MobiCom, IEEE WiSEC, and ACM EWSN.

2.6.6 MAG

MAG's dissemination strategy focuses on the industrial sector. MAG will participate in cyber security trade shows, industrial dissemination events, workshops and industrial level cyber security publications. In addition, CyberSANE will feature in MAG 's online marketing strategy and will be highly featured in the corporate responsibility activities. Furthermore, due to its strong background and research and dedicated R&D department, MAG will collaborate with academic partners in academic publications, such as peer-reviewed conference and journal papers. (CyberSANE Consortium, 2019)

2.6.7 UBI

UBI as a technical partner plans to disseminate the project results to relevant actors and stakeholders in the information and communication technologies (ICT), digital security (DS), big data (BDVA) and data analytics scientific community. Also, UBI will focus on several

D11.1 – Dissemination, Communication and Exploitation Plans

vertical industrial sectors, communities, markets and domains with high interest in digital security, privacy, risk assessment and web intelligence area – targeting its dissemination efforts and activities on its long list of industrial and software partners, business associates and customers.

During the course of the CyberSANE project, UBI intends to disseminate information about the project scope, objectives and developments to a wide range of stakeholders in the relevant business, industrial and research communities, starting from the preliminary and first results (e.g. framework, architecture, models) at the early stages of the project to more technological mature results (e.g. prototypes, software components, integrated platform, pilots, evaluation) near the end of the project. In particular, UBI is going to utilize the following dissemination channels: (a) publication on its corporate website and company newsletter, (b) active participation to EU organized events and conferences, (c) scientific publications in topic-specific journals, conferences and workshops, (d) editing and publication of brochures, press releases and announcements.

Relevant conferences where dissemination activities will be pursued: International Conference on Data Science, Technology and Applications, SIG SIDAR Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), and Infosecurity Europe.

2.6.8 JSI

JSI manages the Videlectures.NET (www.videlectures.net) platform, which is free and open access educational video lectures repository. The lectures, webinars and presentations that will be given by the CyberSANE project on events like conferences, summer schools, special sessions, workshops and science promotional events will be video-recorded and published. All lectures are accompanied by presentation and related open educational materials. JSI as a holder of UNESCO Chair for Open Technologies for Open Educational Resources and Open learning (<https://unesco.ijs.si>) would promote the open educational material (also videos) in scope of the project and would communicate it through its dissemination channels not only in European Union, but across a worldwide scale too.

The consortium will support the transfer of knowledge also to scientific communities through various high-ranking scientific events in cybersecurity, privacy, crypto, and eHealth domains, such as: IEEE European Security & Privacy Symposium, IEEE Security & Privacy Workshops, IEEE Symposium on Security and Privacy, Network and Distributed System Security Symposium, USENIX Security Symposium, ACM Computer and Communications Security, ACM Security & Privacy in Wireless and Mobile Networks, CRYPTO, EUROCRYPT, SECRIPT, ARES, ESORICS, IAPP Privacy, Security and Risk Conference.

2.6.9 FORTH

FORTH is going to disseminate project results to the scientific community via conferences and journal publications. This will be done in line with FORTH's strategic mission of transforming research results into industry applications in contract research or as a starting point for spin-offs, through STEP-C and PRAXI network. Additionally, the results stemming from the project will be presented also to suppliers of CII systems, service providers, policy makers and several EU security stakeholders like ENISA. Furthermore, CyberSANE's

D11.1 – Dissemination, Communication and Exploitation Plans

contribution will support the training of PhDs and Master candidate students, whose integration into the European industry contributes towards growing and sustaining the innovation capacity of European companies. The knowledge, expertise and prototyping know-how gained within CyberSANE will also benefit training of engineering students (lab activities and degree projects) and will enhance communication outreach conducted at the various academic and research partners through our open days and participation in forums.

2.6.10 STS

STS will participate in cyber security trade shows, industrial dissemination events, workshops and industrial level cyber security publications. Furthermore, due to its strong background and research and dedicated R&D department, STS will collaborate with academic partners in academic publications, such as peer-reviewed conference and journal papers. (CyberSANE Consortium, 2019)

2.6.11 KU LEUVEN

KUL as academic partner will contribute to the dissemination of the project results through the publication of papers, through presentations in conferences and workshops, through its internal channels of online dissemination and through its teaching activities.

KUL will contribute to the dissemination of the project results through the publication of scientific articles in international peer reviewed journals and through the presentation of the results at high-level international conferences and workshops. Online dissemination channels within KUL include collaboration platforms, personal websites, blogs, and social media pages. For instance, the CiTiP blog is being regularly updated with current issues on privacy, data protection, cybersecurity, e-Health, media and other. In addition, substantial findings supporting fundamental research topics will be scrutinized against their suitability at being integrated within the teaching activities of CiTiP. Specific dissemination activities will be then oriented towards future decision makers through academic courses to students, some of which courses are specialized in IT law.

Relevant journals where scientific publications will be pursued: Computer Law and Security Report, International Journal of Law and Information Technology, Law Innovation and Technology, and European Data Protection Law Review Relevant conferences where dissemination activities will be pursued: Computer, Privacy and Data Protection Conference, ENISA conferences, IEEE conferences, BILETA annual Conference, Amsterdam Privacy Conference, and Privacy Law Scholars Conference.

2.6.12 SID

SID as a technical partner and a research-oriented SME will communicate and disseminate CyberSANE's results in two main pillars. SID intends to enhance CyberSANE dissemination plans in a) publishing scientific articles in international, peer-reviewed journals and conference. SID will carry out high-level research, the results of which will be published in popular IEEE, ACM, Elsevier and Springer journals and well-known International Conferences. In addition, SID will contribute in project's dissemination activities by b) preparing public material and c) establishing communication channels in Cyprus and in the southern Europe.

D11.1 – Dissemination, Communication and Exploitation Plans

In order to communicate CyberSANE's results, SID will utilise the following dissemination channels: (a) publication on its corporate website and company newsletter, (b) active participation to EU organized events and conferences, (c) scientific publications in topic-specific journals, conferences and workshops, (d) editing and publication of brochures, press releases and announcements.

2.6.13 UoB

The University of Brighton will engage with both internal and external communication and dissemination channels to report to a wide audience the activities and results of the CyberSANE project.

Internally the project activities and results will be communicated through regular workshops and meetings at Centre, School and University level as well as engagement with various University of Brighton partners. Especially those partners with interest in the areas of cyber incident handling requirements analysis, privacy analysis, forensic requirements analysis, threat analysis, and security ontologies. Externally, we will make use of our communication channels (e.g. LinkedIn, Twitter) to reach a wide audience but we will also communicate and disseminate project results through scientific and research conferences and journal publications, as well as through the organization of relevant events (such as workshops, presentations) to appropriate stakeholder groups.

Improvement of public knowledge of growing security problems is also a goal of the university, therefore UoB will contribute to outlets that target a much wider general audience such as newspapers and magazines and deliver presentations at a variety of different events. These activities will also be used to explain how EU funded research can be used to increase society's resilience to advanced cyber security threats.

2.6.14 VPF

VPF has a close relationship with several companies in the port community, so it can promote CyberSANE project results to the local/national public authorities dealing with security issues, e.g. Police, Customs and Maritime administrations, managers of CILs and so on.

Furthermore, VPF has several communication channels with the port community. A bimonthly newsletter, with the main results; the Twitter, Facebook and LinkedIn accounts, for publishing the main events and results; the website, with the basic information of the project; and a YouTube channel for promotional videos. In addition, VPF can contribute to the dissemination of the project through its participation in local/national/international port fairs and security conferences where the CyberSANE can be presented.

2.6.15 LSE

As a technical partner and an SME based in Research and Development (R&D), Lightsource Labs Ltd (LSE) will communicate and disseminate CyberSANE's results via:

- Company Media – publication via LSE website
- Company Publications – where relevant; company newsletter, events and conferences

D11.1 – Dissemination, Communication and Exploitation Plans

- **Company Social Media** – cooperate social media (Facebook, Twitter and LinkedIn etc.)

LSE will also actively participate in drafting, editing and the publication of CyberSANE brochures, press releases, announcements etc.

2.6.16 KN

KN will inform on the project results within their community and their personnel. In addition, they will contribute to the dissemination of the project through its participation in health and security conferences and promoting project CyberSANE to their local/national public authorities dealing with security issues. (CyberSANE Consortium, 2019)

The communication and dissemination activities presented in this section will be executed and performed according to the communication needs of each one of the phases presented in Chapter 2. All of them will display the brand of the project, which must be considered as a key element of the communication strategy since it reflects the soul of the project in a visual way. All partners in all communications must consider the guidelines to ensure coherence and contribute to the positioning of CyberSANE among stakeholders. The identity of the project is composed by:

- Logo: Features two intertwined “C”s creating an “S” on contrast, with the name of the project in bold and regular typography. The project logo on different versions is available for all partners at the repository:



Figure 4: CyberSANE Logo



Figure 5: CyberSANE Logo in White



Figure 6: CyberSANE Logo with background



Figure 7: CyberSANE Symbol

- Colour Palette: Based on the symbolism of colour psychology, the main colours are:
 - Steel blue has a calming impact on viewers. The use of this colour conveys a message of confidence and success and expresses positive emotions and no

D11.1 – Dissemination, Communication and Exploitation Plans

negative emotions while transmitting safeness, security, authority, and trustworthiness.

- Silver Grey goes well with other colours and is used for its neutral shade. It evokes modesty, strength, authority, sophistication, and elegance.
- White signifies purity and it is used to evoke feelings of simplicity, perfection, and innocence. However, it is advisable to use white cleverly with other colours.

These colours are being used in every communication and material developed to reinforce the visual identity. The following image presents the colours of the palette with HEX, RGB and CMYK codes.

