Horizon 2020 Program (2014-2020)

Cybersecurity, Trustworthy ICT Research & Innovation Actions
Security-by-design for end-to-end security
H2020-SU-ICT-03-2018

Cyber security cOmpeteNCe fOr Research anD InnovAtion[1]

Work package 5: *Exploitation, dissemination, certification and standardization*
Deliverable D5.2: *1st year report on exploitation, dissemination, certification and standardization*

Abstract: This document represents the 1st year report on activities performed by the CONCORDIA project on exploitation, dissemination, communication, certification and standardization, within the Work Package 5. The effort is reported in three main sections, one for each of the main tasks of this Work Package. Several key achievements of the consortium within the first year of the project are presented in this document, ranging from the efforts to collect available and reachable incubators and accelerators for potential startups coming out of the CONCORDIA consortium, the communication activities of the consortium such as scientific papers published, invited talks, white papers written and published, activity on social media and attention that the project has received, to the efforts related to the identification of the connection between CONCORDIA tasks and existing standards, the contribution in existing standardization activities and the identification of certification potential.

Contractual Date of Delivery	*M12*
Actual Date of Delivery	27/12/2019
Deliverable Dissemination Level	*Public*
Editors	*Nicolas Kourtellis, Ph.D.*
Contributors	*TUVA, MUNI, ATOS, FORTH*
Quality Assurance	*Christos Papachristos, FORTH* *Argyro Chatzopoulou, TUVA* *Jürgen Schönwälder, JUB* *Cora Lisa Perner, ACS* *Alexander Laux, ACS*

[1] The research leading to these results has received funding from the European Union Horizon 2020 Program (2014-2020) under grant agreement n° 830927.

The CONCORDIA Consortium

CODE	Research Institute CODE (Coordinator)	Germany
FORTH	Foundation for Research and Technology - Hellas	Greece
UT	University of Twente	Netherlands
SnT	University of Luxembourg	Luxembourg
UL	University of Lorraine	France
UM	University of Maribor	Slovenia
UZH	University of Zurich	Switzerland
JUB	Jacobs University Bremen	Germany
UI	University of Insubria	Italy
CUT	Cyprus University of Technology	Cyprus
UP	University of Patras	Greece
TUBS	Technical University of Braunschweig	Germany
TUD	Technical University of Darmstadt	Germany
MUNI	Masaryk University	Czech Republic
BGU	Ben-Gurion University	Israel
OsloMET	Oslo Metropolitan University	Norway
ICL	Imperial College London	UK
UMIL	University of Milan	Italy
BADW-LRZ	Leibniz Supercomputing Centre	Germany
EIT DIGITAL	EIT DIGITAL	Belgium
TELENOR	Telenor	Norway
ACS	Airbus Cybersecurity	Germany
SECT	secunet Security Networks	Germany
IFAG	Infineon	Germany
SIDN	SIDN	Netherlands
SNET	SurfNet	Netherlands
CYD	Cyber Detect	France
TID	Telefonica I+D	Spain
RD	RUAG Defence	Switzerland
BD	Bitdefender	Romania
ATOS	Atos Spain S.A.	Spain
SAG	Siemens	Germany
Flowmon	Flowmon Networks	Czech Republic
TUVA	TÜV TRUST IT GmbH	Germany
TI	Telecom Italia	Italy
EFA	EFACEC	Portugal
ALBV	Arthur’s Legal B.V.	Netherlands
EI	eesy innovation	Germany
DFN-CERT	DFN-CERT	Germany
CAIXA	CaixaBank	Spain
BMW	BMW	Germany

GSDP	Ministry of Digital Policy, Telecommunications and Media	Greece
RISE	RISE Research Institutes of Sweden AB	Sweden
Ericsson	Ericsson AB	Sweden
SBA	SBA Research gemeinnutzige GmbH	Austria
IJS	Institut Jozef Stefan	Slovenia
UiO	University of Oslo	Norway
ULANC	University of Lancaster	UK
ISI	ATHINA-ISI	Greece
UNI PASSAU	University of Passau	Germany
RUB	Ruhr University Bochum	Germany

Document Revisions & Quality Assurance

Internal Reviewers

- *Christos Papachristos, FORTH*
- *Argyro Chatzopoulou, TUVA*
- *Jürgen Schönwälder, JUB*
- *Cora Lisa Perner, ACS*
- *Alexander Laux, ACS*

Revisions

Ver.	Date	By	Overview
0.01	*4/10/2019*	*Nicolas Kourtellis*	*Table of Contents*
0.02	*08/11/2019*	*Nicolas Kourtellis*	*Contribution from TID*
0.03	*15/11/2019*	*Argyro Chatzopoulou*	*Contribution from TUVA*
0.04	*22/11/2019*	*Martin Horak*	*Contributions from MUNI*
0.05	*22/11/2019*	*Nicolas Kourtellis*	*Merging all contributions, editing, commenting, adjusting template based on new version*
0.06	*29/11/2019*	*Nicolas Kourtellis*	*New version with comments addressed and feedback from the GA in Vienna*
0.07	*02/12/2019*	*Argyro Chatzopoulou*	*Updates from TUVA with comments addressed and feedback from the GA in Vienna*
0.08	*0.2/12/2019*	*Martin Horak*	*Updates from MUNI with comments addressed and feedback from the GA in Vienna*
0.09	*03/12/2019*	*Nicolas Kourtellis*	*Final version with all comments addressed and to be delivered to FORTH for QA reviews.*
0.10	*13/12/2019*	*Nicolas Kourtellis, Martin Horak, Argyro Chatzopoulou*	*First round of reviews in with comments for TID, TUVA, MUNI addressed*
0.11	*16/12/2019*	*Nicolas Kourtellis*	*Review comments addressed by all partners, in consolidated version*
0.12	*23/12/2019*	*Nicolas Kourtellis, Martin Horak, Argyro Chatzopoulou*	*Second round of reviews in with comments for TID, TUVA, MUNI addressed individually*
0.13	*23/12/2019*	*Nicolas Kourtellis*	*Second round of review comments addressed by TID, TUVA, MUNI in a consolidated version*
0.14	*26/12/2019*	*Nicolas Kourtellis*	*Final version sent for submission*

Executive Summary

The present document is the second deliverable of Work Package 5 (WP5), and represents the 1st year report on exploitation, dissemination, communication, certification and standardization. The work package's objective is to enhance the impact of CONCORDIA's outcomes through strategic exploitation, dissemination, and standardization. From an exploitation perspective, WP5 will develop a comprehensive exploitation plan, that will be executed during the four years of the project, in alignment with the partners' commercial and research interests. Furthermore, the standardization activities in WP5 aim to enhance the impact of CONCORDIA by transferring project results to relevant industry standardization and best practice working groups.

WP5 is organized into three main tasks for:

- exploitation and incubators
- dissemination and communication
- certification and standardization

This deliverable D5.2 has three main sections, one for each of these corresponding tasks. In each of these sections, the achievements of the consortium within the first year of the project are described.

Overall, the activities performed in this project demonstrate that the consortium has achieved all Key Performance Indicators (KPIs) defined in the DoA and related to this WP for the duration of the first 12 months of the project. In fact, due to the intense activity of the partners in the dimensions of WP5, some of the KPIs have been already reached. We elaborate on the KPIs achieved in the Introduction of the deliverable.

In general, the effort to collect and report the activities performed by each partner within this work package revealed a great wealth of different activities. In particular, the consortium partners have performed communication and dissemination activities to promote the project, its goals and its results, efforts to improve existing standards and create new certifications and standards. In addition, several partners have demonstrated great reach to many incubators and accelerators that can help CONCORDIA in the near future to deploy its novel technics and build successful and profitable business models around them.

Contents

1. Introduction

As identified in activities executed in Work Package 1 (WP1), the focus on security in networks, devices, systems, applications, data, and user-centricity meets the emerging needs for secure and innovation-driven functionality for all users, by public entities, companies, or end users. Therefore, research and product development in these areas will address the consequent extension of existing and demanded functionality, as well as the security-relevant development of the future European workforce.

This overall R&D activity can lead to novel business areas and can develop potential markets. New fields of activity can arise for startups, as well as companies of all sizes in Europe. One of the CONCORDIA project's goals is to help such companies establish themselves in newly created business fields in the general area of cyber security, based on their own know-how and, thus, to create new business sectors and jobs in Europe.

In fact, CONCORDIA's mission is to create the CONCORDIA ecosystem, a Cybersecurity Competence Network (CCN) with leading research, technology, industrial and public competences, that will build the future European secure, resilient and trusted ecosystem. As it can be demonstrated by partners involved in Work Package 2 (WP2), CONCORDIA has strong EU industry involvement with piloting and building long-term community access incubators for sector-specific and cross-sector solutions, complemented by marketable solutions. CONCORDIA stands also for building bridges between research, industry and public sector to develop solutions in a fast and agile fashion.

To achieve these goals, the project has defined in its main activities the WP5, whose primary objective is to enhance the impact of CONCORDIA's outcomes through strategic activities in exploitation, dissemination, and standardization. From an exploitation perspective, WP5 is developing a comprehensive plan that will be executed during the project, in alignment with the partners' commercial and research interests. This plan will help partners to push their cybersecurity-related technology built within CONCORDIA to the EU market. The project, via WP5 activities, is also committed to strong dissemination and communication of the project results to the public and key stakeholders through social media posts, blog posts and other announcements in the website and news channels. Furthermore, the standardization activities in WP5 aim to enhance the impact of CONCORDIA by transferring project results to relevant industry standardization and best practice working groups.

Finally, CONCORDIA's partners will also ensure an adequate level of dissemination of all the project results, both scientific and industrial, and using the most appropriate communication channels. This effort will ensure that the public is aware of the main challenges addressed within the project. Feedback from the public (both at the academic and industrial level) will be collected over various events and via different communication channels (e.g., communication events, social media channels, etc.). In the final year of the project (2023), WP5 will also produce a sound plan for providing sustainability to the project's outcomes.

To achieve these project goals, the WP5 is broken down into 3 main tasks, that allow CONCORDIA to build on necessary activities in exploitation, dissemination, communication, certification and standardization:

- Task T5.1: Exploitation and incubators (Lead: TID)
- Task T5.2: Dissemination and communication activities (Lead: MUNI)
- Task T5.3: Certification and standardization activities (Lead: TUVA)

Key Performance Indicators on Impact:

The project has defined a list of Key Performance Indicators (KPIs) to quantify the impact of the project's results. Next, we selected the KPIs that are relevant for the activities pertaining WP5 (all KPIs are listed in the DoA), and report progress made for each of these KPIs, at the end of the M12 of the project (i.e., ¼ of the project's duration):

Table 1: Completion of CONCORDIA's Key Performance Indicators related to WP5

General KPI	Goal in 4 years	Performed in M1-M12	Unit of measure
Publish papers in journals and conferences	100+	50+	Scientific Papers (see Section 3 for details and Deliverable D1.1)
CONCORDIA in social media	15000	16400+	Views + Likes (see Section 3 for details)
Publication of Case Studies Documents – White Papers	-	16	Blog posts (see Section 3 for details)
Downloads for public deliverables, prototypes, promotional material	500+	600+	Downloads
Dissemination material in the form for documents, papers, deliverables, technical reports, presentations, fact sheets	-	Done	Flyers, deliverables, papers, technical reports, presentations, etc. (see Section 3 for details)
Organization of workshops and conferences	At least 1 major event and 3 satellite or special events	1	Open Door Event (see Section 3 for details, and Deliverable D4.7)
Targeted focus groups with EU officials, policy makers, ECSO and cPPP officials	-	Done	Engagement with key EU and market stakeholders via meetings and group activities (see Section 3 for details)

To reach these KPIs, the project has invested a lot of effort in the dimensions of exploitation via different avenues, dissemination, communication, standardization, and certification.

The project had several achievements in this Work Package, that are reported in separate sections, one per main Task.

- Efforts on Exploitation (Section 2):
  - 19 incubators and accelerators have been identified, information was collected for each one, including number of startups they support, capital,

    - market focus, maturity of startups supported, contact information, etc
    - 11 exploitable results have been already identified, that can lead to separate startups or new business units within the partners reporting them
- Efforts on Dissemination and Communication (Section 3):
    - 50+ scientific papers published in different conferences and journals.
    - 61 events / conferences / invited talks / seminars held or attended by the consortium partners and its members.
    - 16 blog posts published on CONCORDIA website or in prominent technology websites, written by CONCORDIA partners explaining technology they built, their services offered, etc.
    - 9000 users visited the CONCORDIA website from around the world during the first year of the project.
    - 261 Twitter posts / 125 Facebook posts / 250 LinkedIn posts.
    - 16400+ of total engagements across social media platforms.
    - 18 announcements posted on the CONCORDIA website.
    - 59 news and other web articles published providing high publicity to the project's activities.
    - 4 events / conferences sponsored by the project or its partners.
- Efforts on Certification and Standardization (Section 4)
    - 32 Standards Developing Organizations have been identified from the consortium partners as organizations that they collaborate with for the development of new standards, and improvement of existing ones.
    - 54 Standards in preparatory stages (draft, pending, etc.) from the consortium partners.
    - 295 standards to be studied from the consortium partners for their relevance in their activities in the cyber security sector.

Roadmap of the Deliverable:

In the next three sections, we analyze the objectives of each of the main tasks of the WP5, the strategy to achieve them, and progress in each one, until the time this deliverable was submitted. Finally, we conclude this deliverable in Section 5.

2. Efforts on Exploitation

2.1. Objectives of Task (T5.1)

The CONCORDIA project aims to achieve its goals on exploitation of its results from academia and industry, by focusing on the following two sub-objectives, detailed in task T5.1 of the project and in the General Agreement of the project:

- To analyze the exploitation possibilities of the CONCORDIA project
- To develop ways that build sector-specific incubators

The consortium identified the following core activities that need to be carried out within this task for the duration of the project, to fully achieve these objectives (also detailed in the General Agreement of the project):

- **A1:** Set-up exploitation steering sub-committee that will meet twice per year to review potential of technology built within the project's technical work packages and use case pilots, and assess progress made by each partner towards the exploitation of this technology.
- **A2:** Develop business plans to formalize exploitation strategy based on technology results and IPR; protection and licenses will be granted outside the consortium.
- **A3:** Set-up protected knowledge management area within the CONCORDIA website for controlled dissemination and exploitation among partners and the public, as well as establish standard procedures for exploitation routes, licensing, patenting, etc.
- **A4:** Perform commercial exploitation based on strong presence of industry in the CONCORDIA consortium, outcomes used internally in consortium, and externally in the market, by launching and incubating new startups.
- **A5:** Create joint environment for deployment and validation of prototypes before large-scale roll-outs, to complement testing and validation labs, and offer academia extra real-world feedback for staying ahead of the curve.
- **A6:** Carry-out continuous sector monitoring, attending special interest group (SIG) meetings with key stakeholders who are invited to demo-days, and kept informed of CONCORDIA's progress and are actively involved in its ecosystem.

2.2. Strategy to Achieve Task Objectives

The overall strategy of the project for achieving T5.1's objectives has been to put effort during the first 12 months in the following below steps:

- Form the exploitation steering sub-committee of the project, which can collect ideas on how to achieve the expected outcomes from this task, as well as discuss, filter, provide advice on and prioritize the received input from partners and key outside stakeholders. Related activities: A1, A5, and further discussed in Section 2.2.1.
- Receive input (via surveys) from partners for critical activities of this task such as declaration of exploitable results, important technology built, etc. Related activities: A2, A3, A4, and further discussed in Section 2.2.2.
- Communicate to partners material collected and placed in the knowledge management area of CONCORDIA, and request for further input, corrections and updates. Related activities: A3, and further discussed in Section 2.2.2.
- Consult with outside key stakeholders for extracting new insights and capturing important trends outside the project. Related activities: A6, and further discussed in Section 2.2.3.

2.2.1. Subcommittee formation

In the second General Assembly of CONCORDIA, the Exploitation & Innovation Subcommittee was formed, with the task to review the potential of technology built within the project's technical work packages and use case pilots, and assess progress made by each partner towards the exploitation of this technology. Within these efforts, the committee's first tasks were to: 1) define what Exploitable Results are (explained in subsequent subsection), 2) provide guidance on the business model definition, 3) define important dimensions that should be collected from partners regarding incubators and accelerators available within or associated with the consortium.

2.2.2. Strategy in collecting, ranking and sharing partner input

In order to collect and rank input provided from the partners, the committee followed the below strategy. However, in the future it may expand the means of collecting input, to diversify and complement the already received input.

Data collection:
The strategy to collect data from partners, so far, has been primarily via web surveys and communications (emails) within the consortium and key stakeholders. The agreed-upon plan is to request input from partners every six months, to always maintain an up-to-date list of exploitable results, business plans, incubators and accelerators available to the consortium, and technology built within and available to the consortium.

Input Ranking:
Following already published methodologies[2],[3], several criteria can be used to rank exploitable results declared by the partners:

- Type of result (product, process, software, service, etc.)
- Innovation and differentiation from state of art
- Completeness in terms of features, functionalities, references, etc.
- Stakeholder interest
- Technical maturity (e.g. size and scope of verification and validation, type of environment used for testing etc.)
- Contribution to or positioning in a specific market
- Delivery, execution and transfer capability
- Protection and IPR issues
- Benefits to customers, collaboration of partners, public, etc.

In addition to the above criteria, there is a need to define a scale for assessing the level that each of the criteria was achieved, and a minimum threshold for considering an exploitable result worth to consider. Methodologies outlined already on the web for assessing the achievement of each criterion will be considered[3], and applied when partners 1) report completion of these exploitable results, and 2) readiness to push them to the market.

Result Sharing:
The material collected from partners using these surveys, after it has been sanitized and ranked, is going to be shared again with the partners of the consortium, so that they are

[2] https://ampsocal.usc.edu/files/2017/05/Attachment-2-Exploitable-Results-Exercise.pdf

[3] https://www.focusonfof.eu/downloads/results/exploitt-dossier.pdf

aware of all the exploitable efforts in the project. Each partner will also be asked to submit updates on the input they already provided in this initial input collection, based on the status of their tasks and progress they have made with their technology, as well as what other partners have contributed. This updated input will be requested at least every six months.

Furthermore, the results will be collected, analyzed and stored in a knowledge sharing space accessible by the consortium. We envision this to become the “go-to” place for the consortium partners for getting ideas on technology built within the project. In this way, we can facilitate the forging of collaborations between partners for sharing technology built, as well as requesting help to resolve pending cyber security problems some partners may face. Furthermore, this sharing space will be used for announcing exploitable results and for dissemination purposes to external public stakeholders.

At the end of the first year, preliminary results were shared with the partners through presentations and accessible documents on project’s online common work space (Confluence[4]). Overall, we had 11 exploitable results declared by consortium partners (detailed in Section 2.3). The final knowledge management space is under design and will be implemented and populated with the first round of exploitable results and incubators / accelerators, in the first half of the second year of the project (M12-M18).

2.2.3. Strategy to communicate results to key stakeholders

We perform constant monitoring of the sector via participation of key events in industrial and academic meetings and other types of relevant events. This activity is executed in collaboration with partners in T3.4. Furthermore, in order to communicate our results from the collection effort to the key stakeholders of the project, we have not only participated in several relevant events, but also organized the first CONCORDIA Open Door event (COD) in Luxembourg, in mid-October 2019. At COD, we presented key results of the project, and demonstrated with posters and demos the technology and the use-cases of the project. We also regularly participate in conferences and industrial forums and meetings to disseminate project results, and keep key stakeholders engaged with the project and involved in the CONCORDIA ecosystem. Details on these events are given in Section 3.

