Artificial Intelligence Threat Reporting and Incident Response System

D8.2 Plans for Dissemination, Communication, and Exploitation

Project Title:	Artificial Intelligence Threat Reporting and Incident Response System
Project Acronym:	IRIS
Deliverable Identifier:	D8.2
Deliverable Due Date:	30/11/2021
Deliverable Submission Date:	26/11/2021
Deliverable Version:	Final
Main author(s) and Organisation:	Maria Tsirigoti (ICCS)
Work Package:	WP8 Dissemination, Communication and Exploitation of Results
Task:	Task 8.1 Dissemination and Communication Outreach
Dissemination Level:	PU: Public

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Quality Control

	Name	Organisation	Date
Editor	Maria Tsirigoti	ICCS	15/11/2021
Peer Review 1	Gonçalo Cadete	INOV	19/11/2021
Peer Review 2	Nathan Hue	CLS	23/11/2021
Submitted by (Project Coordinator)	Nelson Escravana	INOV	26/11/2021

Contributors

Organisation
CLS
CEA

Document History

Version	Date	Modification	Partner
ToC	06/10/2021		Maria Tsirigoti
v.01	01/11/2021	Input from CLS (exploitation plan)	Irene-Maria Tabakis
v.02	15/11/2021	Input from CEA (clustering activities)	Sebastien Bardin
Final Draft	15/11/2021	Implementation of the input	Maria Tsirigoti
Final Version	24/11/2021	Implementation of the reviewers' comments	Maria Tsirigoti

Legal Disclaimer

IRIS is an EU project funded by the Horizon 2020 research and innovation programme under grant agreement No 101021727. The information and views set out in this deliverable are those of the author(s) and do not necessarily reflect the official opinion of the European Union. The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any specific purpose. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein. The IRIS Consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

Contents

List of Figures

List of Tables

List of Abbreviations and Acronyms

Abbreviation/ Acronym	Meaning
D	Deliverable
GA	Grant Agreement
ICCS	Institute of Communication & Computer Systems
EU	European Union
EC	European Commission
WP	Work Package

Executive Summary

Task T8.1 ‘Dissemination and communication outreach’ of work package WP8 ‘Dissemination, Communication and Exploitation of Results’ undertakes project dissemination and all public communication outreach activities with the aim to promote and disseminate the project’s accomplishments as broadly as possible. The current document D8.2 ‘Plans for Dissemination, Communication and Exploitation’ is the main output of Task 8.1 and outlines the communication and dissemination strategy we have devised for IRIS project along with the plan to be followed within the project to ensure significant engagement with key stakeholders and audiences during the project.

The project's dissemination, communication and exploitation plan, is a step-wise process that includes all incremental steps, such as:

- ✓ definition of main objectives for Dissemination and Communication.
- ✓ identification of the project key audiences and the messages to be used to reach out to them,
- ✓ the means and channels to be used.
- ✓ the dissemination process to be followed by individual partners.
- ✓ the initial communication and dissemination tools that are created for maximizing awareness about the project and communicating the proper messages across stakeholders.
- ✓ the exploration of the means of delivering the IRIS innovations to the market.

The IRIS dissemination, communication and exploitation strategy is dynamic and should be adapted both according to time and project results. In the beginning of the project, it is vital to quickly communicate the project's goal and expected impact. On a later stage, and as project results are becoming available, communication and dissemination activities need to focus on the presentation of these results to specific audiences. Emphasis will be given in activities and channels that will be able to maximise the project results' impact while still providing the general project's vision and how this is facilitated.

All partners are expected to take part in the aforementioned activities on a different scale, appropriate for each partner's role and individual plans within the project.

1 INTRODUCTION

1.1 Project Introduction

As existing and emerging smart cities continue to expand their IoT and AI-enabled platforms, this introduces novel and complex dimensions to the threat intelligence landscape linked with identifying, responding and sharing data related to attack vectors, based on emerging IoT and AI technologies.

IRIS's vision is to integrate and demonstrate a single platform addressed to CERTs/CSIRTs for assessing, detecting, responding to and sharing information regarding threats & vulnerabilities of IoT and AI-driven ICT systems. To achieve this, IRIS brings together experts in cybersecurity, IoT, AI explainability, automated threat detection, response, and recovery.

IRIS aims to help European CERTs/CSIRTs minimise the impact of cybersecurity and privacy risks as well as threats introduced by cyber-physical vulnerabilities in IoT platforms and adversarial attacks on AI-provisions and their learning/decision-making algorithms.

The IRIS platform will be demonstrated and validated on three (3) highly realistic environments with the engagement of 3 smart cities (Helsinki, Tallinn and Barcelona) along with the involvement of national CERTs/CSIRTs, and cybersecurity authorities.

The project duration extends from September 2021 to August 2024.

1.2 Deliverable Purpose

This document presents an overview of how the dissemination, communication and exploitation objectives will be achieved and provides the framework to guide dissemination and communication activities within IRIS project. It identifies the target groups for dissemination and communication activities and explains the way they will be reached and the channels that will be used. It describes the main communication and dissemination tools to be developed to create awareness and achieve a high level of impact for the project and its outcomes.

1.3 Intended Readership

This is a public deliverable. The intended readership comprises the IRIS consortium members, the European Commission's Project Officer of IRIS project and the general public.

It will be of high interest for the consortium members to use it as a reference for planning the project's dissemination, communication and exploitation activities and contributing to raising awareness about the project.

1.4 Structure of the Deliverable

The deliverable D8.2 Plans for Dissemination, Communication and Exploitation is comprised of **9 chapters** and **9 annexes**. The first chapter introduces the reader to the IRIS project. It describes the scope of the current deliverable, the audience that is addressed to, its relation to other WP8 deliverables and tasks and defines the key concepts used. The second chapter presents the dissemination and communication approach and objectives, targeted audiences and the messages that will be used. The third chapter presents the project's identity and templates, whereas the fourth chapter presents the suitable tools and channels planned to be used and sets the success criteria for evaluating the performed dissemination activities per year within the IRIS project. The fifth chapter refers to the obstacles that the project faces regarding their dissemination and communication activities due to the COVID-19 pandemic. The sixth chapter presents the IRIS consortium's role and forms a roadmap accompanied by a preliminary action plan and informs about the dissemination procedures used within IRIS. The seventh chapter presents the Key Performance Indicators agreed in the G.A and the eighth chapter shortly refers to the Exploitation plan that will be followed by the consortium partners. Lastly, the ninth chapter concludes this document.

1.5 Relation with other Deliverables and Tasks

The deliverable D8.2 'Plans for Dissemination, Communication and Exploitation' is the main output of task T8.1 and is also linked to tasks T8.2 'Market analysis, business models and exploitation', and T8.3 'Clustering Activities'. Furthermore, it is closely related to the following project deliverables:

D8.1: Project website, which presents in detail the structure of the official project's website;

D8.3: Initial report on dissemination, communication, standardisation and exploitation, which will include all dissemination and communication activities that have been undertaken, during the first twelve months of the project, and those still planned;

D8.4: Interim report on dissemination, communication, standardisation and exploitation, which will include all dissemination, communication and standardisation activities that have been undertaken, during the first two years of the project, and those still planned;

D8.5: Final report on dissemination, communication, standardisation and exploitation which will document all dissemination, communication and standardisation activities that have been undertaken, during the second half of the project duration. It will also summarise the most important dissemination, communication and standardisation achievements of IRIS during the project lifetime.

Beside the above-mentioned tasks and deliverables, the document has a close indirect relation to all project's achievements that need to be disseminated and communicated.

1.6 Key Concept Definitions

Dissemination, Communication and Exploitation are key elements for the success of any H2020 project. The table below presents their differences based on the IPR helpdesk brochure "Making the Most of Your H2020 Project. Boosting the impact of your project through effective communication, dissemination and exploitation" [1].

	Dissemination	Communication	Exploitation
Definition	The public disclosure of the results by any appropriate means (other than resulting from protecting or exploiting the results), including scientific publications in any medium.	Communication on projects is a strategically planned process that starts at the outset of the action and continues throughout its entire lifetime, promoting the action and its results. It requires strategic and targeted measures for	The utilisation of results in further research activities other than those covered by the action concerned, or in developing, creating and marketing a product or process, or in creating and providing a service, or in standardisation activities.

	Dissemination	Communication	Exploitation
		communicating (i) the action and (ii) its results to a multitude of audiences, including the media and the public and possibly engaging in a two-way exchange.	
Objectives	Transfer knowledge & results with the aim to enable others to use and take up results, thus maximising the impact of EU funded research.	Reach out to society and show the impact and benefits of EU-funded R&I activities, e.g., by addressing and providing possible solutions to fundamental societal challenges.	Effectively use project results through scientific, economic, political or societal exploitation routes aiming to turn R&I actions into concrete value and impact for society
Focus	Describe and ensure results available for others to use. Focus given on results only	Inform about and promote the project and its results/success.	Make concrete use of research results (not restricted to commercial use.)
Target Audiences	Audiences that may take an interest in the potential use of the results (e.g., the scientific community, industrial partners, policymakers).	Multiple audiences beyond the ' 'project's own community incl. Media and the broad public.	People/organisations including project partners themselves that make concrete use of the project results, as well as user groups outside the project

Table 1: Key Concept Definitions

2 DISSEMINATION AND COMMUNICATION PLAN

2.1 Approach

The IRIS Dissemination and Communication plan will be based on a five-step approach, as presented below:

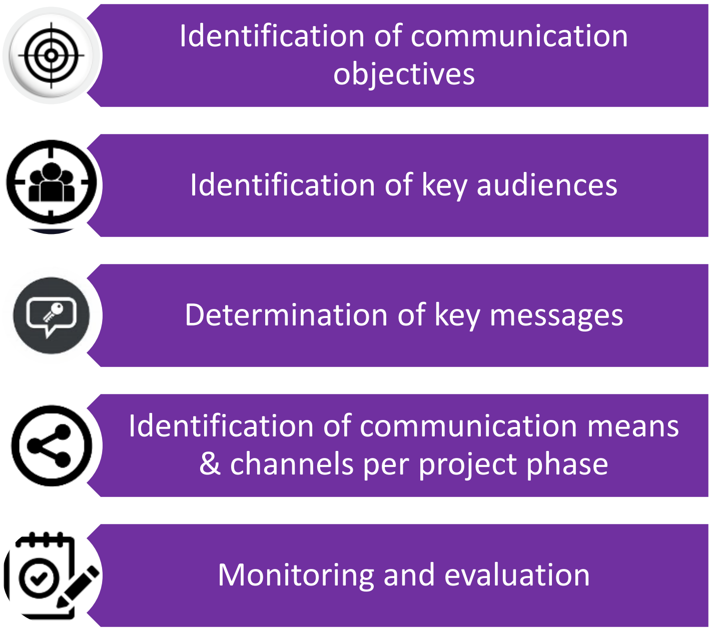

Identification of communication objectives
Identification of key audiences
Determination of key messages
Identification of communication means & channels per project phase
Monitoring and evaluation

Figure 1: The five-step approach

2.2 Dissemination and Communication Goals

The first step in having a Dissemination and Communication strategy is to clearly set the goals to be achieved and then define the suitably designed activities in order to meet those goals.

The goals of all dissemination and communication actions can be summarised as follows:

- ✓ To raise public awareness about the project, providing a clear view of the project's vision, goals and how the expected solutions will positively affect the European citizens' life.
- ✓ To identify the suitable channels and means for communicating the project's progress and outcomes both to the identified stakeholders and to non-technical audiences.
- ✓ To liaise with relevant EU-funded projects to create strong cooperation links and exchange knowledge.
- ✓ To inform the European CERTs/CSIRTs about the added value that the realization of the innovations brings-in.
- ✓ To disseminate IRIS scientific results and receive useful feedback from other scientists and relevant key expert communities, interested in the respective topic.

2.3 Key Audiences

The key element for maximizing the project's potential impact, is the definition of the key audiences and the understanding of their special characteristics and needs so that we could direct the resources to the most relevant and interested actors.

Key Audiences → Communication Channel ↓	Decision-makers & Public Authorities	CERT/ CSIRTs	European/ international organizations & networks for cybersecurity	EU City authorities and Smart City Research Centers	Academic and scientific actors	General Public
Website		✓	✓	✓	✓	✓
Social media			✓	✓	✓	✓
Dissemination material	✓	✓	✓	✓	✓	✓
Video	✓		✓	✓		✓
E-newsletters		✓	✓	✓	✓	✓
Press Activities	✓	✓	✓	✓	✓	✓
Participation in conferences /events	✓	✓	✓	✓	✓	✓
Scientific publications			✓	✓	✓	
Training		✓			✓	
Workshops/Webinars		✓	✓		✓	
Final Event	✓	✓	✓	✓	✓	✓

Table 2: Communication *Channel per* Key *Audience*

2.4 Key Messages

There is a number of key messages that can be used by the project partners in order to present the vision of the project and provide a coherent branding of the project. The key messages should be considered a baseline, meaning they should be adapted depending on their possible use and the targeted audience.

2.4.1 General Message

As existing and emerging smart cities continue to expand their IoT and AI-enabled platforms, this introduces novel and complex dimensions to the threat intelligence landscape linked with identifying, responding and sharing data related to attack vectors, based on emerging IoT and AI technologies.

IRIS's vision is to integrate and demonstrate a single platform addressed to CERTs/CSIRTs for assessing, detecting, responding to and sharing information regarding threats & vulnerabilities of IoT and AI-driven ICT systems. To achieve this, IRIS brings together experts in cybersecurity, IoT, AI explainability, automated threat detection, response, and recovery.

IRIS aims to help European CERTs/CSIRTs minimise the impact of cybersecurity and privacy risks as well as threats introduced by cyber-physical vulnerabilities in IoT platforms and adversarial attacks on AI-provisions and their learning/decision-making algorithms.

2.4.2 Key Words

- Exercise and simulation training,
- Risks and vulnerabilities assessment,
- Cybersecurity, Information Security Technologies,
- Autonomous cyber threat analytics,
- Collaborative threat intelligence,
- MeliCERTes enhanced trusted and secure collaboration,
- Cyber range for training and testing automated remediation strategies.

2.4.3 Tailored Key Messages

The table below presents the different key messages per target audience. The target audiences are also mentioned in section 2.3:

Target Audiences	Key Message
1. Decision-makers & Public Authorities 2. European/international organizations & networks for cybersecurity 3. Academic and scientific actors 4. General Public	IRIS contributes towards a European strategic autonomy in IoT and AI cybersecurity
1. Decision-makers & Public Authorities 2. CERTs/CSIRTs 3. European/international organizations & networks for cybersecurity 4. EU City authorities and Smart City Research Centers	IRIS equips CERTs/CSIRTs with a state-of-the-art incident response toolkit to mitigate large-scale cybersecurity incidents
1. Decision-makers & Public Authorities 2. CERTs/CSIRTs 3. European/international organizations & networks for cybersecurity 4. EU City authorities and Smart City Research Centers	IRIS addresses the key challenges on the IoT and AI cybersecurity threads with a collaborative-first approach, centered around CERTs/CSIRTs
1. Decision-makers & Public Authorities 2. CERTs/CSIRTs 3. European/international organizations & networks for cybersecurity 4. EU City authorities and Smart City Research Centers 5. Academic and scientific actors 6. General Public	IRIS will provide hands-on, collaborative & immersive cybersecurity training
1. Decision-makers & Public Authorities 2. CERTs/CSIRTs 3. European/international organizations & networks for cybersecurity 4. EU City authorities and Smart City Research Centers 5. Academic and scientific actors 6. General Public	IRIS provide a set of tools that will help CERTs and CSIRTs tackle IoT and AI related cybersecurity threats
1. Decision-makers & Public Authorities 2. CERTs/CSIRTs	IRIS aims to help European CERTs/CSIRTs minimise the impact of cybersecurity and privacy risks as well as threats introduced by

Target Audiences	Key Message
3. European/international organizations & networks for cybersecurity 4. EU City authorities and Smart City Research Centers 5. Academic and scientific actors	cyber-physical vulnerabilities in IoT platforms and adversarial attacks on AI-provisions and their learning/decision-making algorithms
1. Decision-makers & Public Authorities 2. CERTs/CSIRTs 3. European/international organizations & networks for cybersecurity 4. EU City authorities and Smart City Research Centers	IRIS will help on the preparation of CERTs/CSIRTs to collaboratively protect critical infrastructures and systems against cross-border AI and IoT threats
1. Decision-makers & Public Authorities 2. EU City authorities and Smart City Research Centers 3. Academic and scientific actors 4. General Public	IRIS will provide European Smart Cities with a cybersecurity solution that will protect their critical infrastructures

Table 3: Key Messages per Target Audiences

3 PROJECT IDENTITY AND TEMPLATES

3.1 Project Identity

The IRIS project has been trying to build a strong project identity through effective branding and delivering clear messages to a variety of target audiences. To this end, a project's logo, a colour palette, a dedicated brand book was designed to create a consistent appearance that will be used throughout the whole project in all applicable communication and dissemination channels (website, leaflets, poster, templates, and presentations). This is the most effective way to ensure that a consistent identity of IRIS is widely communicated. The official logo, the colour palette and the brand book are all available in IRIS repository for the IRIS partners and on the website for the general public.