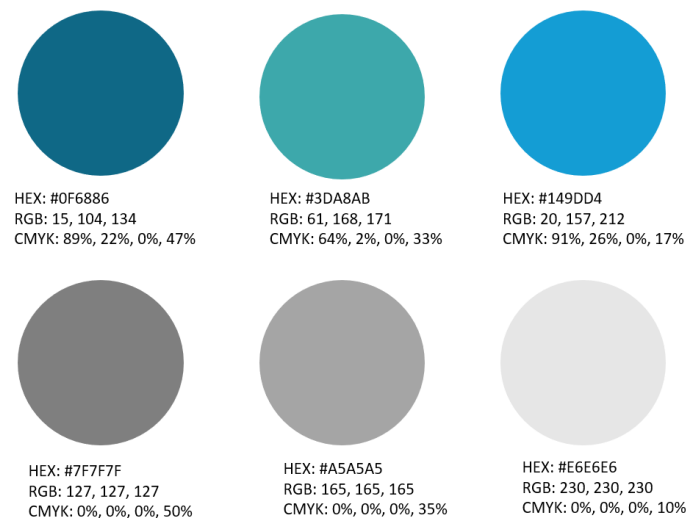


Figure 8: Colour Palette

- Tagline: Cyber Security Incident Handling, Warning and Response System for the European Critical Infrastructures
- Imagery: CyberSANE communications (press releases, social media posts, website content, leaflets, etc) should be accompanied with images that transmit and reflect the main purpose of the project in terms of cybersecurity for Critical Information Infrastructure for Health Care, Energy and Transport. These images can have multiple colours, but blue, grey, black and white should be the predominant ones. In addition to consider the use of these images on communication and dissemination material produced by the project, they will also be a fundamental part of the social media strategy with the development of Tweet Cards. In fact, it is proven that Tweets with images are 34% more likely to be retweeted than tweets with no images³, which means that the use of imagery and designs is fundamental to boost engagement and give CyberSANE more visibility across Social Networks The latter also contribute to increasing the web traffic of project's website. The following figure shows some examples:

³ (Postcron, 2020)

D11.1 – Dissemination, Communication and Exploitation Plans

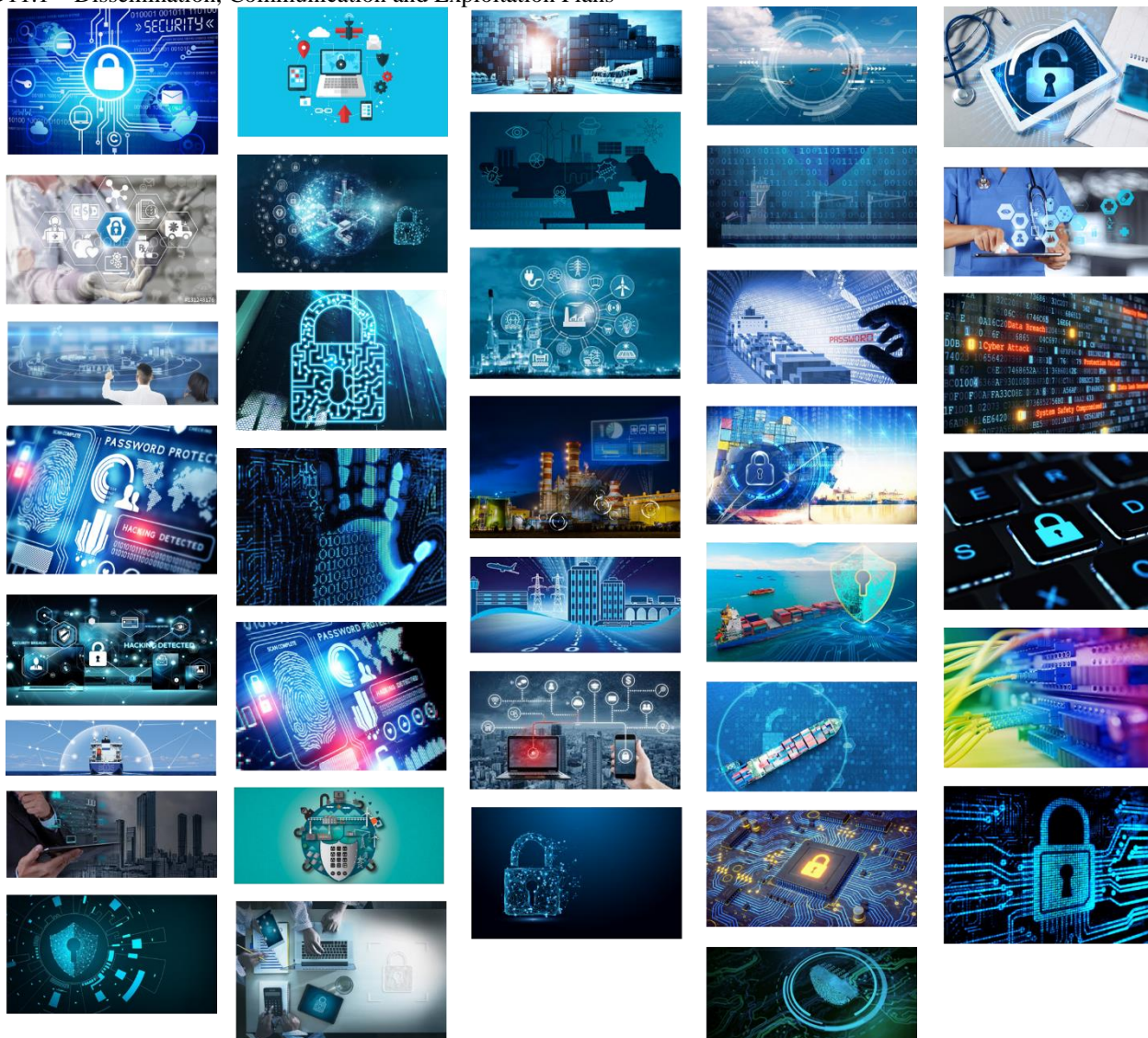


Figure 9: CyberSANE Imagery

The branding elements described above support the aim of the communication and dissemination strategy on reflecting the principal characteristics and features provided by the CyberSANE system and its components, linked to the competitive advantages they provide due to the integration of state-of-the-art technologies which will contribute to the enhancement of cybersecurity on CII and to a better understanding of the current and future threats.

3.1 CyberSANE Website

CyberSANE website has been available since M4 of the project at <http://www.cybersane-project.eu>, and it constitutes the main communication channel of the project towards stakeholders. It presents the vision and the most relevant information about the project such as objectives, organization, and partners of the CyberSANE project, and it is a living site that will continuously publish ongoing events, meetings (intra and inter consortium), new scientific publications and results. It also displays the regular newsletters. In terms of design, it follows the project visual guidelines and has adopted the best SEO techniques and accessibility features.

D11.1 – Dissemination, Communication and Exploitation Plans

The website has been developed by INRIA under T11.2 and will be also managed and updated regularly according to the communication needs of each stage of the communication plan by INRIA.

- **Homepage:** Offers a comprehensive view of the sections of the website and the content available. It includes a table with information about the grant agreement, topic, funding, and relevant dates, followed by a section which addresses the problem that CILs experiment nowadays regarding cybersecurity and threats. It features the icons and links to the project social media accounts, a live Twitter feed, a subscription form for the newsletter, and a section of recent posts. The footer includes the disclaimer of the EC. Also, a search tool allows visitors to search for specific content using keywords that enhance the overall experience on the website.
- **Project:** Presents the scope of the project and describe the components of the CyberSANE system. It has a submenu gathering information related to the objectives of the project, the work packages and their descriptions, and the pilots' scenarios where the system will be validated.
- **Communication:** Contains information related to participation at events, conferences, press releases, articles published, newsletters, and any other type of communication material produced. This section will be updated regularly to contribute to the SEO positioning of the website, and each new post will be promoted through social media owned accounts.
- **Partners:** Includes basic information about the consortium partners such as logo, name, location, and link to the work packages section under the “project” section.
- **Contact us:** Provides information about the project coordinators and includes a contact form which allows visitors to get in touch with the administration team.
- **Privacy policy:** Dedicated section informing how we manage the information of visitors and how we collect the data from comments/contact forms. It includes information on the web analytics integrated in the website to draw statistic on visits.



Figure 10: CyberSANE Website - Home Page / Project Page / Communication Page

The traffic of the website is measured on a monthly basis in order to make sure that we are attracting relevant stakeholders by providing useful content, allowing us at the same time to further improve our strategy and performance with good practices.

3.2 CyberSANE Social Media Strategy

To increase the visibility of the project and the website, social networks are an essential element to communicate the progress and different activities that the project is executing. For this purpose, Twitter and LinkedIn accounts have been created, as their audience and focus are more professional and helps us reach relevant stakeholders.

The messages posted in these social media accounts will be news, milestones, relevant activities, interactive and engagement material, and any content that contributes to generating awareness about CyberSANE as a European project and its importance in the cybersecurity field for sectors such as Health Care, Energy, and Maritime Transport. In addition, a chat service shall be also provided in order to gain feedback from stakeholders.

The social media strategy has been divided into:

- **Owned Social Media:**

CyberSANE social media accounts created after an analysis of the target and potential to impact relevant stakeholders.