2.3. Exploitable Results

Exploitable Result (ER) is considered any form of tangible or intangible project result:

- **Intangible result:** technical or business consulting, system integration capacity, etc.
- **Tangible result:** software component, tool, prototype, service suite, etc.

Such items are candidates to become CONCORDIA Exploitable Results. Each ER has an assigned owner that serves as the main contact point. Also, when possible, the partners were asked to briefly discuss the level of maturity of the declared ER, and even use a Technological Readiness Level (TRL)[5] encoding to declare the maturity of the ER. The list of collected ERs will be reviewed by the committee every six months, during the regular biannual meetings.

The first round of input received from partners on ERs is summarized in Table 2. Already 11 ERs have been declared, with mostly tangible results to be expected of varying type: software, tools, methods, educational material and documents.

[4] https://www.atlassian.com/software/confluence

[5] TRL: https://ec.europa.eu/research/participants/data/ref/h2020/other/wp/2016_2017/annexes/h2020-wp1617-annex-g-trl_en.pdf

Table 2: Exploitable results declared in the first round of input collected from partners.

Partner/Owner	Contact Info	Exploitation Result	Type of Result	Level of Maturity / Current Status (partner defined)	Expected Delivery
Flowmon	info@flowmon.com pavel.minarik@flowmon.com	TLS 1.3 metadata visibility module	Tangible: Software	Available to all Flowmon users or customers as part of Flowmon 10.3 release, part of the product. It supports T1.2, topic "Analysis of Encrypted Traffic".	06/2020
Flowmon	info@flowmon.com pavel.minarik@flowmon.com	Custom IoCs module	Tangible: Software	available to all Flowmon users or customers as part of Flowmon ADS 10.0 release, part of the product. It supports T2.1, detection of malicious activities using custom IoCs.	06/2020
BGU	yairme@post.bgu.ac.il, shabtaia@bgu.ac.il	Model for generating a detectability score / rank for a combination of (1) an IoT device model and (2) an attack scenario	Tangible: Expert-based method	Now finalizing the design of the questionnaire, towards collection of responds and analysis.	06/2020
DFN-CERT	Christian Keil	CCH	Tangible: Software	We are extending our already existing and operational CCH in CONCORDIA. Extensions and integrations are planned to be close to or operational at the end of the project (D3.5). We are also developing metrics and analytics on the data. This is planned to reach TRL 7 at the end of the project (D3.5). Development will be iteratively with intermediate results being released during the project's duration.	12/2023
EI	ruiz.quero@eesy-innovation.com	Firmware Update system definition/description	Tangible: Document	Technical solution and knowledge transfer which is expected to be reviewed between different partners (Not defined yet).	10/2020

Partner/Owner	Contact Info	Exploitation Result	Type of Result	Level of Maturity / Current Status (partner defined)	Expected Delivery
ATOS	aljosa.pasic@atos.net rodrigo.diaz@atos.net josefrancisco.ruiz@atos.net	Threat Intelligence Exchange for Financial sector (TINEF)	Tangible: software	To be defined, probably based on MISP.	12/2023
CYD	l.werner@cyber-detect.com jean-yves.marion@loria.fr	Gorille Pro	Tangible: software	This is the interface of our tools based on morphological analysis in order to detect malware. It will be presented at CES Las Vegas, Jan 2020.	01/2020
JSI	primoz@e5.ijs.si atanja@e5.ijs.si	Onyx/VulNET	Tangible: Software	TRL 7	12/2023
EIT Digital	felicia.cutas@eitdigital.eu	Education Content	Tangible: nano-MOOCs, micro-masters, courses for teachers	Under design and development.	2021-2022
TID	nicolas.kourtellis@telefonica.com	Privacy Threats IoCs module	Tangible: software/tool	Under design / discussion with other telco partners.	12/2021
Telenor	thanh-van.do@telenor.com	Machine Learning Platform for Anomaly Detection	Tangible: software/tool	Under design and integration.	12/2023

2.4. Incubators and Accelerators

Background:

Venture capital (VC) is a well-known type of finance, where an outside group takes partial ownership of a company in exchange for capital. The percentages of ownership to capital can be negotiated, but it is only recommended when there is expected or already demonstrated high growth potential. In some cases, where the risk is high, a kind of public funds can be used (e.g., EIT digital). Data shows that out of the total investment into European scale-ups in 2019, the vast majority (74%) comes from venture capitals and private investors. Fintech has been the largest industry in Scaleup Europe, followed by Cyber Security, Energy, and Cleantech as the fastest growing rates with roughly 3B Euros new investments in each. In addition, the news is full of alerts about fundraising. For example, British Darktrace raised 6 million in a Series A funding round led by Flint Capital, next to another 50M Euros in a round led by Vitruvian VC. Also, the Cybersecurity Ventures program in Spain gives grants up to 120K Euros and the list of 2019 finalists has been published in June. This overall activity demonstrates a healthy ecosystem of VC and public funds available for startups in EU for the various sectors and especially the cyber security sector, that the CONCORDIA consortium is focused on.

Furthermore, in addition to VC type of funding, there is the strategic partner financing option. This funding can be given in VC-type of agreement, as it resembles an equity sale, but it can also be royalty-based. This type of funding can be of interest to the CONCORDIA partners as it is based on a kind of special access to know-how provided by specific consortium partners to the sponsor(s) willing to fund or purchase it. In fact, this option is particularly relevant to CONCORDIA in the context of the network of National Coordination Centers, and the Cybersecurity Competence Community and EU Cybersecurity Industrial, Technology and Research Competence Centre that CONCORDIA envisions to build. CONCORDIA is interested to explore options of strategic partner financing, where strategic partner can be a single organization or a node of the future Competence Community.

Therefore, it becomes clear that CONCORDIA needs to identify potential avenues for startup funding (e.g., VC or strategic partner financing) or other support (e.g., accelerators and incubators) for technology built within the project and is ready to be published in the EU cybersecurity market. Towards this end, the exploitation and innovation subcommittee requested input from the CONCORDIA partners regarding incubators and accelerators that are closely tied to the consortium, or that the consortium is aware of, and the committee and/or the management board should approach. At the same time, the partners were asked to provide information about new startups that have been launched from partners in the cybersecurity domain, as a demonstration of active contribution to the domain.

General remarks on collected results:

Overall, the collection of incubators and accelerators provided by the consortium partners revealed a vast reach into the startup ecosystem across Europe, with great potential for exposing European funding organizations and the market to technology built within the CONCORDIA project and from its consortium partners.

This collection of incubators and accelerators has been shared with partners managing and contributing in Task T3.5, which is related to developing and supporting a community for startups that want to use the results of CONCORDIA project. This community will act as a "startup-factory", providing guidance for establishing startups, business models, offering service such as best practices, IPR management, identification and refinement of proposals/ideas, feedback about team building, go-to-market strategies, etc.

Given the clear connection between these two tasks (T3.5 and T5.1), this investigation revealed the possible need for a more dedicated effort in the next few years on collecting such information on incubators, accelerators and startups, and organizing the partners in a community that enables them to exploit their CONCORDIA-based results using internal and external to the project resources.

Survey structure:

The input requested regarding this activity was grouped in the following main categories. We analyze further each category in dimensions that partners were asked to provide input:

1. Basic details
2. Type of incubator/accelerator
3. Geographical and sector characteristics
4. Level of ties with partner declaring it
5. Comments

1. Basics details:

- Name of Partner
- Name of Incubator/Accelerator
- Website of the Incubator/Accelerator
- Capital size in USD (if known)
- Number of startups supported
- Contact person for more information

2. Type of incubator/accelerator:

- Maturity of startups it supports (low/medium/high)
- General startups (yes/no)
- IT Specific (yes/no)
- Cybersecurity Specific (yes/no)

3. Geographical and sector characteristics

- Worldwide (if yes, state countries it operates)
- EU (if yes, state countries it operates)
- National (if yes, state cities it operates)

4. Level of ties with partner declaring it

- Partner participates directly (yes/no)
- Partner has good relation/knowledge to it (yes/no)
- Partner just knows of its existence (yes/no)

Using the above dimensions, we collected input from the consortium partners which we summarize below under the different dimensions mentioned.

Indicative names on accelerators & incubators:

The accelerators and incubators that the consortium partners have indicated so far are the following 19:

1. Wayra

2. Pier01
3. La Salle Technova
4. University of Luxembourg Incubator
5. EIT Digital Accelerator & Venture Program
6. Cybersecurity incubator based in London
7. Bayern startup
8. Filarete Servizi
9. Tovarna Podjemov
10. CEDRA SPLIT
11. Incubateur Lorrain
12. BGN Technologies Ltd
13. Health Hub Vienna
14. INiTS
15. weXelerate
16. ABC Accelerator
17. Primorski Tehnološki Park
18. Ljubljanski Univerzitetni Inkubator
19. pos4work

Indicative capital invested by such entities:

The capital invested by these entities ranges from a few million to hundreds of millions of Euros (2M, 20M, 30M, 50M, 60M, 80M, 160M).

Number of startups supported by such entities:

The entities identified by the consortium partners support a wide range of startups, from a few tens to hundreds. Figure 1 provides a quick summary of portion of these entities broken down by the number of startups they currently support. We notice that the majority is medium-sized, with up to 100 startups supported, but in some cases, the identified accelerators / incubators support up to 500 startups.

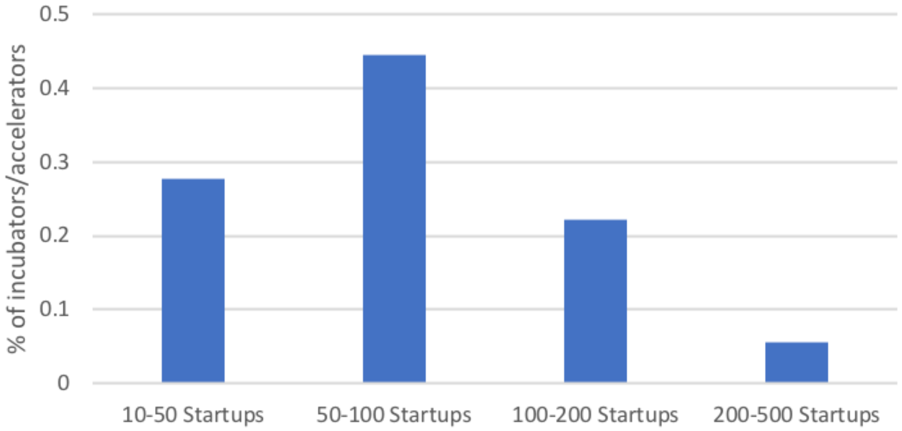


Figure 1: Number of startups supported per identified incubator / accelerator.

Maturity of supported startups:

We also look into the maturity of startups that these organizations prefer to support. Maturity was either declared by the organizations' websites or communicated to the CONCORDIA partners contacting them. Our collection had the following breakdown:

- early: 33%
- medium: 44%
- high: 23%

Again, the majority of accelerators / incubators focus on startups that are in their early or medium stage, with about ¼ of entities supporting high-maturity startups.

Focus of incubator/accelerator:

Regarding the type of startups that each entity supports, we had the following breakdown, with respect to general, specific to IT, and specific to cybersecurity:

General:	37%
IT specific:	40%
Cybersecurity:	23%

About 2/3rds of the entities support IT and cybersecurity specific startups, which gives the consortium a good starting point for pushing technology produced.

Geographical coverage:

Most entities identified (85-90%) focus on EU-based startups, and in some cases only in startups that operate in specific countries. Some exceptions exist which support startups in a worldwide arena (10-15%).

Accessibility of incubators & accelerators from CONCORDIA partners:

Finally, we examine the accessibility of each entity identified, with respect to a partner having an established relationship or ties with the said entity or just being aware of its existence:

Partner participates directly:	17%
Partner has knowledge/relation:	39%
Partner is aware of the entity:	44%

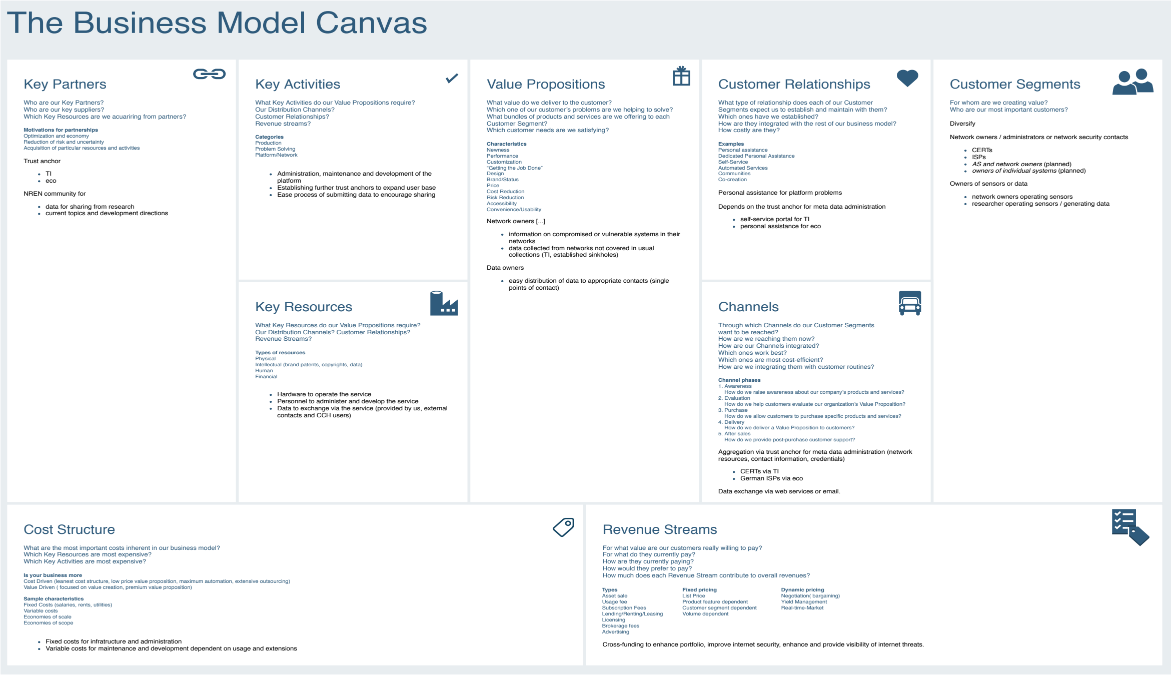
The above breakdown shows that about half of the incubators/accelerators identified are either directly linked to a partner, or the partner has some knowledge or loose ties with the entity. However, the other half of entities are not directly linked to the project, and reveals potential space for effort to be placed in the next years to establish such relationships.

2.5. Business Models

The committee requested input from the consortium partners, in order for them to perform a first attempt in what could be considered a business model for their exploitable results. This input request was intended for the partners to assess and understand the maturity of their idea(s), the potential it has with respect to the market it targets, resources it needs to become viable, potential competitors in each market. The input for this request can be provided as a business canvas, and/or a table with Porter analysis, to record possible effort that can be rolled out in the future, and be transformed into a real startup.

Indeed, some partners responded with preliminary business canvases. We can see some examples in Figure 2 and Figure 3. The committee acknowledged that it is too early in the project for all the partners to have a proper and well formalized business model that can be shared. Therefore, more rounds of such data collections will be executed in the future, for the committee to have an always up-to-date view of the business models of partners.

Furthermore, the committee identified the need for the execution of dedicated sessions with the partners for educational and support purposes, to help and guide them through the process of creating a business canvas and building a successful business model. These sessions will need to be structured with the participation of partners who have experience in business building and supporting, as well as the consortium partners who are interested in pursuing their (research and innovation) ideas into full business startups. The consortium will look into the appropriate planning of such sessions within the next year.



The Business Model Canvas

Key Partners

Who are our Key Partners?
Who are our key suppliers?
Which Key Resources are we acuariring from partners?

Motivations for partnerships
Optimization and economy
Reduction of risk and uncertainty
Acquisition of particular resources and activities

Trust anchor

- TI
- eco

NREN community for

- data for sharing from research
- current topics and development directions

Key Activities

What Key Activities do our Value Propositions require?
Our Distribution Channels?
Customer Relationships?
Revenue streams?

Categories
Production
Problem Solving
Platform/Network

- Administration, maintenance and development of the platform
- Establishing further trust anchors to expand user base
- Ease process of submitting data to encourage sharing

Key Resources

What Key Resources do our Value Propositions require?
Our Distribution Channels? Customer Relationships?
Revenue Streams?

Types of resources
Physical
Intellectual (brand patents, copyrights, data)
Human
Financial

- Hardware to operate the service
- Personnel to administer and develop the service
- Data to exchange via the service (provided by us, external contacts and CCH users)

Value Propositions

What value do we deliver to the customer?
Which one of our customer's problems are we helping to solve?
What bundles of products and services are we offering to each Customer Segment?
Which customer needs are we satisfying?

Characteristics
Newness
Performance
Customization
"Getting the Job Done"
Design
Brand/Status
Price
Cost Reduction
Risk Reduction
Accessibility
Convenience/Usability

Network owners [...]

- information on compromised or vulnerable systems in their networks
- data collected from networks not covered in usual collections (TI, established sinkholes)

Data owners

- easy distribution of data to appropriate contacts (single points of contact)

Customer Relationships

What type of relationship does each of our Customer Segments expect us to establish and maintain with them?
Which ones have we established?
How are they integrated with the rest of our business model?
How costly are they?

Examples
Personal assistance
Dedicated Personal Assistance
Self-Service
Automated Services
Communities
Co-creation

Personal assistance for platform problems

Depends on the trust anchor for meta data administration

- self-service portal for TI
- personal assistance for eco

Channels

Through which Channels do our Customer Segments want to be reached?
How are we reaching them now?
How are our Channels integrated?
Which ones work best?
Which ones are most cost-efficient?
How are we integrating them with customer routines?

Channel phases
1. Awareness
How do we raise awareness about our company's products and services?
2. Evaluation
How do we help customers evaluate our organization's Value Proposition?
3. Purchase
How do we allow customers to purchase specific products and services?
4. Delivery
How do we deliver a Value Proposition to customers?
5. After sales
How do we provide post-purchase customer support?

Aggregation via trust anchor for meta data administration (network resources, contact information, credentials)

- CERTs via TI
- German ISPs via eco

Data exchange via web services or email.

Customer Segments

For whom are we creating value?
Who are our most important customers?

Diversify

Network owners / administrators or network security contacts

- CERTs
- ISPs
- *AS and network owners* (planned)
- *owners of individual systems* (planned)

Owners of sensors or data

- network owners operating sensors
- researcher operating sensors / generating data

Cost Structure

What are the most important costs inherent in our business model?
Which Key Resources are most expensive?
Which Key Activities are most expensive?