3.1.1 Logo

A dedicated logo has been agreed by the project's partners since the proposal of the project and later on it was optimised in order to act as a trademark, promote instant public recognition and trigger reactions from the viewers even from the first performed communication and dissemination activities.

IRIS's logo was chosen to be simple, easily recognizable and attractive so that people could immediately differentiate it among others. The IRIS project logo focuses on its technological dimension through a minimalist approach, giving the project's character as simple and concise as possible for its optimum usability in any visual communication action required.

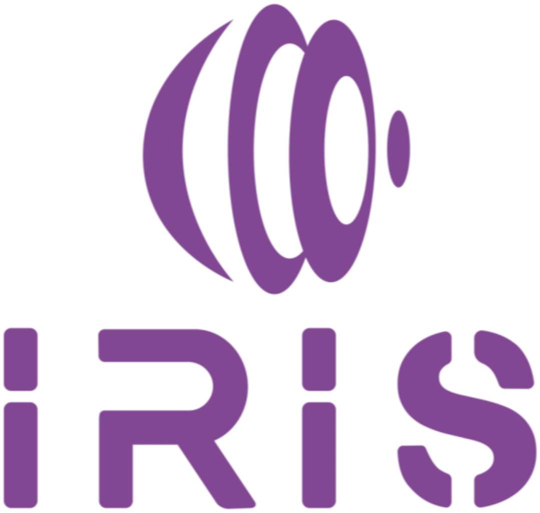


Figure 2: IRIS official logo

3.1.2 Colour Palette

IRIS's logo is made up of a range of colours that were carefully chosen and specified from the very beginning of the project. Keeping the project's colours cohesive in print and digital use creates a strong and consistent visual presence.

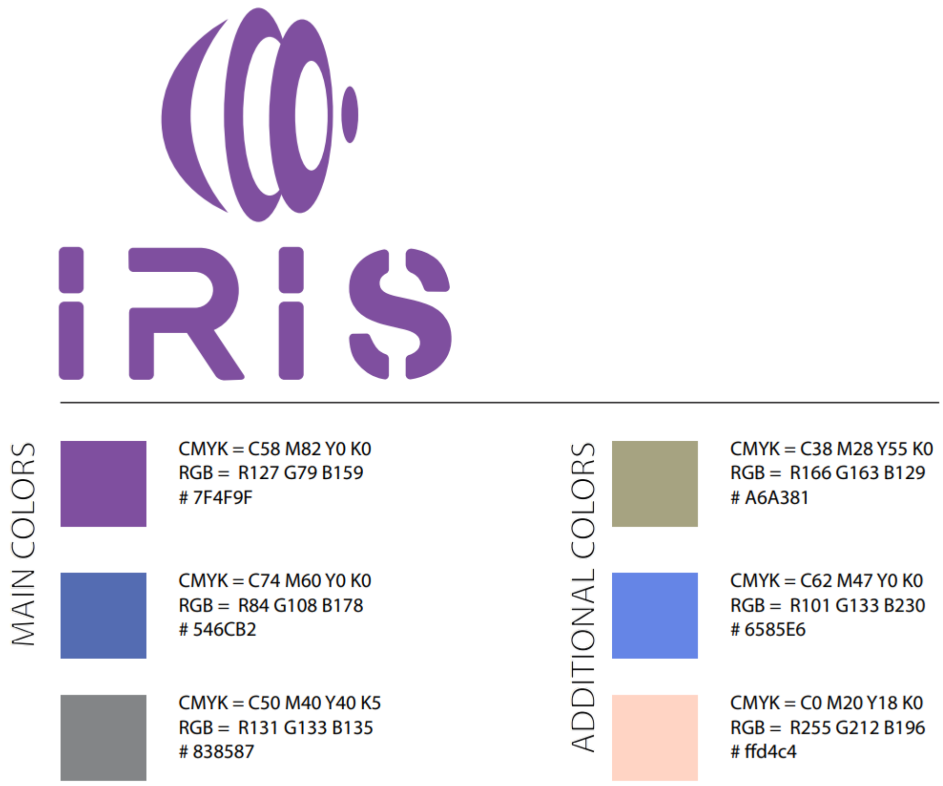
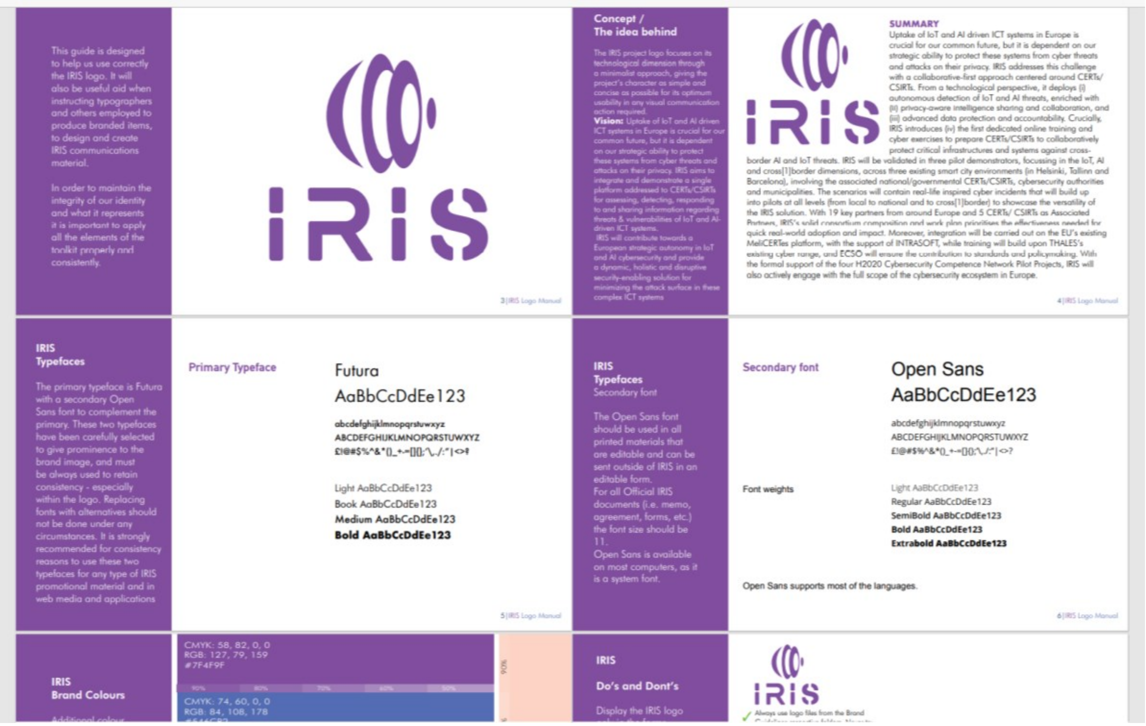


Figure 3: IRIS colour palette

3.1.3 Brand Book

A dedicated brand book was created in order to ensure the proper use of the logo, maintaining the integrity of the project's brand identity and what represents. The brand book contains several logo variations, the colour palette guide, the logo proper and improper use, the social media usage and the brand typography. The Brand Book is available in the website.



This guide is designed to help us use correctly the IRIS logo. It will also be useful aid when instructing typographers and others employed to produce branded items, to design and create IRIS communications material.

In order to maintain the integrity of our identity and what it represents it is important to apply all the elements of the toolkit properly and consistently.

3|IRIS Logo Manual

Concept / The idea behind

The IRIS project logo focuses on its technological dimension through a minimalist approach, giving the project's character as simple and concise as possible for its optimum usability in any visual communication action required.
Vision: Uptake of IoT and AI driven ICT systems in Europe is crucial for our common future, but it is dependent on our strategic ability to protect these systems from cyber threats and attacks on their privacy. IRIS aims to integrate and demonstrate a single platform addressed to CERTs/CSIRTs for assessing, detecting, responding to and sharing information regarding threats & vulnerabilities of IoT and AI-driven ICT systems.
IRIS will contribute towards a European strategic autonomy in IoT and AI cybersecurity and provide a dynamic, holistic and disruptive security-enabling solution for minimizing the attack surface in these complex ICT systems

SUMMARY
Uptake of IoT and AI driven ICT systems in Europe is crucial for our common future, but it is dependent on our strategic ability to protect these systems from cyber threats and attacks on their privacy. IRIS addresses this challenge with a collaborative-first approach centered around CERTs/CSIRTs. From a technological perspective, it deploys (i) autonomous detection of IoT and AI threats, enriched with (ii) privacy-aware intelligence sharing and collaboration, and (iii) advanced data protection and accountability. Crucially, IRIS introduces (iv) the first dedicated online training and cyber exercises to prepare CERTs/CSIRTs to collaboratively protect critical infrastructures and systems against cross-border AI and IoT threats. IRIS will be validated in three pilot demonstrators, focussing in the IoT, AI and cross[1]border dimensions, across three existing smart city environments (in Helsinki, Tallinn and Barcelona), involving the associated national/governmental CERTs/CSIRTs, cybersecurity authorities and municipalities. The scenarios will contain real-life inspired cyber incidents that will build up into pilots at all levels (from local to national and to cross[1]border) to showcase the versatility of the IRIS solution. With 19 key partners from around Europe and 5 CERTs/ CSIRTs as Associated Partners, IRIS's solid consortium composition and work plan prioritises the effectiveness needed for quick real-world adoption and impact. Moreover, integration will be carried out on the EU's existing MeliCERTes platform, with the support of INTRASOFT, while training will build upon THALES's existing cyber range, and ECSO will ensure the contribution to standards and policymaking. With the formal support of the four H2020 Cybersecurity Competence Network Pilot Projects, IRIS will also actively engage with the full scope of the cybersecurity ecosystem in Europe.

4|IRIS Logo Manual

IRIS Typefaces

The primary typeface is Futura with a secondary Open Sans font to complement the primary. These two typefaces have been carefully selected to give prominence to the brand image, and must be always used to retain consistency - especially within the logo. Replacing fonts with alternatives should not be done under any circumstances. It is strongly recommended for consistency reasons to use these two typefaces for any type of IRIS promotional material and in web media and applications

Primary Typeface

Futura
AaBbCcDdEe123

abcdefghijklmnopqrstuwxyz
ABCDEFGHIJKLMNOPQRSTUWXYZ
£!@#$%^&*()_+-=[]{};'\,./:"|<>?

Light AaBbCcDdEe123
Book AaBbCcDdEe123
Medium AaBbCcDdEe123
Bold AaBbCcDdEe123

5|IRIS Logo Manual

IRIS Typefaces
Secondary font

The Open Sans font should be used in all printed materials that are editable and can be sent outside of IRIS in an editable form.
For all Official IRIS documents (i.e. memo, agreement, forms, etc.) the font size should be 11.
Open Sans is available on most computers, as it is a system font.

Secondary font

Open Sans
AaBbCcDdEe123

abcdefghijklmnopqrstuwxyz
ABCDEFGHIJKLMNOPQRSTUWXYZ
£!@#$%^&*()_+-=[]{};'\,./:"|<>?

Font weights

Light AaBbCcDdEe123
Regular AaBbCcDdEe123
SemiBold AaBbCcDdEe123
Bold AaBbCcDdEe123
Extrabold AaBbCcDdEe123

Open Sans supports most of the languages.

6|IRIS Logo Manual

IRIS Brand Colours

CMYK: 58, 82, 0, 0
RGB: 127, 79, 159
#7F4F9F

CMYK: 74, 60, 0, 0
RGB: 84, 108, 178

IRIS

Do's and Dont's

Display the IRIS logo

✓ Always use logo files from the Brand

Figure 4: IRIS brand book

3.2 Templates

A set of IRIS MS office templates has been created based on the project brand in order to be used in all internal and external events. More specifically, two PowerPoint presentation templates have been developed. One to be used for the project internal meetings and one for the public events. Moreover, a word Deliverable template has been prepared for submitting the IRIS deliverables, a Meeting Minutes template for keeping minutes within the Consortium's meetings and an Agenda template. In addition, an IRIS General Presentation has been created and will be used by the partners in communication events.

All the templates are available to all partners on the IRIS repository and are also presented in Annex 1.

4 COMMUNICATION TOOLS AND ACTIONS

4.1 Online Tools

4.1.1 IRIS Website

The IRIS website has been designed to be the backbone of the communications' activities, the main dissemination tool and gateway for everyone interested in the project. It will serve as a key element of engagement with the identified key audiences, and it will remain live for at least 2 years after the project end.

The website presents the project's general description, its objectives and impact, its consortium and project's news. All the public deliverables and scientific publications will be uploaded along with the IRIS dissemination material and the newsletters, which will be downloadable. Finally, there is a Blog section in which partners will write an article based on the work they have performed or will perform within the project. These articles will also be used in the E-newsletters and the project's social media. To ensure smooth production of articles by the partners, a time plan has been created and circulated among the partners. It is also presented in Annex 2 of this document.

All the details regarding the website are included in the D8.1 Project Website which was submitted on M1.