- Twitter ([@CyberSANEH2020](https://twitter.com/CyberSANEH2020)) – Used to spread the word about the project activities and news (milestones, events, releases, components, etc), and to cover internal and external events in real-time to increase engagement with the audience. Part of the strategy also focus on posting third party news about cybersecurity and CII's protection to attract the interest of stakeholders and position ourselves as experts in the matter. Some tactics that are and will be followed to boost our presence on Twitter include:

- Interact with target groups (mention, RT, like, DM, etc)
- Engage with influential people in the cybersecurity and research fields
- Strategic selection of the people, companies, projects, communities, etc, we want to follow and engage with
- Use of visuals (Use of pictures increase RT's by 34%) (Postcron, 2020)
- Including CTA's
- Use of hashtags and emojis



Figure 11: CyberSANE Twitter Account

D11.1 – Dissemination, Communication and Exploitation Plans

- LinkedIn ([CyberSANE](#)) – Social Media channel focused on business, employment and corporate communication where we will share content focused on the project, milestones, success stories, and events participation. This channel will help us to reach the CIIs market, attract decision makers and identify potential users of the CyberSANE system. Some tactics to boost our presence on LinkedIn are:

- Page set up as “Company” profile to allow consortium members to add it on their personal profiles – More visibility
- Engaging with relevant communities, projects and pages
- Tag relevant people, companies, organisations, etc, on the posts to increase connections and visibility
- Use hashtags to get discovered
- Upload videos

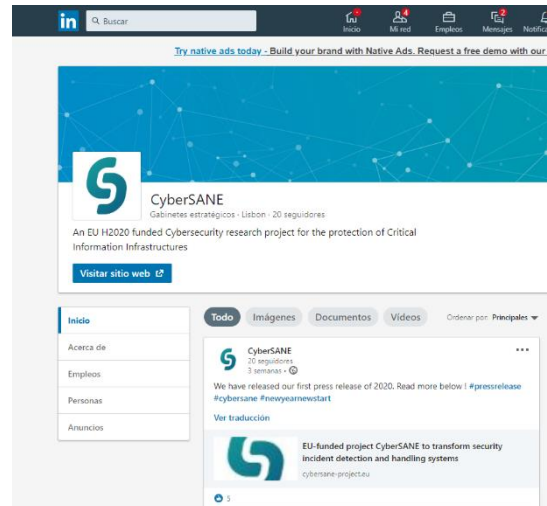


Figure 12: CyberSANE LinkedIn Account

- Shared Social Media:

Refers to the social media accounts and websites owned by CyberSANE partners which will also contribute to spread and share the messages of the project in order to continue increasing the impact and reach of the project, its objective, the components, technical progress, participation at events, pilots, etc. Some of the accounts identified are presented in the following table:

Partner	Website	Twitter	LinkedIn
PDMFC	https://www.pdmfc.com/	@PDMFC	https://www.linkedin.com/company/pdmfc/
Atos	https://atos.net/en/ http://booklet.atosresearch.eu/	@Atos @AtosES @ARIMarc omm	https://www.linkedin.com/company/atos/
CNR	https://www.cnr.it/en	@Stampa Cnr	https://www.linkedin.com/company/consiglio-nazionale-delle-ricerche/
S2	https://s2grupo.es/en/home/ https://www.securityartwork.es/	@s2grupo	https://www.linkedin.com/company/s2-grupo/
INRIA	https://www.inria.fr/en	@Inria	https://www.linkedin.com/company/inria/
MAG	https://www.maggioli.com/	@Gruppo Maggioli	https://www.linkedin.com/company/gruppo-maggioli/
UBI	https://www.ubitech.eu/	--	https://www.linkedin.com/company/ubitech/

D11.1 – Dissemination, Communication and Exploitation Plans

JSI	https://www.ijs.si/ijsw http://videlectures.net/ https://ct3.ijs.si/	@JSI_SL @videolectures	https://www.linkedin.com/groups/VideoLectures-4139916/ https://www.linkedin.com/company/jozef-stefan-institute/about/
FORTH	https://www.forth.gr/	@FORTH _ITE	https://www.linkedin.com/company/foundation-for-research-&-technology-hellas-forth-/
STS	http://www.sphynx.ch/	--	--
KU	https://www.kuleuven.be/	@Leuven U	https://www.linkedin.com/company/ku_leuven/
SID	https://sidroco.com/	--	--
UoB	https://www.brighton.ac.uk/csius/index.aspx	@CSIUS Brighton	https://www.linkedin.com/in/csius/
VPF	http://www.fundacion.valenciaport.com/	@FValenciaport	https://www.linkedin.com/company/fundaci-n-valenciaport/
LSE	https://www.lightsourcebp.com/	@LightsourceBP	https://www.linkedin.com/company/lightsourcebp/
KN	https://www.klinikum-nuernberg.de/	@KlinikumNbg	https://www.linkedin.com/company/klinikum-nuernberg/

Table 2: Shared Social Media accounts

- **Earned Social Media:**

Refers to coverage achieved as a result of public and influencer relations efforts, and the development of interesting and relevant content created that results in mentions, likes, shares, reposts, etc, that increase the impact and visibility of the project on social media. The aim here is to generate and increase engagement and conversations among the key stakeholders identified and boost the visibility of CyberSANE through their social media channels.

INRIA has created the accounts and will oversee the community management tasks and activities. For this purpose, they have created a calendar to manage the posts on both Twitter and LinkedIn, receiving also valuable information and posts suggestions from partners every month.

D11.1 – Dissemination, Communication and Exploitation Plans

CyberSANE Twitter plan

Archivo Editar Ver Insertar Formato Datos Herramientas Complementos Ayuda Calendar Integration

100% 12 B I A

Week

	A	B	C	D	E	F	G	H	I
1	Week	Date	Tag	Type	Subject	Text (Char limit 280, if red too long)	Info	Media	Media info
2	01	01 Jan	Calendar Event		New Year 2020	[emoji] Happy New Year from #CyberSANE! [emoji] Let's begin the new year with some good security resolutions: Do security updates, change your passwords and remember, VPNs are your friend! #NewYear / #Christmas #H2020		✓	Gif of website with fireworks
3	02	08 Jan	Partners	Presentation	PDM	[Partners [emoji]] @PDMFC is the #CyberSANE project coordinator, lead by Luis Miguel Campos. The Portuguese IT company was founded in 1993 and has coordinated many EU projects since 2009. Click below for more information! [emoji] [url] #Partners #Collaboration #H2020		✓	Site URL
4	03	16 Jan	Announcement		URL	[Announcement [emoji]] Our website is up and running. Come and visit us! Click below [emoji] #Announcement #CyberAnnounce #H2020		✓	Link to CyberSANE page
5	04	21 Jan	Information		January Press Release	[Information [emoji]] We have released our first Press Release of the decade! [emoji][emoji] Read more below [emoji] #pressrelease #Information #CyberInfo #H2020		✓	Link to press release article
6	04	23 Jan	Announcement		Cyberwatching	[Announcement [emoji]] #CyberSANE has been registered on @cyberwatchingeu! [emoji] Go and check them out here [emoji] #Cyberwatching #Announcement #CyberAnnounce #H2020		✓	Link to article : https://cyberwatching.eu/projects/1690/cyber-security-incident-handling-warning-and-response-system-european-critical-infrastructures
7	05	01 Feb	Cyber News		Michelangelo	[Cyber News [emoji]] On this day in 1991, the Michelangelo virus was discovered in Australia. The undetectable boot sector virus layes dormant until the 6th March each year, then activates, moving the main drives boot sector preventing the PC from booting. #DidYouKnow #CyberNews #H2020		□	
8	06	07 Feb	Cyber News		DoS 2000	[Cyber News [emoji]] The 7th February 2000, a 14 year old named Mafiaboy took down Yahoo! using a DoS attack, making it the first of its kind. He also targeted Ebay, CNN and Amazon over the following week with Distributed Denial of Service (DDoS) attacks. #DidYouKnow #CyberNews #H2020		□	
9	07	12 Feb	Partners	Presentation	ATOS	[Partners [emoji]] ATOS #Partners #Collaboration #H2020		✓	Site URL
10	08	17 Feb	Meeting	Technical Meeting	2nd start	[Meeting [emoji]] Kickoff of the 2nd #CyberSANE Technical Meeting, in Mediterranean city of Valencia, Spain #Meeting #CyberWork #H2020	At start of meeting	✓	Photo of meeting room
11	08	19 Feb	Meeting	Technical Meeting	2nd end	[Meeting [emoji]] Thank you to @Fvalenciaport for hosting the 2nd #CyberSANE technical event in the city of Valencia, Spain #Meeting #CyberWork #H2020	End of meeting	✓	Link to website article
12	09	26 Feb						□	
13	10	04 Mar						□	

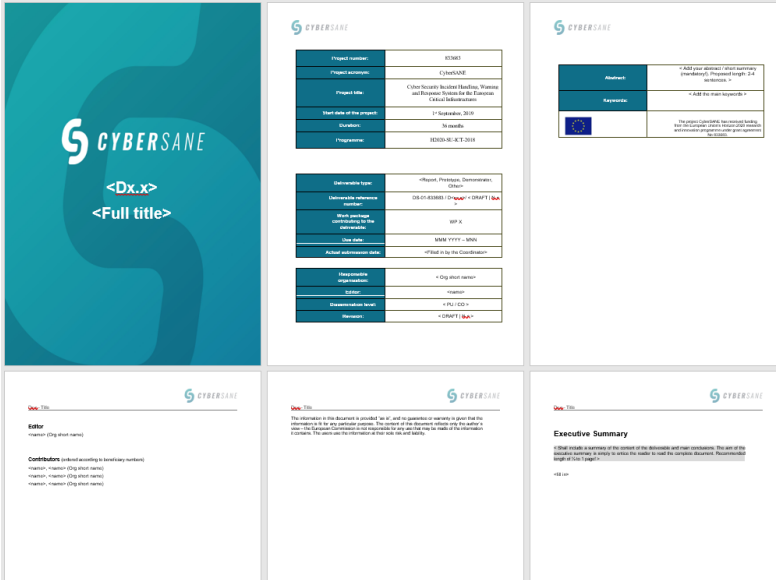
Tags Plan 2020 Plan 2021 Plan 2022 Cyber News Partners Meeting Calendar Event Event Announcement Results Information

Figure 13: CyberSANE Social Media Calendar

3.3 Communication Material

Printed communication and dissemination material will be part of the strategy to position CyberSANE and spread the messages of the project on different scenarios where the project is having presence such as events, conferences, workshops, exhibitions, among many others.

So far, the development of material has been focused on templates to be used by the consortium, but the plan for the first year foresees the development of a brochure, a roll-up, and a video. This material will be included and reported on D11.2 – Initial Report on Dissemination and Communication Activities. For the complete duration of the project, we will produce at least 3 brochures, and a series of short videos will be also produced according to the communication needs to the project.