Is your business more
Cost Driven (leanest cost structure, low price value proposition, maximum automation, extensive outsourcing)
Value Driven (focused on value creation, premium value proposition)

Sample characteristics
Fixed Costs (salaries, rents, utilities)
Variable costs
Economies of scale
Economies of scope

- Fixed costs for infratructure and administration
- Variable costs for maintenance and development dependent on usage and extensions

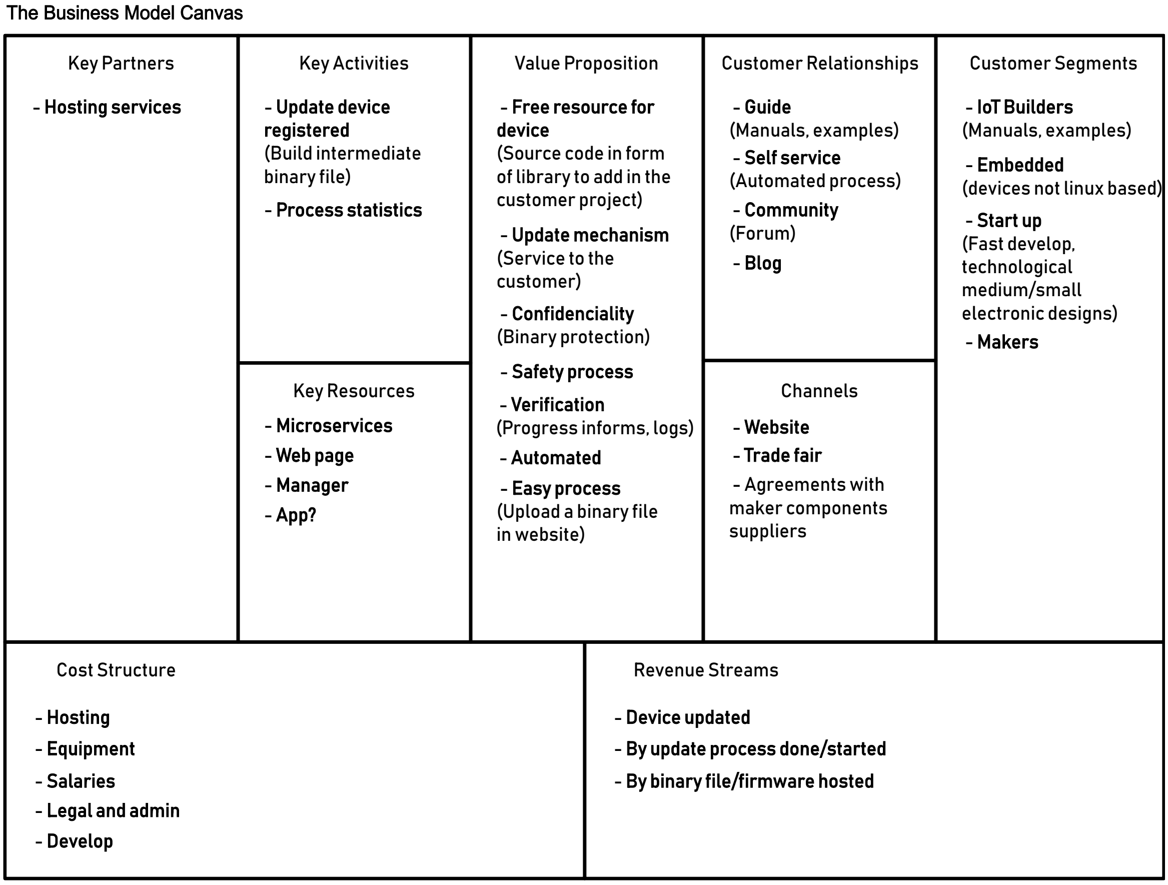
Revenue Streams

For what value are our customers really willing to pay?
For what do they currently pay?
How are they currently paying?
How would they prefer to pay?
How much does each Revenue Stream contribute to overall revenues?

Types	**Fixed pricing**	**Dynamic pricing**
Asset sale	List Price	Negotiation(bargaining)
Usage fee	Product feature dependent	Yield Management
Subscription Fees	Customer segment dependent	Real-time-Market
Lending/Renting/Leasing	Volume dependent	
Licensing		
Brokerage fees		
Advertising		

Cross-funding to enhance portfolio, improve internet security, enhance and provide visibility of internet threats.

Figure 2: The business model canvas from DFN-CERT on their product, CCH.



The Business Model Canvas

Key Partners

- **Hosting services**

Key Activities

- **Update device registered** (Build intermediate binary file)
- **Process statistics**

Key Resources

- **Microservices**
- **Web page**
- **Manager**
- **App?**

Value Proposition

- **Free resource for device** (Source code in form of library to add in the customer project)
- **Update mechanism** (Service to the customer)
- **Confidenciality** (Binary protection)
- **Safety process**
- **Verification** (Progress informs, logs)
- **Automated**
- **Easy process** (Upload a binary file in website)

Customer Relationships

- **Guide** (Manuals, examples)
- **Self service** (Automated process)
- **Community** (Forum)
- **Blog**

Channels

- **Website**
- **Trade fair**
- Agreements with maker components suppliers

Customer Segments

- **IoT Builders** (Manuals, examples)
- **Embedded** (devices not linux based)
- **Start up** (Fast develop, technological medium/small electronic designs)
- **Makers**

Cost Structure

- **Hosting**
- **Equipment**
- **Salaries**
- **Legal and admin**
- **Develop**

Revenue Streams

- **Device updated**
- **By update process done/started**
- **By binary file/firmware hosted**

Figure 3: The business model canvas from EI on their proposed product.

2.6. Next Steps on Exploitation and Incubators

As the present investigation into avenues for exploitation has revealed, CONCORDIA has a deep reach into major accelerators and incubators across Europe and worldwide. This means great potential for the companies that will be initiated within the consortium based on technology built within CONCORDIA's duration, as well as afterwards.

However, there are several efforts that should be made in the upcoming years of the project, to connect deeper the academic and industrial partners, and enable closer collaboration with respect to the academic partners solving problems the industrial partners are facing, via true knowledge transfer between them. In particular, more efforts need to be placed in the collection of exploitable and other technology results by the participating partners and shared via the knowledge space of CONCORDIA.

CONCORDIA is committed to strong exploitation of all results that are exploitable from its industrial and academic partners. For this to happen, the consortium needs to dedicate resources and attention to its partners that need help with 1) identifying which components of their technology are novel, patentable, and worthy to support, and 2) defining appropriate and profitable business models. In this way, CONCORDIA can become a true innovation hub on cybersecurity in Europe, in which industrial and academic teams can exchange information and learn from each other.

3. Efforts on Dissemination & Communication

This part reports on the work executed in task T5.2 on Dissemination and Communication activities, with respect to the Communication strategy of CONCORDIA project. The reported effort is organized in three sections, namely:

1. The description of goals and objectives of this Task.
2. The strategy to achieve these goals.
3. The description of communication and dissemination activities performed in the first year of the project.

3.1. Objectives of Task (T5.2)

Communication activities are essential for the CONCORDIA project and a dedicated task was designated for their implementation (Figure 4). T5.2 organizes the transfer of knowledge and of project results, both within the consortium and to the outside world. It ensures that all involved organizations are kept informed and can promote project results. The interactive and online dissemination channels are of particular importance for influencing prospective adopters of the CONCORDIA technologies. Most importantly, this task will leverage the CONCORDIA working groups created in task T4.1, to engage the communication at large, and effectively promote the cybersecurity roadmap coming out of task T4.4.

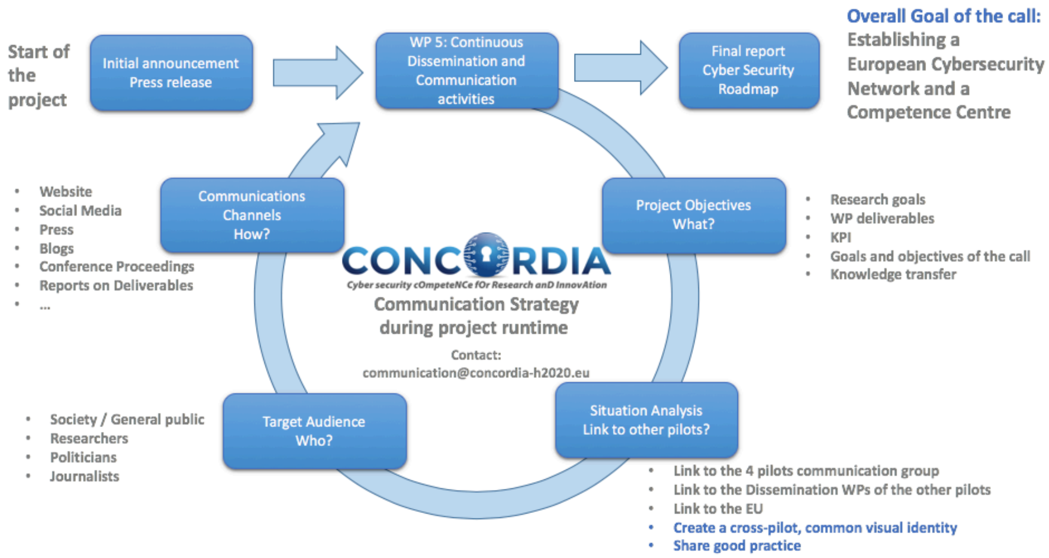

Start of the project
Initial announcement Press release
WP 5: Continuous Dissemination and Communication activities
Final report Cyber Security Roadmap
Overall Goal of the call:
Establishing a European Cybersecurity Network and a Competence Centre
Website
Social Media
Press
Blogs
Conference Proceedings
Reports on Deliverables
...
Communications Channels How?
Project Objectives What?
Research goals
WP deliverables
KPI
Goals and objectives of the call
Knowledge transfer
CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion
Communication Strategy during project runtime
Contact: communication@concordia-h2020.eu
Society / General public
Researchers
Politicians
Journalists
Target Audience Who?
Situation Analysis Link to other pilots?
Link to the 4 pilots communication group
Link to the Dissemination WPs of the other pilots
Link to the EU
Create a cross-pilot, common visual identity
Share good practice

Figure 4: CONCORDIA communications during project runtime.

Involvement in communication activities and work on the communication goals of the project is a common task of all partners. In charge of coordinating and implementing strategic communication activities is a communication group. The group is led by Masaryk University (MUNI) and has seven members, including work package leaders and the project coordinator.

Goals:

The primary purpose of communication is to support the achievement of project goals. Therefore, we set four general goals, which are aligned with the CONCORDIA objectives (Table 3).

Table 3: CONCORDIA communication goals.

Goal	Description
1	To build and to position the CONCORDIA brand to strengthen trust and raise awareness about the project.
2	To enhance the impact of CONCORDIA's outcomes by spreading knowledge and disseminating project results through all relevant channels to the outside world.
3	To exploit consortium communication potential by internal dissemination, gathering content about members activities and actively fostering their engagement.
4	To participate in building a common brand and in coordinated communication activities with the other cybersecurity pilots (SPARTA, ECHO and CyberSec4Europe).

Communication objectives:

In order to achieve the aforementioned goals, we defined specific objectives and activities that will be executed by the project. These communication objectives and activities defined below in Table 4 can be updated during the project in order to support communication goals appropriately.

Table 4: CONCORDIA Communication Objectives (CO).

CO	Name	Description	When
1	CONCORDIA website	We will create and regularly iterate the project website (www.concordia-h2020.eu). It will serve as a single-entry point to all the information about the project (project's presentations, deliverables, events, papers and publications, news, software updates etc.) and will support all of our communication goals. We expect more than 5,000 accesses per year worldwide.	M2 creation / continuous updates
2	CONCORDIA visual identity	We will prepare and constantly apply a CONCORDIA visual identity in order to build our brand. Specifically, this means the logo and various types of templates.	M1-M3 preparation M3-M48 application
3	Internal communication instructions	We will create internal instructions for partners that accurately describe what to do to support our goals, while keeping communications consistent. Involvement in communication activities and work on our goals is a common task of all project partners. We will actively foster the consortium members and our partners to engage in communication activities	M1-M6 preparation, M6-M48 regularly updates and reminders
4	Printed materials	We will prepare printed materials (e.g. banners, posters and flyers) to raise awareness regarding the project and build the CONCORDIA brand by delivery of key messages to our target audiences.	M1-M6 preparation updates when needed

5	Event participation	We will participate in relevant events in order to build our brand and share our results.	M1-M48
6	Blog posts	We will regularly publish blog posts on the CONCORDIA project activities. The purpose of the blog posts is to raise public awareness of the project by increasing understanding of what we do and what the benefits are. We want to deliver useful content about our work in CONCORDIA. To achieve this CO, it was also necessary to create an internal plan, a blog post template and appropriate processes for successful implementation.	M9-M48
7	Social media presence	We will be actively present on Twitter, Facebook and LinkedIn. The activity will be monitored based on the total number of views and likes (15,000 as KPI-DC-10).	M1-M48
8	Dissemination of results	We will use various forms to disseminate the project results (e.g. documents, papers, deliverables, technical reports, presentations, fact sheets, infographics or even video clips). Specific forms will be selected based on the available skillset and context. The number of unique materials generated is counted as KPI-DC-3 and downloads of them are counted as KPI-DC-4 (500).	M6-M48
9	Publicity activities	We will exploit all relevant communication opportunities which will occur during the project to support our communication goals. For example – workshops and webinars, media relations, sponsorship, cooperation with cybersecurity initiatives, education activities, targeted focus groups with EU officials, policymakers, ECSO and cPPP officials and other stakeholder organizations.	M3-M48
10	CCN coordinated communication activities	We will participate in coordinated communication activities withthe other pilots (ECHO, SPARTA, CYBERSEC4ERUPE) This includes meetings, group calls, chairing the coordination communication group for six months every two years, preparation of events, and creating relevant content.	M1-M48 - chairing the coordination communication group for six months every two years (start M1-M6)

Communication phases:

CONCORDIA communication and dissemination activities are, in general, divided into five distinctive phases, as explained in the next Table 5: the starting phase of the project, the phase where publicity about the project is increased, the phase for disseminating project results, the closing phase where the project is finishing, and finally, the phase after the project's termination, in which we promote further the CONCORDIA's results to influence the definition of the future cybersecurity roadmap of EU.

Table 5: CONCORDIA communication phases.

Phase	Description	Time	Dependencies
Starting phase	The purpose of this phase is to prepare the basic starting points for the successful implementation of communication activities. Especially, preparation of basic communication channels, the formation of a communication group and specification of communication strategy.	M1-M6	
Publicity phase	The purpose of this phase is to increase publicity of the project and support the building and positioning of the CONCORDIA brand. We use a wide range of communication tactics and focus on professionals and the general public. We try to communicate with them in particular the basic facts about the project and our key messages.	M6-M15	Cooperation of Consortium
Dissemination phase	At this phase, in addition to strengthening our brand, we will focus primarily on sharing project results and increasing their impact.	M15-M36	Technical and scientific achievements of the project and Cooperation of Consortium
Closing phase	This phase will build on the activities of the previous ones and, moreover, its purpose will be to promote the cybersecurity roadmap (Task 4.4) and summarize the overall results and benefits of the CONCORDIA project.	M36-M48	Technical and scientific achievements of the project and Cooperation of Consortium
After project phase	During this phase, we will ensure that the website will stay alive for at least three (3) years after the completion of the project. This way all available material will be available to future projects and whoever is interested in the outcomes of CONCORDIA. The social media channels will also be active because the results of the project can also be found through those channels as well through internet search engines.	Three years	

3.2. Strategy to Achieve Task Objectives

In order to achieve our goals, we focus on strategic planning. Our communication strategy answers the following questions:

- What do we want to communicate?
- To whom do we communicate?
- How do we communicate?

3.2.1. What do we want to communicate?

To support our communication goals, we will focus on the communication of facts about the project, project results and our key messages.

CONCORDIA facts:

This covers many topics which are not directly related to our work packages. For example, our successes, introducing of project partners, "backstage" information, planned actions, consortium internal events, etc.

CONCORDIA results with communication potential:

We communicate about project results with communication potential from all work packages 1, 2, 3, 4, 5 and 6.

CONCORDIA narrative:

The leitmotiv for our communications activities in one sentence: We formed the CONCORDIA consortium to take the lead in connecting European cybersecurity competencies in order to overcome future challenges and threats.

CONCORDIA key messages:

Key messages are based on the narrative, and their purpose is consistency in communication about basic facts of the project.

- Who we are and what is our purpose: We are a dedicated consortium of 51 partners (27 research, 24 industry) Our purpose is to lead the boosting of Europe's cybersecurity future.
- What we do: We are leading the integration of Europe's excellence cybersecurity competencies into a network of expertise to build a secure, resilient and trusted ecosystem in Europe.
- Why it matters: The cybersecurity ecosystem will be one of the pillars of Europe's future. We need to be secure and resilient against cybersecurity threats which are increasingly relevant to our whole society and also to the life of each of us.
- What is our relation to other cybersecurity pilots: We are one of several Horizon 2020 projects, all of which share the purpose to help the EU retain and develop the cybersecurity technological and industrial capacities necessary to secure its Digital Single Market and to strengthen Europe's cybersecurity and place Europe in a leading position in cybersecurity.
- How we differ from other cybersecurity pilots:
    - We comprehensively interconnect academia, SME, CERTs, public bodies, policymakers and moreover we have engaged several strong industry partners to ensure the lasting impact of our work.
    - CONCORDIA is the first competence network which takes a holistic, scalable and technology-adaptive data-centric approach to cybersecurity.
    - We are developing solutions like Threat Intelligence for Europe, DDoS Clearing House as building blocks of a European cybershield.
    - We are developing innovative cybersecurity solutions with the industry in five vertical sectors.
    - We are building a comprehensive European cybersecurity educational ecosystem.
- What are the benefits of the CONCORDIA project? Creating a European cybersecurity competence network will bring many benefits. In fact, it will:

  - Unite the fragmented European cybersecurity landscape which will lead to better cooperation and better use of research results;
  - Bring innovation into research, education, policy, roadmaps and governance;
  - Increase industry impact by actively considering its problems;
  - Develop industrial pilots and next-generation cybersecurity solutions;
  - Launch Open Calls to allow entrepreneurs and individuals to stress their solutions with the development;
  - Devise a cybersecurity roadmap to establish technology, socio-economic, legal and privacy directions for Europe;
  - Provide expertise to European policymakers and industry;
  - Improve quality of life through advanced and safer services in Telecommunications, e-Health, Finance and e-mobility;
  - Enhance Europe's digital sovereignty.
- Call to action: Follow us on:
  - Website: https://www.concordia-h2020.eu
  - Twitter: https://twitter.com/concordiah2020
  - LinkedIn: https://www.linkedin.com/in/concordia-h2020/
  - Facebook: https://www.facebook.com/concordia.eu/

3.2.2. To whom do we communicate?

For the CONCORDIA project, the following target audiences are especially relevant.

General public:
We address the general public to support the image of CONCORDIA’s brand and to raise public awareness and interest in the project by increasing understanding of what we do and what are the benefits from the project. We also promote other H2020 cybersecurity pilots.

Consortium members and partners:
We address the consortium members and partners to support the image of CONCORDIA’s brand, to enhance the impact of CONCORDIA’s outcomes and to exploit consortium communication potential.

Industry, professionals and stakeholders:
We address the industry, professionals and CONCORDIA stakeholders (T4.6) to support the image of CONCORDIA’s brand and enhance the impact of CONCORDIA’s outcomes.

Scientific community:
We address the scientific community to support the image of CONCORDIA’s brand and enhance the impact of CONCORDIA’s outcomes which are relevant for the scientific community.

Policymakers:
We address the policymakers to support the image of CONCORDIA’s brand and to enhance the impact of CONCORDIA’s outcomes and to promote the cybersecurity roadmap (task T4.4).