KPI
1 website launched by M2
5000 visitors per year

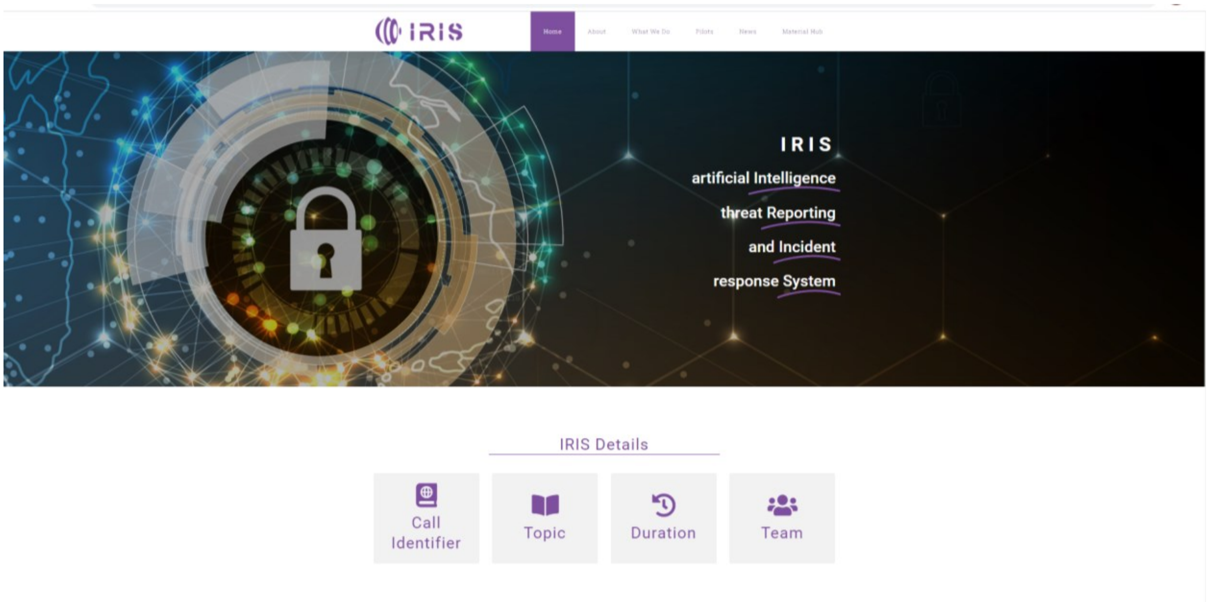


Figure 5: IRIS website

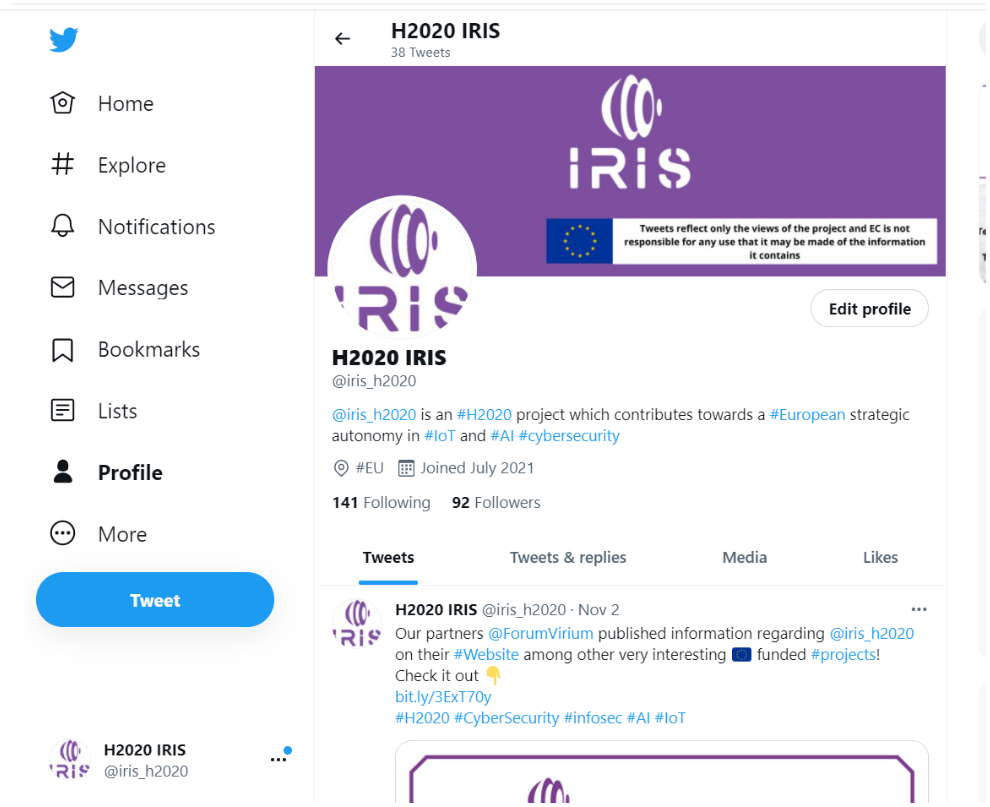
4.1.2 IRIS Social Media

According to the Social media guide for EU funded R&I projects, social media allow us to reach an extremely wide — but also targeted — audience, maximising the impact and successful exploitation of our research results. Therefore, the IRIS project will make extended use of social media platforms, namely Twitter and LinkedIn, in order to create awareness and communicate the project's progress and results as well as to diffuse the project's news and activities.

4.1.2.1 Twitter

Twitter is a social networking platform that is ideal for real-time spreading news and engaging with users. @iris_h2020 is mostly used to raise awareness about the project's progress, interact with key stakeholders, build relationships with other H2020 projects as well as to disseminate the project's news and current results. The twitter account follows EU institutions, agencies and officials, policy officers and staff linked to cybersecurity field, technology and H2020 themes, scientific and research organisations, industry representatives, public authorities, other H2020 projects as well as other targeted audiences' representatives.

KPI
300 followers



H2020 IRIS
38 Tweets

Tweets reflect only the views of the project and EC is not responsible for any use that it may be made of the information it contains

H2020 IRIS
@iris_h2020

@iris_h2020 is an #H2020 project which contributes towards a #European strategic autonomy in #IoT and #AI #cybersecurity

#EU Joined July 2021

141 Following 92 Followers

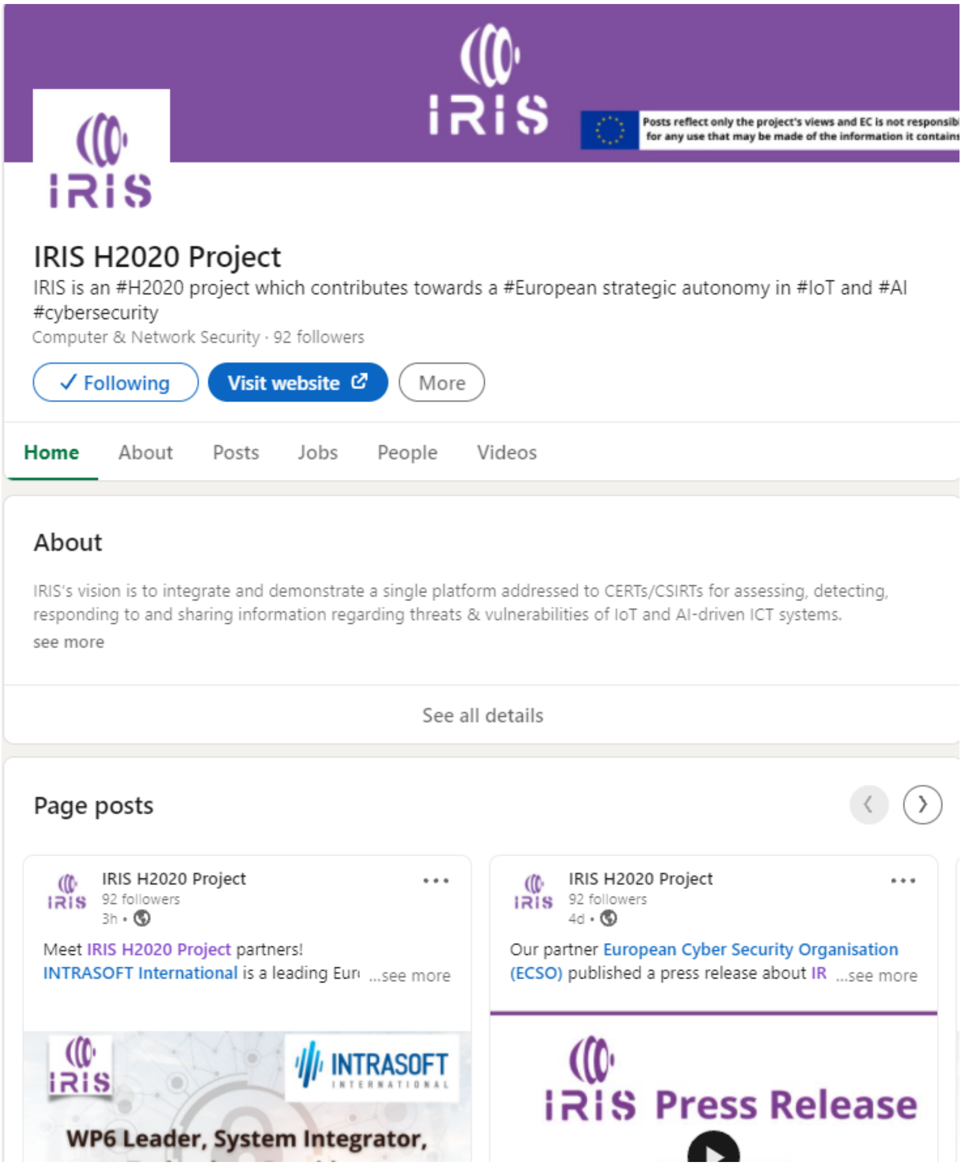
H2020 IRIS @iris_h2020 · Nov 2
Our partners @ForumVirium published information regarding @iris_h2020 on their #Website among other very interesting 🇪🇺 funded #projects!
Check it out 👇
bit.ly/3ExT70y
#H2020 #CyberSecurity #infosec #AI #IoT

Figure 6: IRIS Twitter account

4.1.2.2 LinkedIn

LinkedIn hosts more than 500 million professional accounts thus tends to be the most popular social networking platform and the most powerful among professionals. Registered members are able to establish connections with professionals who are in their interest and interact in group discussions. IRIS H2020 Project account will enable to build a strong network with some of the project's key audiences, such as research institutes, industry, policymakers, and individuals.

KPI
100 followers


IRIS
Posts reflect only the project's views and EC is not responsibl
for any use that may be made of the information it contains
IRIS
✓ Following
Visit website
More
Home
About
Posts
Jobs
People
Videos
See all details
IRIS
IRIS
INTRASOFT
INTERNATIONAL
WP6 Leader, System Integrator,
IRIS Press Release

IRIS H2020 Project

IRIS is an #H2020 project which contributes towards a #European strategic autonomy in #IoT and #AI #cybersecurity

Computer & Network Security · 92 followers

About

IRIS's vision is to integrate and demonstrate a single platform addressed to CERTs/CSIRTs for assessing, detecting, responding to and sharing information regarding threats & vulnerabilities of IoT and AI-driven ICT systems.

see more

Page posts

IRIS H2020 Project
92 followers
3h •

Meet IRIS H2020 Project partners!
INTRASOFT International is a leading Eur ...see more

IRIS H2020 Project
92 followers
4d •

Our partner European Cyber Security Organisation (ECSO) published a press release about IR ...see more

Figure 7: IRIS LinkedIn account

4.1.3 Social Media Hashtags

A hashtag is prefaced by the hash symbol: #. Hashtags is a way to connect social media content to a specific topic, event, theme, or conversation. Moreover, they make it easier to discover posts around those specific topics because hashtags aggregate all social media content with that same hashtag. The usage of specific hashtags will help to increase the post's visibility and the followers' engagement to the posts.

IRIS project has been using the hashtags: #H2020, #CyberSecurity, #EUfunded, #EUresearch , #infosec, #IoT #AI

4.2 Dissemination and Communication Material

4.2.1 Brochure, Roll up Banner

The first version of the IRIS brochure and roll-up banner are available in IRIS repository and the IRIS website for all partners to use at conferences, workshops, meetings and events. A second version of the brochure and another two versions of the roll-up banner will be produced by the end of the project. The first version of the brochure and the roll-up banner are also shown in Annex 3 of this document.

KPI
2 Brochures
3 Roll up banners

4.2.2 Video

A general video, including animations or interviews or live footage, will be created by the end of the project with the main aim to visually explain the project results and solution to non-technical audiences and the general public.

KPI
1 video

4.2.3 E-newsletters

The IRIS e-newsletters will be sent to the dedicated registrants by email. There is a dedicated section on the website in which people can register for the newsletter. They will be also published on the IRIS website and the project's social media. The newsletters will include news and updates on the project’s progress, blog articles written by the consortium and the project’s latest publications. The E-newsletters will be created using Mailchimp which is a marketing automation platform designed and developed for businesses using email to reach out to their target markets.

KPI
6 E-newsletters

4.3 Press Activities

The project's press releases will be developed by ICCS upon specific project's achievements to several media communication channels such as online press, television and radio.

A kick-off press release had been created and is available on the IRIS repository as well as on the project's website. Two more press releases were published by two partners and are available also on their websites (ECSO, TalTech). More partners are expected to publish the IRIS press release, soon.

The IRIS partners will use their press contacts to communicate the developments of the project and will be responsible for translations and regional adaptations. Partners efforts will also focus on publishing major IRIS achievements through channels and means offered by the European Commission (i.e., the Horizon Magazine, research*EU results magazine, Futuris Magazine etc.)

Finally, according to the Article 38 of the IRIS GA, before engaging in a communication activity expected to have a major media impact, the beneficiaries must inform the Agency. Therefore, whenever a communication activity that is expected to reach the general public (not the specialized press or media) like an interview of the Coordinator for the national TV, an article in a national newspaper, etc., is scheduled, the project coordinator should inform the Project Officer.

KPI
6 Press Releases
3 Media Appearances

4.4 Conferences and Events

IRIS project plans to organize its own dissemination events as well as take advantage of other established highly recognizable Cyber-Security, ICT, AI sector conferences, fairs and events to present the project results to a wider audience. The list of identified international conferences and related events where IRIS may present its outcomes is available in the IRIS repository and in Annex 4. The list will be regularly updated to include further dissemination opportunities, while relevant information will be sent to the Consortium on a regular basis via direct mailing.

KPI
18 Conference Presentations
2 Project presentations in main technical events
5 Project presentations in events
3 Demonstration booths

4.5 Publications

IRIS will make a major effort in publishing peer-reviewed scientific papers in high-impact factor peer-reviewed journals and conference proceedings. To assist partners in planning their dissemination activities, a list, including prestigious journals, has been distributed to the

Consortium and is available in the IRIS repository for the consortium and is also presented in Annex 5.

IRIS will sustain the Gold and Green Model, upon which publishing peer-reviewed scientific articles resulting from the project will be available in the open-access model. The EU guidelines regarding the Open Access have been presented to the consortium and are available in the IRIS repository for the consortium, are also presented in Annex 6. Partners have been strongly advised to use Open Research Europe, the new open access publishing platform, for the publication of research stemming from Horizon 2020 funding.

The list of accepted and submitted publications by the CitySCAPE partners will also be maintained and updated.

KPI
3 Publications in journals or conference proceedings

4.6 Networking with other H2020 projects

Networking with other relevant H2020 projects is very important. The synergies will ensure knowledge exchange and avoidance of overlaps and double work. A list of relevant projects has already been created and discussion with the representatives of the H2020 projects will start as soon as possible. IRIS intends to create a cluster of H2020 projects and then proceed in several common dissemination and communication activities.

As a cluster of projects, we could organise common webinars and workshops, participate to each other's plenary meetings, organise special sessions at well-known events, have common booths at conferences, apply to Horizon Booster and many more.

Project	Cordis Information
ERATOSTHENES	cordis.europa.eu/project/id/101020416
SOTERIA	cordis.europa.eu/project/id/101018342
ARCADIAN-IoT	cordis.europa.eu/project/id/101020259
TRUST aWARE	cordis.europa.eu/project/id/101021377
IDUNN	cordis.europa.eu/project/id/101021911
CyberSEAS	cordis.europa.eu/project/id/101020560
SECANT	cordis.europa.eu/project/id/101019645
SENTINEL	cordis.europa.eu/project/id/101021659

4.7 Clustering Activities

We will focus on creating synergies and raising awareness of the IRIS solution's capabilities with the European cybersecurity community. On the one hand, we will conduct dedicated clustering, engagement and awareness raising activities with potential stakeholders. These activities will target the industrial communities, namely the communities that hold more potential in commercially exploiting the results and applying them in daily practice. On the other hand, we will support the Cybersecurity cPPP programme by exploiting synergies and fostering the collaboration with other cPPPs, as well as with the four SU-ICT-03-2018 pilots (CyberSec4Europe, SPARTA, CONCORDIA, and ECHO), with the goal to position IRIS results with regards to existing European cybersecurity roadmaps, and facilitate future technical developments based on those results, and a sustainable exploitation of those results.

Concretely:

- *Three Stakeholders and Industrial Workshops* (SIW) will be held during the project (M16, M26, and M34) where IRIS partners will present the most mature results to industrial stakeholders along with methodological insights. Cross-sector practitioners, policy makers, investors, and researchers will be invited to those workshops to ensure a balanced attendance and fruitful discussions.
    - led by ICCS
    - 3 dedicated workshops (SIW)
- Clustering actions with the cybersecurity community at large through liaising with the SU-ICT-03 pilots (CyberSec4Europe, SPARTA, CONCORDIA, and ECHO) will also be performed. Integration and feedback to SPARTA’s roadmap and participation to relevant partnership activities will be made to maximize the project's impact by improving its positioning in the cybersecurity landscape.
    - led by CEA
    - integration and feedback to the SPARTA roadmap
    - organization of a workshop co-located with a SPARTA event
    - integration to the roadmap and event co-localization with one of the other three SU-ICT-03-2018 pilots

5 DISSEMINATION AND COMMUNICATION CHALLENGES DUE TO COVID19 PANDEMIC

Communication and dissemination actions are an important pillar of the IRIS project and the consortium will ensure that the actions will be delivered despite the challenges created by the COVID-19 pandemic.

Due to the COVID-19 pandemic, many conferences and events are held virtually, some others try to become physical again or at least to become hybrid. IRIS will monitor the situation and will try to participate in as many conferences and events as possible, regardless their format.

Moreover, until the cease of the pandemic, beside the conferences, IRIS will organize webinars along with other EU-funded projects and a podcast series that will promote the project. Finally, it will focus more on its virtual presence through online media, its website, and social media.