The template consists of three pages:

- Cover Page:** Features the CyberSANE logo, a title field (<Dx.x> <Full title>), and a footer with the CyberSANE logo and project name.
- Page 1:** Contains a table for project information (Project acronym, Project acronym, Project title, Start date of the project, Duration, Programme) and a table for dissemination information (Dissemination type, Dissemination reference number, Dissemination reference number, Dissemination reference number, Dissemination reference number, Dissemination reference number).
- Page 2:** Contains a table for dissemination information (Dissemination type, Dissemination reference number, Dissemination reference number, Dissemination reference number, Dissemination reference number, Dissemination reference number) and an Executive Summary section.

Figure 14: CyberSANE Word Template

D11.1 – Dissemination, Communication and Exploitation Plans

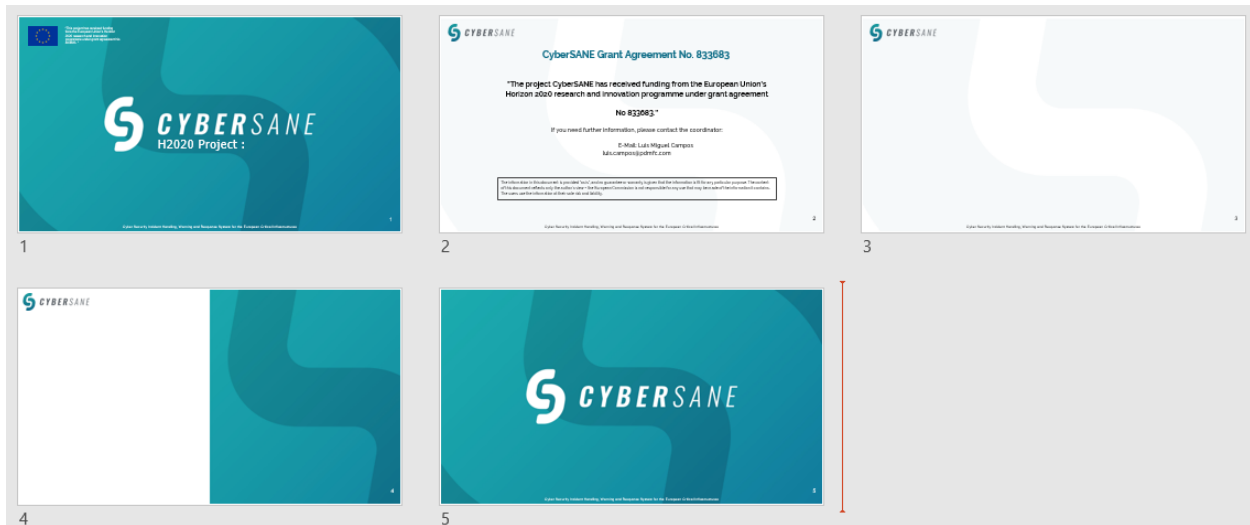


Figure 15: CyberSANE PPT Template

3.4 Journal Publications and Scientific Papers

The development and publication of scientific papers and white papers in specialized magazines, journals, and conferences is an essential activity to attract the attention of interested and related parties regarding the development and results of the CyberSANE project which are especially focused on the research and academic communities. Therefore, CyberSANE consortium will seek to publish this kind of scientific content on several international refereed, scientific and technical journals and conferences in security, such as:

Journals	Link
IEEE Transactions on Affective Computing	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=5165369
IEEE Security & Privacy	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8013
International Journal of Critical Infrastructure Protection	https://www.journals.elsevier.com/international-journal-of-critical-infrastructure-protection
IEEE/ACM Transactions on Networking	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=90
Computers & Security	https://www.journals.elsevier.com/computers-and-security
IEEE Control Systems magazine	http://ieeecss.org/publication/ieee-control-systems-magazine
IEEE Transactions on Industrial Informatics	http://www.ies.org/pubs/transactions-on-industrial-informatics
ACM Transactions on Information and System Security	https://www.scimagojr.com/journalsearch.php?q=28875&tip=sid
International Journal of Law and Information Technology	https://academic.oup.com/ijlit
IEEE Transactions on Information Forensics and Security	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10206

D11.1 – Dissemination, Communication and Exploitation Plans

International Journal of Information Security	https://link.springer.com/journal/10207
--	---

Table 3: Journals targeted for papers publications

Conferences	Link
Critical Infrastructure Protection and Resilience Europe, International Conference on Cybersecurity and Resilience of Cyber Physical Systems (ICCRCPs)	http://www.cipre-expo.com/conference/call-for-papers/
12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade	https://www.cycon.org/
CRITIS: International Conference on Critical Information Infrastructures Security	https://critis2020.blogs.bristol.ac.uk/
Fourteenth IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection	http://www.ifip1110.org/Conferences/
Workshop on Cyber-Physical Systems Security & Privacy (CPS-SPC)	https://cps-spc.org/2019/
CyberSA	https://www.c-mric.com/csa2020
ACM Conference on Computer and Communications Security (CCS)	https://www.sigsac.org/ccs/CCS2020/
European Symposium on Research in Computer Security	http://esorics2020.sccs.surrey.ac.uk/
International Conference on Information Security and Privacy Protection	https://www.ifipsec.org/
InfoSec	https://www.infosecurityeurope.com/
ISC: International Security Conference	http://isc2020.petra.ac.id/
TRA: Transport Research Arena	https://traconference.eu/
International Open Data Conference	https://opendatacon.org/
Protekt	http://www.protekt.de/en/
IEEE Symposium on Security and Privacy	https://www.ieee-security.org/

Table 4: Scientific conferences targeted for papers publications

So far the submission and acceptance of one paper was achieved. Nevertheless, we must mention that this publication does not correspond to project's funding period, given that the paper was written and published once the consortium was aware of the evaluation results of the call, but before the official date of the start of the project on September 2019. The publication resulted in an invitation for an extended journal paper, which is currently under revision. The details of this publication are:

- Title: "Cyber Security Incident Handling, Warning and Response System for the European Critical Information Infrastructures (CyberSANE)"
- Authors: Spyridon Papastergiou and Eleni-Maria Kalogeraki from the Department of Informatics, University of Piraeus; and Haralambos Mauratidis from the School of Computing, Engineering and Mathematics, University of Brighthon
- Published for Springer - EANN 2019, Engineering Applications of Neural Networks, for the 20th International Conference of Engineering Applications of Neural Networks in Crete, Greece - https://rd.springer.com/chapter/10.1007/978-3-030-20257-6_41

D11.1 – Dissemination, Communication and Exploitation Plans

A calendar with important dates for submission of papers has been prepared and shared among partners. This calendar will be updated constantly in order to achieve an overall submission of 7 journal papers and 12 conference papers during the lifetime of the project.

 Call for Papers Radar 2020/21 Please insert events to keep in the radar or events you have confirmed participation				
Status	Submission Deadline	Conference/ Journal	More Info	Partners interested in submitting a paper?
	22/02/2020	8th International Conference of Security, Privacy and Trust Management	https://csit2020.org/sptm/index.html	
	28/02/2020	Critical Infrastructure Protection and Resilience Europe Conference	http://www.cipre-expo.com/conference/abstract-submittal-form/	
	Regular Technical Papers: 30/04/2020	The 15th International Conference on Critical Information Infrastructures Security 2020	https://critis2020.blogs.bristol.ac.uk/regular-technical-papers/	
	Call for Speakers 31/07/2020	Cybersecurity Leadership Summit 2020	https://www.kuppingercole.com/events/csls2020/callforspeakers	

Figure 16: CyberSANE Call for Papers Radar

3.5 Media and PR strategy

Press releases are a means to communicate and distribute information about CyberSANE specific achievements and progress to media with mass communication purposes, in order to create awareness and improve the positioning of the project among the general audience. The relevance and impact of press releases, in conjunction with the goal to reach wider audiences, is fundamental and that is why a strong media and PR strategy is foreseen during the duration of the project to communicate the milestones.

For this purpose, all the partners will distribute all CyberSANE press releases within their internal and external networks to achieve publications with the aim of generating awareness. We will develop and issue press releases on strategic moments of the project, such as the beginning, mid-life, and end of the project, as well as whenever an important milestone has been accomplished or a relevant activity has been performed and must be communicated to general audiences.

The tone used in press release must be serious but fresh and catchy, trying to describe the scope, aim, and benefits of the CyberSANE system and its components in an easy way that allows any reader to understand what we are trying to communicate.

The project has launched a first press release on January describing the objectives of the project, the current cybersecurity threats CII's are dealing with, the expected outcomes, and the pilots that will be performed to validate the technologies developed.

During the first year, at least one more press release will be developed and issued, and for



Figure 17: CyberSANE 1st Press Release

D11.1 – Dissemination, Communication and Exploitation Plans

the upcoming years, it is foreseen the development of 2 press releases per year to reach a total of 6 press releases developed during the life of the project. All press releases and clippings achieved will be highly promoted through owned and shared Social Media accounts.