Cybersecurity initiatives:
We address the media and cybersecurity initiatives to support the image of CONCORDIA’s brand and to build relations with initiatives in the cybersecurity domain (e.g. cyberwatching.eu) by sharing knowledge and project results.

Media:
We address the media to support the image of CONCORDIA's brand and to enhance the impact of CONCORDIA's most promising outcomes.

3.2.3. How do we communicate?

This section describes how we communicate to our target audiences in order to reach our communication goals. It describes our channels and methods.

Project website (www.concordia-h2020.eu):
This is a single-entry point to all the information about the project (project's presentations, deliverables, events, papers and publications, news, software updates, etc.). This channel is relevant to all our target audiences and all our communication goals. The project website will also be propagated by all other channels. Website's traffic will be monitored via Google Analytics.

Visual identity:
This is essential for brand building, as it represents one of its most visible external representations. Together with our narrative and key messages, visual identity is an important tool that helps us to be consistent in our communication activities. By visual identity is meant especially the logo and templates for presentations, printed materials and posters.

Printed materials:
Items such as roll ups, banners, posters, flyers, etc., are a complementary communication channel designed to raise awareness of the project and build its brand by delivery of project key messages to our target audiences.

Social media:
These are in general relevant to all our target audiences, and they will primarily support the building of the CONCORDIA's brand, raising public awareness and enhancing the impact of CONCORDIA's outcomes. We will use these channels:

- Twitter: https://twitter.com/concordiah2020
- Facebook: https://www.facebook.com/concordia.eu/
- Linkedin: https://www.linkedin.com/company/concordia-eu/

Internal communication channels:
Such channels will be used to transfer knowledge and project results within the consortium and also to gather the content about consortium members activities and foster their engagement. The main communication channels of CONCORDIA are:

- Email (Email mailing lists)
- Synchronized file repository (GIT, Confluence)
- Audio/video conferences.
- Physical face-to-face meetings.

They are described in more detail in the Project Handbook (Deliverable D6.1).

Blog posts:
The purpose of the blog posts is to raise public awareness of the project by increasing understanding of what we do and what the benefits are. We want to deliver useful content about our work in CONCORDIA.

Consortium members and partners owned media:

There is huge potential in partners' owned media for spreading the knowledge and project results (their websites, social media channels, bulletins, events, etc.). These media have the potential to help us reach our communication goals and address multiple audiences.

Cybersecurity initiatives:

We will cooperate with initiatives in the cybersecurity to support the image of CONCORDIA's brand and to enhance the impact of CONCORDIA's outcomes especially for industry, professionals and scientific community.

Consortium activities with communication potential:

The consortium will engage in many activities which have communication potential to disseminate the project results. Examples of such activities are dissemination activities, scientific events, workshops, webinars, conferences, education activities, targeted focus groups with EU officials, policymakers, ECSO and cPPP officials and other stakeholder organizations. These activities will also be used to support the image of CONCORDIA's brand and to enhance the impact of CONCORDIA's outcomes.

Various dissemination forms:

We can use different forms to disseminate the project results (e.g., documents, papers, deliverables, technical reports, presentations, fact sheets, infographics or even video clips). Specific forms will be selected based on the available skillset and context. One of the special forms for dissemination can be media relations for amplifying the most promising outcomes through cybersecurity relevant media or even through media in general via press releases or other suitable methods.

H2020 cybersecurity pilots coordinated communication activities:

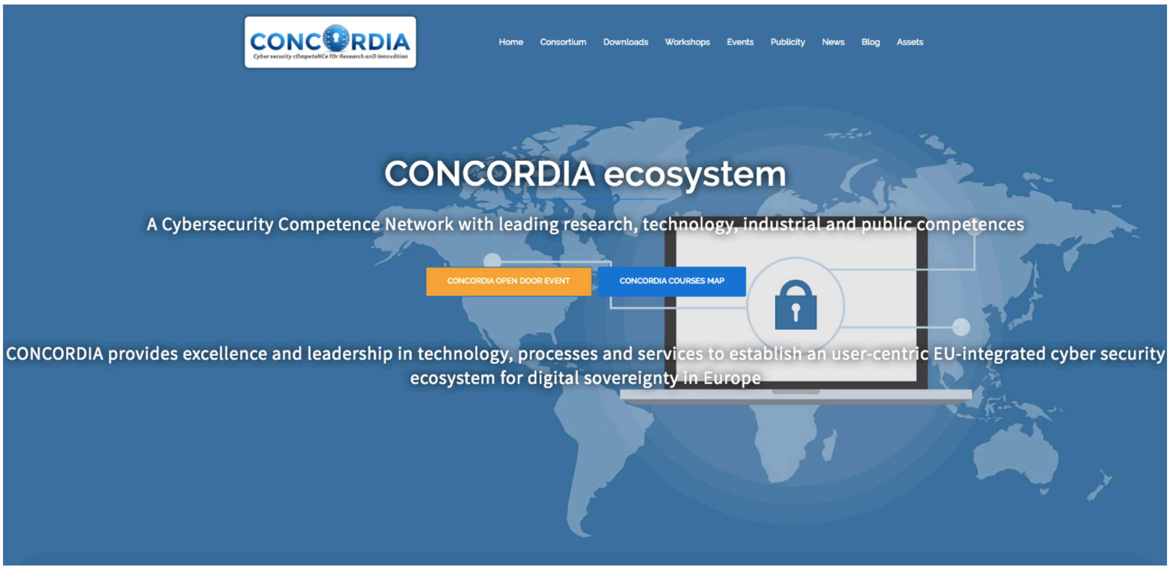
We will engage in all coordinated communication activities of H2020 cybersecurity pilots, especially common website, events and we will use shared visual identity in relevant situations.

3.3. Communication & Dissemination Activities

This section describes the communication and dissemination activities carried out during the first year of the CONCORDIA project. It is structured according to our communication objectives, which were mentioned in the previous paragraphs.

3.3.1. CONCORDIA website

The CONCORDIA website (www.concordia-h2020.eu) is a single-entry point to all the information about the project and also one of the main dissemination channels. Our target audiences will gain access to CONCORDIA results, publications, news and new tools developed in the context of this project through the website. The basic version of the website was prepared at the beginning of the project and since then it has been regularly iterated and new content uploaded. The website is designed in such a way that it meets the communication and dissemination needs of wide range of users.



CONCORDIA ecosystem

A Cybersecurity Competence Network with leading research, technology, industrial and public competences

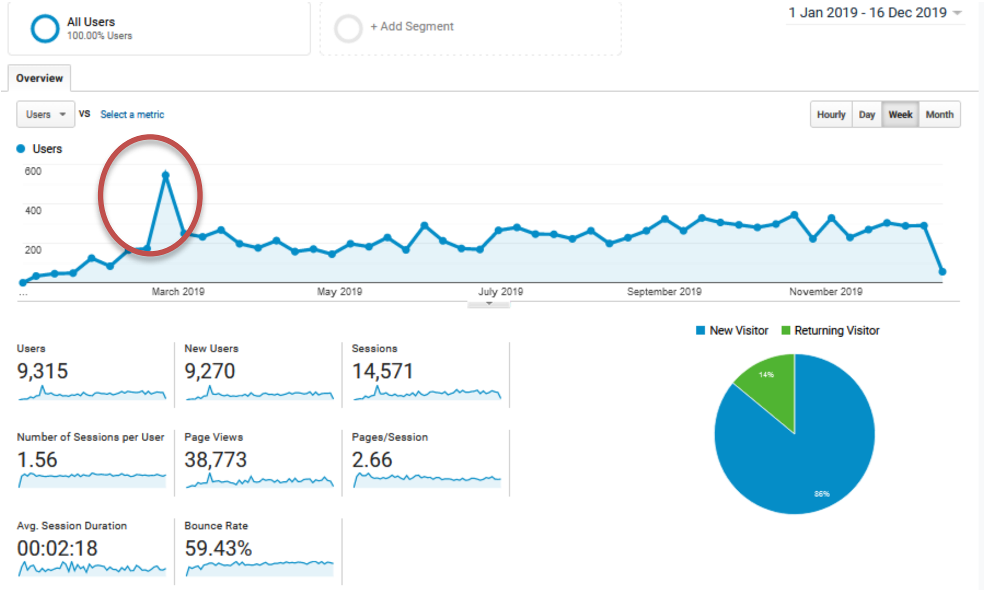
CONCORDIA provides excellence and leadership in technology, processes and services to establish an user-centric EU-integrated cyber security ecosystem for digital sovereignty in Europe

Figure 5: CONCORDIA website (homepage).

More information on how the website has been implemented, the various sections offered to the visitor and some more technical details are included in the deliverable D5.1: Website and Social Media presences, which is listed under the Publications sections. In this section, we will provide only statistics for the first year of the project (2019).

Website Visitors and Trend:

The users that were served by the CONCORDIA website per week during the first year of the project can be seen in the
Figure **6**. We can see that more than 9000 users were recorded in this period. This means that we had an approximate of more than 20 visits per day. The spike during March is due to the publicity gained from the meeting in Strasbourg with the Commissioner, the DG Director and the Project Officer. The figure also presents that these visitors created 14K sessions against the website which resulted in 38K served webpages. This is about 100 webpages per day.



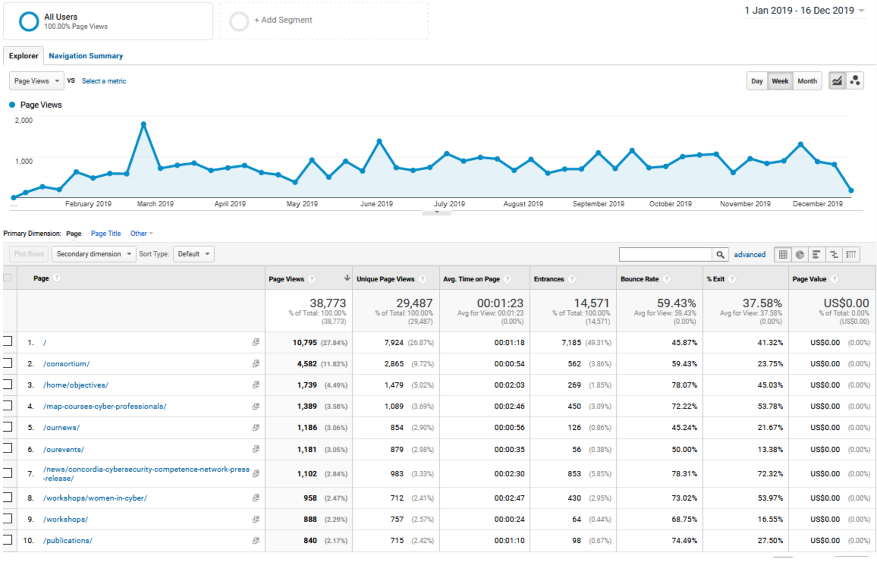
Users	New Users	Sessions
9,315	9,270	14,571

Number of Sessions per User	Page Views	Pages/Session
1.56	38,773	2.66

Avg. Session Duration	Bounce Rate
00:02:18	59.43%

Figure 6: Users per week that visited the CONCORDIA website. With red circle we mark the meeting in Strasbourg.

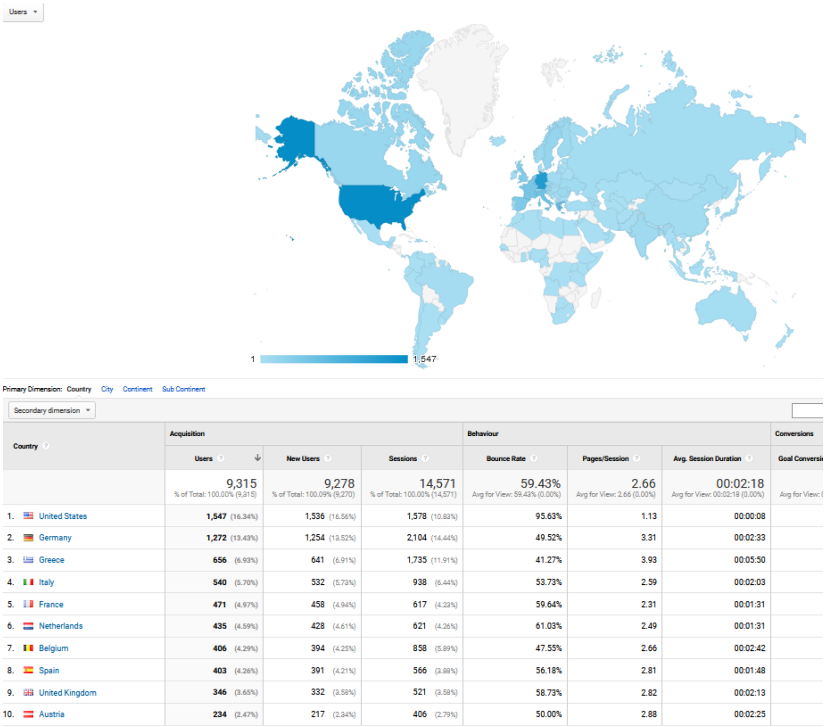
Figure 7 presents the most popular pages of the website during the reporting period. Naturally the most visited page in the welcome page followed by the Consortium page and the Objectives page of the project respectively. A quite normal behaviour for a visitor who is willing to learn more about the CONCORDIA consortium (who are they?) and the Objectives of the project (what are they trying to achieve?). Moreover, we can see that visitors were interested in the CONCORDIA courses map, the women in cybersecurity activities, the workshops (including the CONCORDIA Open Door event) and the publications produced.



	Page	Page Views	Unique Page Views	Avg. Time on Page	Entrances	Bounce Rate	% Exit	Page Value
		38,773 % of Total: 100.00% (38,773)	29,487 % of Total: 100.00% (29,487)	00:01:23 Avg for View: 00:01:23 (0.00%)	14,571 % of Total: 100.00% (14,571)	59.43% Avg for View: 59.43% (0.00%)	37.58% Avg for View: 37.58% (0.00%)	US$0.00 % of Total: 0.00% (US$0.00)
1.	/	10,795 (27.84%)	7,924 (26.87%)	00:01:18	7,185 (49.31%)	45.87%	41.32%	US$0.00 (0.00%)
2.	/consortium/	4,582 (11.82%)	2,865 (9.72%)	00:00:54	562 (3.86%)	59.43%	23.75%	US$0.00 (0.00%)
3.	/home/objectives/	1,739 (4.49%)	1,479 (5.02%)	00:02:03	269 (1.85%)	78.07%	45.03%	US$0.00 (0.00%)
4.	/map-courses-cyber-professionals/	1,389 (3.58%)	1,089 (3.69%)	00:02:46	450 (3.09%)	72.22%	53.78%	US$0.00 (0.00%)
5.	/ournews/	1,186 (3.06%)	854 (2.90%)	00:00:56	126 (0.86%)	45.24%	21.67%	US$0.00 (0.00%)
6.	/ourevents/	1,181 (3.05%)	879 (2.98%)	00:00:35	56 (0.38%)	50.00%	13.38%	US$0.00 (0.00%)
7.	/news/concordia-cybersecurity-competence-network-press-release/	1,102 (2.84%)	983 (3.33%)	00:02:30	853 (5.85%)	78.31%	72.32%	US$0.00 (0.00%)
8.	/workshops/women-in-cyber/	958 (2.47%)	712 (2.41%)	00:02:47	430 (2.95%)	73.02%	53.97%	US$0.00 (0.00%)
9.	/workshops/	888 (2.29%)	757 (2.57%)	00:00:24	64 (0.44%)	68.75%	16.55%	US$0.00 (0.00%)
10.	/publications/	840 (2.17%)	715 (2.42%)	00:01:10	98 (0.67%)	74.49%	27.50%	US$0.00 (0.00%)

Figure 7: CONCORDIA pages with the most page views.

Additionally, in Figure 8 we show the geographic origin of visitors who requested all the previously mentioned pages from the CONCORDIA webserver. Most visitors come from US and Germany, followed by visitors in Greece, Italy, France, Netherlands and Belgium.



	Country	Acquisition			Behaviour			Conversions
		Users	New Users	Sessions	Bounce Rate	Pages/Session	Avg. Session Duration	Goal Conversi
		9,315 % of Total: 100.00% (9,315)	9,278 % of Total: 100.09% (9,270)	14,571 % of Total: 100.00% (14,571)	59.43% Avg for View: 59.43% (0.00%)	2.66 Avg for View: 2.66 (0.00%)	00:02:18 Avg for View: 00:02:18 (0.00%)	Avg for View: (
1.	🇺🇸 United States	1,547 (16.34%)	1,536 (16.56%)	1,578 (10.83%)	95.63%	1.13	00:00:08	
2.	🇩🇪 Germany	1,272 (13.43%)	1,254 (13.52%)	2,104 (14.44%)	49.52%	3.31	00:02:33	
3.	🇬🇷 Greece	656 (6.93%)	641 (6.91%)	1,735 (11.91%)	41.27%	3.93	00:05:50	
4.	🇮🇹 Italy	540 (5.70%)	532 (5.73%)	938 (6.44%)	53.73%	2.59	00:02:03	
5.	🇫🇷 France	471 (4.97%)	458 (4.94%)	617 (4.23%)	59.64%	2.31	00:01:31	
6.	🇳🇱 Netherlands	435 (4.59%)	428 (4.61%)	621 (4.26%)	61.03%	2.49	00:01:31	
7.	🇧🇪 Belgium	406 (4.29%)	394 (4.25%)	858 (5.89%)	47.55%	2.66	00:02:42	
8.	🇪🇸 Spain	403 (4.26%)	391 (4.21%)	566 (3.88%)	56.18%	2.81	00:01:48	
9.	🇬🇧 United Kingdom	346 (3.65%)	332 (3.58%)	521 (3.58%)	58.73%	2.82	00:02:13	
10.	🇦🇹 Austria	234 (2.47%)	217 (2.34%)	406 (2.79%)	50.00%	2.88	00:02:25	

Figure 8: Top 10 countries visiting the CONCORDIA website.

3.3.2. CONCORDIA visual identity

The visual identity authenticates and strengthens the communication and dissemination activities of CONCORDIA and helps to build our brand. It ensures that all communication and dissemination products, including reports, the website, flyers, posters and presentation slides have a consistent look. The core element of the project's visual identity is the CONCORDIA logo.