6 IMPLEMENTATION OF THE DISSEMINATION AND COMMUNICATION PLAN

6.1 Partners’ Role

ICCS is the Task 8.1 leader and responsible for managing and monitoring the communication and dissemination activities of the IRIS project. ICCS will be engaging with all project partners to ensure that the communication and dissemination activities of the project are effective and impactful. All partners will contribute to the communication and dissemination activities of the project by using all their available networks and communication channels, including websites, press contacts, social networking webpages etc. and through their participation in the main international events, publishing research papers and articles in journals and conferences as it is mentioned in the articles 29.1 and 38.1 of the IRIS G.A.

All partners were asked to plan their dissemination activities (namely participation in events and social media presence) regarding the first phase (M1-M12) of the project's lifetime and fill in the appropriate forms. The template is presented in Annex 7 of this document and the filled forms are available in the IRIS repository for the consortium. The same procedure will be followed for the next two project's phases (M12-M24 & M24-M36).

Also, the consortium partners were asked to fill in a questionnaire, giving their thoughts and opinion about several topics regarding the dissemination and communication of H2020 projects, so that we could all agreed on the steps followed to have a successful communication of the IRIS project. The filled questionnaires are available in the IRIS repository for the consortium’s partners and are also presented in Annex 8.

6.2 Roadmap

The communication roadmap that has been determined for the whole duration of the project, provides an outline of the way that the communications channels and tools will be used for reaching each of the specified key audiences per year of the project. Moreover, a preliminary action plan is presented, showing the planned actions that will be performed per activity in order to have a complete and successful communication of the project and reach the KPIs agreed in the GA. However, not all the communication actions are yet planned, and changes are likely to occur as the project evolves.

The Dissemination and Communication Roadmap is presented below in detail:

Phase & Months	Description	Communication Activities	Planned Actions per activity for successful communication & reaching KPIs	Deliverables
Phase 1 M1-M12	In the first phase of the IRIS project, more emphasis will be given to the communication activities. The dissemination activities will become more	Creation of the **IRIS brand identity** (project logo, colour palette, brand book, templates)	**The brand identity** (project logo, colour palette, brand book, templates) was ready before the KoM	D8.1 Project Website (M2) D8.2 Plans for Dissemination, Communication and Exploitation (M3)
		Creation of **the communication material**	1st version of the brochure and roll-up banner by M3	

Phase & Months	Description	Communication Activities	Planned Actions per activity for successful communication & reaching KPIs	Deliverables
	intensive as soon as the initial project's results will be available, towards the end of this phase. Communication activities will focus on **raising awareness** and **providing information** about the project's vision and expected impact to relevant stakeholders.	Creation of project **website**	The website was launched in M2 and there will be constant content update	
		Set up of **social media** channels and continuous networking	Social media (were ready before the KoM) will reach 100 followers in Twitter & 100 in LinkedIn	
		Publication of **media articles/interviews**	Publication of at least 1 media article or interview	
		Publication of **press releases**	Publication of at least 2 press releases	
		Publication of **e-newsletters**	Creation and publication of 2 E-newsletters	
		Presentations in **conferences** and other **events**	4 conference presentations, 2 project presentations in other events	
		Establishing Liaison & **networking** activities with related projects	Connect with at least 2 H2020 projects	
		Workshops and Webinars/Seminars	1 workshop	
Phase 2 M12-24	The activities will concentrate on the effective communication of the available project results and findings and will try to raise further awareness on project related issues, in a collaborative engaging way.	**Website** and **social media updates**	Weekly updates on the website & social media, reach 200 followers in Twitter & exceed 100 followers in LinkedIn	D8.3 Initial report on dissemination, communication, standardisation and exploitation (M12) D8.4 Interim report on dissemination, communication, standardisation and exploitation (M24)
		Presentations in **conferences** and other **events**	7 conference presentations, 2 project presentations in other events 1 booth	
		Publication of **media articles/interviews**	Publication of at least 1 media article or interview	
		Publication of **e-newsletters**	Creation and publication of 2 e-newsletters	

Phase & Months	Description	Communication Activities	Planned Actions per activity for successful communication & reaching KPIs	Deliverables
		Publication of **press releases**	Publication of at least 2 press releases	
		Establishing Liaison & networking activities with related projects	Organisation of joint activities with other projects	
		Training	1 training session 2 MSc & 4 PhD students supervision	
		Project code repository	1 contribution to open source projects	
		Workshops/Webinars	Organisation of 1 workshop & 1 seminar/webinar	
Phase 3 M24-M36	In the final phase of the project, a major effort will be made in effectively disseminating the final project's **results** to the target audiences to maximize the exploitation and future use of the outcomes.	**Website** and **social media updates**	Weekly updates on the website & social media, reach 300 followers in Twitter & exceed 100 followers in LinkedIn	D8.5 Final report on dissemination, communication, standardisation and exploitation (M36)
		Video	Creation & production of 1 general video	
		Presentations in **conferences** and other **events**	7 conference presentations, 2 project presentations in other events 1 booth	
		Publication of **media articles/interviews**	Publication of at least 1 media article or interview	
		Publication of **e-newsletters**	Creation and publication of 2 e-newsletters	
		Publication of **press releases**	Publication of at least 2 press releases	
		Establishing Liaison & networking activities with related projects	Organisation of joint activities with other projects	
		Training	1 training session 2 MSc & 4 PhD students supervision	
		Project code repository	1 contribution to open source projects	
		International Standards	2 standards contributions	

Phase & Months	Description	Communication Activities	Planned Actions per activity for successful communication & reaching KPIs	Deliverables
		Workshops/Webinars	Organisation of 2 workshops & 2 seminars/webinars	

Table 4: Dissemination and Communication Roadmap

6.3 Dissemination Procedures

In order to ensure high-quality publications, presentations and other communication material, avoid overlaps and possible disclosure of restricted or confidential information as well as monitor and record the project's communication and dissemination activities, the IRIS Dissemination Procedures have been created and should be followed by all partners.

The step-by-step procedure was presented to the Consortium and is available for all in IRIS repository and is also presented in Annex 9.

6.4 EU Acknowledgement

The EU Acknowledgement and the EU flag should be included in all dissemination and communication activities so that it is always clear that the project is funded by the EU. In detail:

1. The EC emblem (flag) and the following acknowledgement text should be included in **all scientific publications (journals/conference proceedings) related to the IRIS work**:

"This work is a part of the IRIS project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021727. This content reflects only the authors' view and the European Commission is not responsible for any use that may be made of the information this publication contains."

2. For **other communication activities**, please add the EC emblem (flag), with the following sentence:

"This work is a part of the IRIS project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021727. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains."

3. For **infrastructure, equipment and major results**, please add the EC emblem (flag) and the following sentence:

"This [infrastructure] [equipment] [insert type of result] is part of the IRIS project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021727. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains."

7 MONITORING OF DISSEMINATION AND COMMUNICATION ACTIVITIES

The table below is showing the Key Performance Indicators regarding the dissemination and communication activities that have been agreed in the G.A. All the activities have and will be designed in such way to reach and in some cases exceed these KPIs.

Action	KPI
Website	5000 visitors per year
Social media	Twitter: 300 followers LinkedIn: 100 followers
Dissemination material	2 brochures 3 roll up banners
Video	1 general video
Press Activities	6 press releases 3 media appearances
E-newsletters	6 e-newsletters
Journal Publications/ Conferences Proceedings	3 scientific papers
Conferences/Events	• 18 presentations in conferences • 7 project presentations ➢ 5 in communications events ➢ 2 in technical events • 3 booth demonstrations
Training	• 3 training sessions • 2 MSc & 4 PhD students supervision
Project code repository	2 contributions to open source projects
International Standards	2 standards contributions
Workshops/Webinars	3 workshops 3 seminars/webinars

Table 5: Key Performance Indicators

8 EXPLOITATION PLAN

The IRIS consortium will work together to design and develop a comprehensive and market-oriented solution for automated threat analytics and intelligence sharing, threat response and self-recovery, as well as for hands-on cybersecurity training. Emphasis will be given to activities that will maximize the market adoption of the IRIS solution throughout the different project phases. More specifically, the exploitation action plan of IRIS will involve:

- **Validation of the IRIS solution through pilots:** the three large scale pilot use cases that the IRIS partners will carry out under 'WP7 – Large-Scale Pilot Demonstration and Evaluation' will demonstrate and validate the benefits of the IRIS solution in real-world settings.
- **Execution of the IRIS dissemination and communication plan:** under the task T8.1 *'Dissemination and communication outreach*', the IRIS dissemination and communication activities coordinated by IRIS's Dissemination & Communication (D&C) manager, will create a link between the consortium and various external stakeholders, raising awareness of the IRIS solution and attracting future adopters.
- **Exploitation and business plan execution:** the IRIS exploitation activities (Task 8.2 - Market analysis, business models, and exploitation) will identify how the participation in the project can maximize the potential benefits for the IRIS partners and the commercialization of the IRIS solution.
- **Promotion of the IRIS results through clustering, liaising and standardization activities:** under the tasks T8.3 *'Clustering activities'*, T8.4 *'Policy recommendation and standardization*' and T8.5 '*Community building and liaison with relevant stakeholders*', the IRIS partners will promote the project's results through liaising with external stakeholders of relevant projects and by contributing to international standards. These activities aim to raise awareness of the IRIS project, especially towards relevant stakeholders and target customer segments.

During the project lifetime, a detailed exploitation plan will be defined, aiming to deliver the IRIS business plan for the exploitation of the results either **individually** or by a group of partners (**joint exploitation**). This plan will initially examine the issues related to the potential exploitation and commercialization strategies of the IRIS solution as well as its viability in the medium term. Towards this direction, all the stakeholders and the interested parties will be identified, while a feasibility study will be conducted to define the **go-to-market strategy**.

Next, we provide an overview of the joint exploitation plan of the IRIS consortium, as drafted during the proposal preparation phase.

8.1 Joint Exploitation Plan, Market Positioning and Tentative Business Plan

Developing a business plan for the commercial exploitation of the IRIS outcomes is a crucial enabler for the project's success. Next, an initial business model plan is presented that was developed by the project's consortium for the joint commercial exploitation of the project's outcomes during the proposal preparation phase.

Market Positioning

The threat intelligence market reached a value of 4 billion USD in 2018 with a projected annual growth rate of 14% and 21% for the next five years [2], [3]. The market growth in this sector is attributed to challenges in the overall information security field such as:

- The amount and complexity of cyber threats (e.g., phishing, ransomware, insider attacks) is rising and thus increasing the risk of cybersecurity incidents for organizations across verticals [2].
- The increased adoption of IoT, BYOD and other networking solutions significantly increases the number of connected devices and thus expands the available attack surfaces [3].
- Strict regulations regarding data protection are imposed on the national/international level (e.g., GDPR), driving organizations to adopt cybersecurity solutions for compliance purposes [3].
- The lack of a consolidated solution to manage cybersecurity creates a complicated landscape for both security engineers, who must implement, deploy, and maintain multiple cybersecurity-related products, and security analysts, who need to interact with different solutions to gather information during incident analysis [4].

The above challenges constitute threat intelligence platforms as critical security tools. Current and forecasted market trends create fertile ground for the development and deployment of next-generation, streamlined solutions which will fulfil the need for evidence-based decision making in cybersecurity. At its current state, the market is driven by large industry players (e.g., Cisco Systems, IBM, Sophos, Symantec, Kaspersky Labs), which continuously expand their product line by acquiring start-ups [2]. North America maintains the major market share (40% in 2018) while, in Europe, the market is continuously growing mainly driven by the need of compliance to regulations and the early adoption of new technologies (e.g., AI, IoT, 5G) in various business sectors [2]. Based on verticals, banking, financial services, and insurance (BFSI) and IT and telecommunication are the leading sectors in adopting threat detection solutions followed by government and defense, energy and utilities, healthcare, manufacturing, transportation, and retail [3]. Finally, in terms of deployment model segmentations, the market is currently dominated by on-premises deployment solutions with a 75% market share. Nonetheless, a solid growth trend (20% predicted annual growth) is observed in cloud deployment solutions, mainly by SMEs, due to the inexpensive nature of this deployment model in terms of infrastructure [3].

Based on the insights gathered from the market analysis, the IRIS consortium has structured an indicative business plan to exploit the project's results. The needs of the threat intelligence market revolve around a comprehensive solution able to cover the novel attack surfaces created by new technologies in modern and interconnected vertical sectors. IRIS aspires to offer such a solution to a broad audience in a dual-release approach. More specifically, since the IRIS consortium favors open-source policies, a demo version of the developed product will be offered free of charge in an open-source manner to gather insights from the experiences of its users. A complete version, exploiting the full capabilities of the IRIS solution, will be made commercially available through a subscription-based model. This does not apply to the penultimate beneficiaries of the IRIS solution, namely the CERTs/CSIRTs. To foster the adoption of the IRIS solution by these teams, the IRIS consortium envisages making its complete version available to CERTs/CSIRTs free of charge. The Business Model Canvas for IRIS that will be devised, will serve as a dynamic business plan observatory and scoreboard able to capture, report and monitor the sequence of steps to be made before IRIS reaches its market potential.

Customer Segments

The initial IRIS business model envisions the following customer segments:

- **Municipal, regional and national CERTs/CSIRTs**, as both providers and consumers of threat intelligence, require privacy-orientated tools that lower the regulatory barriers for sharing threat intelligence. Their analysts also need open threat intelligence and enhanced taxonomies of AI-based threats so they can efficiently identify and respond to these threats. In addition, they need a representative training ecosystem that supports cross-border collaborative incident response and intelligence exercises. Finally, advanced threat telemetry related to emerging IoT, and AI attacks could also help them proactively prioritize risks and vulnerabilities targeting their systems.
- **Smart City end-users** need their sensitive data and physical space to be kept secure and private as a potential breach could cause severe financial consequences damaging their organization's reputation. They also need their IoT and AI-driven systems to be resilient to disruption to be able to trust them and use them.
- **Security analysts** who typically curate and analyze threat intelligence and/or aid ongoing incident response processes need tools that automate response and self-recovery to prevent high-impact attacks. They also need tools and training that can help them identify new IoT and adversarial AI attack vectors. Furthermore, and to deal with high volumes of attack alerts and threat intelligence, they need orchestration capabilities in their cyber threat intelligence toolkits that will enable them to automate the incident response.
- **Cybersecurity education providers**, including consultants, trainers, and academic researchers, require access to a platform where threat intelligence can be disseminated and simulated in training scenarios.

Competitor Analysis

IRIS has assessed the current market landscape intending to highlight the major competitors in the current marketplace, and continuously re-assess our analysis throughout the project's lifetime. Whilst other initiatives provide typical standalone products and solutions (see Table 6), IRIS is the only solution provider that fosters the parallel development and eventual integration of highly novel technologies contributing to the delivery of an automated cyber threat analytics and sharing platform for improving the response of CERTs/CSIRTs to large-scale cybersecurity incidents and crises. Table 6 shows the current landscape of such technologies and specifically IRIS's position in this landscape. It is evident that current offerings cover only a small subset of the requirements addressed by IRIS. Also, the EU is currently severely underrepresented; IRIS will help address this issue.

Product	Offered as a Service	Threat intel sharing	Secure data exchange	Secure comms	Security training	AI-based analytics	Incident Response
Uppercase (US) [5]	✓	✓				✓	
McAfee (US) [6]	✓	✓	✓				
Cyware (US) [7]	✓	✓	✓			✓	
Anomali (US) [8]	✓	✓	✓				
Kaspersky (RU) [9]	✓	✓	✓				

Product	Offered as a Service	Threat intel sharing	Secure data exchange	Secure comms	Security training	AI-based analytics	Incident Response
Microsoft ITP (US) [10]	✓	✓		✓		✓	
Atos ADR (EU) [11]	✓	✓				✓	
Thales CTI (EU) [12]	✓	✓			✓	✓	
MeliCERTes-II (EU) [13]	✓	✓	✓	✓			✓
IRIS (EU)	✓	✓	✓	✓	✓	✓	✓

Table 6: Current landscape of threat intelligence & incident sharing and where IRIS sits

Measurement

The main types of metrics to be used by IRIS are the following:

- **Pre-commercialisation activities** to create early impact and pre-market trials with the key stakeholders.
- **Techno-economic analysis** to evaluate the commercial viability of the project's offerings.
- Analysis of the viability of different schemes (individual, collaborative on individual tools, a start-up or joint venture for the complete platform) through **market analysis, SWOT analysis and road-mapping**. The SWOT analysis will also be used for the evaluation of the different aspects of the product against its competitors and the identification of new market opportunities.
- **Financial reports** used to measure the profit and loss and identify the revenue streams necessary to meet the various overheads.
- **Real-life demonstration performance analysis**, used to highlight the value of the IRIS offering in vertical use cases; and
- **Self-awareness check**, consisting of regular meetings of the IRIS team to evaluate their business development and discuss new business ideas, requirements and opportunities that emerge as the project progresses.