The following table presents the clippings achieved until now, including publications referring to the project on partners' websites and media outlets:

Name	Type	Title	Link	Audience Reached ⁴
Atos Research and Innovation Booklet	Partner Website	EU-funded project CyberSANE to transform security incident detection and handling systems	Link	1.860
PDMFC	Partner Website	CyberSANE: Cyber Security Incident Handling, Warning and Response System for the European Critical Infrastructures	Link	500
Sidroco Holdings	Partner website	EU-funded project CyberSANE to transform security incident detection and handling systems	Link	200
FORTH-ICS	Social Media	EU-funded project CyberSANE to transform security incident detection and handling systems	Link Link	1.651 2.843
S2 Grupo	Partner Website	CyberSANE, un proyecto europeo en favor de la ciberseguridad	Link	3.660
Automática e Instrumentación	Media Outlet	CyberSANE, un proyecto europeo en favor de la ciberseguridad	Link	8.460
Capa8	Media Outlet	CyberSANE, un proyecto europeo en favor de la ciberseguridad	Link	300
Diario Médico	Media Outlet	Ciberseguridad española para la sanidad europea	Link	142.860
Cadena de Suministro	Media Outlet	Proyecto CyberSane para el desarrollo de soluciones de ciberseguridad	Link	43.800
KU Leuven	Partner Website	CYBERSANE Cyber-Resilience and Critical Infrastructures: All the more reasons for a CyberSANE solution (Blog)	Link Link	1.080.090
Maggioli	Partner Website	A Cybersecurity Incident Handling, Warning and Response System for the European Critical Infrastructures	Link	500
UoB	Partner Website	Brighton joins a European fight against cyber attacks	Link	87.930

⁴ Audience calculated by Monthly Unique Visitors estimations based on the data provided by the tool SiteWorthTraffic and Alexa Traffic Rank, and/or by number of followers on Social Media

D11.1 – Dissemination, Communication and Exploitation Plans

VPF	Partner Website	EU-funded project CyberSANE to transform security incident detection and handling systems	Link	18.780
UBI	Partner Website	UBITECH kicks off the CyberSANE Innovation Action on cybersecurity incident handling, warning and response	Link	17.970
JSI	Partner Website	A CYBERSECURITY INCIDENT HANDLING, WARNING AND RESPONSE SYSTEM CyberSANE to transform security incident detection and handling systems	Link Link	2.800
Veinte Pies	Media Outlet	El proyecto CyberSANE de la Fundación Valenciaport transformará la seguridad	Link	6.120
Naucher	Media Outlet	El proyecto CyberSANE, financiado por la UE, transformará los sistemas de detección y gestión de incidentes de seguridad	Link	13.410
La Vanguardia	Media Outlet	Cosco Shipping Lines se incorpora al Patronato de la Fundación Valenciaport	Link	8.955.390
Spanish Ports	Media Outlet	El proyecto CyberSANE, financiado por la UE, transformará los sistemas de detección y gestión de incidentes de seguridad	Link	4.920
Diario del Puerto	Media Outlet	El proyecto CyberSANE transformará los sistemas de detección y gestión de incidentes de seguridad	Link	32.760
InfoSeguridad	Media Outlet	El proyecto CyberSANE, financiado por la UE, transformará los sistemas de detección y gestión de incidentes de seguridad	Link	1.000
Cyberwatching .eu	3rd Party Website	CYBER SECURITY INCIDENT HANDLING, WARNING AND RESPONSE SYSTEM FOR THE EUROPEAN CRITICAL INFRASTRUCTURES	Link	2.250
Empresa Exterior	Media Outlet	Cosco Shipping Lines Spain se incorpora al Patronato de la Fundación Valenciaport	Link	30.510
CORDIS	3rd Party Website	EU-funded project CyberSANE to transform security incident detection and handling systems	Link	12.932.460
Diario Valencia Maritima	Media Outlet (Printed)	El proyecto CyberSANE de la Fundación Valenciaport transformará la seguridad	n/a	3.000

D11.1 – Dissemination, Communication and Exploitation Plans

				
--	--	--	--	--

Table 5: Website Publications / Press Clippings

3.6 Newsletter

CyberSANE newsletter will be essential marketing tool to gather leads and reach interested stakeholders from the cybersecurity field, and Health Care, Energy, and Maritime Transport sectors looking forward to protecting their critical information with advanced solutions and cooperate with other organisations to deepen the understanding of current threats in order to minimise the risks and attacks impact.

It will be sent bi-annually to generate awareness about CyberSANE project and keep audiences informed about the progress done on the different work packages. A newsletter template has been created following CyberSANE *look and feel*, and a plug-in has been integrated on the website for the mailing of short newsletters. Every newsletter is automatically sent for each five new posts uploaded to the news section of our website. For the purpose of attracting subscribers, a feed registration form has been also included in the home section of the website, and this will also be promoted through Owned and Shared Social Media accounts.

A short newsletter was sent in January to promote the 1st Press Release, and the first edition of the CyberSANE newsletter is planned for Spring 2020. Currently, the team is working on a content calendar aligned with milestones and progress of technical WPs.

3.7 Events

The participation in external events and the organisation of events and workshops is a fundamental element of the communication and dissemination plan of CyberSANE. Taking profit of the ones already existing, with a track record and positioning in the market, ensure

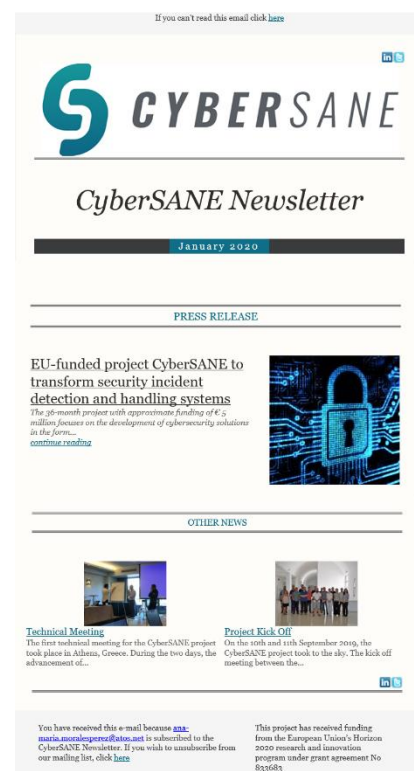


Figure 18: CyberSANE Newsletter

D11.1 – Dissemination, Communication and Exploitation Plans

the impact and the ROI for the resources dedicated to these events. Furthermore, the organisation of events contributes to spread the word about the project and positioning it among specific audiences we would like to target.

The participation in EU clustering and concentration events is foreseen in order to exchange knowledge, results and experiences with other projects already identified, and communicate the project progress at EU level. The participation on this type of events also goes in line with the liaison and standardisation bodies tasks.

On the other hand, the participation in exhibitions and conferences during the project lifetime is aligned with the presentation of scientific publications, but in here it also extends its range of audiences to industrial and sectorial events where we can raise awareness about the project results among Health, Energy, and Transportation CI's. The aim, for the CyberSANE Consortium, is to participate in at least four events or exhibitions during the funding period.

Last, the organisation of three stakeholders' workshops will be fundamental to spread the word and show tangible results through demonstration to all stakeholders associated including Healthcare, Energy, Transport operators, CII's operators, integrators, researchers, policy makers, standardisation bodies, among others. These workshops will be organised between M20 and M36.

The following table shows some events targeted. This list will be updated constantly to make sure we participate on relevant events during the life of the project:

Name	Link
Cyber Security & Cloud Expo Global	Link
CPDP Data Protection & AI	Link
Cybersecurity Standardisation Conference	Link
ENISA Industry Event	Link
Annual Privacy Forum	Link
ENISA Maritime Cybersecurity Workshop	Link
eHealth Security Conference	Link
Transport Cyber Security Conference	Link
Europol-ENISA IoT Security Conference	Link
Cyber Security for Critical Manufacturing - MANUSEC Europe	Link
PrivaSec	Link
Command Control - The European Cybersecurity Summit	Link
InfoSecurity	Link
Malware Analyst Conference	Link
AI&ML for the Smart Grid	Link
International Conference of Security, Privacy and Trust Management (SPTM)	Link
International Conference on Critical Information Infrastructures Security (CRITIS)	Link
CyberTech Europe	Link
Critical Infrastructure Protection & Resilience Europe	Link
Cybersecurity Leadership Summit	Link
Cyber Security & Data Protection Summit	Link

Table 6: Conferences and Exhibitions targeted

D11.1 – Dissemination, Communication and Exploitation Plans


 Events Radar 2020/21 Please insert events to keep in the radar, or events you have confirmed participation								
Status	Name	Description	Date	Venue	Link	Type of Participation	Target Audience	Estimated # of persons reached
	Command Control - The European Cybersecurity Summit	Top speakers from industry, academia and politics will gather in the ICM – Internationales Congress Center München—to give presentations and discuss cybersecurity with particular reference to this year's central theme of cyber resilience. In the forefront are two central questions: What happens if my company is successfully attacked? And how do I safeguard my operations and therefore also the commercial success of my company if the IT systems are no longer accessible?	03-04/03/2020	Munich, Germany	https://www.command-control.com/	TBC	Industry	TBC
	Cyber Security & Cloud Expo Global	The fifth Cyber Security & Cloud Expo event is co-located with the IoT Tech Expo, AI & Big Data Expo, 5G Expo and Blockchain Expo, so you can explore the future of these convergent technologies under one roof. Expand your knowledge and gain the security skills needed to steer your organisation to a more secure future.	17-18/03/2020	London, UK	https://www.cybersecuritycloudexpo.com	TBC	Industry	9000
	InfoSecurity Europe	Infosecurity Europe is the three-day show that brings together the leaders, change-makers and forward thinkers of information security. The conference reveals emerging threats and defences, and defines the big trends shaping our industry. Exhibitors run on-stand sessions to provide practical insights from experts demonstrating their products.	02-04/06/2020	London, UK	https://www.infosecurityeurope.com/	TBC	Industry	15.000
	Annual Privacy Forum	Focus on EU legal framework on personal data protection in an effort to better control the processing of personal data while ensuring an adequate level of protection - Organised by ENISA, DG CONNECT and the Católica University of Portugal	04-05/06/2020	Lisbon, Portugal	https://privacyforum.eu/	TBC	Policy Makers	TBC
	The 15th International Conference on Critical Information Infrastructures Security 2020	Aims to bring together researchers, professionals from academia, critical (information) infrastructure operators, industry, defence and governmental organisations working in the field of security of critical (information) infrastructure systems. The event offers vast opportunities to meet and connect with company	2-3/09/2020	Bristol, UK	https://critic2020.blogs.bristol.ac.uk/	TBC	Industry + Scientific Community + Policy Makers	TBC

Figure 19: CyberSANE Events Radar

Chapter 4 Dissemination and Communication Reporting

This chapter presents the KPIs established to have quantitative measures regarding the effectiveness of the communication and dissemination plan of CyberSANE described in this deliverable. In order to guarantee the success and accomplishment of both, the general objectives of the project, and the communication and dissemination ones, the partners responsible for T11.1 and T11.2 will continuously monitor and measure the KPIs to take corrective actions in time if necessary and identify best practices that are generating awareness of the project among key stakeholders.