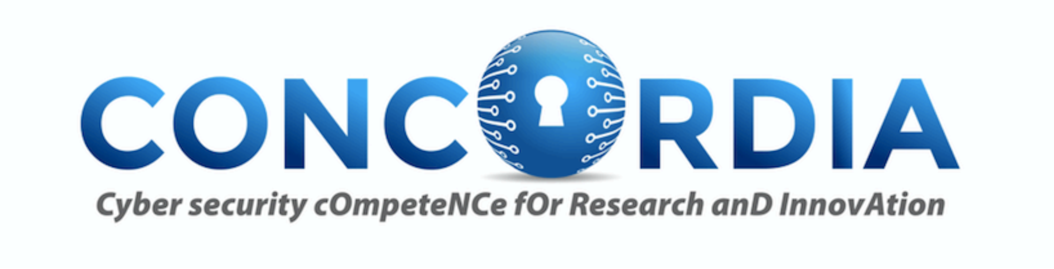
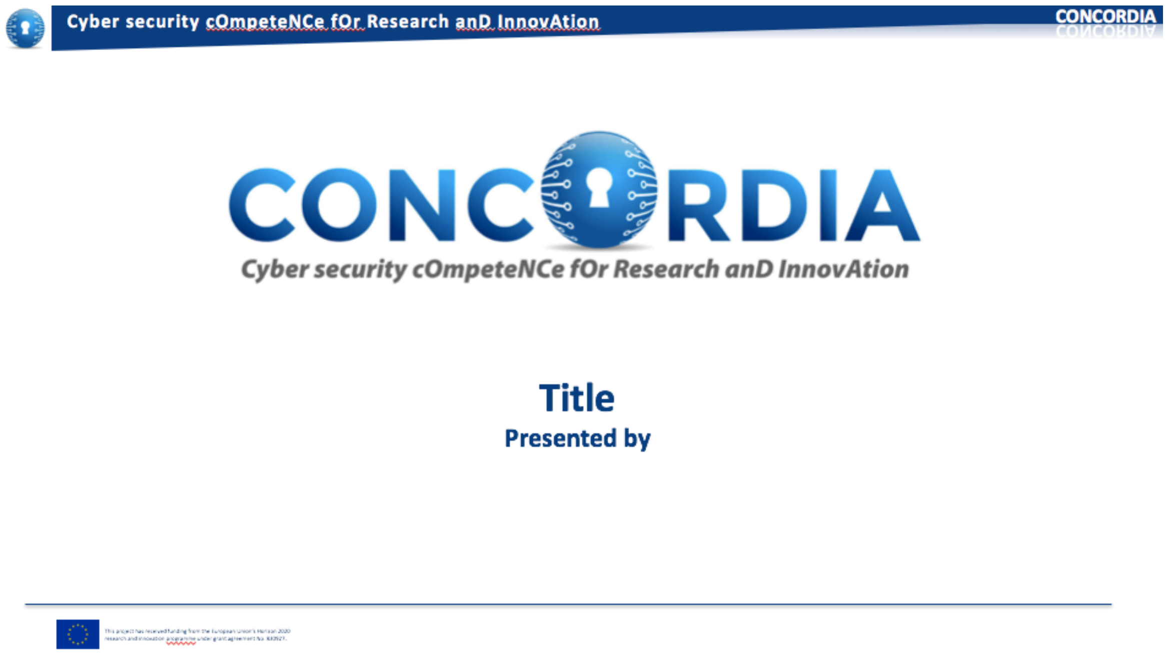


Figure 9: CONCORDIA logo.

Templates for different uses were developed and distributed for mandatory use within the consortium. Templates are based on our visual identity and include our key messages. All templates were created from scratch, but experience from similar projects was considered in their development. Currently, we have templates for:

- Presentations
- Posters
- Invitations
- Flyers
- Postcards
- Rollups
- Deliverables



Cyber security cOmpeteNCe fOr Research anD InnovAtion

CONCORDIA

CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

Title

Presented by

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830927.

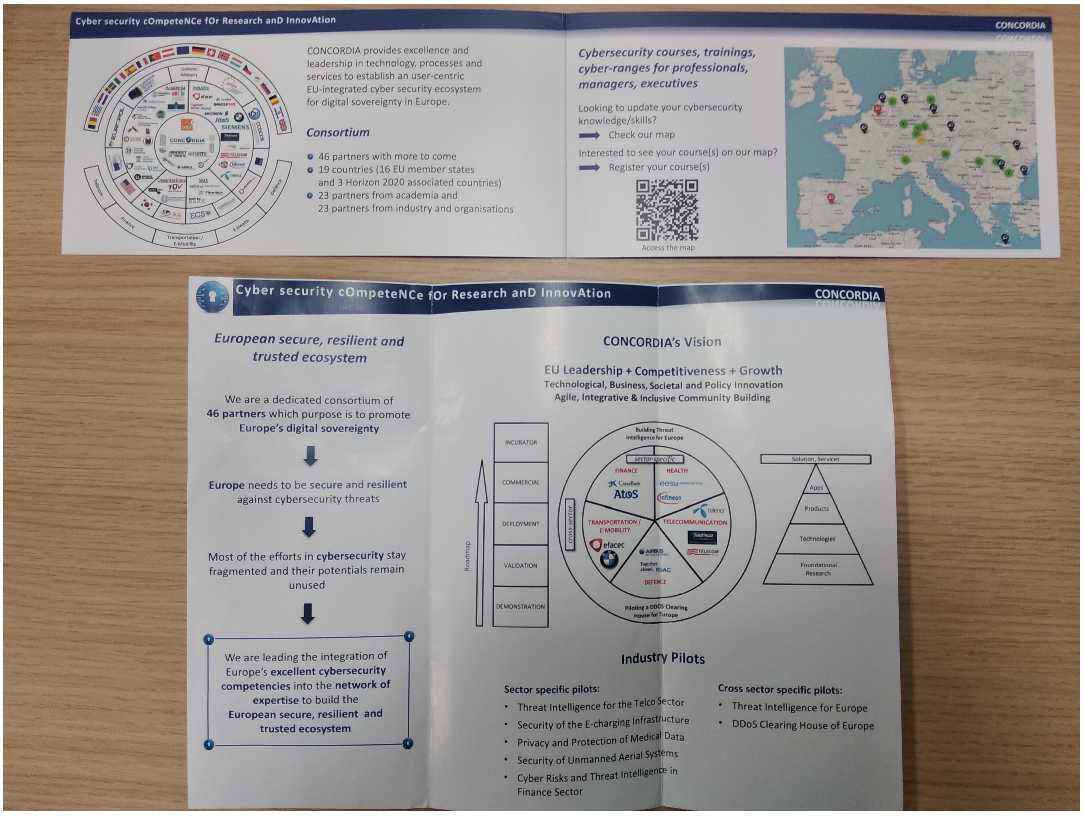
Figure 10: Example of CONCORDIA templates (template for presentations).

3.3.3. Internal communication instructions

The CONCORDIA project consortium has officially 51 partners and continues to grow. With such a large number of partners, it is important to work to make our communication consistent. That is why we created a simple internal document - "CONCORDIA's communication cheat sheet", which purpose is to equip all members of the consortium with the necessary knowledge about our communication strategy and their involvement into communication activities. This document also describes which content should task leaders and other project partners send to the communication group. This document is further updated and shared within the consortium via our internal communication channels.

3.3.4. Printed materials

We have prepared two types of printed flyers (Figure 11) that serve as supporting communication materials for raising awareness of the project and building its brand. They are used mainly at CONCORDIA project events. We have also prepared several banners that summarize the key project news. The specific printed output was "Women in Cyber - a Manifesto for TODAY", which was produced as an output from the specialized task in Work Package 4 (WP4).



Cyber security cOmpeteNCe fOr Research anD InnovAtion

CONCORDIA provides excellence and leadership in technology, processes and services to establish an user-centric EU-integrated cyber security ecosystem for digital sovereignty in Europe.

Consortium

- 46 partners with more to come
- 19 countries (16 EU member states and 3 Horizon 2020 associated countries)
- 23 partners from academia and 23 partners from industry and organisations

Cybersecurity courses, trainings, cyber-ranges for professionals, managers, executives

Looking to update your cybersecurity knowledge/skills?

➡ Check our map

Interested to see your course(s) on our map?

➡ Register your course(s)

Access the map

CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

CONCORDIA

European secure, resilient and trusted ecosystem

We are a dedicated consortium of **46 partners** which purpose is to promote **Europe's digital sovereignty**

⬇

Europe needs to be secure and **resilient** against cybersecurity threats

⬇

Most of the efforts in **cybersecurity** stay fragmented and their potentials remain unused

⬇

We are leading the integration of Europe's **excellent cybersecurity competencies** into the **network of expertise** to build the **European secure, resilient and trusted ecosystem**

CONCORDIA's Vision

EU Leadership + Competitiveness + Growth
Technological, Business, Societal and Policy Innovation
Agile, Integrative & Inclusive Community Building

Industry Pilots

Sector specific pilots:

- Threat Intelligence for the Telco Sector
- Security of the E-charging Infrastructure
- Privacy and Protection of Medical Data
- Security of Unmanned Aerial Systems
- Cyber Risks and Threat Intelligence in Finance Sector

Cross sector specific pilots:

- Threat Intelligence for Europe
- DDoS Clearing House of Europe

Figure 11: CONCORDIA flyers.

3.3.5. Event participation

The following table includes a list of 61 conferences, workshops and other events where CONCORDIA was present through participation of its partners. The events are of different types and the table presents the title, type of event, date it was performed and location in the world.

Table 6: Events where CONCORDIA was present

Title	Event	Date	Place
Implementing AI pipelines for Cyber Security	ENISA Artificial Intelligence – An opportunity for the EU cyber-crisis management blueprint workshop	June 3-4, 2019	Athens, Greece
Cyber Autonomous Response, Cyber Threat Detection and Security Automation	ENISA Artificial Intelligence – An opportunity for the EU cyber-crisis management blueprint workshop	June 3-4, 2019	Athens, Greece
CONCORDIA in a Nutshell	ITASEC 2019	Sept 12-15, 2019	Pisa, Italy
Cross-industry Innovation Ecosystem for Cyber Security	Market-Driven Innovation in R&D	Sept 25-27 2019	Berlin, Germany
Who Let The Trolls Out? Towards Understanding State-Sponsored Trolls	ACM International Web Science Conference (WebSci), 2019	June 30 – July 3, 2019	Boston, USA
Disinformation Warfare: Understanding State-Sponsored Trolls On Twitter And Their Influence On The Web	Workshop On Computational Methods In CyberSafety, Online Harassment And Misinformation, 2019	May 13, 2019 - May 14, 2019	San Francisco, California, USA
Strengthen Cybersecurity by an Data-driven Adaptive Approach	Vienna Cybersecurity Week (March 11-15, 2019), Session on "The future of cyber security: research and expectations"	15.3.2019	Vienna, Austria
TUD CyberSecurity Info Workshop: Cyber Techniques for CIP	TUD Solicitation of Industry Challenges in CIP CyberSecurity	16.01.2019	Darmstadt, Germany
CONCORDIA's System-Centric Security Approaches	IFIP WG10.4 Workshop on Autonomous Security	22-28.01.2019	Champery, Switzerland
Security in the Smart Grid	Embedded World Conference	28.02.2019	Nurenberg, Germany
Security Hardening of Distributed Software	Seminars	21-28.02.2019	New York, USA
A Systems View on CyberSecurity	Seminars+Meetings	05-17.03.2019	USA
The Big MAC Angle in CyberSecurity: Metrics, Abstractions and Compositions	German Cybersecurity Doctoral Workshop + Siemens	10-12.04.2019	Passau, Germany
Towards Holistic IoT Security: Continuous Security Assurance in the Cloud		14.05.2019	Darmstadt, Germany
Kicking & Fixing Software	BT, Turing Institute	07-08.05.2019	London, UK

Validating Cyber secure Safety-Critical Software	Airbus	17.05.2019	Hamburg, Germany
Threat Modeling for Cloud Environment	IEEE Symposium on Security and Privacy 2019	20-22.05.2019	San Francisco, USA
Assessing the State and Improving the Art of Parallel Testing for C	ACM SIGSOFT International Symposium on Software Testing and Analysis	17-19.07.2019	China
National cyber/ICT security updates, threats to inter-state relations stemming from the use of ICTs and good practices for regional co-operation	OSCE sub-regional training	7-8.02.2019	Athens
Protection of Critical Infrastructures - NIS directive	Cyber security workshop, EKDAA	20.03.2019	Athens
Cyber Security Strategy of Greece: the way ahead	2nd SAINT workshop	22.03.2019	Athens
Risks, threats and challenges of Cyberspace	7th Exposec-Defenseworld Conference	07.05.2019	Athens
Cybersecurity in the public sector in Greece	1.1.1.1.1. 18th European Conference on Cyber Warfare and Security	04.07.2019	Coimbra
CONCORDIA	SnT Partnership Day	04.06.2019	Luxembourg
Cookie Synchronization: Everything You Always Wanted to Know but were afraid to ask	The 30th International Web Conference (WWW)	13-17.05.2019	San Francisco, USA
TALON: An automated framework for Cross-Device Tracking Detection	22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2019)	23-25.09.2019	Beijing, China
Nothing is free in the web: Transparency on RTB with YourAdvaluetool	Cybersecurity and Privacy (CySeP) Summer School	10-14.06.2019	Stockholm, Sweden
Revisiting Rowhammer attacks in Embedded Systems	14th IEEE International Conference on Design & Technology of Integrated Systems in Nanoscale Era	16-18.04. 2019	Mykonos, Greece
Online user tracking and personal data leakage in the big data era	Colloquium @University of Cyprus	23.05.2019	Nicosia, Cyprus
Security Management and Visualization in a Blockchain-based Collaborative Defense	IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (ICBC 2019)	14-17.05.2019	Seoul, South Korea
No More Chasing Waterfalls: A Measurement Study of the Header Bidding Ad-Ecosystem	ACM Internet Measurement Conference	21-23.10.2019	Amsterdam, Netherlands

The drawbacks of blackholing	Asia-Pacific Network Information Centre (APNIC) blog	16.07.2019	
Presentations of the 4 EU-Pilots CONCORDIA, ECHO, SPARTA, CyberSec4Europe by the Coordinators plus Workshops	CODE Annual Conference	10-11.07.2019	Neubiberg, Germany
MENTOR: The Design and Evaluation of a Protection Services Recommender System	15th International Conference on Network and Service Management (CNSM 2019)	21-25.10.2019	Halifax, Canada
SEConomy: A Framework for the Economic Assessment of Cybersecurity	16th International Conference on Economics of Grids, Clouds, Systems, and Services (GECON 2019)	17-19.09.2019	Leeds, UK
Wireless SDN for Highly Utilized MANETs	Workshop ICT4PPRR @WiMOB	21-23.10.2019	Barcelona, Spain
Security in smart towns: good practices and results of research projects	Conference "Resilient Cities: between digital and physical world"	16.9.2019	Ljubljana, Slovenia
Evaluating TCP Connection Healthiness	International Telecommunication Networks and Applications Conference ITNAC 2019	27-29.9.2019	Auckland, New Zealand
Wireless SDN for Highly Utilized MANETs	6th Workshop: ICT Systems for Public Protection and Risk Reduction at the International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2019)	21.10.2019	Barcelona, Spain
MENTOR: The Design and Evaluation of a Protection Services Recommender System	15th International Conference on Network and Service Management (CNSM 2019)	21.10.2019	Halifax, Canada
Update on Economic Aspects of Cybersecurity	CONCORDIA Open Door	16.10.2019	Luxembour g
TradeMap: A FINMA-compliant Anonymous Management of an End-2-end Trading Market Place	15th International Conference on Network and Service Management (CNSM 2019)	22.10.2019	Halifax, Canada
A Cybersecurity Competence Network with Leading Research, Technology, Industrial, and Public Competence	Workshop on "Outlining Future Challenges of Cybersecurity - the CANVAS Results"	24.10.2019	Zürich, Switzerland
Introduction to Blockchains & Distributed Ledgers and Their Relevance for Responsible Business Conduct	OECD Workshop on "Responsible Business Conduct and Digitalization"	4.11.2019	Paris, France
CONCORDIA: Cyber Security Competence for Research and Innovation	1st CYBERWISER.eu Open Pilots Workshop	5.11.2019	Pisa, Italy

Machine Learning for Security at the IoT Edge - A Feasibility Study	International Workshop on Machine Learning Security and Privacy: Experiences and Applications, 2019	5.11.2019	Monterey, CA, USA.
A Cyber Range in the European context of the CONCORDIA project	TELECOM Nancy Cyber Range Launch Event	24.09.2019	Nancy, France
Extracting Safe Thread Schedules from Incomplete Model Checking Results	International Symposium on Model Checking of Software (SPIN) 2019	15-19.07.2019	Beijing, China
Gyro: A Modular Scale-Out Layer for Single-Server DBMSs	Symposium on Reliable Distributed Systems (SRDS) 2019	1-4.10.2019	Lyon, France
Inferring Performance Bug Patterns from Developer Commits	International Symposium on Software Reliability Engineering (ISSRE)	28-31.10.2019	Berlin, Germany
Analyzing and Improving Customer-side Cloud Security Certifiability	IEEE International Workshop on Software Certification (WoSoCeR)	28-31.10.2019	Berlin, Germany
TID: Online user tracking & personal data leakage in the big data era	Colloquium @ University College London	03.10.2019	London, UK
TID: Online user tracking and personal data leakage in the big data era	Colloquium @ Kings College London	09.10.2019	London, UK
TID: TALON: An automated framework for Cross-Device Tracking Detection	Seminar @ BRAVE Browser	10.10.2019	London, UK
TID: Privacy, Anonymity & Tracking of Users from the Online Advertising Ecosystem	Colloquium @ TUDelft	23.10.2019	Delft, Netherlands
TID: Data management and modeling for improved system design and user privacy	Colloquium @IMDEA Networks	12.11.2019	Madrid, Spain
TID: Privacy, Anonymity & Tracking of Users from the Online Advertising Ecosystem	Presentation at Kickoff meeting for EU H2020 Project PIMCITY	03.12.2019	Torino, Italy
Beyond content analysis: Detecting targeted ads via distributed counting	15th International Conference on emerging Networking EXperiments and Technologies (CONEXT 2019)	09-12.12.2019	Orlando, Florida, USA
A Continuous Certification Methodology for DevOps	ACM MEDES 2019	13.11.2019	Limassol, Cyprus
Information Security and Privacy: From Theory to Practice	International Conference on Information Security and Digital Forensics	30.11.2019	Thessaloniki, Greece

3.3.6. Blog posts

We regularly publish blog posts about the CONCORDIA project activities. The purpose of the blog posts is to raise public awareness of the project by increasing understanding of what we do and what the benefits are. The following table lists a number of 16 blogs published already on the CONCORDIA website.

Table 7: CONCORDIA blog posts.

Topic	Link
CONCORDIA presentation at CODE ANNUAL CONFERENCE 2019	https://www.concordia-h2020.eu/blog-post/code-goes-eu-with-concordia/
Cyber Czech exercise	https://www.concordia-h2020.eu/blog-post/cyber-training-defence-exercise/
Innovation management for cybersecurity ecosystem	https://www.concordia-h2020.eu/blog-post/platon-and-aristoteles-joining-concordia-project/
Disinformation and Fake Activity on the Web	https://www.concordia-h2020.eu/blog-post/enhancing-user-centric-security-within-the-concordia-project/
Quantification of IoT attack detectability	https://www.concordia-h2020.eu/blog-post/quantification-of-iot-attack-detectability/
Encrypted traffic analysis while preserving user privacy	https://www.concordia-h2020.eu/blog-post/encrypted-traffic-analysis-while-preserving-user-privacy/
Economic perspectives of cybersecurity and visibility of CONCORDIA at SIGCOMM and GECON conferences	https://www.concordia-h2020.eu/blog-post/concordias-attendance-at-acm-sigcomm-2019-and-gecon-2019/
CONCORDIA workshop on women in cyber	https://www.concordia-h2020.eu/blog-post/women-in-cyber/
Tracking users across multiple device for targeted advertising	https://www.concordia-h2020.eu/blog-post/advertising-ecosystem-what-is-the-cost-on-users-online-privacy/
ENISA FORTH Summer School	https://www.concordia-h2020.eu/blog-post/the-multidimensional-landscape-of-cybersecurity-and-the-enisa-forth-summer-school
CONCORDIA Open Door Event 2019	https://www.concordia-h2020.eu/blog-post/concordia-left-the-door-open-for-you/
European Cybersecurity Ecosystem	https://www.ri.se/en/our-stories/european-cybersecurity-ecosystem https://www.concordia-h2020.eu/blog-post/a-european-cybersecurity-ecosystem/
Privacy by design: Bringing Machine Learning towards the Edge	https://www.concordia-h2020.eu/blog-post/privacy-by-design-bringing-machine-learning-towards-the-edge/
Towards Context-based Vulnerability Analysis & Inference Lancaster University	https://www.concordia-h2020.eu/blog-post/towards-context-based-vulnerability-analysis-inference-lancaster-university/
CODE CTF 2019 The 5th Element	https://www.concordia-h2020.eu/blog-post/code-ctf-2019-the-5th-element/
Assessing blockchains’ network infrastructure: why it matters for cybersecurity	https://www.concordia-h2020.eu/blog-post/assessing-blockchains-network-infrastructure-why-it-matters-for-cybersecurity/

3.3.7. Social media presence

Currently, CONCORDIA’s presence is established in Twitter, LinkedIn and Facebook. Initial information can be found in the deliverable named “D5.1: Website and Social Media presences” which is listed under the Publications sections. In this section we will provide only the report on the social media activity for the first year of the project (2019). KPI-DC-10 for total views and likes in social media is defined as the sum of total likes on LinkedIn, reactions on Facebook and engagements on Twitter.