8.2 Individual exploitation plans of the IRIS partners

The advanced technological maturity which will be achieved by the end of the project in various fields and areas of expertise creates significant exploitation potential for all IRIS partners. An initial version of the individual exploitation strategies for each IRIS partner are presented below.

Industrial partners

CISCO:

As we plan to deploy the network infrastructure, the three main goals are:

1. integrating with the newly proposed solution proving new capabilities to maintain and gain a competitive edge in IoT and AI cybersecurity markets,

2. further develop the testbed network we are working with Barcelona City Council to allow third-party companies to test their smart city solutions in a secure and real environment and
3. based on the results and learnings form that project to develop new cybersecurity capabilities to secure future IoT networks.

As a global player in the IT industry, including cyber-security, Cisco Systems can provide several channels through which it can initiate and realize the commercial opportunities emerging from the project:

- Cisco Solution Partner Program allowing prospective partners to build and sell enterprise solutions that require configuration and are implemented in a customer environment. The partnership with Cisco ecosystem enables increased market share, as well as opens global commercial opportunities through Cisco's global sales channels.
- Cisco DevNet - Cisco's developer program to help developers and IT professionals who want to write applications and develop integrations with Cisco products, platforms, and APIs. The key focus areas are IoT, Cloud, Networking, Data Center, Security, Analytics Automation, Open Source, Collaboration and Mobility. It provides an efficient sandboxing and development environment supported by relevant Cisco technical and business development resource to enable future integration within Cisco solutions.
- Cisco Marketplace is an online platform allowing dedicated online presence for Cisco-based approved solutions by creating a storefront for each of the solutions. The presence and links to Cisco website, its global branding and resources increases visibility both among Cisco sales teams as well as customers, leading to sales channels growth, generation of new leads, and expansion into new markets. In addition, potential buyers visiting the Marketplace can quickly search and discover the solutions, learn about them, and connect with the relevant party.
- Cisco Partner Ecosystem includes a world-spanning network of collaborators with Cisco, enabling addressing all technical and commercial needs to realize a market opportunity. The Ecosystem includes:
    a. Developers – to design, test, and build everything from software to solutions to services.
    b. Integrators, - to combine technologies from many different sources to create solutions.
    c. Builders, - to create new private cloud solutions from scratch.
    d. Providers – to use our technology and services to offer other services.
    e. Consultants - to recommend technology and services from us and other partners.
    f. Lifecycle advisors - to help customers choose the right software and services at every stage of the solution.
    g. Distributors – to package up and sell our software, solutions, and services through resellers.
    h. Resellers – to sell our software, solutions, and services directly to the prospective customers.

The partner ecosystem is critical for coverage of the opportunity. Cisco will lead the identification and engagement of key strategic partners for project outputs. This is a critical first step and intermediate commercial solution while other formal partnership routes, such as those set out below, are worked through.

INTRA:

To support growth and innovation in its products and services portfolio, INTRA participates actively as a project and/or technical coordinator, as well as technology provider, in EU-funded research and development projects, that among others facilitate know-how exchange and business alliances. Furthermore, through its participation in IRIS, INTRA is specifically expecting to:

- Exploit the resulting enhanced MeliCERTes IRIS ecosystem in its current products and services as provider of AI-enabled services/products in diverse market segments. The respective offering could be bundled with its products and services to promote a cybersecurity and threat intelligence sharing culture to its clientele. INTRA is particularly interested to remain close to fast developments in the respective cybersecurity arena.
- Join in joint exploitation paths of the IRIS technological platform with the consortium partners, including of course open sourcing the resulting integrated platform, following the MeliCERTes CSP and MISP paradigms, to allow for wider adoption in the relevant communities
- Investigate the possibility of offering IRIS as a service ecosystem in collaboration with the rest of the Consortium partners (i.e., customization, maintenance, installation, service provision, training).
- Deliver consultancy services to customers interested in deploying similar infrastructures.

ATOS: Atos is a global leader in cybersecurity offering end-to-end security services and well positioned to prepare, implement, and manage sustainable long-term security models, crafted to individual industry sector conditions, for bold IoT and IoE adoption. The activities that Atos will develop in IRIS will allow not only to preserve the current business but also to extend it and provide our clients with the cutting-edge technology that impulses their business. In particular, the advances in threat intelligence and incident response suggested by IRIS project perfectly with the ATOS commitment to provide security, smart and trustworthiness IoE solutions.

Atos offers different types of solutions for cybersecurity, ranging from monitoring and analysis of data transfer to active protection and reaction to cyber critical infrastructures, all together with innovative solutions in a unique portfolio. The involvement of Atos in the development of risk & vulnerability assessment and, threat analytics and detection modules will entail new business opportunities increasing our solutions and services portfolio. For this purpose, the first step is to approach the market through the Atos sales team and to promote the adoption of innovative solutions and emerging technologies. On other hand, Atos is fully committed with the technology transfer derived from R&D projects, promoting an inside-out technology push. Even more, Atos Research & Innovation department serves as the catalyst for innovation, through the different IT Labs, through robust partnerships like the one with Siemens, through Start-up's mechanisms, etc. This project will be carried out by the R&D team of the Cybersecurity Lab who will ensure a continuous investigation in that area after the project. In this sense, the exploitation of IRIS results in current and future R&D projects is also of key importance for the company. Other exploitation activities will be establishing partnerships with the rest of Europe increasing our competitiveness, having the opportunity of exchange know-how with research institutions, public administrations, and industrial partners.

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

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

The innovations brought by IRIS will allow specializing the cyber range platform towards advanced CERT/CSIRT usage, both from a technical and methodological standpoint.

Small and Medium-sized Enterprises

CLS: CyberLens (currently traded as Exalens) is interested in exploiting the outcomes of research and innovation projects by developing and releasing "products" that meet a set of quality requirements such as software tested, accompanying documentation, installation guidelines and best practices.

CLS intends to gain insights from the IRIS project results to reinforce the company's position through the advancement of its products, especially by expanding its existing software (Nightwatch) to address interconnected threats and propagated vulnerabilities in complex ICT infrastructures, systems, and services.

Furthermore, CLS will attempt to showcase the added value that could be brought based on the IRIS results in domains not relevant to the project's scopes (e.g., security approaches applicable to healthcare, maritime, smart power grid, and industrial control systems).

Moreover, CLS will aim to identify opportunities for technology transfer into the industry, e.g., by transferring technological know-how and/or integrating the software components developed in the proposed project in future collaborations with industrial partners, e.g., software vendors, SMEs, and consultants, in the Netherlands and the rest of the EU.

New business collaborations resulting from IRIS will give CLS the capacity to transform its line of business apps in intrusion detection to solutions relevant to incident response & recovery.

CEL: CEL has the following exploitation goals:

- Acquisition of knowledge related to IoT and AI technologies impact on society.
- Reinforce CEL position in the market as an innovative service provider.
- Enlarge CEL network to create new opportunities with new partners and customers for further strategic services.
- Create awareness through a strong dissemination and communication action on the project field.

The approach and activities to achieve the exploitation plans include:

- Provide privacy and ethics compliance in new and emergent sectors.
- Enhance consultancy services for clients such as the public administration or private companies.
- Formulate new training courses in the educational field.
- Reinforce company business model based on Privacy and Ethics as Service. Participate to further research and innovation activities.

SID: SID will engage the target audience about the technological benefits of IRIS, including the deployment of secure infrastructure and software. SID will also take advantage of IRIS' findings on Cyprus and Southern Europe's activities and private domain. To show the benefits of IRIS in dealing with cyber threats, SID will develop connections and exchanges with private sector companies during 2022 in Cyprus.

Stakeholders

ECSO: IRIS objectives are in line with the ongoing work in ECSO. The project outcomes will be able to leverage ECSO's policy engagement activities and ECSO's broad cybersecurity community which is supported by the European Commission. ECSO's network of members includes all categories of stakeholders representing 27 EU Member States. This network will be utilized to transfer and scale up project outcomes at the EU, regional, national, and local levels. Furthermore, ECSO will align project outcomes with its own activities in WG3 on strengthening Cyber Resilience of Economy, Infrastructure and Services through the CISOs European Community, WG1 on standardization and Certification, and WG5 on Education, Skills and Cyber Ranges. Finally, ECSO is in a good position to align project outcomes with market demand, cyber range environments, and relevant EU policies and strategies.

ECSO will ensure exploitation through:

i. European level outreach - reaching national / regional / local stakeholders through its members
ii. Leveraging on social media presence to communicate results and messages beyond the lifetime of the project
iii. Linking project outcomes with the activities of ECSO WGs (especially WG1, WG3, and WG5) and the CISO Community
iv. Advocating for alignment of project outcomes with existing EU policies and strategies

esCERT: esCERT will exploit the insights gained from its participation in PUC1 to extend the capabilities of the Barcelona IoT and Smart City infrastructure while also significantly strengthening its cybersecurity posture. Another expected benefit from esCERT's participation in IRIS is the background knowledge that it will gain which will facilitate participation in future projects in the public and private sectors.

KEMEA: KEMEA as the think tank of the Hellenic Ministry of Citizen Protection regarding to security policies, R&D and innovation actions will bring the IRIS project's outcomes to the attention of the Ministry and will promote the project's validated solutions as prototype to the Ministry's supervised and associated entities to enhance and support the First Responders services. KEMEA will exploit the IRIS platform to enhance its research expertise, consultancy services and portfolio in the relevant security domain.

IMI: As a public administration, Institut Municipal d'Informàtica (IMI) will exploit the results of IRIS proposal to impulse new public services and improve the existing ones. Thanks to the knowledge generated during the project and the pilot conducted in Barcelona, IMI will have the opportunity to test new architectures were Cloud and Edge will have a central role.

The information and experience gathered during the project will be useful to inspire and provide orientation to future development of tools that help on the management of increasing municipal resources and generate reporting for services stakeholders (users, contractors, public responsible, infrastructure coordinators and infrastructure contractors). In this domain, the project will help to energize and generate opportunities to the local companies working in the technological domain, helping them to become more competitive.

FVH: FVH will exploit the project results through the Urban Open Platform and Lab, which will design and trial various jointly created smart city pilots, like IRIS, in a real-life environment, such as autonomous cars, smart street lighting etc. also aspires to create smart and sustainable models for future cross-border smart cities.

CERT-RO: In accordance with the requirements of the NIS directive, CERT-RO plays the role of the national competent authority. CERT-RO also plays the role of Single point of contact at national level for cyber issues and National CSIRT. Thus, ensuring cyber security is part of our CERT-RO interests. At national level, CERT-RO will exploit outcomes of the project to strengthen the cyber security level. The project will be useful to expand the partners' collaboration network regarding new research and development initiatives.

Academic and Research Partners

INOV: INOV will carefully study the project results and define a specific strategy accordingly with each specific output. Since INOV is a private non-profit research institute, direct commercial exploitation is not a goal. However, INOV plans to exploit the project results by using the know-how gained through the IRIS project to explore new business opportunities, either related to the project itself or the technologies developed and demonstrated by the Consortium. The exploitation will mainly consist of an extended collaboration with the project partners after the project, aiming to license the DLT technology developed for industrial partners and the prosecution of further research and partnerships for results exploitation.

CERTH: CERTH plans to exploit the IRIS project results by reinforcing its research competencies in the area of Cyber Threat Intelligence (CTI) enrichment through advanced CTI extraction, analysis, and correlation techniques, and also by building and updating cybersecurity-related dynamic taxonomies and ontologies in an (semi-) automated manner, as well as in the area of sharing CTI among relevant stakeholders. Furthermore, CERTH aims to exploit the outcomes of IRIS by commercialising the developed modules : (1) through the Information Technologies Institute of CERTH that has all the necessary legal and business management support in order to create innovative enterprises, or (2) through its spinoff company Infalia (www.infalia.com) which is also active in the cybersecurity domain through its participation in the SPIDER project (https://spiderproject.eu), or (3) by licensing the developed services to interested clients. Furthermore, part of CERTH's business plan is to participate in joint spin-off commercial companies capable of exploiting its research when new market needs and solutions are identified.

CEA: IRIS will complement the efforts of CEA List to develop and transfer its binary-level code analysis platform BINSEC. Thanks to IRIS, CEA List will lift its cyber-reasoning capabilities to detect vulnerabilities, opening both new research lines towards increasingly complex attacks and a new application domain to its core technology. IRIS will also set to CEA List the opportunity to showcase both its technology and its skills through the demonstrator. These activities will benefit from the proactive technology transfer mission of CEA List to its partners by means of the following mid- to long-term mechanisms:

1. Joint Laboratories, consisting of specific contracts aiming at transferring some well-defined intellectual property from CEA to industry, possibly using a team of dedicated personnel,
2. patents and intellectual properties sale, and
3. the creation of start-up companies.

These means have already been applied in the LSL laboratory in the recent past, thus demonstrating their potential and effectiveness.

ICCS: Exploitation targets include the production of research results, of knowledge dissemination and of pursuing the potential of a spin-off company to exploit established experience in Cybersecurity training by deploying simulation environments. The main target group will be CERTs/CSIRTs at national and European level. The above goals will be achieved:

i. At a scientific level, it will acquire in depth knowledge with respect to technologies enabled on cyber preparedness and protection tools and environments as well as enhance its visibility through collaborating with strategic industrial players of the consortium thus adding an application-oriented direction in its activities.
ii. At an R&D level, the gain of experience and increased reputation in the field of Cybersecurity competent authorities and actors through IRIS will enable successful participations of ICCS in future related R&D projects.

TUD: TUD will be planning to exploit the project results by reinforcing its research and engineering competencies in the areas of secure data encryption, data recovery and DLT. Furthermore, TUD will be aiming to exploit the project results in a commercial manner through local Dutch companies and industrial partners, e.g., Philips, and Dutch Blockchain Coalition.

TUD will be planning to exploit the outcomes of IRIS in a commercial manner through its industrial partners or licensing the developed services to interested partners. The university has all the necessary legal and business management support to collaborate with innovative enterprises.

TALTECH:

- Understanding better the existing and possible future cybersecurity risks for the cities, research institutions, companies using Urban Data Platforms (UDP) for developing their services, business models, activities.
- UDP is a basis for visualization of e.g., city infrastructures data and an attack that manipulates the data can result in diminished number of users for the UDP (loss of trust). Therefore, a functioning cyber-threat information sharing, and analytics system is a “must-have” for UDP.
- The risk of cyber-attacks can be a reason for the cities and companies to refuse to use the UDP or to submit their data to the UDP. Having a working solution for this problem could enhance the use of UDP by different stakeholders.

TalTech Smart City of Excellence FinEst Twins (FT-CoE) is developing in close collaboration with FVH an urban open data platform (UOP) that brings together data flows across different city systems like infrastructure, environmental sensors and from private and public sectors. One of the goals of FT-CoE is to enhance the use of UOP in cross-border context of the cities of Tallinn and Helsinki, with up-scaling possibility to other cities in Estonia and Finland. The data that comes into UOP is translated into open standards and is ready to be further developed by public, private sector or by people to solve different social, environmental and economic problems. In Europe, Urban Data Platforms (UDP) are being developed in ca 80 cities. UDP is becoming an important information and communication channel for people as well as for public and private sectors. Therefore, the IRIS project offers a great possibility for TalTech FT-CoE to understand better cybersecurity risks connected with UDP and test solutions for protecting the data flows from IoT devices. The results of the projects could be up-scalable for other cities using UDP-s and offer a good basis for information sharing and for debating cybersecurity risks and solutions with other EU cities.

9 CONCLUSION

IRIS project is considered to have a major impact on the cybersecurity sector and in order to maximize this impact, the project results will be communicated to a wide scientific community, CERT/CSIRTs, decision-makers and public authorities, CERTs/CSIRTs, European and international organizations and networks for cybersecurity, European city authorities and smart city research centers, as well as the general public.