4.1 Key Performance Indicators (KPIs)

The different KPI have been specified to evaluate the visibility of CyberSANE:

CyberSANE OBJECTIVES								
GENERAL OBJECTIVE	SPECIFIC OBJECTIVES		ACTIONS		KPI'S Y1	KPI'S Y2	KPI's Y3	TOTAL KPI's
Positioning CyberSANE among its stakeholders as a state of the art cybersecurity solution for the efficient detection and analysis of threats and	Awareness	Generate awareness about the project and its impact in the cybersecurity arena through the implementation of a digital strategy including the	Development of website (Structure + Basic Content)		1	0	0	1
			Website Update - Blog Content		6	6	6	18
			Website Metrics to measure through Google Analytics Report		500 Unique visitors	800 Unique Visitors	1000 Unique Visitors	2300
					1000 Pageviews	1200	1500	3700
					300 Sessions	500	700	1500
			Social Media	Monthly	10	12	12	34

D11.1 – Dissemination, Communication and Exploitation Plans

attacks, while providing support to professionals to increase preparedness and improve cooperation, through the development and execution of a communication and dissemination plan involving relevant and creative actions to generate visibility, awareness and maximise the impact of the project.		development of project website and set up of social media channels targeting key audiences and related project to generate brand recognition.		Metrics Report				
				Twitter	180 Tweets	180 Tweets	180 Tweets	540
					80 Followers	150	250	250
					150 RT/Like	200	250	600
					6000 Impressions	7000	8000	21000
				LinkedIn	20 Followers	50	70	70
					1000 Impressions	1200	1500	3700
	Visibility	Boost online and offline visibility of the project by the creation and development of valuable content in different formats, regarding the project activity and results, to be shared	Dissemination Material	Brochure	1	1	1	3
				Roll up	1	0	0	1
				Video	1	3	1	5
			Press Releases		2	2	2	6
			Audience reached with press releases		1000	2000	2500	5500
			Newsletter		2	2	2	6
			# of Subscribers		40	60	100	100
			Scientific/Academic Papers Journals		1	3	3	7
			Scientific/Academic Papers Conferences		2	5	5	12

D11.1 – Dissemination, Communication and Exploitation Plans

		through several channels (website, social media, partners websites, media outlets, scientific journals etc).					
	Action/Engagement	Maximize interest among key target audiences to generate engagement , interaction and feedback through the active presence and participation in events, and the organization of	Participation in External Events	1	1	2	4
			Organization of events/workshops with stakeholders	0	1	2	3
			Audience reached	100	200	500	800
			Participants per workshop	0	20	50	70

D11.1 – Dissemination, Communication and Exploitation Plans

		CyberSANE workshops.					
--	--	----------------------	--	--	--	--	--

Table 7: Communication and dissemination KPI's

5.1 Introduction

CyberSANE will focus on creating steady bonds, with regular interaction with standardization / policy making bodies (e.g. ENISA, IMO, NATO) and other major research projects (e.g. CONCORDIA, SAURON, ECHO), that are actively working on the security and protection of CIs. This will be a key goal and a major element contributing to the project's dissemination and sustainability strategy. The main focus of the task will be to create liaisons with the aforementioned bodies and with many others through the organisation of shared activities such as presentations, participation in workshops and providing recommendations based on the experienced gained in the lifetime of the project.

We are aiming to foster bi-directional channels through our liaisons that will i) raise awareness and disseminate the projects' results and ii) collect feedback such as comments, suggestions and new insights that will allow us to fine tune the project's results. Dedicated workshops will be held, with the participation of external organizations that are active in the areas of security incident handling and cyber security. These stakeholders will be invited through the business networks of CyberSANE's partners and through the partners' participation in relevant standardization and agencies.

Another aim that is going to be explored through this task is to foster dissemination liaisons with Standardization Bodies (e.g. the NIS (Network Information Security Platform) and the European Program for Critical Infrastructure Protection (EPCIP)).

The results of the project will actively be disseminated to standardizations bodies in order to provide recommendations on cybersecurity across the value chain. The goal of this kind of dissemination liaison will be to raise awareness about CyberSANE's capabilities within standardization experts and NIS participants, in order to gradually establish the CyberSANE approach as an EU wide best practice for cyber-security in digital Healthcare, Energy and Transportation environments. The current plan of these activities is described in 5.3 in more detail. Partners involved in this specific CyberSANE plan have to give regular presentations of the CyberSANE system to all established liaison connections.

5.2 Individual Standardisation Activities

Contributing and creating standards is a long and hard procedure that cannot be fully converted in the lifespan of a 36 months' project. Thus, we are aiming in studying, monitoring and, if possible, adhering some of the standards that our industrial partners are following. In this section, we present the individual activities of each partner that are closely related with standards and cybersecurity standards.

UBI has established and operates a certified (by TÜV AUSTRIA HELLAS) quality management framework and system, which is compatible with the EN ISO 9001:2008 quality standard, for the "design, development, integration, production, installation, deployment, hosting and technical support of software solutions and information technology systems", as well as for the "design, development, execution, management and delivery of research and technological development information technology projects", determining the corporate policies and defining the quality responsibilities for all corporate processes. Also, as IT Security is a top priority area for UBI, they have implemented and deployed internally a

D11.1 – Dissemination, Communication and Exploitation Plans

management system for information security in accordance with the ISO 27001:2005 quality standard, for the " design, development, integration, production, installation, deployment, hosting and technical support of software solutions and information technology systems", the "implementation and management of the information technology projects", and the "delivery of Software-as-a-Service and Platform-as-a-Service services". The deployed information security management framework and system reassures the protection of information and information infrastructure assets of both UBI and its customers against the risks of loss, misuse, disclosure or damage.

ISO/IEC JTC 1/SC 27 "Information Security, cybersecurity and privacy protection" is a subcommittee of the Joint Technical Committee ISO/IEC JTC1 of the International Organization for Standardization (ISO)⁵ and the International Electrotechnical Commission (IEC)⁶. SC 27 aims at developing standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as Security requirements capture methodology, management of information and ICT security, cryptographic and other security mechanisms, security aspects of identity management, biometrics and privacy, conformance assessment, accreditation and auditing requirements in the area of information security management systems, security evaluation criteria and methodology.

Atos is involved in the committee ISO/ IEC JTC1/SC 27, and has participated particularly in the working group WG5 contributing to several standards as ISO 29003, 29115 (related to ARIES⁷ project), and also 27005 and 27010 (related to Cyberwiser⁸ and Concordia⁹ projects respectively).

Atos also takes part of the WG1 of ECSO¹⁰, the European Cyber Security Organisation¹¹. This working group provides to ENISA with common priorities and industrial needs for definition of certification schemes on products, process and services. Atos may collaborate with this WG disseminating the standardization activities developed within the CyberSANE consortium.

5.3 Standardisation and Liaison Activities in CyberSANE

5.3.1 External stakeholders

A list of external stakeholders, that will be reached in order to enhance the Standardisation and Liaisons Activities within CyberSANE, is compiled in this section. Additionally, we aim to present, on a regular basis, the standardisation and technical aspects of CyberSANE, receive feedback and promote certain advancements and recommendations that could possibly affect the creation of future standards. We are currently focusing on three (3) main categories: standardization & Policy Making Bodies, organizations- companies-associations with close relations to industry and standards, Research projects. The complete list can be found in the following table.

⁵ <https://www.iso.org/home.html>

⁶ <https://www.iec.ch/>

⁷ <https://www.aries-project.eu/>

⁸ <https://www.cyberwiser.eu/>

⁹ <https://www.concordia-h2020.eu/>

¹⁰ <https://ecs-org.eu/working-groups/wg1-standardisation-certification-and-supply-chain-management>

¹¹ <https://ecs-org.eu/>

D11.1 – Dissemination, Communication and Exploitation Plans

External Stakeholder	Type	Responsible Partner	Description
ENISA - European Union Agency for Cybersecurity	EU-Agency Policy Maker	FORTH	Dr. Sotiris Ioannidis of FORTH is member of ENISA Advisory Group(AG)
CONCORDIA	EU Cybersecurity Pilot Project	FORTH	Dr. Sotiris Ioannidis of FORTH is acting as deputy Coordinator of this Pilot Project. KUL as the legal and ethical partner
PRAXI Network	Technology Transfer Organization	FORTH	It is a distinct administrative unit operating within the Foundation for Research and Technology – Hellas (FORTH)
CNCS	National Cybersecurity Agency (CNCS Portugal)	PDMFC	PDMFC is a close partner with CNCS and is involved in the activities promoted at national level by CNCS
ECISO		UBITECH	Dr. Panos Gouvas of UBI is representing the team in Cybersecurity events, investor days and Working Groups (i.e. WG1, WG3 and WG 4)
DataVaults	Research Project	UBITECH	Dr. Panos Gouvas leads the implementation of the Risk Management Monitor, which is a service that offers near real-time monitoring and evaluation of an individual's privacy risks.
SDN-microSense	Research Project	UBITECH	Entso Velio (Security Engineer) leads the development of a risk assessment framework in the face of emerging threats and vulnerabilities in the smart grid energy domain.
SPIDER	Research Project	UBITECH	Dr. Panos Gouvas is acting as the technical manager of the Project having the responsibility of the integrated Cyber Range as a Service (CRaaS) Platform.
CyberSec4Europe	EU Cybersecurity Pilot Project	Maggioli	Several members of Maggioli's team participate in CyberSec4Europe as external security consultants
NATO Maritime Interdiction Operational Training Centre (NMIOTC)	Training facility for NATO	Maggioli	MIOTC runs a variety of activities to contribute to ACT processes in the area of Maritime Security and MIO such as: Conferences, Workshops and

D11.1 – Dissemination, Communication and Exploitation Plans

			Seminars (NMIOTC Annual Conference, ATP-71 Doctrine Development Workshop, Cyber Security Conference)
SAURON	Research Project	KUL	KUL is the legal and ethical partner of the project, ensuring that legal and ethical considerations are being taken into account
ROLECS	Research Project	KUL	KUL is the legal and ethical partner of the project, ensuring that legal and ethical considerations are being taken into account
SAFECARE	Research Project	KUL	KUL is the legal and ethical partner of the project, ensuring that legal and ethical considerations are being taken into account

Table 8: External Stakeholders list

5.3.2 Plan & Potential Liaisons

Taking into account the list of external stakeholders presented in 1.3.1, a list of potential events in which CyberSANE can participate is compiled in this section and presented in full in Table 9. This list will be updated during the lifespan of the project and new events can be added based on the continuous research of new standardisation as well as on policy makers' events, the recommendations of the Consortium, the External Advisory Board and the reviewers of the project.