LinkedIn activity:

Currently, we have 440 connected accounts. There were 250 posts published from these accounts, which in total achieved 2963 likes and 113291 views. The data were obtained using the LinkedIn site for posts and activity management.

Table 8: LinkedIn activity

Months	Posts	Likes	Views
M1-M3	38	488	14146
M4-M6	57	536	24942
M7-M9	72	1021	34776
M9-M12	83	918	39427
M1-M12	**250**	**2963**	**113291**

Facebook activity:

Currently, we have 259 likes on our project profile. There were 125 posts published which, in total, achieved 2543 reactions and achieved a reach of 31887. The data were obtained via Facebook Insights.

Table 9: Facebook activity

Months	Posts	Reactions	Reach
M1-M3	17	603	7619
M4-M6	9	103	3202
M7-M9	49	969	10881
M9-M12	50	718	10185
M1-M12	**125**	**2543**	**31887**

Twitter activity:

Currently, we have 780 followers on our profile. There were 142 original posts published, which had collectively 8335 engagements and 371346 impressions. The data were obtained via Twitter Analytics.

Table 10: Twitter activity

Months	Posts	Engagements	Impressions
M1-M3	22	954	36596
M4-M6	19	1232	59124
M7-M9	47	2832	127105
M9-M12	54	3317	148521
M1-M12	**142**	**8335**	**371346**

It is also worth to mention the impact of the activity of project partners on Twitter. They have published at least 119 CONCORDIA related posts, which gained 2635 engagements and 169439 impressions. Therefore, in total, the CONCORDIA results were visible more than 500K times in the timelines of various twitter accounts.

Social Media Campaigns:

Over the past year, we ran two main campaigns on our social media channels. The first was aimed at promoting CONCORDIA Open Door Event 2019. A total of 25 unique posts were created and distributed via Facebook, Twitter and LinkedIn. Their purpose was to introduce the program, speakers and attract European stakeholders. The campaign also included a competition for free tickets to the event. The campaign ended with all-day news on our social media from the event.

The second campaign was called "10 Facts about CONCORDIA" and took place in the last ten days of the #cybersecmonth. It consisted of 11 contributions summarizing the most important of the project. The purpose of the campaign was to raise awareness regarding the project. All posts included visual material and were shared via Facebook, Twitter and LinkedIn.

Figure 12: Example of visual material from the publicity campaign "10 Facts about CONCORDIA".

3.3.8. Dissemination of results

CONCORDIA Papers:

More than 50 scientific papers were published at various top conferences and journals. Their list and more detailed information are available in Work Package 1 in Deliverable D1.1.

CONCORDIA News:

We publish news related to the project on our website, that we summarize in Table 11.

Table 11: CONCORDIA News

Topic	Link
Community-building and Strategic Directions event	https://www.concordia-h2020.eu/news/community-building-and-strategic-directions-event/
EC Cybersecurity R&D Roadmap	https://www.concordia-h2020.eu/news/ec-cybersecurity-rd-roadmap/

ITASEC 2019	https://www.concordia-h2020.eu/news/itasec-2019/
CONCORDIA Cybersecurity Competence Network Press Release	https://www.concordia-h2020.eu/news/concordia-cybersecurity-competence-network-press-release/
Meeting in Strasburg with the commissioner Gabriel Mariya	https://www.concordia-h2020.eu/news/meeting-in-strasburg-with-the-commissioner-gabriel-mariya/
CONCORDIA project WP1 F2F meeting in Bremen	https://www.concordia-h2020.eu/news/project-wp1-f2f-meeting-in-bremen/
ACM Workshop on Artificial Intelligence and Security (AISec) 2019	https://www.concordia-h2020.eu/news/acm-workshop-on-artificial-intelligence-and-security-aisec-2019/
Workshop on Cyber Security for Intelligent Transportation Systems (CSITS) 2019	https://www.concordia-h2020.eu/news/workshop-on-cyber-security-for-intelligent-transportation-systems-csits-2019/
Second plenary meeting of the CONCORDIA project	https://www.concordia-h2020.eu/news/second-plenary-meeting-of-the-concordia-project/
CONCORDIA cybersecurity pilot: Boosting the future of cybersecurity in the EU	https://www.concordia-h2020.eu/news/concordia-cybersecurity-pilot-boosting-the-future-of-cybersecurity-in-the-eu/
Towards a European Education Ecosystem for Cybersecurity	https://www.concordia-h2020.eu/news/towards-a-european-education-ecosystem-for-cybersecurity/
Rise has opened 8 new positions	https://www.concordia-h2020.eu/news/rise-has-opened-8-new-positions/
CONCORDIA Open Door Event2019	https://www.concordia-h2020.eu/news/concordia-open-door-event/
NIS 19 Summer School	https://www.concordia-h2020.eu/news/6th-network-and-information-security-nis19-summer-school/
CONCORDIA calendar for cybersecurity courses – plan your autumn before leaving for your summer vacation	https://www.concordia-h2020.eu/news/concordia-calendar-courses/
ACM Internet measurement Conference 2019	https://www.concordia-h2020.eu/news/acm-internet-measurement-conference-2019/
Open Positions at Telefonica Research (Barcelona)	https://www.concordia-h2020.eu/news/open-positions-at-telefonica-research-barcelona/
CONCORDIA map: 60+ cybersecurity courses collected in 6 months	https://www.concordia-h2020.eu/news/concordia-map-60-cybersecurity-courses-collected-in-6-months/

3.3.9. Publicity activities

We monitor communication activities that helped increase the publicity of the project. Last year we had 59 publicity outputs, as summarized in the next table.

Table 12: CONCORDIA Publicity outputs

Publicity Date	Publicity Info	Type
26-11-2019	C. Hesselman and J. Santanna, "Fighting DDoS attacks together on a national scale", SNiC 2019 ResilIT conference (national conference for student associations in computer science), Amersfoort, NL, Nov 2019	Presentation Conference
19-11-2019	Cybersecurity, l'Unione europea accelera sul tandem pubblico-privato https://www.repubblica.it/economia/rapporti/mondo5g/storie/2019/11/11/news/cybersecurity_l_unione_europea_accelera_sul_tandem_pubblico-privato-240010959/	Press

12-11-2019	SC Media UK included Gaby Dreo in EUROPE LIST: 50 Women of Influence in Cyber-security Europe	Magazine
12-11-2019	Gaby Dreo spoke at the opening plenary at the Annual Meeting on Cybersecurity of the World Economic Forum entitled "Making Global Cooperation Work" discussing ecosystems for cooperation and presented CONCORDIA Project as a blueprint for the envisioned European Cybersecurity Competence Network and Center.	Event
11-11-2019	Telecom Italia published an article (in Italian) where CONCORDIA is mentioned	Article
07-11-2019	German Minister of Defence mentioned CONCORDIA in her press statement, visiting CODE	Press Statement
05-11-2019	CONCORDIA was presented in the Event: 9. Handelsblatt Jahrestagung Cybersecurity, 5 and 6 November, Berlin	Event
05-11-2019	C. Hesselman and J. Latour, "The DNS and the IoT: security and stability opportunities, risks, and challenges (for ccTLDs)", ICANN66, Montréal, Canada, Nov 2019	Presentation Conference
17-10-2019	C. Hesselman, "Piloting a DDoS Clearing House for Europe", CONCORDIA Open Door Event, Luxembourg City, Luxembourg, Oct 2019	Presentation Conference
26-09-2019	https://wwwfr.uni.lu/snt/news_events/cybersecurity_buffet_with_diversity_on_the_menu	Website News
02-10-2019	C. Hesselman and J. Santanna, "Fighting DDoS attacks together on a national scale", One Conference, The Hague, NL, Oct 2019	Presentation Conference
02-09-2019	C. Hesselman, C. Hesselman, "Mitigation of IoT-based DDoS attacks", APTLD76, Malasyia, Sep 2019	Presentation Conference
26-07-2019	CONCORDIA was included in the TUV AUSTRIA Group yearly report	Annual Report
03-07-2019	Cybersecurity: Bavaria is helping shape the EU Security Union	Blog
16-06-2019	C. Hesselman, "Increasing trust in the digital infrastructure through a national DDoS clearing house", Africa Internet Summit (AIS2019), Kampala, Uganda, June 2019	Presentation Conference
14-06-2019	Bundeswehr University Munich published in internal Uni magazine https://www.unibw.de/home/presse-und-kommunikation/pressematerial/inside_unibw_ausgabe_03_web_2-1.pdf/	Article
28-05-2019	C. Hesselman, "Increasing the resilience of the Netherlands' digital infrastructure together", ISC2NL Cyber Resilience Event, Amersfoort, The Netherlands, May 2019	Presentation Conference
17-05-2019	C. Hesselman, "Mitigating DDoS attacks from botnets through a national DDoS clearing house", BotLeg Workshop, co-located with TILTing Perspectives 2019, Tilburg, the Netherlands, May 2019	Presentation Conference

14-05-2019	Digital Single Market – Project Story: CONCORDIA cybersecurity pilot: Boosting the future of cybersecurity in the EU https://ec.europa.eu/digital-single-market/en/news/concordia-cybersecurity-pilot-boosting-future-cybersecurity-eu	Blog post
31-03-2019	https://ikt.finance.si/8946535/EU-krepi-kibernetsko-varnost-pri-tem-sodelujejo-tudi-slovenski-strokovnjaki?cctest&	Website and Newspaper news
29-03-2019	https://www.jacobs-university.de/news/better-protection-against-cyber-attacks-jacobs-university-bremen-part-european-research-network	Press release
26-03-2019	http://www.tic-et-plus.com/formation/telecom-nancy-acteur-de-premier-plan-de-la-cyber-securite-europeenne	Article
19-03-2019	https://lastatalenews.unimi.it/progetto-concordia-statale-rete-europea-cybersecurity	Website News
18-03-2019	Journal "Les Tablettes lorraines"	Article
15-03-2019	https://4d.rtvslo.si/arhiv/tele-m/174602155	TV News Report
14-03-2019	http://telecomnancy.univ-lorraine.fr/fr/cyber-securite	Article
13-03-2019	Inštitut za informatiko na razpisu dobil dva projekta	Radio News Report
12-03-2019	Inštitut za informatiko na razpisu dobil dva projekta	Radio News Report
12-03-2019	https://4d.rtvslo.si/arhiv/slovenska-kronika/174601434	TV News Report
12-03-2019	https://www.globalsecuritymag.fr/TELECOM-Nancy-engagee-dans-la,20190312,85291.html	Article
07-03-2019	https://twitter.com/Univ_Lorraine/status/1103694126569177088	Twitter
06-03-2019	http://factuel.univ-lorraine.fr/node/10771	Newsletter
06-03-2019	https://twitter.com/pridinaferi/status/1103253198922489856	Twitter
05-03-2019	https://www.linkedin.com/feed/update/urn:li:activity:6508703112860176384	LinkedIn
05-03-2019	https://ii.feri.um.si/en/2019/03/05/institute-of-informatics-acquired-h2020-project-concordia-cyber-security-competence-for-research-and-innovation/	Website News
05-03-2019	https://feri.um.si/en/news/the-institute-of-informatics-acquired-two-h2020-projects/	Website News
04-03-2019	http://www.tromba.si/fakulteta-za-elektrotehniko-racunalnistvo-in-informatiko-pridobila-dva-h2020-projekta/	Website News

04-03-2019	https://www.um.si/univerza/medijsko-sredisce/novice/Strani/novice.aspx?p=2677	Website News
28-02-2019	http://www.paideia-news.com/index.php?id=109&hid=34279	Website News
27-02-2019	https://www.flowmon.com/en/company/news/releases/eu-greenlights-four-cybersecurity-pilot-projects	Website News
27-02-2019	https://protathlima.com/tepak-ereynitiko-ergo-concordia-gia-tin-kyvernoasfaleia-stin-eyropi/	Press
27-02-2019	https://feri.um.si/novice/institut-za-informatiko-pridobil-dva-h2020-projekta/	Website News
27-02-2019	https://ii.feri.um.si/sl/2019/02/27/institut-za-informatiko-pridobil-h2020-projekt-concordia-cyber-security-competence-for-research-and-innovation/	Website News
27-02-2019	http://delano.lu/d/detail/news/lux-heart-eu-cybersecurity-efforts/203802	Website News
27-02-2019	https://www.sba-research.org/partner-of-sba-research-concordia-h2020/	Website News
27-02-2019	Europa vernetzt sich in der Cybersicherheit	Website News
27-02-2019	https://cyprustimes.com/tepak-ereynitiko-ergo-concordia-gia-tin-kyvernoasfaleia-stin-eyropi/	Press
27-02-2019	https://www.kathimerini.com.cy/gr/kypros/paideia/tepak-ereynitiko-ergo-concordia-gia-tin-kynernoasfaleia-stin-eyrwpi	Press
26-02-2019	http://www.sigmalive.com/news/oikonomia/market-news/556583/erevnitiko-ergo-concordia	Website News
26-02-2019	https://paideia-news.com/tepak-ereynitiko-ergo-concordia-gia-tin-kybernoasfaleia-stin-eyropi-34279c	Press
26-02-2019	https://wwwen.uni.lu/snt/news_events/snt_at_heart_of_major_eu_cybersecurity_push	Website News
26-02-2019	https://twitter.com/TELECOMNancy/status/1100419157819092992	Twitter
26-02-2019	https://twitter.com/TELECOMNancy/status/1100418478975172608	Twitter
26-02-2019	https://www.facebook.com/TELECOMNancy/posts/2305877292770041	Facebook
23-02-2019	C. Hesselman, "Collaboratively increasing the resilience of critical services in the Netherlands through a national DDoS clearing house", Internet Infrastructure Security Day at APRICOT2019, Daejeon, South Korea, February 23, 2019	Presentation Conference

04-02-2019	https://c4e.cz/news/concordia-project	Website News
28-01-2019	C. Hesselman, "Task 3.2: Piloting a DDoS Clearing House for Europe", CONCORDIA Kickoff Meeting, Jan 28-29, 2019, München, Germany	Presentation Conference
16-01-2019	https://www.flowmon.com/en/company/news/releases/flowmon-joins-concordia-european-cyber-defence	Website news

Sponsorship:

Sponsorship of an event is a specific type of publicity. Last year we sponsored four events and conferences, as summarized in the following table.

Table 13: Events sponsored by CONCORDIA.

Name	Link
Cybersecurity Week Luxembourg 2019	https://cybersecurityweek.lu/
ESORICS 2019	https://esorics2019.uni.lu
The 30th International Symposium on Software Reliability Engineering (ISSRE 2019)	https://www.2019.issre.net/
International Conference on Internet Measurements 2019	https://conferences.sigcomm.org/imc/2019/

Cyberwatching.eu:

We cooperate with Cyberwatching.eu, the European observatory of research and innovation in the field of cybersecurity and privacy. We enclose summary of cyberwatching.eu promotion of CONCORDIA project in the following table.

Table 14: Cooperation with the Cyberwatching.eu observatory.

Type of promotion	Stats
Website posts: 8	Page visits: 2263
Twitter posts: 30	Views (total): 35737
Twitter cards: 30	Twitter Views: 34838
Twitter Retweet: 120	Likes (total): 263
Twitter Engagement: 758	Twitter Engagement Rate: 69.9%
LinkedIn posts: 18	LinkedIn Views: 899
Events: 1	Participants: 79

3.3.10. Cyber Competence Network coordinated communication activities

This section focuses only on what has been achieved while the CONCORDIA project chaired the communication group of the four pilots.

Coordination framework:

Being the first period of working together, a lot had to be done internally. With the help of the EC, CONCORDIA has developed an informal common coordination framework which is acknowledged by all pilots. It is based on six months chairing of the communication group by each of the four pilots, creating and maintaining a database of important information (e.g., the event table) and regular communication of the group. The order of the chairs of the coordination group is decided:

1. CONCORDIA (till 30th June 2019)
2. ECHO (starting 1st July 2019)
3. SPARTA (starting 1st January 2020)
4. CYBERSEC4EUROPE (starting1st July 2020)

Internal communication channels and IT infrastructure are also set up.

Social media activity:

The four pilots were active on social media. Each pilot produced approximately 10 unique posts that focused on collaboration between pilots. In addition, many other stakeholders and influencers have been involved in spreading information about the four pilots. Especially we want to mention the cooperation with https://cyberwatching.eu, which has generated considerable publicity for all pilots.

Meeting in Strasbourg:

The 4 pilots met the Commissioner Mariya Gabriel in Strasbourg on 13 March 2019. Tasks performed from CONCORDIA were the following:

1. CONCORDIA approached a few key members of the European Parliament and proposed to schedule a meeting with the project coordinators after the meeting with the Commissioner.
2. CONCORDIA approached the European Parliament liaison offices in the 5 EU Member States with the highest number of partners involved (Germany, Spain, France, Italy, Belgium) in the projects requesting them to inform the local journalists about the presence of the pilots in the EP, and acted as a contact point for journalists (for providing additional information and organise interview).
3. CONCORDIA was in charge of coordinating the content for the a 'Line To Take' (LTT) for the media – including some general messages as well as defensives for a few key questions.
4. CONCORDIA took notes from the meeting in view of creating content for web and social media

Results from this meeting were the following:

- 9 members of the European Parliament contacted
- 10 press offices contacted: Germany (Berlin) - very interested to learn more and stay in contact; they also forwarded the message to press officers from other countries. Italy (Milano) and Spain (Madrid) also reacted positively to our messages. There was finally one interview organised in Strasbourg (for Lithuania broadcaster).

Common website and visual identity:

All four pilots collaborated and prepared a common website and also designed a common visual identity for Cyber Competence Network. The website can be found here: https://cybercompetencenetwork.eu/

CONCORDIA event and official launch of the common website:
We exploited the potential of launching the common website. To officially launch the website, Despina Spanou, Director for Digital Society, Trust and Cybersecurity, Angelika Niebler, Member of the European Parliament, and Gabi Dreo Rodosek, the coordinator of CONCORDIA, pressed a symbolic button at CONCORDIA's second plenary meeting in Brussels on 5 June 2019. The video can be found here:
https://twitter.com/shahidraza/status/1136384772178087943

Cyber Competence Network Events:
The following table includes a list of 11 events where the Cyber Competence Network was present when CONCORDIA project chaired the Communication Group of the four pilots.