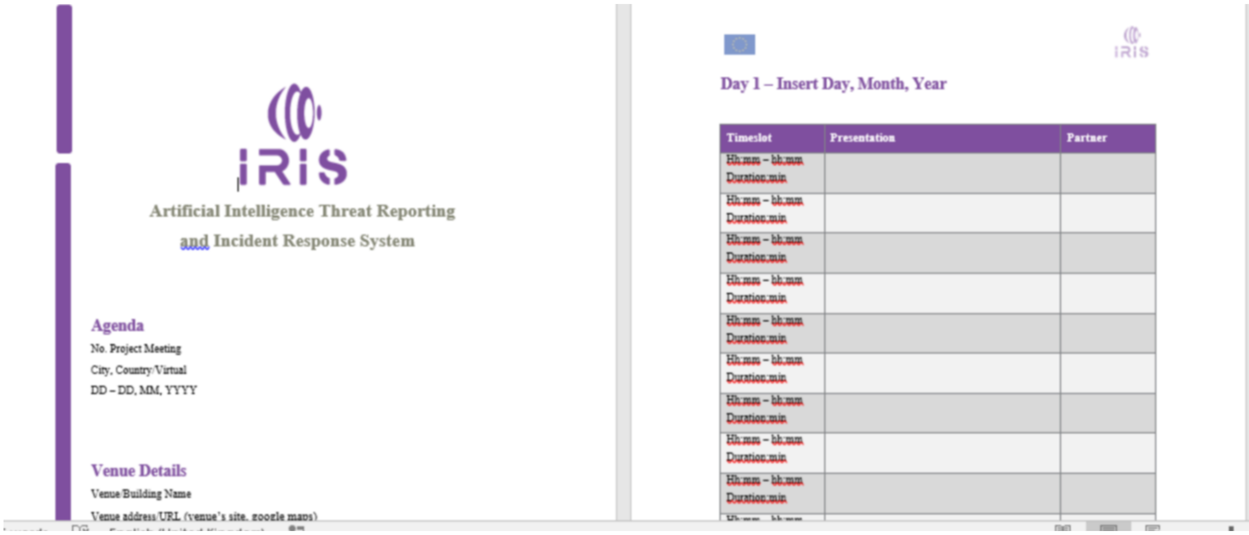
This deliverable D8.2 'Plans for Dissemination, Communication and Exploitation' presents information on the most suitable dissemination and communication activities that will be adopted by the IRIS project. A set of communication and dissemination tools are (and will be) in place to serve communication and dissemination purposes. These include, but are not limited to: a website, brochures and roll-up banners, e-newsletters, a video, press releases, social media presence, workshops and events. All dissemination and communication activities will be monitored and evaluated across well-defined KPIs to ensure maximum impact of project results. Moreover, the significant exploitation potential for all IRIS partners is also shortly presented.

The dissemination, communication and exploitation strategy that will be followed will be dynamic and will be adapted according to the different project phases. The overall goal is to ensure the impact of the project results through tailored and well-targeted activities.

REFERENCES

[1]	European Commission, October 2019, Making the Most of Your H2020 Project. Boosting the impact of your project through effective communication, dissemination and exploitation
[2]	Global Market Insights: Threat Intelligence Market Size & Share - Global Growth Forecasts 2025. February 2019.
[3	Kenneth Research: Global Threat Intelligence Platform Market Research Report. May 2020.
[4]	Parag, P.; Horaist, L.; Goldstein, J.: The Past, Present and Future of SIEM, 2020; online.
[5]	Google Cloud Threat Intelligence for Chronicle. Accessed August 2020; online.
[6]	McAfee: Threat Intelligence Sharing. Accessed August 2020; online.
[7]	Cyware: Cyware Threat Intelligence eXchange. Accessed August 2020; online.
[8]	Anomali: Sharing Threat Intelligence. Accessed August 2020; online.
[9]	Kaspersky: Kaspersky Threat Intelligence. Accessed August 2020; online.
[10]	Microsoft: Microsoft Threat Protection. Accessed August 2020; online.
[11]	Atos Advanced Detection and Response (ADR). Accessed August 2020; online.
[12]	THALES: Cyber Threat Intelligence. Accessed August 2020; online.
[13]	A call for tender to advance MeliCERTes, facility used by the CSIRTs to cooperate & exchange data. May 2019; online.

ANNEX 1: IRIS TEMPLATES



Artificial Intelligence Threat Reporting and Incident Response System

Agenda

No. Project Meeting

City, Country/Virtual

DD – DD, MM, YYYY

Venue Details

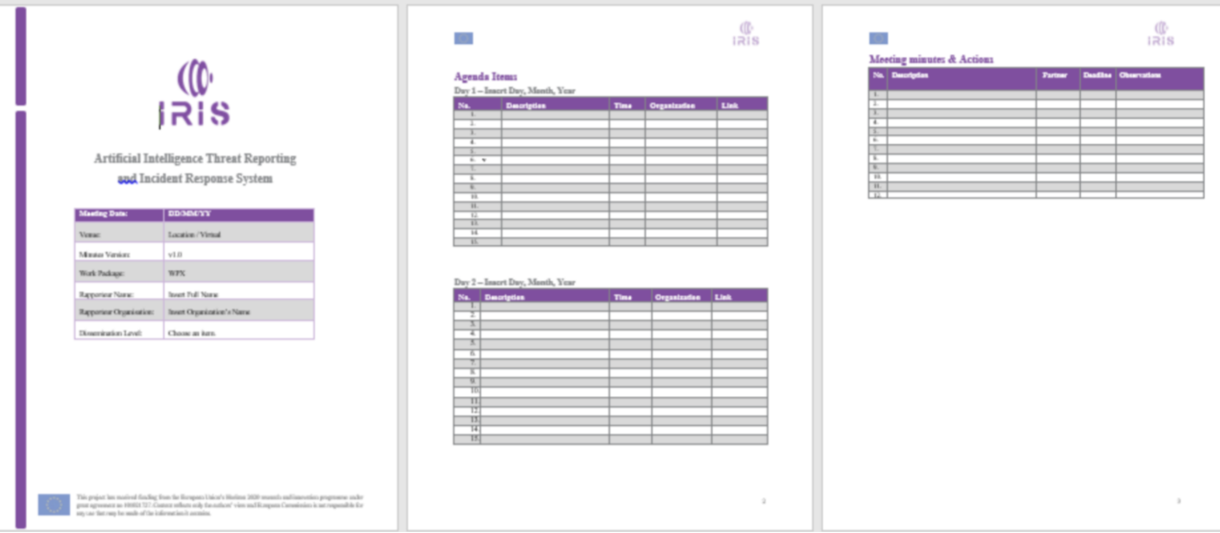
Venue/Building Name

Venue address/URL (venue's site, google maps)

Day 1 – Insert Day, Month, Year

Timeslot	Presentation	Partner
Hh:mm – hh:mm Duration:min		
Hh:mm – hh:mm Duration:min		
Hh:mm – hh:mm Duration:min		
Hh:mm – hh:mm Duration:min		
Hh:mm – hh:mm Duration:min		
Hh:mm – hh:mm Duration:min		
Hh:mm – hh:mm Duration:min		
Hh:mm – hh:mm Duration:min		
Hh:mm – hh:mm Duration:min		

Figure 8: IRIS Agenda Template



Artificial Intelligence Threat Reporting and Incident Response System

Meeting Date:	DD/MM/YY
Venue:	Location / Virtual
Minutes Version:	v1.0
Work Package:	WPX
Rapporteur Name:	Insert Full Name
Rapporteur Organisation:	Insert Organization's Name
Dissemination Level:	Choose an item.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Agenda Items

Day 1 – Insert Day, Month, Year

No.	Description	Time	Organization	Link
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

Day 2 – Insert Day, Month, Year

No.	Description	Time	Organization	Link
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

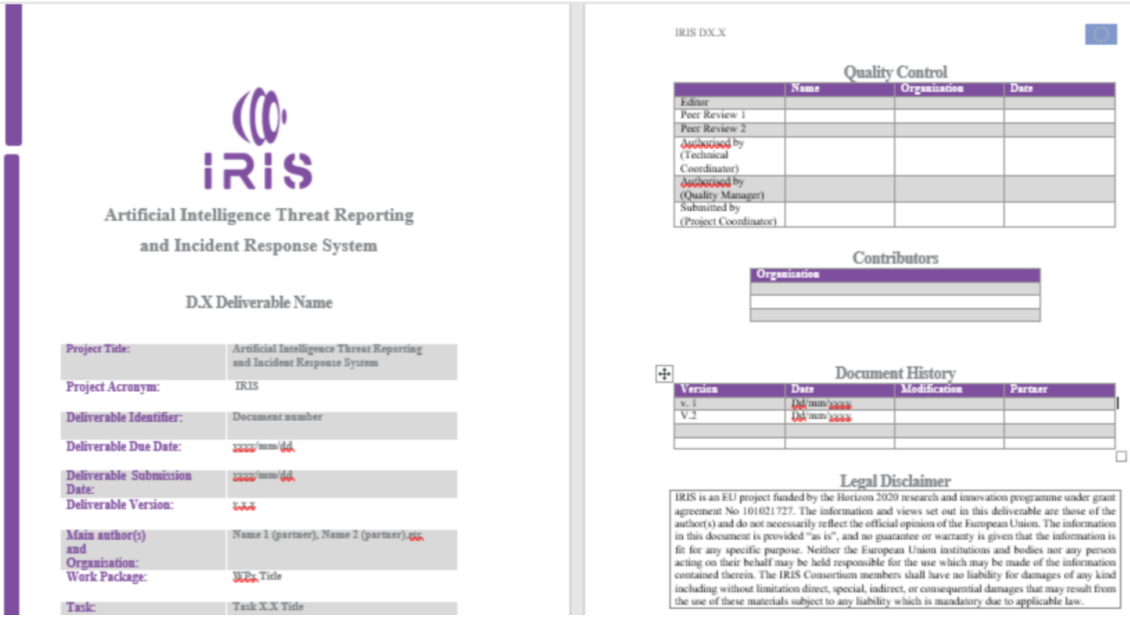
2

Meeting minutes & Actions

No.	Description	Partner	Deadline	Observations
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				

3

Figure 9: IRIS Meeting Minutes Template



Artificial Intelligence Threat Reporting and Incident Response System

D.X Deliverable Name

Project Title:	Artificial Intelligence Threat Reporting and Incident Response System
Project Acronym:	IRIS
Deliverable Identifier:	Document number
Deliverable Due Date:	yyyy/mm/dd
Deliverable Submission Date:	yyyy/mm/dd
Deliverable Version:	v.x.x
Main author(s) and Organisation:	Name 1 (partner), Name 2 (partner),etc.
Work Package:	WPx Title
Task:	Task X.X Title

IRIS DX.X

Quality Control

	Name	Organisation	Date
Editor			
Peer Review 1			
Peer Review 2			
Authorised by (Technical Coordinator)			
Authorised by (Quality Manager)			
Submitted by (Project Coordinator)			

Contributors

Organisation

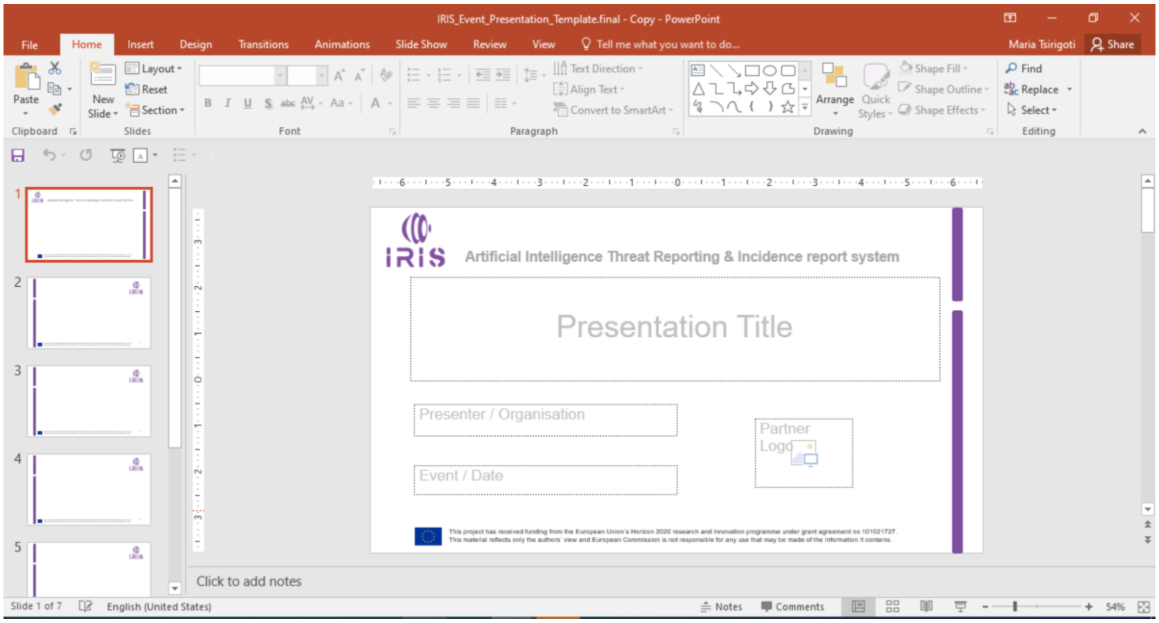
Document History

Version	Date	Modification	Partner
v. 1	Dd/mm/yyyy		
V.2	Dd/mm/yyyy		

Legal Disclaimer

IRIS is an EU project funded by the Horizon 2020 research and innovation programme under grant agreement No 101021727. The information and views set out in this deliverable are those of the author(s) and do not necessarily reflect the official opinion of the European Union. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any specific purpose. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein. The IRIS Consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

Figure 10: IRIS Deliverable Template



Artificial Intelligence Threat Reporting & Incidence report system

Presentation Title

Presenter / Organisation

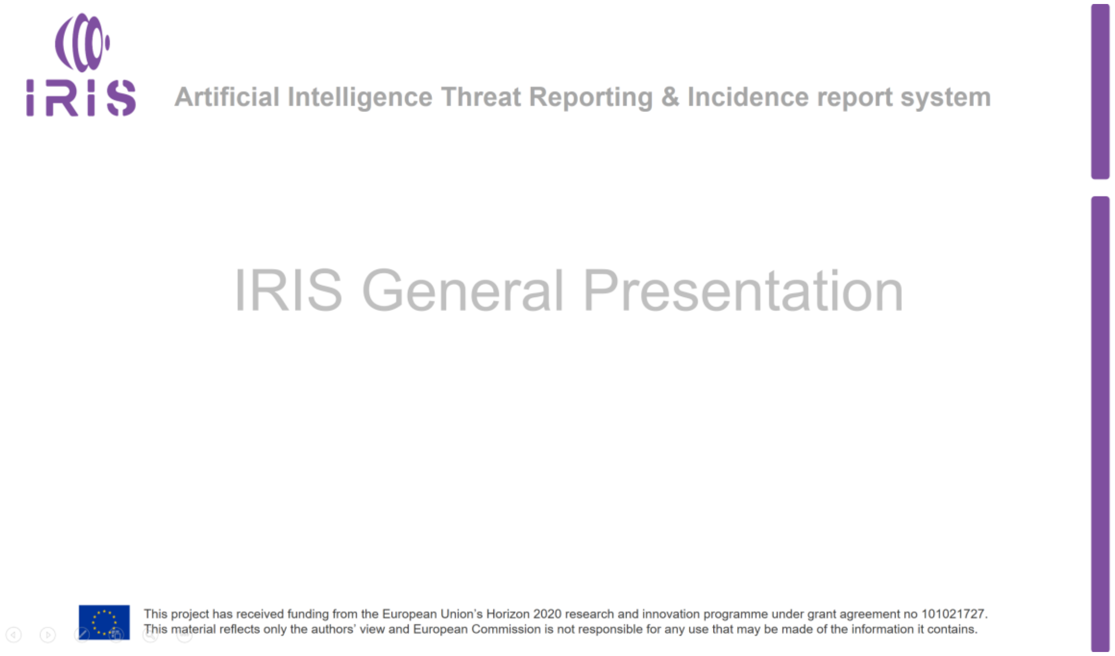
Event / Date

Partner Logo

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Click to add notes

Figure 11: IRIS ppt Template



Artificial Intelligence Threat Reporting & Incidence report system

IRIS General Presentation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Figure 12: IRIS General Presentation (1st slide)