Proposed Event	External Stakeholder	Date	Responsible Partner	Description
Cybersecurity Standardization Conference	ENISA - European Union Agency for Cybersecurity	TBA	FORTH	The conference will discuss the challenges in the standardisation landscape for Cybersecurity in light of the EU Cybersecurity Act.
CONCORDIA OPEN DOOR 2020	CONCORDIA	TBA	FORTH	Engagement with CONCORDIA. panels and talks animated by experts in cybersecurity, legal and economic aspects of cybersecurity, and participate in the future roadmap of cybersecurity.
CYBER INVESTOR	ECSO	May 2020	UBI	This event focuses on both the access-to-market & the

D11.1 – Dissemination, Communication and Exploitation Plans

DAYS IN BRUSSELS				access-to-finance (funds) support.
International conferences/events organized by CyberSec4Europe	CyberSec4Europe	TBA	Maggioli	Participation in meeting, conferences and workshops in the field of incident handling, security of critical information infrastructures and cyber-security in order establish communication channels with Standardization Bodies and Other External Groups
4th NMIOTC Cyber Security Conference in Maritime Domain	NMIOTC	30th of September to 1st of October 2020	Maggioli	The 4th NMIOTC Cyber Security Conference in Maritime Domain is going to be held at NMIOTC premises in Chania, Crete , Greece from 30th of September to 1st of October 2020
11th NMIOTC Annual Conference	NMIOTC	Wednesday the 3rd to Thursday the 4th June 2020	Maggioli	The 11th NMIOTC Annual Conference will take place at NMIOTC premises, in Souda Bay Crete, Greece, from Wednesday the 3rd to Thursday the 4th June 2020, with the following theme: “Interagency and whole of society solutions to maritime security challenges”
LAILEC		TBA	KUL	Annual Conference organised by KUL – CiTiP, inviting partners and relevant stakeholders from academia and policy to participate and exchange knowledge and experiences

Table 9: List of events for standardisation liaison activities

Detailed description

UBI actively participates in ECSO and chairs the DIN SPEC 91337 technical committee. It aspires to reach these channels in order to promote and advance the CyberSANE artefacts in situational awareness, security and privacy technologies. UBI will also build synergies with other relevant projects including DataVaults, SDN-microSense and SPIDER focusing in individual's data privacy, robust and cyber-resilient services and advanced risk assessment in smart grids and Cyber Range as a Service activities, respectively.

D11.1 – Dissemination, Communication and Exploitation Plans

As mentioned before, KUL as academic partner can reach out to a vast audience of academics, stakeholders and policy makers through its dissemination activities. Such activities, as aforementioned, include publishing of papers, journal articles and blog posts, hosting, networking and presenting in conferences and workshops on a national and European level, using internal channels of communication and synergies with national and European projects and diffusing the acquired knowledge through its educational activities. In particular, KU Leuven - CiTiP is currently involved in more than 40 research projects, funded by the EU (FP7 and Horizon 2020), the Belgian Research Council, FWO, and various other parties. CiTiP provides programs and courses both in Dutch and in English, both on undergraduate and graduate levels on the KU Leuven campus in Leuven and Brussels. CiTiP is also among the founding members of the Leuven Center on Information and Communication Technology (LICT) and of the Flemish digital research and incubation center iMinds (www.iminds.be) that recently merged with imec, a world-leading research and innovation hub in nano-electronics and digital technologies (www.imec.be). It is finally involved in various interdisciplinary initiatives in Belgium, such as Cybersecurity Initiative for Flanders, the Knowledge Centre for Data and Society and Leuven.AI.

6.1 Overview

The exploitation strategy of the CyberSANE project will follow a step wise approach and will be based on the combination of a bouquet of activities which will span throughout the project duration but will vary in intensity based on the amount of information that can be made available and the results that will be produced during the project lifetime.

The consortium partners have already established the preliminary strategy which will be further expanded and detailed as the project matures and as the consortium partners begin to have a clearer view of those project's assets that could be commercially and non-commercially exploited. As described in the proposal (CyberSANE Consortium, 2019), the strategy comprises the following steps:

1. Identification of the innovative exploitable assets, whether these are technological components or added value services which the project will deliver to its target users.
2. Conduction of a market analysis, which will identify the market towards which CyberSANE is targeted (e.g. software houses, application developers, networking and computational equipment vendors etc.), its segmentation, the positioning of current competitors and all corresponding emerging trends;
3. Documentation of an analytical IPR management strategy based on the principles outlined in the project CA which will guide the joint and individual exploitation capabilities of the project partners;
4. Analytical definition of all possible commercial and non-commercial exploitation models, which have been preliminary identified and are outlined in the following paragraphs;
5. Analytical definition and evaluation of the sustainability and viability of possible business models and alternative solutions that may be followed for the provision of the project solution and services to the identified stakeholders, including licensing schemes, pricing, etc., and
6. Validation of the aforementioned exploitation activities through the CyberSANE demonstrators.

6.1.1 Exploitation Models

The CyberSANE consortium recognizes two main exploitation models for the project's results:

1. The research exploitation model, which implies the re-utilization of the research know-how acquired in future research activities, and
2. The technological exploitation model, which implies the re-utilization of the technological know-how acquired for the development of innovative products and the provision of advanced services built on top of them.

However, not all project partners and interested stakeholders may exploit all project's results using the models defined above. The exploitation models of the CyberSANE project's results will be dependent upon three main parameters:

- a) the nature and interests of the project partners and stakeholders in general,
- b) the distribution model of the project results and

D11.1 – Dissemination, Communication and Exploitation Plans

- c) the distribution of the IPRs amongst the project partners.

Considering these limitations,

1. the academic and research organizations (both the ones participating in the project as well as the ones outside the consortium) are mainly interested in adopting the research exploitation model for the intermediate project results that will be provided as open source components, integrating them in their research and/or teaching activities and/or setting up future research projects further promoting the project results, and
2. the industrial partners acting as R&D Partners are mainly interested in adopting the technological exploitation model for the intermediate project results that will be provided as open source components for know-how transfer in other products/services.

6.1.2 Exploitation Stakeholders

The CyberSANE consortium identifies the following stakeholders' categories that may be interested in the exploitation of the project results:

Target Group	Description	Expected outcome
A – Business stakeholders	Security operators, CII operators and other stakeholders who might use CyberSANE system in everyday operations	- Benefit of the increased and more cost-efficient handling of incidents associated with Critical Information Infrastructures (CIIs)
B – IT technology providers	IT companies, including SMEs and individual software vendors (ISVs), which provide security solutions to the various CII operators	- Implement and enhance added-value functionalities by blending with in-house artefacts
C – Industry associations and clusters	National and international security agencies in charge of the security of Critical Information Infrastructures (CIIs) such as ENISA, European Health Management Association (EHMA), European Public Health Association (EUPHA), ECSO, ISACA, IMO, NATO	- Facilitate the CyberSANE consortium to access to a large users' base of CIIs operators, including security operators, energy, health and transportation services providers
D – Policy makers and Standardization Organisations	Policy-makers at any level like EC Directorates and Units, Ministries and Governments, Regulatory Agencies, Standardisation Organisations (ETSI, OASIS etc.) on Cybersecurity and Privacy Enhancing Technologies	- Support the evaluation of the project's Social-Technological-Economic-Environmental-Political (STEEP) aspects

Table 10: Exploitation Stakeholders

6.2 Joint Exploitation Plan

The main business targets of the CyberSANE consortium include:

- The development of an exploitation agreement and a final detailed business plan, which will be developed in the frame of Deliverable D11.3.
- The establishment of close and strong relationships with target customers in the countries where the partners have established presence, namely **Italy, Germany, Greece and Spain**.
- The establishment of close relationships with other organizations that could participate in co-marketing and joint sales of the CyberSANE solutions. Those organisations will be mostly dealers/resellers of the CyberSANE system and normally will derive from the technical partners' network. Relevant partnerships will be established in order to pursue win-win market alliances.

6.3 Initial Individual Exploitation Plans

The Individual Exploitation Plans are based on the information presented in the proposal and updated accordingly by some partners. Those partners that did not update their Individual Exploitation Plan are presented with the same plan envisaged in the proposal.¹²

6.3.1 PDMFC

PDMFC will take advantage of CyberSANE project to project itself as a leading cybersecurity company in Europe and beyond. In particular, PDMFC aims to improve its existing proprietary cybersecurity solutions as well as position itself as a centre of excellence in cybersecurity technologies and a most trusted cybersecurity integration partner, able to provide holistic threat and situational awareness to a wide range of industries and governmental organizations. PDMFC will with almost certainty spinoff a company solely dedicated to cybersecurity within the duration of the project (CyberSANE being one of the main catalysts for this decision) given the exponential growth we are experiencing in the last 3 years in the cybersecurity area within the organization.