Table 15: Cyber Competence Network events.

Main organiser	Name of the event	Date	Place
DG HOME / DG CONNECT	Community of Users Event (4 pilots presentation session)	28-29.03.2019	Brussels, BE
Cyberwatching.eu	Cyberwatching.eu Webinar (run by) including the participation of and presentations from all 4 Pilots - online 10-11am	02.04.2019	online
ECSO	ECSO Working Group 6 SRIA Event (all 4 pilots invited)	10.042019	Brussels, BE
EC	Cybersecurity PPP (cPPP) Board of Directors Meeting (cPPP and European Commission - all pilots expected to give updates)	15.05.2019	Brussels, BE
Cyberwatching.eu	Cyberwatching.eu CONCERTATION Event (all 4 pilots invited to participate and facilitate)	04.06.2019	Brussels, BE
CONCORDIA	CONCORDIA Event (all pilots invited) 4 pilots' website https://cybercompetencenetwork.eu/ - launch CONCORDIA map on courses for professionals - launch	05-06.062019	Representation of the Free State of Bavaria in Brussels, BE
EC	Digital Assembly Bucharest	13-14.2019	Bucharest, RO
ECSO	ECSO Board of Directors Meeting and Annual General Assembly (brief pilot updates and short discussion within ECSO)	18.06.2019	
ECSO	EHR4CYBER - workshop	19.06.2019	Brussels, BE
CyberSec4Europe	CyberSec4Europe - Event	04-05.07.2019	Hessen Representation, Brussels, BE
CODE (coordinator CONCORDIA)	CODE annual event (all pilots invited)	10-11.07.2019	Munich, DE

3.4. Next steps on Communication and Dissemination

In the previous paragraphs, we discussed efforts on dissemination and communication. Firstly, we provided description of our goals and objectives. Secondly, we dealt with our strategy to achieve defined goals and objectives. Finally, we provided structured description of communication and dissemination activities performed in the first year of the project. It is important to note that parts of the strategy presented may be refined in the coming years according to the context and objectives of the project. The purpose of communication and dissemination will always be to contribute to the fulfilment of project objectives.

Our plans for the next year are evident from the communication phases of the project (described in Table 5). In M15, we move from the publicity phase to the dissemination phase. At this stage, in addition to strengthening our brand, we will focus primarily on sharing project results and increasing their impact. One of the communication tactics we would like to work with is video material. However, in addition to the plan, we remain ready to use all the opportunities that we have in this area to support our goals.

4. Efforts on Certification & Standardization

4.1. Objectives of Task (T5.3)

This task will focus on the certification and standardization activities of the project. First, it will deliver a comprehensive certification and standardization strategy to be followed and further refined throughout the duration of CONCORDIA. This strategy starts by updating the analysis performed during the proposal writing with the review of certification procedures, standards, and best practices that are relevant to this project. The objective is to ensure alignment with the technologies to be developed (WP1), as well as the pilots (WP2). To this end, the project will monitor continuously the evolving certification, standardization and best practices landscape, in order to timely identify other initiatives that may be linked to CONCORDIA areas of interest. It will also develop the initial engagements/liaisons with the respective governing organizations and will actively engage with external stakeholders aiming at actively engaging with external stakeholders and promoting the achievements resulting from the technical WPs in the appropriate fora.

4.2. Strategy to Achieve Task Objectives

CONCORDIA is a project where different organizations come together to:

- Devise a cybersecurity roadmap to identify powerful research paradigms, to do hands-on experimental validation, prototype and solution development in an agile way to quickly identify successful but also unsuccessful potential product development.
- Develop next-generation cybersecurity solutions by taking a holistic end-to-end data-driven approach from data acquisition, data transport and data usage, and addressing device-centric, network-centric, software- and system-centric, data- and application-centric and user-centric security.
- Develop sector-specific (vertical) and cross-sector (horizontal) industrial pilots with building incubators.

Also, in terms of focus areas, the CONCORDIA project deals with a variety of subjects related to security in devices, network, software, data and users covering various sectors (Telecom, Finance, Transport, E-Health, Defense) and services.

Certification is not one–fits–all practice. For each of the objectives and focus areas, the need for certification has to be identified and individually addressed. Moreover, to find the way that Certification fits the needs of the task and solution, the outcomes of this task and solution have to have reached a certain level of maturity.

In order to achieve all the above, the following strategy was devised:

- Map the standardization needs (explained in further details in Section 4.3.2 on Standardization)
- Identify the certification needs per task
- Design and implement the certification activities per task
- Collaborate internally and externally to promote the certification task results to stakeholders.

In Section 4.2.1, the actions performed regarding the Certification activities are described, in Section 4.2.2, the actions performed regarding the Standardization activities are described, and in Sections 4.3.1. and 4.3.2. the results of these actions up to this point, respectively, are described.

4.2.1. Certification

Certification is the third-party attestation related to products, processes, systems or persons. Whereas attestation, is issue of a statement, based on a decision following review, that fulfilment of specified requirements has been demonstrated.[6] Certification can apply to a product, process, system, person or body. Depending on the subject of certification, different international standards provide the related best practices (e.g. ISO 17021, ISO 17024, ISO 17025, etc.).

Identification of the certification needs per task

As mentioned in the beginning of 4.2, the CONCORDIA project addresses a variety of topics and industry sectors. In order to identify the certification needs, an individual approach had to be adopted. This approach consists of the following two activities:

- Individual discussions have started with the different task leaders, in order to identify the certification potential.
- The project team will review all related deliverables expected to be finished by the end of the year.

From the combination of the collected information, specific input will be provided regarding certification.

At this point, the only task for which certification activities have started is task T3.4: Establishing a European Education Ecosystem for Cybersecurity (Lead: EIT-Digital). More information regarding the activities and results of these efforts can be found in Section 4.3.

4.2.2. Standardization

Before introducing the subject of standardization, it is deemed necessary to provide two simple definitions regarding the term *Standard* and *Standards Developing Organizations* (SDO) in the context of the CONCORDIA project:

- **Standard:** "A standard (French: Norme, German: Norm) is a technical document designed to be used as a rule, guideline or definition. It is a consensus-built, repeatable way of doing something."[7]
- **Standards Developing Organizations (SDO):** "An SDO is an organization that facilitates the development of standards and publication of standards. SDOs include: ANCE (National Association of Standardization and Certification), ASTM (ASTM International), ISA (International Society of Automation), NFPA (National Fire Protection Association), UL (Underwriters Laboratories), ULC Standards" and various others [8].

Considering the above definitions, for the CONCORDIA project, some of the types of documents referred to as Standards are [9]:

[6] ISO/IEC 17000:2004(en) Conformity assessment — Vocabulary and general principles.

[7] CEN, the European Committee for Standardization, is an association that brings together the National Standardization Bodies of 34 European countries, retrieved from the official website

[8] https://ulstandards.ul.com/about/glossary/

[9] CEN, the European Committee for Standardization, is an association that brings together the National Standardization Bodies of 34 European countries, retrieved from the official website

- **International Standards:** An International Standard provides rules, guidelines or characteristics for activities or for their results, aimed at achieving the optimum degree of order in a given context. It can take many forms. Apart from product standards, other examples include: test methods, codes of practice, guideline standards and management systems standards. In the results of the Standardization subtask described below, such standards are identified from various Standards Development Organizations like ISO, IEC, IEEE and others.
- **Standards:** Documents issued by Standards Development Organizations following their individual procedures. In the results of the Standardization subtask described below, such standards are identified from Standards Development Organizations like UL, SAE, ASTM, NASA and others.
- **Technical Specifications:** A Technical Specification addresses work still under technical development, or where it is believed that there will be a future, but not immediate, possibility of agreement on an International Standard. A Technical Specification is published for immediate use, but it also provides a means to obtain feedback. The aim is that it will eventually be transformed and republished as an International Standard. In the results of the Standardization subtask described below, such specifications are identified from Standards Development Organizations like ISO and IEC.
- **Technical Reports:** A Technical Report contains information of a different kind from that of the previous publications. It may include data obtained from a survey, for example, or from an informative report, or information of the perceived "state of the art". In the results of the Standardization subtask described below, such reports are identified from Standards Development Organizations like ISO, IEC and ANSI.
- **Guides:** Guides give rules, orientation, advice or recommendations relating to international standardization and conformity assessment. [10] In the results of the Standardization subtask described below, such guides are identified from Standards Development Organizations like IEC and the International Association of Drilling Contractors.
- **Special Publications:** A type of publication issued by NIST. Specifically, the SP 800-series reports on the Information Technology Laboratory's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations. [11]
- **Recommendations:** The ITU-R Recommendations constitute a set of international technical standards developed by the Radiocommunication Sector (formerly CCIR) of the ITU. They are the result of studies undertaken by Radiocommunication Study Groups on various subjects. The ITU-R Recommendations are approved by ITU Member States. Their implementation is not mandatory; however, as they are developed by experts from administrations, operators, the industry and other organizations dealing with radiocommunication matters from all over the world, they enjoy a high reputation and are implemented worldwide. [12]

Data Collection:

As mentioned in Section 4.2, the CONCORDIA project addresses a variety of topics and industry sectors. As a first step of the Standardization efforts for CONCORDIA, a survey was carried out. The survey aimed to the identification of the following subjects per Work Package, per Task and per Partner:

[10] Information retrieved from the website of IEC: https://www.iec.ch/standardsdev/publications/guide.htm

[11] NIST SP 800-63-3 under Special Publication (SP)

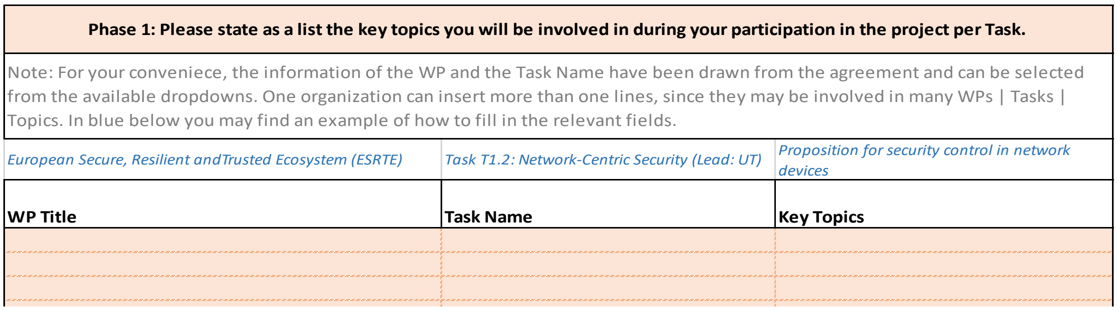
[12] Information retrieved from the website of ITU: https://www.itu.int/pub/R-REC

- The key topics that each partner will be involved in during their participation in the project, per Task.
- The standards each Partner is already using for the performance of each Task.
- The standards each Partner is planning on using for the performance of each Task.
- The standardization activities that each Task member is part of.

The latter, would be considered useful during the process of sharing the results of the related Tasks and contributing to existing standardization efforts. To further simplify the task of filling in the survey, a preliminary search was carried out and 267 standards were identified and included in the document of the survey for quick reference. More information regarding the preliminary survey is provided in Section 4.3.2.

The survey was facilitated through an Excel file that was sent to all partners via e-mail. The e-mail also contained detailed instruction regarding how to fill in the survey file which had the following structure:

Sheet Data_Collector: The purpose of this sheet is to collect data from all partners for this task. Figure 13 shows Phase 1, for collecting contents regarding Key Topics with the Sheet Data_Collector.



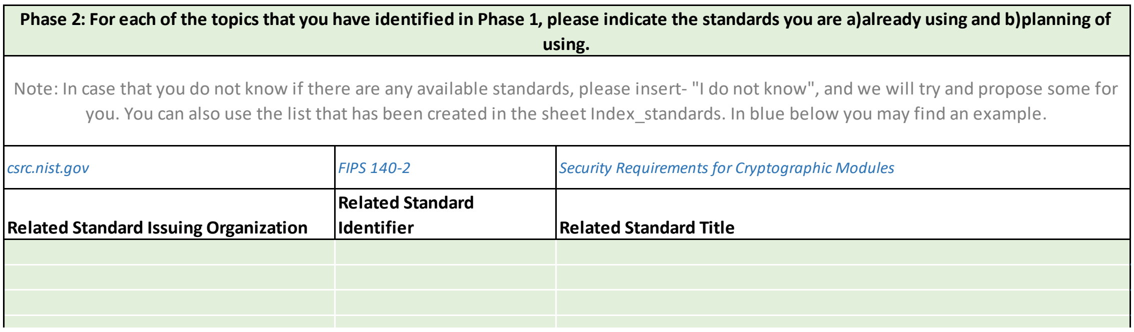
Phase 1: Please state as a list the key topics you will be involved in during your participation in the project per Task.

Note: For your conveniece, the information of the WP and the Task Name have been drawn from the agreement and can be selected from the available dropdowns. One organization can insert more than one lines, since they may be involved in many WPs | Tasks | Topics. In blue below you may find an example of how to fill in the relevant fields.

European Secure, Resilient andTrusted Ecosystem (ESRTE)	*Task T1.2: Network-Centric Security (Lead: UT)*	*Proposition for security control in network devices*
WP Title	**Task Name**	**Key Topics**

Figure 13: Contents of the Sheet Data_Collector regarding Key Topics

Figure 14 shows Phase 2, for collecting contents regarding Standards already being used and Standards that will be used, with the Sheet Data_Collector.



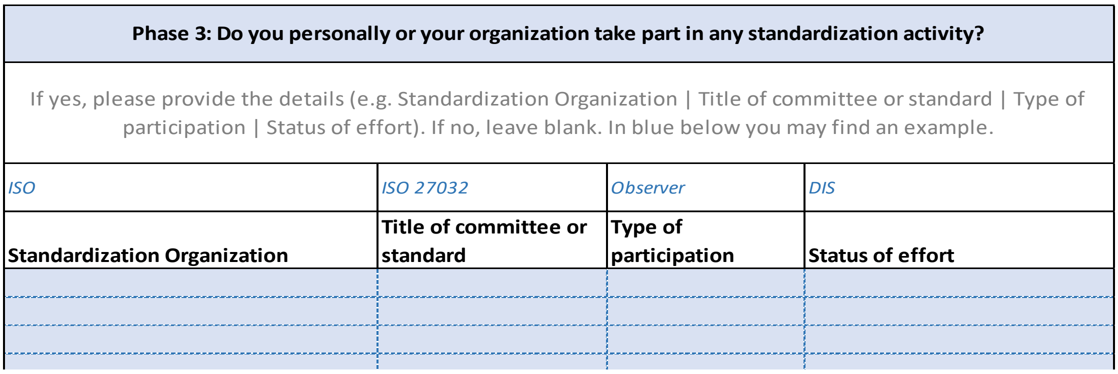
Phase 2: For each of the topics that you have identified in Phase 1, please indicate the standards you are a)already using and b)planning of using.

Note: In case that you do not know if there are any available standards, please insert- "I do not know", and we will try and propose some for you. You can also use the list that has been created in the sheet Index_standards. In blue below you may find an example.

csrc.nist.gov	*FIPS 140-2*	*Security Requirements for Cryptographic Modules*
Related Standard Issuing Organization	**Related Standard Identifier**	**Related Standard Title**

Figure 14: Contents of Sheet Data_Collector regarding Standards already being used and Standards that will be used.

Figure 15 shows Phase 3, for collecting contents regarding involvement in standardization activities, with the Sheet Data_Collector.



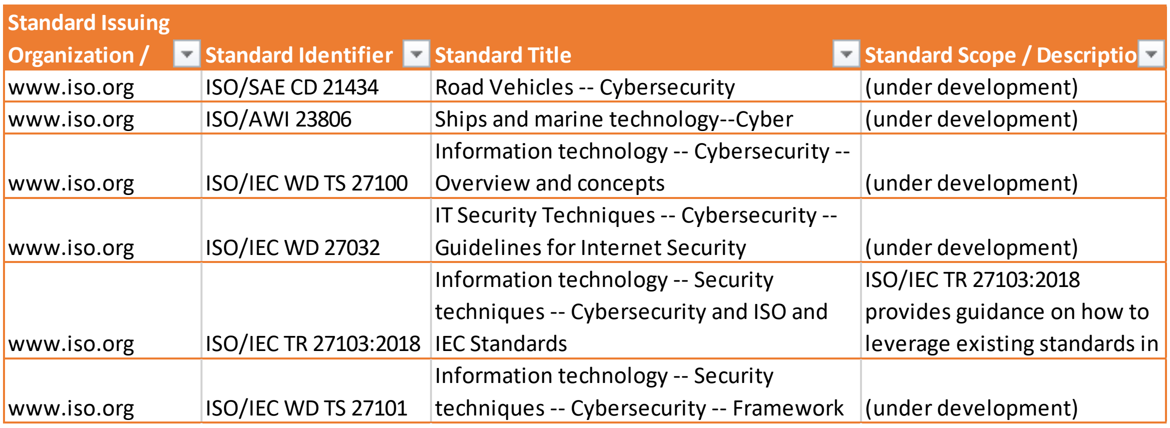
Phase 3: Do you personally or your organization take part in any standardization activity?

If yes, please provide the details (e.g. Standardization Organization | Title of committee or standard | Type of participation | Status of effort). If no, leave blank. In blue below you may find an example.

ISO	*ISO 27032*	*Observer*	*DIS*
Standardization Organization	**Title of committee or standard**	**Type of participation**	**Status of effort**

Figure 15: Contents of the Sheet Data_Collector regarding involvement in standardization activities.

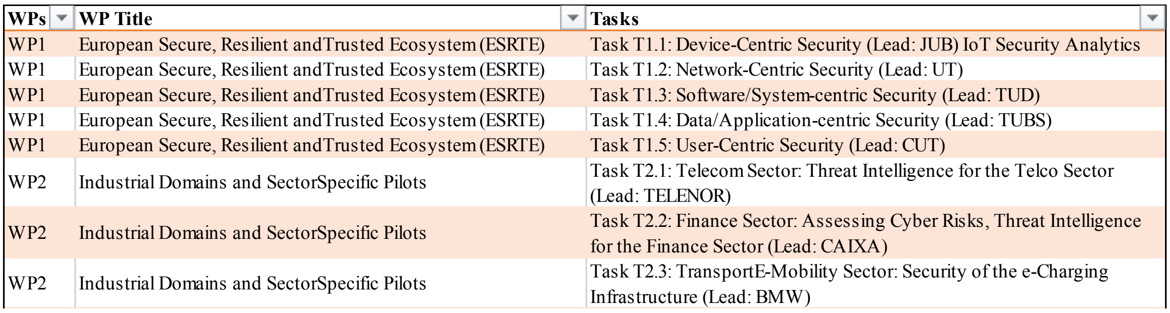
Sheet Index_Standards: The purpose of this sheet is to depict the results of the preliminary search for standards. Figure 16 shows the contents of the Sheet Index_Standards regarding related standards and their status.