ANNEX 2: IRIS BLOG TIME PLAN

Partner	Month
INOV	December 2021, July 2023
ESCO	January 2022, August 2023
DNSC	February 2022, September 2023
INTRA	March 2022, October 2023
THALES	April 2022, November 2023
ATOS	May 2022, December 2023
CISCO	June 2022, January 2024
CLS	July 2022, February 2024
SID	August 2022, March 2024
CEL	September 2022, April 2024
CEA	October 2022, May 2024
CERTH	November 2022, June 2024
ICCS	December 2022, July 2024
TU Delft	January 2023, August 2024
TalTech	February 2023, date before the end of the project
UPC	March 2023, date before the end of the project
KEMEA	April 2023, date before the end of the project
IMI BCN	May 2023, date before the end of the project
FVH	June 2023, date before the end of the project

Table 7: Blog Time Plan

ANNEX 3: DISSEMINATION MATERIAL

Consortium

www.www.iris-h2020.eu

coordinator@iris-h2020.eu

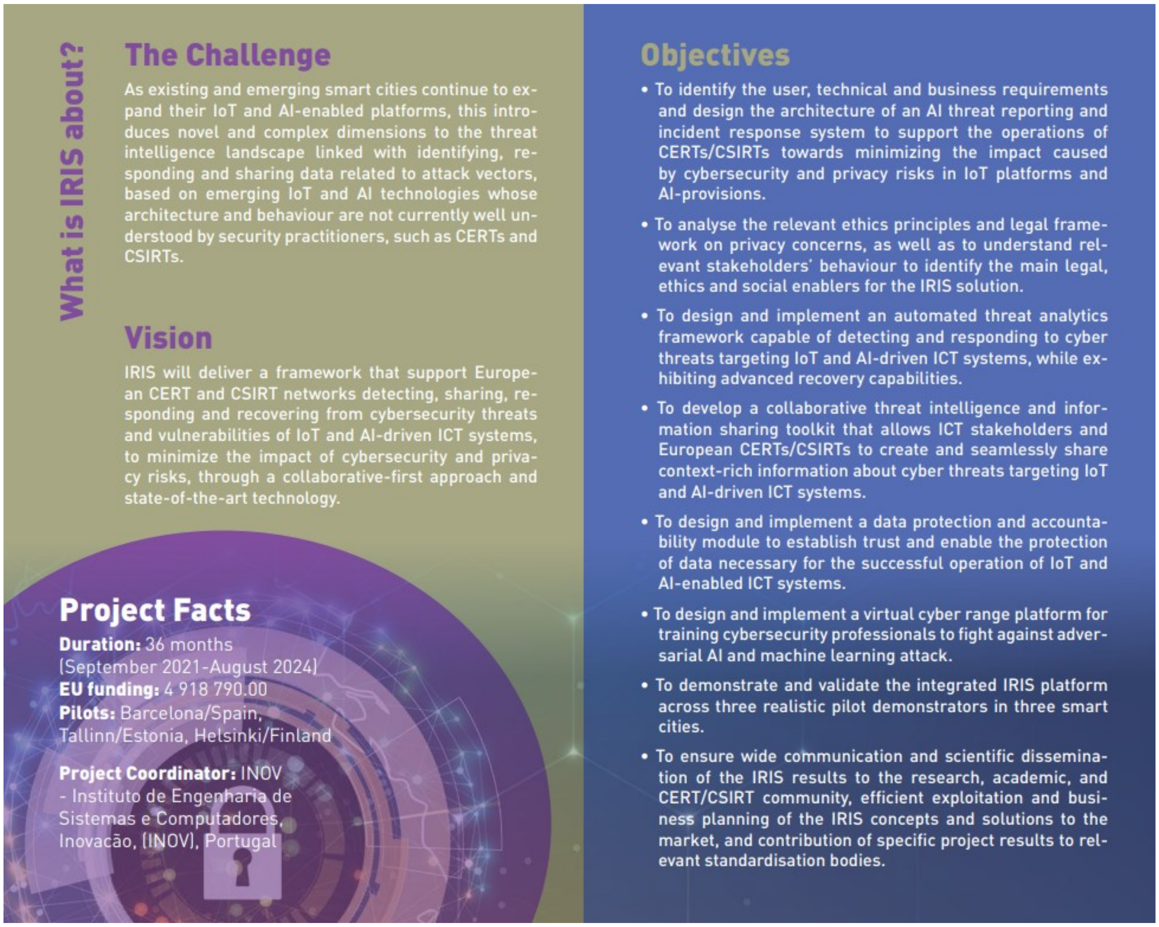
@iris_h2020

IRIS H2020 Project

INOV
ECS
DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICĂ
INTRASOFT INTERNATIONAL
THALES Building a future we can all trust
AtoS
CISCO
EXALENS
SIDROCO
CyberEthicsLab. Responsible Research and Innovation
list
iti Information Technologies Institute
ICCS
TUDelft
FINEST CENTRE FOR SMART CITIES
UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH
KEMEA
Ajuntament de Barcelona
FORUM VIRIUM HELSINKI
IRIS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Figure 13: IRIS Brochure (page1)



What is IRIS about?

The Challenge

As existing and emerging smart cities continue to expand their IoT and AI-enabled platforms, this introduces novel and complex dimensions to the threat intelligence landscape linked with identifying, responding and sharing data related to attack vectors, based on emerging IoT and AI technologies whose architecture and behaviour are not currently well understood by security practitioners, such as CERTs and CSIRTs.

Vision

IRIS will deliver a framework that support European CERT and CSIRT networks detecting, sharing, responding and recovering from cybersecurity threats and vulnerabilities of IoT and AI-driven ICT systems, to minimize the impact of cybersecurity and privacy risks, through a collaborative-first approach and state-of-the-art technology.

Project Facts

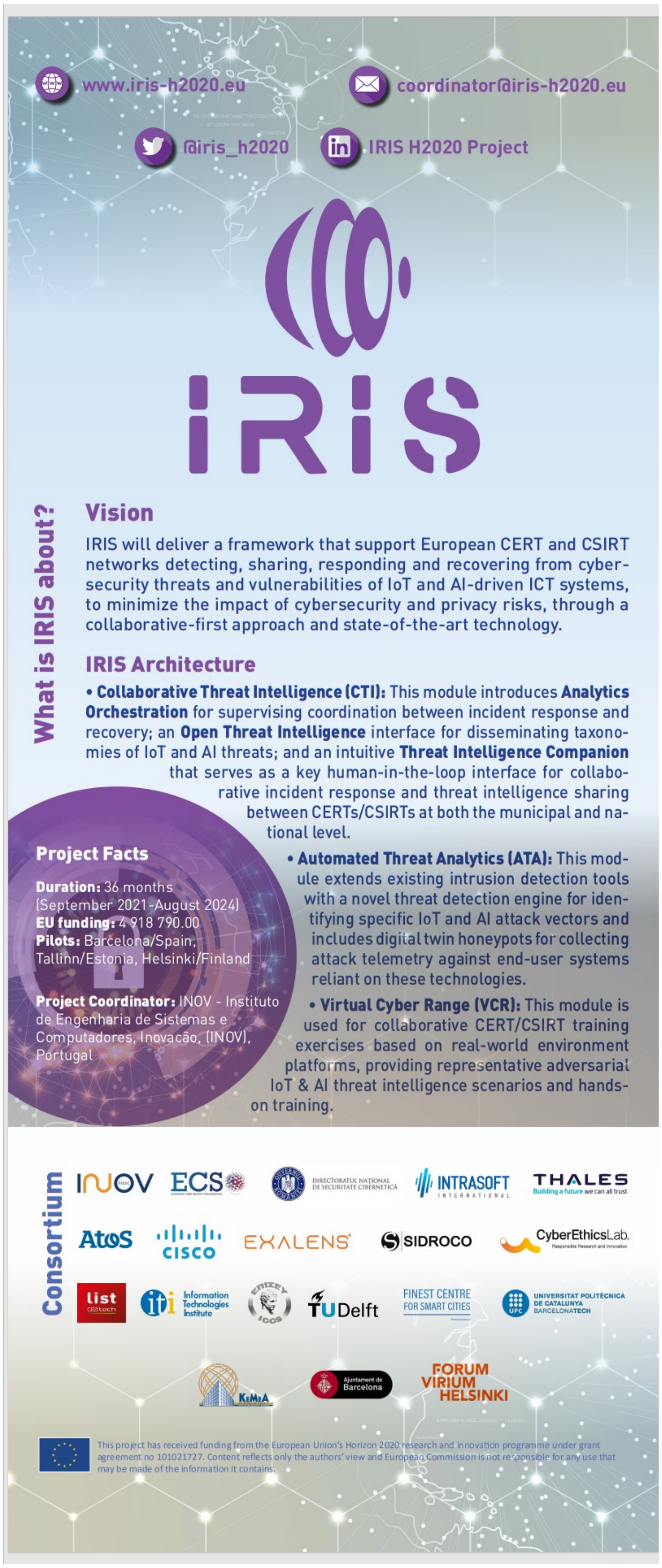
Duration: 36 months
(September 2021-August 2024)
EU funding: 4 918 790.00
Pilots: Barcelona/Spain,
Tallinn/Estonia, Helsinki/Finland

Project Coordinator: INOV
- Instituto de Engenharia de
Sistemas e Computadores,
Inovacão, (INOV), Portugal

Objectives

- To identify the user, technical and business requirements and design the architecture of an AI threat reporting and incident response system to support the operations of CERTs/CSIRTs towards minimizing the impact caused by cybersecurity and privacy risks in IoT platforms and AI-provisions.
- To analyse the relevant ethics principles and legal framework on privacy concerns, as well as to understand relevant stakeholders' behaviour to identify the main legal, ethics and social enablers for the IRIS solution.
- To design and implement an automated threat analytics framework capable of detecting and responding to cyber threats targeting IoT and AI-driven ICT systems, while exhibiting advanced recovery capabilities.
- To develop a collaborative threat intelligence and information sharing toolkit that allows ICT stakeholders and European CERTs/CSIRTs to create and seamlessly share context-rich information about cyber threats targeting IoT and AI-driven ICT systems.
- To design and implement a data protection and accountability module to establish trust and enable the protection of data necessary for the successful operation of IoT and AI-enabled ICT systems.
- To design and implement a virtual cyber range platform for training cybersecurity professionals to fight against adversarial AI and machine learning attack.
- To demonstrate and validate the integrated IRIS platform across three realistic pilot demonstrators in three smart cities.
- To ensure wide communication and scientific dissemination of the IRIS results to the research, academic, and CERT/CSIRT community, efficient exploitation and business planning of the IRIS concepts and solutions to the market, and contribution of specific project results to relevant standardisation bodies.

Figure 14: IRIS Brochure (page 2)



www.iris-h2020.eu

coordinator@iris-h2020.eu

@iris_h2020

IRIS H2020 Project

IRIS

What is IRIS about?

Vision

IRIS will deliver a framework that support European CERT and CSIRT networks detecting, sharing, responding and recovering from cyber-security threats and vulnerabilities of IoT and AI-driven ICT systems, to minimize the impact of cybersecurity and privacy risks, through a collaborative-first approach and state-of-the-art technology.

IRIS Architecture

- **Collaborative Threat Intelligence (CTI):** This module introduces **Analytics Orchestration** for supervising coordination between incident response and recovery; an **Open Threat Intelligence** interface for disseminating taxonomies of IoT and AI threats; and an intuitive **Threat Intelligence Companion** that serves as a key human-in-the-loop interface for collaborative incident response and threat intelligence sharing between CERTs/CSIRTs at both the municipal and national level.
- **Automated Threat Analytics (ATA):** This module extends existing intrusion detection tools with a novel threat detection engine for identifying specific IoT and AI attack vectors and includes digital twin honeypots for collecting attack telemetry against end-user systems reliant on these technologies.
- **Virtual Cyber Range (VCR):** This module is used for collaborative CERT/CSIRT training exercises based on real-world environment platforms, providing representative adversarial IoT & AI threat intelligence scenarios and hands-on training.

Project Facts

Duration: 36 months (September 2021-August 2024)
EU funding: 4 918 790.00
Pilots: Barcelona/Spain, Tallinn/Estonia, Helsinki/Finland

Project Coordinator: INOV - Instituto de Engenharia de Sistemas e Computadores, Inovacão, (INOV), Portugal

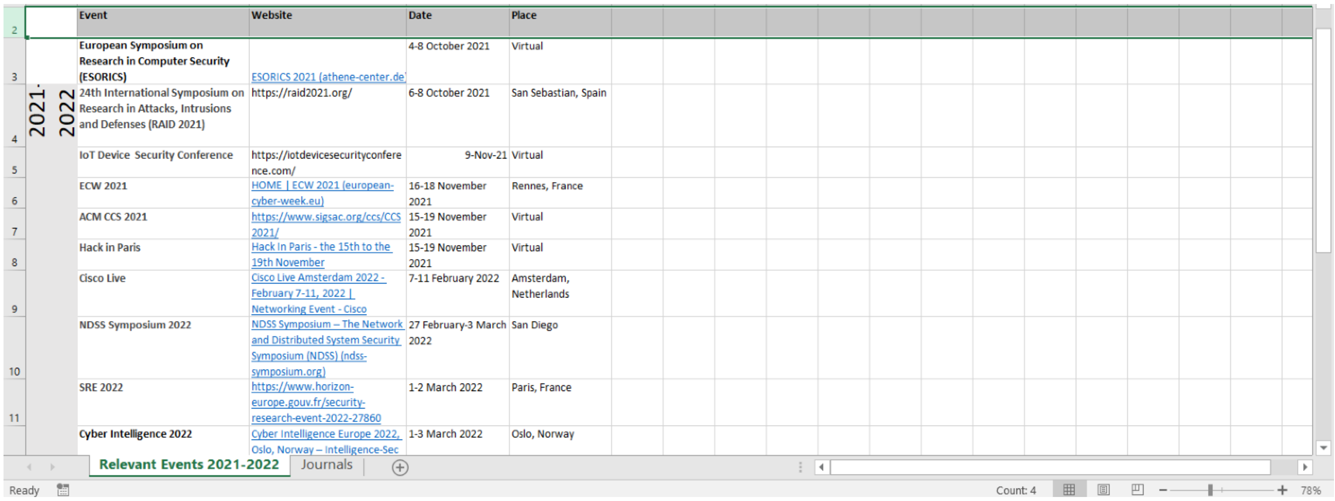
Consortium

INOV
ECS
Directoratul Național de Securitate Cibernetică
INTRASOFT International
THALES Building a future we can all trust
AtoS
CISCO
EXALENS
SIDROCO
CyberEthicsLab. Responsible Research and Innovation
list
iti Information Technologies Institute
TUDelft
FINEST CENTRE FOR SMART CITIES
Universitat Politècnica de Catalunya BarcelonaTech
KEMEA
Ajuntament de Barcelona
FORUM VIRIUM HELSINKI

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Figure 15: IRIS Roll up Banner

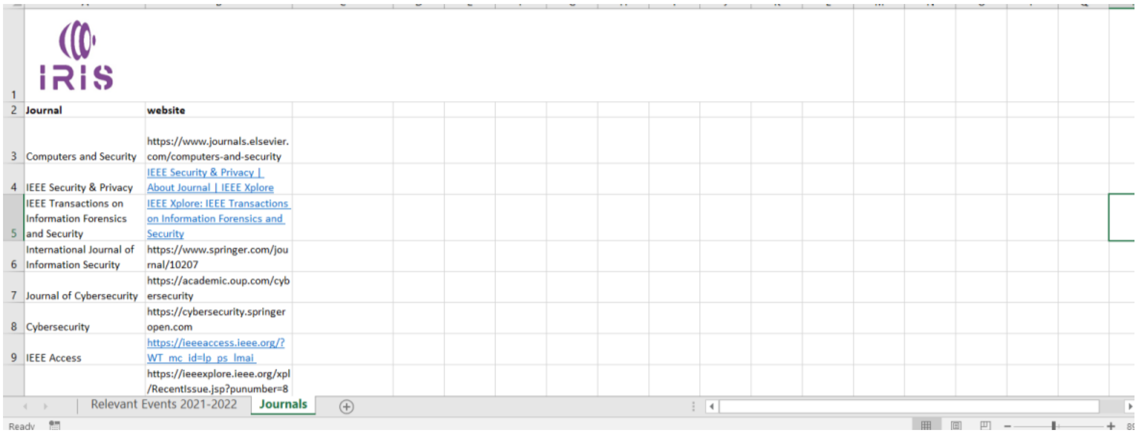
ANNEX 4: IRIS RELEVANT EVENTS



	Event	Website	Date	Place
2021-2022	**European Symposium on Research in Computer Security (ESORICS)**	ESORICS 2021 (athene-center.de)	4-8 October 2021	Virtual
	24th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2021)	https://raid2021.org/	6-8 October 2021	San Sebastian, Spain
	IoT Device Security Conference	https://iotdevicesecurityconference.com/	9-Nov-21	Virtual
	ECW 2021	HOME | ECW 2021 (european-cyber-week.eu)	16-18 November 2021	Rennes, France
	ACM CCS 2021	https://www.sigsac.org/ccs/CCS2021/	15-19 November 2021	Virtual
	Hack in Paris	Hack In Paris - the 15th to the 19th November	15-19 November 2021	Virtual
	Cisco Live	Cisco Live Amsterdam 2022 - February 7-11, 2022 | Networking Event - Cisco	7-11 February 2022	Amsterdam, Netherlands
	NDSS Symposium 2022	NDSS Symposium – The Network and Distributed System Security Symposium (NDSS) (ndss-symposium.org)	27 February-3 March 2022	San Diego
	SRE 2022	https://www.horizon-europe.gouv.fr/security-research-event-2022-27860	1-2 March 2022	Paris, France
	Cyber Intelligence 2022	Cyber Intelligence Europe 2022, Oslo, Norway – Intelligence-Sec	1-3 March 2022	Oslo, Norway