6.3.2 ATOS

Atos will evolve and exploit the following results after the project has been completed:

- The L-ADS system monitors network traffic in real-time as well as anomaly detection, providing machine-learning capabilities to perform deep-packet inspection using the resulting info for correlation of attacks.
- XL-SIEM is a Security Information and Event Management (SIEM) solution which provides an added high-performance correlation engine to deal with large volumes of security information.

CyberSANE will help Atos to improve both, the XL-SIEM and the L-ADS, including new monitoring capabilities with the objective of identifying potential security breaches within these critical infrastructures, as well as to propose mitigation measures.

¹² (CyberSANE Consortium, 2019)

D11.1 – Dissemination, Communication and Exploitation Plans

Therefore, CyberSANE offers an opportunity for Atos to enhance its solution portfolio in the scope of security for Critical Infrastructures, and gain expertise that may be offered to Atos customers further on.

Considering Atos as a Managed Security Provider, the components owned by Atos can be positioned within the Atos portfolio of several internal business lines. It is worth mentioning the following three:

- The division Big Data & CyberSecurity (BDS) is in charge of solutions addressed to the protection of Critical Infrastructures and Homeland Security. Atos components may be presented to BDS managers, to analyze how to provide added value to the portfolio division.
- Atos Worldgrid is an Atos business unit delivering real-time integration between IT and OT¹³ with sophisticated vertical solutions for energy and utility companies (<https://atos.net/en/solutions/worldgrid>).

Atos components could complement the Worldgrid functionalities providing new capabilities to monitor and prevent cybersecurity attacks in oil, gas and water systems.

- AHPS (Atos High Performance Security) service that is managed SIEM (Security Information and Event Management) service provided by Atos, is targeting customers with more than 3000 monitored devices (event sources), and billions of collected events per month. CyberSANE results will be presented to this offering line to define how they can contribute to the AHPS services portfolio.

6.3.3 CNR

The activities that CNR will develop in CyberSANE will continue to consolidate the research expertise in information sharing (especially for cyber treats information) as well as in the development of cyber treats management systems and infrastructures. CNR is committed (also leading currently the C3ISP project) to develop innovative technologies for information sharing and analytics, also in the ambit of the new cyber security observatory that CNR is developing at Italian level. (CyberSANE Consortium, 2019)

6.3.4 S2

The S2 Grupo exploitation strategy is based on two pillars: (i) S2 Grupo will adapt and improve its cyber security monitoring products, such as Captor, which is Europe's first APT detection tool. These improved products are sold in combination with S2 managed security services, which are handles by S2 CERT 24h security centre; and (ii) S2 Grupo will use CyberSANE to increase the readiness of its solution in the Industrial Automation and Control Systems cyber security sector. (CyberSANE Consortium, 2019)

6.3.5 INRIA

INRIA, as an academic partner, will investigate new secured techniques for intrusion and malicious behavior detections in wireless environment together with bypassing and healing distributed techniques. As other academic, INRIA does not have commercial exploitation interests but intend to publish his work throughout the best international scientific conferences and revues in the area of wireless communication in medical devices. (CyberSANE Consortium, 2019)

¹³ Operation Technology Systems

6.3.6 MAG

MAG has a rich portfolio of public sector accounts in different domains including healthcare, mobility and transport, and security. It will therefore use know-how and results from CyberSANE in order to integrate risk and vulnerability analysis aspects as part of its integrated solutions to local, regional and national healthcare organisations. Italy is the primary market where solutions based on CyberSANE results will be introduced. However, the company will gradually integrate CyberSANE results in its solutions' portfolio for the rest countries where MAG is present, including Spain, Balkan Countries and Latin America. (CyberSANE Consortium, 2019)

6.3.7 UBI

UBI aspires to reinforce its solutions portfolio through the offering of innovative and specialised applications and services not yet present in the market or through the expansion and optimization of its current services and prototypes (in particular, OLISTIC that constitutes the company's enterprise risk assessment and management platform), exploiting the acquired know how and the technological results of the proposed project in order to proceed to the implementation of integrated vertical solution in the field of cybersecurity, privacy and incident handling. This way it will increase its competitiveness, targeting in both the public and private sectors and especially the industry. Thus, UBI aspires to include the proposed project' exploitable outcomes to the overall corporate offerings and promote, exploit and commercialize the developed framework and models to its existing clients list. (CyberSANE Consortium, 2019)

6.3.8 JSI

JSI will exploit the project results in many ways: (i) All applications that will be developed in the frame of the project will become a part of the JSI text garden library of OSS code; (ii) continuation of the research in the large scale networks and complex systems; (iii) continuation of the research stream in using knowledge, semantics and cognitive systems technologies in different scenarios; (iv) Provision of quality knowledge and competences in the form of video lectures and curriculum for videolectures.net;(v) providing to the Slovenian industry knowledge, competences, expertise and tools to strengthen its competitiveness; and (vi) exploitation through the creation of spin-off companies. (CyberSANE Consortium, 2019)

6.3.9 FORTH

A core part of FORTH's exploitation activities will be to demonstrate the novel approaches towards anomaly detection, threat intelligence and cyber incident handling developed in CyberSANE to CII in general. This will be done in line with FORTH's strategic mission of transforming research results into industry applications in contract research or as a starting point for spin-offs. Additionally, the results stemming from the project will be presented also to suppliers of CII systems and service providers. FORTH's exploitation goals for CyberSANE is focused on leveraging the know-how on anomaly and threat detection and on the application, propagation models for cascading effects of complex attack scenarios. The novelties and extensions are going to be presented to the scientific community by publishing in high-quality journals and giving talks at pertinent conferences.

6.3.10 STS

STS will use the outcomes of CyberSANE for strengthening its service and product portfolio. STS plan is to augment the capabilities of its security assurance and certification platform in ways that will enable it to support the delivery of cyber security training programmes (e.g., providing monitoring and dynamic testing, establishing interoperability with emulation and simulation environments etc) and, therefore, be used as a tool for this purpose. STS will also seek to develop consultancy services in setting up training programmes for establishing cyber security assurance assessment schemes, based on the outcomes of the project. (CyberSANE Consortium, 2019)

6.3.11 KUL

As far as KUL's involvement in the project is concerned, the outcomes of the project and of the research undertaken therein will be elicited in further research proposals and in several potential publications. As such, KUL has a non-commercial exploitation interest relating to the development of the specific technologies by the consortium partners. In sum the exploitation interests of the KU Leuven consist of the experience that we will build throughout the project and the reputational benefits that will result from its successful completion. (CyberSANE Consortium, 2019)

6.3.12 SID

SID will exploit the results and the products of the CyberSANE project by utilising its capacity in creating, maintaining and optimising the usage of visualised IDS and IDPS systems. Also, the penetration testing suite for critical infrastructure will be enlarged and expanded to include more tests in line with modern, sophisticated threats and attacks. The usage of the visual-based anomaly detection will be further advanced by SID in delivering more services and applications after the project. (CyberSANE Consortium, 2019)

6.3.13 UoB

The University of Brighton is committed to the development of an 'innovation culture' based on the generation of knowledge. The results of the CyberSANE project will allow UoB to improve its existing research strengths in the areas of cyber incident handling requirements analysis, privacy analysis, forensic requirements analysis, threat analysis, and security ontologies. (CyberSANE Consortium, 2019)

6.3.14 VPF

VPF' exploitation strategy for CyberSANE is focused on the protection of the CII's and the supply chain using the systems developed to improve the cyber security in the port of Valencia. The knowledge gathered during the development of the project will further improve port systems and allow providing consulting services to other companies and ports that need to improve their security. VPF will assess the main port requirements to transfer the solutions along the supply chain. (CyberSANE Consortium, 2019)

6.3.15 LSE

LSE will exploit the knowledge acquired in the project to optimize its system security and daily operation. We will deploy and operate the CyberSANE system in order to support our

D11.1 – Dissemination, Communication and Exploitation Plans

incident handling process. In addition, LSE will integrate the positive project outcome into the operational standards of the company and will train its staff to make the best use of it. (CyberSANE Consortium, 2019)

6.3.16 KN

KN exploitation strategy for CyberSANE aims at improving the security awareness within their organization and enhancing their incident handling and response capabilities. The results of the project will be used to define and manage cybersecurity policies in hospital and health services providers. (CyberSANE Consortium, 2019)

Chapter 7 Summary and Conclusion

This deliverable provides information about the activities and strategy to be implemented for the management and execution of communication and dissemination activities within WP11 (T11.1 and T11.2), aiming at positioning CyberSANE among key stakeholders. The communication and dissemination strategy considers the different stakeholders involved in the protection of CII from cyber-attacks, and outlines the main phases and messages that must be communicated and delivered in each stage of the technical development with the purpose of providing visibility, generating awareness and engagement. The definition of the project graphical identity has been established in order to guarantee the coherent and aligned visibility of the project across all the materials developed and activities performed.

A couple of the aforementioned actions have been already initiated, such as the development of the project's website and the social media accounts (Twitter and LinkedIn), in which different messages have been published related to the project objectives, ambitions, expected outcomes, as well as cybersecurity news and fun facts to engage with the audience, according to the Social Media strategy; the development of the first press release which already has had a great impact of publications, especially in Spain; and the setup of actions to manage the reporting of activities within the Consortium.

The deliverable presents the plan for the upcoming years, considering the communication and dissemination objectives, and the activities that will support the achievement of them. Hence, the KPIs for measuring the effectiveness of the plan are presented in order to monitor the effectiveness and plan corrective actions if it is deemed necessary. The actions executed in the upcoming months will be reported on D11.2, D11.4, and D11.6.

CyberSANE Consortium. (2019). Grant Agreement - 833683 - CyberSANE.

Postcron. (24 de 01 de 2020). 8 Surprising Twitter Statistics That Will Help You Get More Engagement. Obtenido de <https://postcron.com/en/blog/8-surprising-twitter-statistics-get-more-engagement/>