Standard Issuing Organization /	Standard Identifier	Standard Title	Standard Scope / Descriptio
www.iso.org	ISO/SAE CD 21434	Road Vehicles -- Cybersecurity	(under development)
www.iso.org	ISO/AWI 23806	Ships and marine technology--Cyber	(under development)
www.iso.org	ISO/IEC WD TS 27100	Information technology -- Cybersecurity -- Overview and concepts	(under development)
www.iso.org	ISO/IEC WD 27032	IT Security Techniques -- Cybersecurity -- Guidelines for Internet Security	(under development)
www.iso.org	ISO/IEC TR 27103:2018	Information technology -- Security techniques -- Cybersecurity and ISO and IEC Standards	ISO/IEC TR 27103:2018 provides guidance on how to leverage existing standards in
www.iso.org	ISO/IEC WD TS 27101	Information technology -- Security techniques -- Cybersecurity -- Framework	(under development)

Figure 16: Contents of the Sheet Index_Standards regarding related standards and their status

Sheet Index WP_Activities: The purpose of this sheet is to provide the information related for Tasks and Work Packages. Figure 17 shows the contents of the Sheet Index WP_Activities.



WPs	WP Title	Tasks
WP1	European Secure, Resilient andTrusted Ecosystem (ESRTE)	Task T1.1: Device-Centric Security (Lead: JUB) IoT Security Analytics
WP1	European Secure, Resilient andTrusted Ecosystem (ESRTE)	Task T1.2: Network-Centric Security (Lead: UT)
WP1	European Secure, Resilient andTrusted Ecosystem (ESRTE)	Task T1.3: Software/System-centric Security (Lead: TUD)
WP1	European Secure, Resilient andTrusted Ecosystem (ESRTE)	Task T1.4: Data/Application-centric Security (Lead: TUBS)
WP1	European Secure, Resilient andTrusted Ecosystem (ESRTE)	Task T1.5: User-Centric Security (Lead: CUT)
WP2	Industrial Domains and SectorSpecific Pilots	Task T2.1: Telecom Sector: Threat Intelligence for the Telco Sector (Lead: TELENOR)
WP2	Industrial Domains and SectorSpecific Pilots	Task T2.2: Finance Sector: Assessing Cyber Risks, Threat Intelligence for the Finance Sector (Lead: CAIXA)
WP2	Industrial Domains and SectorSpecific Pilots	Task T2.3: TransportE-Mobility Sector: Security of the e-Charging Infrastructure (Lead: BMW)

Figure 17: Contents of the Sheet Index WP_Activities regarding work packages and tasks of the project.

4.3. Results on Certification and Standardization

4.3.1. Certification

Certification of Cybersecurity Skills under Task 3.4

One of the aims of Task T3.4 is to “provide a certification framework for professional courses; going beyond professionals and industry to address the wider society by engaging new generations and “teaching the teacher”. To facilitate the above goals, the need arose for the development of a framework in the context of Cybersecurity to ease the process of delivering, obtaining, securing and verifying of certificates for well-defined Cybersecurity skills.

In order to create the Certification Scheme for Cybersecurity Skills mentioned above, the following activities have to be implemented:

- **Create a Feasibility study**: The purpose of this study is to describe the need that the Certification Scheme is going to fill, to identify existing efforts and to define the exact profile of the proposed certification.
- **Create a Certification Framework**: The purpose of the Certification Framework is to define the rules under which the Certification Scheme will operate.
- **Create Supporting material for the implementation of the Scheme**: Depending of the design of the scheme as described in the Certification Framework, the relevant supporting material (exam environment, exam items, examination mechanisms, etc) will be created.

In order to be able to further exploit the certification scheme, it has been chosen that all outputs of these activities will be compatible to the requirements of ISO 17024 Standard.

At this time, the Feasibility Study has been conducted and is under review and the efforts on the Certification Framework have started. The results of these efforts are presented in the relevant Deliverables under Task 3.4. For avoiding repetition, we do not include them here.

4.3.2. Standardization

Preliminary standards survey results:

The project team researched the different existing public and proprietary standards (in their various stages of development) and documented the results in the Sheet Index_Standards. The objective was to identify standards related to cybersecurity covering various different aspects. The preliminary standards survey produced the following consolidated results:

Table 16: Number of Standards per SDO. Preliminary results before the CONCORDIA partners provided their contribution.

Standards Developing Organization	Number of Identified Standards
Alliance for Telecommunication Industry Solutions	1
ANSI	2
ASTM	1
CSA	1
DIN	1
ETSI	3

FDA	11
IEC	41
IEEE	21
Internet Engineering Task Force (IETF)	12
International Association of Drilling Contractors	2
ISA	6
ISO	12
International Telecommunication Union	10
NASA	1
NATO Cooperative Cyber Defence Centre of Excellence	1
Naval Aviation	2
NEMA	1
NERC	17
NIST: Computer Security Resource Center National Cybersecurity Center of Excellence (NCCoE)	 59 61
OASIS	2
SAE	1
Siemens	1
UL	9
Total Standards Identified	**279**

Number of identified:

- Standards Developing Organizations: 25
- Standards: 279
- Standards in preparatory stages (Draft, Pending, etc): 54

The identified standards during this preliminary research covered the area of cybersecurity from various aspects:

- Technical (e.g. Guidelines for Securing Wireless Local Area Networks (WLANs))
- Introductory (e.g. Ships and marine technology--Cyber safety)
- Sector Specific (e.g. Road Vehicles -- Cybersecurity engineering)
- Technology specific (e.g. Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection NISTIR 8219), etc.

Partner input survey results:

The inputs of the partners regarding Standardization as described above were consolidated, and one document containing all of them was created. The key topics identified for those that responded in the survey are contained in the following table (Table 17). Note: As mentioned above (Section 4.2.2) the key topics represent the areas where each partner will be involved in during their participation in the project, per Task. The objective for collecting the key topics is twofold: 1) To facilitate the identification of applicable standards and 2) To facilitate communication of tangible results to the related organizations.

Table 17: Key topics identified based on the inputs from CONCORDIA partners.

Accelerators	Deep learning	Machine learning techniques for learning utility of data of users
Anonymity of data	Detection of indicators of compromise in telco environment	Machine learning techniques for protection
Assets	Development of intel sharing platform	Medical devices
Attestation	Device security based on trustzone	Metrics for situational awareness based on sharing platform data
Automation/security orchestration	E-health	Monitoring and analysis of encrypted traffic preserving user privacy
Blockchain	Emerging threats	Network device configuration
Blue light communication - emergency	End-to-end security architecture for 5g-controlled drone	Personal data leakage detection
Business plan	Enhancing capabilities of cyber ranges	Privacy and data protection
Client identification and authentication (physically and virtually)	Exploitation strategy	Reliable detection of DDOS attacks
Cloud security	Firmware updates (IoT)	Representation of incident response actions
Cryptography primitives and cryptography operation in embedded system environment	Sharing of infected and vulnerable systems with owners of systems	Secure communication
Cyber ranges for cybersecurity training	Full stack IoT security	Secure zero touch deployment of industrial IoT devices in low-power lossy network (lln)
Cyber threat analysis	Generic pki for IoT	Security policy development
Cyber threat training models	Hardware security	Security-by-design and privacy preservation (anonymization)
Cyber threat assessment	Hardware security assessment	Smart home
Cyber threat intelligence	Hardware security tokens	Software security for IoT
Cyber threat intelligence platform (for cybersecurity technical ioc and financial ioc)	Honeypots	Start-ups
Cyber threat landscape	Identity management	Tactical ad hoc networks
Cyber threat reporting	Identity related information discovery	Tactical software defined networks
Cyber threat visualization	Incubators	Tech-transfer
Cyber threat/intrusion detection system - AI based	Information sharing (federated machine learning over a common model)	Transparency in the web ad-ecosystem
Cybersecurity roadmap	IoT devices	Trusted execution environments
Data-centric threat modeling	IoT security	Trusted execution environment for arm cortex m3
DDOS	Ipr	Vehicle security
DDOS clearing house	Know your customer	Vulnerabilities
Knowledge management		
Accelerators	Deep learning	Machine learning techniques for learning utility of data of users
Anonymity of data	Detection of indicators of compromise in telco environment	Machine learning techniques for protection

Assets	Development of intel sharing platform	Medical devices
Attestation	Device security based on trustzone	Metrics for situational awareness based on sharing platform data
Automation/security orchestration	E-health	Monitoring and analysis of encrypted traffic preserving user privacy
Blockchain	Emerging threats	Network device configuration
Blue light communication - emergency	End-to-end security architecture for 5g-controlled drone	Personal data leakage detection
Business plan	Enhancing capabilities of cyber ranges	Privacy and data protection

The total number of subjects found was 74. For these key Topics, 104 distinct standards were identified as relevant by the various CONCORDIA Partners. These standards were cross-checked against the results of the Preliminary Standards Survey, and the list was enriched accordingly. The new (updated) list of standards now contains 295 entries (16 new entries added) in Table 18.

Table 18: Number of Standards per SDO. Results after the CONCORDIA partners provided their contribution.

Standards Developing Organization	Number of Identified Standards
ACDC project	1
Alliance for Telecommunication Industry Solutions	1
ANSI	2
ASTM	1
CSA	1
CENELEC	1
DIN	1
ECMA	1
ETSI	3
FDA	11
IEC	41
IEEE	21
Internet Engineering Task Force (IETF)	14
International Association of Drilling Contractors	2
ISA	6
ISO	13
International Telecommunication Union	11
MITRE	2
NASA	1
NATO Cooperative Cyber Defence Centre of Excellence	1
Naval Aviation	2
NEMA	1
NERC	17

NIST: Computer Security Resource Center National Cybersecurity Center of Excellence (NCCoE)	 59 61
OASIS	7
Open Charge Alliance	1
SAE	1
Siemens	1
UL	9
X-arf	1
Total Standards Identified	**295**

Number of identified:

- Standards Developing Organizations: 32
- Standards: 295
- Standards in preparatory stages (Draft, Pending, etc): 54

Furthermore, in some cases, as shown in the following table (Table 19), assistance in the identification of related standardization efforts was requested by the respective CONCORDIA partners from the Standardization task leader (TUVA).

Table 19: Tasks and key topics where assistance was requested by a CONCORDIA partner from the project's Certification and Standardization task leader.

Work Package	Task	Key Topic
European Secure, Resilient and Trusted Ecosystem (ESRTE)	Task T1.4: Data/Application-centric Security (Lead: TUBS)	Cloud Security, Threat Visualization, Threat Assessment level, Threat Analysis
Industrial Domains and Sector Specific Pilots	Task T2.1: Telecom Sector: Threat Intelligence for the Telco Sector (Lead: TELENOR)	Data-centric threat modeling
Community impact and sustainability	Task T3.3: Developing the CONCORDIA's Ecosystem: Virtual Lab, Services and Training (Lead: CODE)	Cyber ranges for cybersecurity training , Cyber threat and training models
Industrial Domains and Sector Specific Pilots	Task T2.3: Transport E-Mobility Sector: Security of the e-Charging Infrastructure (Lead: BMW)	Vehicle Security, Secure communication, Security policy development
European Secure, Resilient and Trusted Ecosystem (ESRTE)	Task T1.2: Network-Centric Security (Lead: UT)	Monitoring and analysis of Encrypted Traffic preserving user privacy
European Secure, Resilient and Trusted Ecosystem (ESRTE)	Task T1.2: Network-Centric Security (Lead: UT)	Reliable detection of DDoS attacks
Industrial Domains and Sector Specific Pilots	Task T2.5: Defence (Dual Use): Security of Unmanned Aerial Systems (UAS) (Lead: ACS)	Tactical Ad Hoc Networks, Tactical Software Defined Networks
European Secure, Resilient and Trusted Ecosystem (ESRTE)	Task T1.1: Device-Centric Security (Lead: JUB) IoT Security Analytics	Hardware Security Assessment
European Secure, Resilient and Trusted Ecosystem (ESRTE)	Task T1.3: Software/System-centric Security (Lead: TUD)	Security-by-Design and privacy preservation (anonymization)

Industrial Domains and Sector Specific Pilots	Task T2.1: Telecom Sector: Threat Intelligence for the Telco Sector (Lead: TELENOR)	Threat Intelligence
Community impact and sustainability	Task T3.2: Piloting a DDoS Clearing House for Europe (Lead: SIDN)	DDoS
European Secure, Resilient and Trusted Ecosystem (ESRTE)	Task T1.1: Device-Centric Security (Lead: JUB) IoT Security Analytics	Firmware update in resource constrained IoT devices
Industrial Domains and Sector Specific Pilots	Task T2.4: e-Heath Sector: Privacy and Data Protection (Lead: IFAG)	medical devices, smart home, blue light communication - emergency, IoT devices

Finally, the following table summarizes the various standardization efforts that CONCORDIA partners are participating in.

Table 20: Standardization efforts that CONCORDIA partners are participating.

SDO	Title of committee or standard
OASIS	STIX
CORD	OpenCORD
OSM	Open Source MANO
CEN/CENELEC CWA	Workshop on "Requirements and Recommendations for Assurance in Cloud Security (RACS)”.
ETSI	Cloud Standard Coordination
OASIS	eXtensible Access Control Markup Language (XACML)
International Telecommunication Union-T	X.series
IETF	6TISCH Working Group RFC draft Zero - Touch Secure Join Connect, 6TiSCH secure minimal architecture
IETF	DNSOP WG
ETSI	TC CYBER
GSMA	Fraud and security Architecture Group
NGMN	Security Competence Team
IETF	TEEP
IETF	RATS
IETF	SUIT
IETF	NETCONF/YANG
IETF	RFC 7744
IETF	CoRE WG - Object Security for Constrained RESTful Environments (OSCORE)
IETF	CoRE WG - Group OSCORE - Secure Group Communication for CoAP
IETF	CoRE WG - Group Communication for the Constrained Application Protocol (CoAP)
IETF	CoRE WG - Discovery of OSCORE Groups with the CoRE Resource Directory
IETF	ACE WG - Key Provisioning for Group Communication using ACE
IETF	ACE WG - Key Management for OSCORE Groups in ACE
IETF	ACE WG - EST over secure COaP (EST-coaps)
IETF	ACE WG - Authentication and Authorization for Constrained Environments (ACE) using Oauth 2.0 Framework (ACE-OAuth)
IETF	ACE WG - Additional OAuth Parameters for Authorization in Constrained Environments (ACE)
IETF	ACE WG - OSCORE profile of the Authentication and Authorization for Constrained Environments Framework
IETF	ACE WG - Datagram Transport Layer Security(DTLS) Profile for Authentication and Authorization for Constrained Environments (ACE)
IETF	ACE WG - Proof-of-Prossession Key Semantics for CBOR Web Tokens (CWTs)

IETF	ACE WG - CBOR Profile of X.509 Certificates
IETF	Network Working Group - ACE Clients in Disadvantaged Networks
IETF	ACE WG - Protecting EST payloads with OSCORE
IETF	6TiSCH WG - Robust Scheduling against Selective Jamming in 6TiSCH Networks

4.4. Next Steps in Certification and Standardization

Next steps on certification efforts:

During the next period of the project, the project team aims to do the following:

- Finalization of the Feasibility study and determination of the selected Cybersecurity Skills profile.
- Implementation of the Certification Framework for Cybersecurity Skills.
- Implementation of the Supporting material for the Certification Framework for Cybersecurity Skills.
- Implement further discussions with the other Task Leaders, in order to determine the next Cybersecurity certification scheme.

Next steps on standardization efforts:

During the next period of the project, the project team aims to do the following:

- Communicate with the majority of the partners (at least those related to solutions and pilots – WP2 and WP3) in order to update the standardization information.
- Conduct further research on standardization efforts related to the identified key topics.
- Provide feedback to partners that have not identified any related standards.
- Identify areas where standards do not exist (e.g., via follow-up surveys) and would benefit from the CONCORDIA outputs.
- Create liaisons with standardization organizations on the topics of interest of CONCORDIA project.

5. Conclusion

To achieve these goals, the project has defined in its main activities the Work Package 5 (WP5), whose objective is to enhance the impact of CONCORDIA's outcomes through strategic exploitation, dissemination, and standardization. From an exploitation perspective, WP5 is developing a comprehensive exploitation plan, executing it during the duration of the project, in alignment with the partners' commercial and research interests. Furthermore, the standardization activities in WP5 aim to enhance the impact of CONCORDIA by transferring project results to relevant industry standardization and best practice working groups.

Finally, CONCORDIA's partners will also ensure an adequate level of dissemination of all the project results, both scientific and industrial, and using the most appropriate communication channels. This effort will ensure that the public is aware of the main challenges addressed within the project. Feedback from the public (both at the academic and industrial level) will be collected over various events and via different communication channels (e.g., communication events, social media channels, etc.). By the end of the final year (Year 4), WP5 will also produce a sound plan for providing sustainability to the project's outcomes, after the end of its duration.

To achieve these goals, the WP5 is broken down into 3 main tasks, that allow the project to build on its necessary activities in exploitation, dissemination, communication, certification and standardization. This deliverable reported on the activity and efforts performed from each of these tasks to achieve the main goals of the work package, as well as the individual objectives of each task, as explained in each corresponding section of the present report.

Deviations:
No deviations were observed during the course of the first year of the project.

Key Achievements:
The project had several key achievements reported in the present deliverable.

- Exploitation efforts:
  - 19 incubators and accelerators have been identified and contacted
  - 11 exploitable results have been already identified
- Dissemination & Communication efforts:
  - 50+ scientific papers published
  - 61 events / conferences / invited talks / seminars performed
  - 16 blog posts written and published on CONCORDIA website
  - 9000 website visits from users in more than 30 different countries
  - 261 Twitter posts / 125 Facebook posts / 250 LinkedIn posts
  - 16400+ of total engagements across social media platforms
  - 18 announcements posted
  - 59 publicities from news performed or received
  - 4 events / conferences sponsored
- Certification & Standardization efforts:
  - 32 Standardization Organizations identified
  - 295 Standards to be further studied
  - 54 Standards where CONCORDIA partners have an active participation
- Cross-Work Package collaboration between scientific & industrial partners, as demonstrated by the dissemination and communication activities, as well as

technology planned to be built and used, and further described in Deliverables D1.1 and D2.1.

Conclusion & Future Plans:

All objectives set in the project's WP5 have been so far achieved or exceeded, if we consider that the project has just finished its first year. This is reflected by the key achievements reported through the report and the level of completion of the KPIs, outlined in the Introduction of this deliverable. Although the KPIs have been achieved at this level, the consortium will continue to put effort and resources in the upcoming years, to improve its effectiveness in exploiting results from the consortium, disseminating its message to key stakeholders and the general public, as well as helping its partners have impact on standardization in cybersecurity.

List of Acronyms

ANSI	American National Standards Institute
ASTM	American Society for Testing and Materials
CA	Consortium Agreement
CSA	Cloud Security Alliance
CSRC	Computer Security Resource Center
DIN	Deutsches Institut für Normung
DoA	Description of Action
EC	European Commission
ER	Exploitable Result
ETSI	European Telecommunications Standards Institute
EU	European Union
FDA	Food And Drug Administration
GA	Grant Agreement
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoC	Indicator of Compromise
ISA	International Society of Automation
ISO	International Organization for Standardization
ITU	International Telecommunication Union
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NCCOE	National Cybersecurity Center of Excellence
NEMA	National Electrical Manufacturers Association
NERC	North America Electric Reliability Center
NIST	National Institute of Standards and Technology
oasis-open	Organization for the Advancement of Structured Information Standards
SAE	Society of Automotive Engineers
TRL	Technology Readiness Level