Figure 16: IRIS Relevant Events

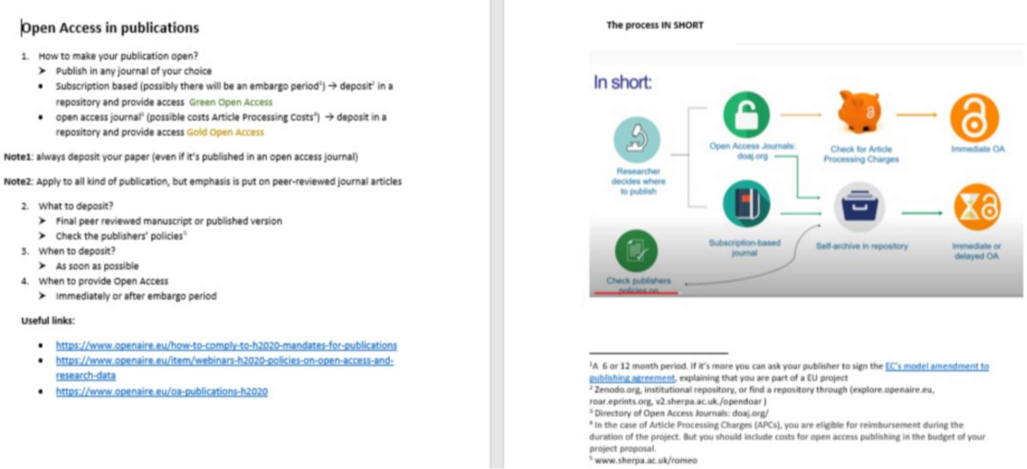
ANNEX 5: IRIS RELEVANT JOURNALS



Journal	website
Computers and Security	https://www.journals.elsevier.com/computers-and-security
IEEE Security & Privacy	IEEE Security & Privacy | About Journal | IEEE Xplore
IEEE Transactions on Information Forensics and Security	IEEE Xplore: IEEE Transactions on Information Forensics and Security
International Journal of Information Security	https://www.springer.com/journal/10207
Journal of Cybersecurity	https://academic.oup.com/cybersecurity
Cybersecurity	https://cybersecurity.springeropen.com
IEEE Access	https://ieeeaccess.ieee.org/?WT_mc_id=lp_ps_lmai
	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8

Figure 17: IRIS Relevant Journals

ANNEX 6: OPEN ACCESS GUIDELINES



Open Access in publications

1. How to make your publication open?
   - ➤ Publish in any journal of your choice
   - Subscription based (possibly there will be an embargo period[1]) → deposit[2] in a repository and provide access Green Open Access
   - open access journal[3] (possible costs Article Processing Costs[4]) → deposit in a repository and provide access Gold Open Access

Note1: always deposit your paper (even if it's published in an open access journal)

Note2: Apply to all kind of publication, but emphasis is put on peer-reviewed journal articles

2. What to deposit?
   - ➤ Final peer reviewed manuscript or published version
   - ➤ Check the publishers' policies[5]
3. When to deposit?
   - ➤ As soon as possible
4. When to provide Open Access
   - ➤ Immediately or after embargo period

Useful links:

- https://www.openaire.eu/how-to-comply-to-h2020-mandates-for-publications
- https://www.openaire.eu/item/webinars-h2020-policies-on-open-access-and-research-data
- https://www.openaire.eu/oa-publications-h2020

The process IN SHORT

In short:
Researcher decides where to publish
Open Access Journals: doaj.org
Check for Article Processing Charges
Immediate OA
Subscription-based journal
Self-archive in repository
Immediate or delayed OA
Check publishers policies on

[1]A 6 or 12 month period. If it's more you can ask your publisher to sign the EC's model amendment to publishing agreement, explaining that you are part of a EU project

[2] Zenodo.org, institutional repository, or find a repository through (explore.openaire.eu, roar.eprints.org, v2.sherpa.ac.uk./opendoar)

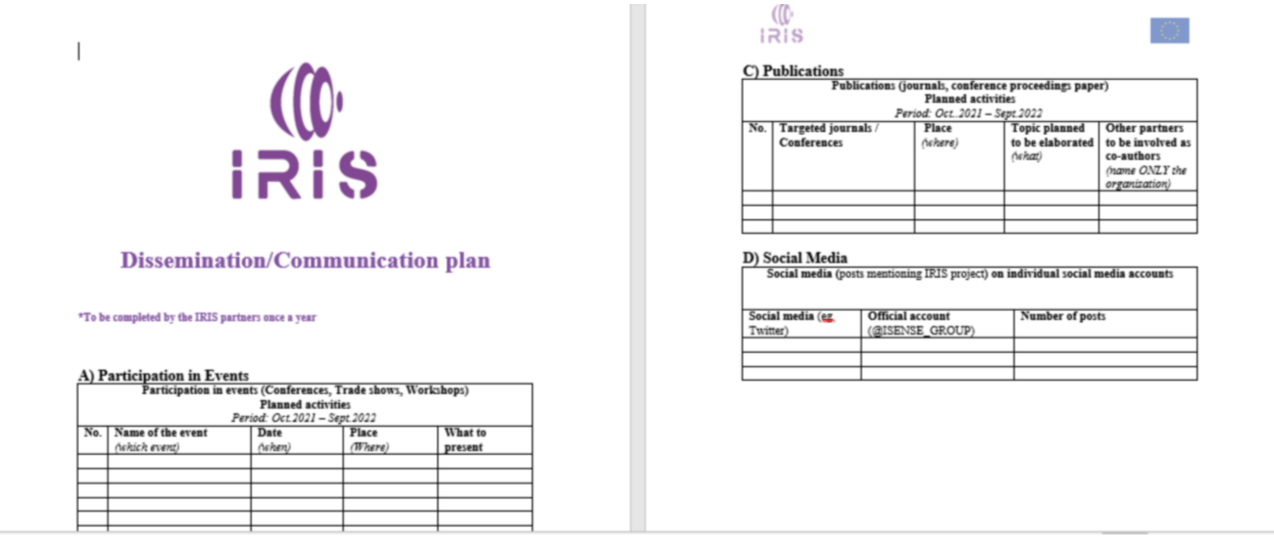
[3] Directory of Open Access Journals: doaj.org/

[4] In the case of Article Processing Charges (APCs), you are eligible for reimbursement during the duration of the project. But you should include costs for open access publishing in the budget of your project proposal.

[5] www.sherpa.ac.uk/romeo

Figure 18: Open Access Guidelines

ANNEX 7: PARTNERS DISSEMINATION & COMMUNICATION PLANS



Dissemination/Communication plan

*To be completed by the IRIS partners once a year

A) Participation in Events

Participation in events (Conferences, Trade shows, Workshops) Planned activities *Period: Oct.2021 – Sept.2022*				
No.	Name of the event *(which event)*	Date *(when)*	Place *(Where)*	What to present

C) Publications

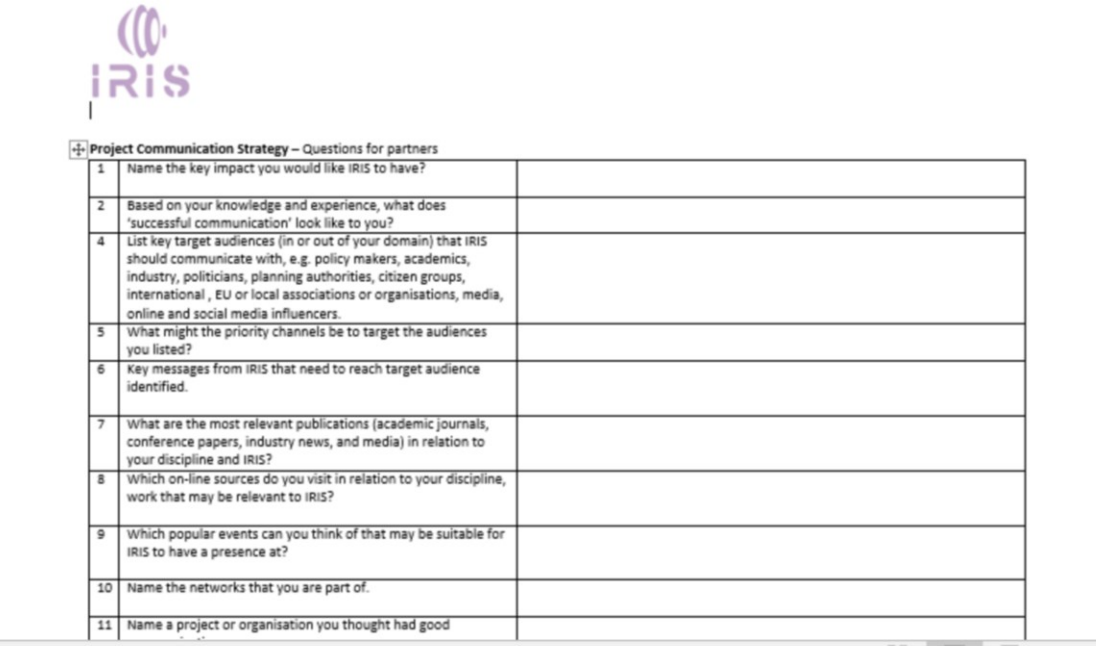
Publications (journals, conference proceedings paper) Planned activities *Period: Oct..2021 – Sept.2022*				
No.	Targeted journals / Conferences	Place *(where)*	Topic planned to be elaborated *(what)*	Other partners to be involved as co-authors *(name ONLY the organization)*

D) Social Media

Social media (posts mentioning IRIS project) on individual social media accounts		
Social media (eg Twitter)	Official account (@ISENSE_GROUP)	Number of posts

Figure 19: IRIS Partners' Dissemination & Communication Plans

ANNEX 8: QUESTIONNAIRES ABOUT COMMUNICATION



IRIS

Project Communication Strategy – Questions for partners

1	Name the key impact you would like IRIS to have?	
2	Based on your knowledge and experience, what does 'successful communication' look like to you?	
4	List key target audiences (in or out of your domain) that IRIS should communicate with, e.g. policy makers, academics, industry, politicians, planning authorities, citizen groups, international , EU or local associations or organisations, media, online and social media influencers.	
5	What might the priority channels be to target the audiences you listed?	
6	Key messages from IRIS that need to reach target audience identified.	
7	What are the most relevant publications (academic journals, conference papers, industry news, and media) in relation to your discipline and IRIS?	
8	Which on-line sources do you visit in relation to your discipline, work that may be relevant to IRIS?	
9	Which popular events can you think of that may be suitable for IRIS to have a presence at?	
10	Name the networks that you are part of.	
11	Name a project or organisation you thought had good	

Figure 20: IRIS Questionnaire about Communication

ANNEX 9: IRIS DISSEMINATION STEP BY STEP PROCEDURE

Description and purpose

The participation of consortium Partners in any event with an opportunity for dissemination and promotion of (conferences, workshops, etc.), as well as the performance of every dissemination activity related to IRIS (presentations, paper submissions, material distribution etc.), has to be communicated beforehand to the Dissemination Manager Ms Maria Tsirigoti (maria.tsirigoti@iccs.gr)

Please keep in mind that if the content is just for a purely internal meeting, and is not meant to be published or further disseminated, this procedure is not necessary.

Basic objectives

- Production of high-quality IRIS publications, presentations and other communication material;
- Avoidance of overlaps and possible disclosure of restricted or confidential information;
- Monitoring and recording of project communication and dissemination activities and their impact in an effective and efficient way.

Step by step procedure

1. When an opportunity is identified, please:

✓ notify the Dissemination Manager Ms Maria Tsirigoti (maria.tsirigoti@iccs.gr) of your intention by email **at least 45 working days in advance**, and

✓ register the activity in the dedicated excel file "Dissemination Register Requests", specifying the details of the activity (type of activity, date, title, audience) and your role in it related to the IRIS project (presenter, organiser, speaker in a session, author etc.).

✓ share the abstract/draft paper/draft poster, presentation etc., a**s soon as available** in the dedicated folder, entitled Dissemination Activities, set up in the IRIS repository (**creating a corresponding folder named after the related event**), and inform the Dissemination Manager when it is done.

2. The Dissemination Manager sends the request within 2 working days to the **Consortium partners** and the **Security Advisory Board** for approval, modification and request for extra information/clarifications or rejection.
3. The **Consortium partners** and the **Security Advisory Board** have to reply to the Dissemination manager within 30 working days; **no response is considered as an approval**.
4. The Dissemination manager informs the initiator of the dissemination activity and the Project Coordinator about the decision.

In case of Approval

4.1 The initiator may proceed with the submission or realisation of the planned dissemination activity.

In case of Conflict or Objection

4.2 Any Consortium member can object to the proposed dissemination activity, in cases of overlaps or risk of disclosure of restricted or confidential information. The objection has to include a clear reasoning as well as a precise request for necessary modifications. The issue is discussed among the Coordinator, the Security Advisory Board and the involved partners.

Note: If a conflict is created or further material is needed, then, the material is proposed again and the previous procedure is followed.

5. Within 10 working days after the implementation of the approved dissemination activity, the partner:

- ✓ Should fill in the dedicated excel file "Dissemination Register Completed Actions"
- ✓ Store the **final** dissemination material (final paper, presentation, poster etc.) in the dedicated folder, entitled Dissemination Activities, set up in the IRIS repository (see step 1).
- ✓ Uploads photos from the activity, if any, in the same folder (in a "photos" sub-folder);

NOTE:

If partners wish to present or release material **already approved**, such as public presentation/material, then no formal approval is required, but the Dissemination Manager has to be informed. In case a partner wishes to organise a workshop or special event related to IRIS, the approval of the Dissemination manager is needed **2 months** before the realisation of this dissemination activity.

GDPR: If the material contains a reference to other partners or the name or photo of an individual, publishing this content should be agreed with the person/partner in question before the dissemination request is made.

Language: If the material is in a national language other than English, the procedure should still be followed. A brief description in English should be added (not a complete translation). Any other partners who understand the same language are especially invited to comment.

Acknowledgment

1. The EC emblem (flag) available here and the following acknowledgement text should be included in **all scientific publications (journals/conference proceedings) related to the IRIS work**:

"This work is a part of the IRIS project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021727. This content reflects only the authors' view and the European Commission is not responsible for any use that may be made of the information this publication contains."

2. For **other communication activities**, please add the EC emblem (flag) available here, with the following sentence:

"This work is a part of the IRIS project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021727. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains."

3. For **infrastructure, equipment and major results**, please add the EC emblem (flag) available here and the following sentence:

"This [infrastructure] [equipment] [insert type of result] is part of the IRIS project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021727. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains."

Non-European Travel

For non-European travels, the Project Officer should be informed and an approval from his side is required. Please fill-in the Non-European Travel Report Template (available here) at least two months before the travel and send the form to the project Coordinator (nelson.escravana@inov.pt, iris-coordination@iris-h2020.eu), to inform the EC. For possible enquiry by the auditors in the future, it is recommended to keep the form and EC's response with the respective travel documents.