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[†]

Work Package 5: Exploitation, dissemination, certification and standardization
Deliverable D5.3: 2nd year report on exploitation, dissemination, certification and standardization

Abstract: This document represents the 2nd 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 produced content, organized campaigns and 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	*M24*
Actual Date of Delivery	*30.12.2020*
Deliverable Dissemination Level	*Public*
Editors	*Martin Horák, Nicolas Kourtellis, Argyro Chatzopoulou*
Contributors	*MUNI, TID, TUVA, FORTH*
Quality Assurance	*Shahid Raza (RISE)* *Julien Etienne Mascolo (CRF)* *Marco Caselli (Siemens)* *Neeraj Suri (ULANC)*

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

The CONCORDIA Consortium

UniBW/CODE	University Bundeswehr Munich / 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
JACOBSUNI	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
~~TUDA~~	~~Technical University of Darmstadt~~	~~Germany~~
MU	Masaryk University	Czech Republic
BGU	Ben-Gurion University	Israel
OsloMET	Oslo Metropolitan University	Norway
Imperial	Imperial College London	UK
UMIL	University of Milan	Italy
BADW-LRZ	Leibniz Supercomputing Centre	Germany
EIT DIGITAL	EIT DIGITAL	Belgium
TELENOR ASA	Telenor ASA	Norway
AirbusCS-GE	Airbus Cybersecurity GmbH	Germany
SECUNET	secunet Security Networks AG	Germany
IFAG	Infineon Technologies AG	Germany
SIDN	Stichting Internet Domeinregistratie Nederland	Netherlands
SURFnet bv	SURFnet bv	Netherlands
CYBER-DETECT	Cyber-Detect	France
TID	Telefonica I+D SA	Spain
RUAG	RUAG AG (as replacement for RUAG Schweiz AG)	Switzerland
BITDEFENDER	Bitdefender SRL	Romania
ATOS	Atos Spain S.A.	Spain
SAG	Siemens AG	Germany
Flowmon	Flowmon Networks AS	Czech Republic
TÜV TRUST IT	TUV TRUST IT GmbH	Germany
TI	Telecom Italia SPA	Italy
Efacec	EFACEC Electric Mobility SA (as replacement for EFACEC Energia)	Portugal
ARTHUR’S LEGAL	Arthur’s Legal B.V.	Netherlands
eesy-inno	eesy-innovation GmbH	Germany
DFN-CERT	DFN-CERT Services GmbH	Germany
CAIXABANK SA	CaixaBank SA	Spain

~~BMW Group~~	~~Bayerische Motoren Werke AG~~	~~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
CRF	Centro Ricerche Fiat	Italy
ELTE	EOTVOS LORAND TUDOMANYEGYETEM	Hungary
Utimaco	Utimaco Management GmbH	Germany

Document Revisions & Quality Assurance

Internal Reviewers

1. Shahid Raza (RISE) (review lead)
2. Julien Etienne Mascolo (CRF)
3. Marco Caselli (Siemens)
4. Neeraj Suri (ULANC)

Revisions

Ver.	Date	By	Overview
0.01	*8/10/2020*	*Martin Horak*	*Table of Contents*
0.02	*9/11/2020*	*Nicolas Kourtellis*	*Contribution from TID*
0.03	*9/11/2020*	*Argyro Chatzopoulou*	*Contribution from TUVA*
0.04	*13/11/2020*	*Martin Horak*	*Contributions from MUNI*
0.05	*23/11/2020*	*Martin Horak*	*Merging all contributions, editing, commenting, adjusting template based on a new version*
0.06	*30/11/2020*	*Martin Horak*	*Content update, editing.*
0.07	*8/12/2020*	*Anum Khurshid*	*Comments from review team added*
0.08	*9/12/2020*	*Argyro Chatzopoulou*	*Updated version of section 4.*
0.09	*11/12/2020*	*Nicolas Kourtellis*	*Updated version of section 2.*
0.10	*14/12/2020*	*Martin Horak*	*Updated version of section 3. All comments from the review team addressed.*
0.11	*19/12/2020*	*Martin Horak*	*Revision before submission.*
0.12	*28/12/2020*	*Martin Horak*	*Final version sent for submission.*

Disclaimer:
The sole responsibility of this document lies with the authors. The European Commission is not responsible for any use that may be made of the information contained therein.

Executive summary

The present document is the third deliverable of Work Package 5 (WP5), and represents the 2nd 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.

WP5 is organized into three main tasks for:

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

This deliverable D5.3 has three main sections, one for each of these corresponding tasks. In each of these sections, the achievements of the consortium within the second 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 24 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

CONCORDIA project has defined in its main activities the WP5, whose purpose is to boost the impact of the project 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 (2022), 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 M24 of the project (i.e., 1/2 of the project's duration):

Table 1: KPIs relevant for WP5 activities during the second year of the project

General KPI	Goal in 4 years	Performed in M1-M24	Unit of measure
CONCORDIA in social media	15000	38 100 +	Views + Likes (see Section 3.3.3 for details)
Publication of Case Studies Documents – White Papers	-	55	Blog posts (see Section 3.3.2 for details)
Downloads for public deliverables, prototypes, promotional material	500 +	4 000 +	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	2	Open Door Event (see Section 3.3.5 and Deliverable D4.8)

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):
    - 26 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
    - 30 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):
    - 10 761 users visited the CONCORDIA website from around the world during the first year of the project.
    - 39 blog posts published on CONCORDIA website or in prominent technology websites, written by CONCORDIA partners explaining technology they built, their services offered, etc.
    - 19 videos about our work, especially focused on demonstrating the value.
    - 16 infographics to which covers various project outputs and lots of other different form of content.
    - 46 events / conferences / invited talks / seminars held or attended by the consortium partners and its members.

  - 248 Twitter posts / 269 Facebook posts / 281 LinkedIn posts.
  - 21700+ of total engagements across social media platforms.
  - 9 communication campaigns focused on different topics.
  - 34 announcements posted on the CONCORDIA website.
  - 36 news and other web articles published providing high publicity to the project's activities.
  - Cooperation with other subjects and active participation in CCN communication group.
- Efforts on Certification and Standardization (Section 4)
  - 37 Standards Developing Organizations have been identified from the consortium partners as organizations developing standards that are relevant to the work performed within the CONCORDIA project.
  - 396 standards to be studied from the consortium partners for their relevance in their activities in the cyber security sector.
  - CONCORDIA partners have declared that they participate in the activities of 18 Standards Developing Organizations and Stakeholder Groups
  - CONCORDIA partners have declared that they participate in 48 activities of these organizations or groups

Roadmap of the Deliverable:

In the next three sections, we analyze the objectives of the main tasks of WP5, discuss the strategy adopted to achieve them and highlight the progress of each task upto the submission of this deliverable.

2. Efforts on Exploitation

2.1. Objectives of this 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 analyse the exploitation possibilities of the CONCORDIA project
- To develop ways that build sector-specific incubators

After the 1st year review, it was observed that this task has activities that overlap with Task T3.5. Therefore, it was deemed ideal to attempt a merging of the two tasks, by creating a new task T5.1 which takes on this overlapping set of activities. Therefore, the consortium identified the following core activities that need to be carried out within this redefined task T5.1, for the remaining duration of the project, to fully achieve these objectives (also detailed in the corresponding amendment AMD-28 of the project, which was submitted for consideration from the Project Officer and was approved on 30.11.2020):

- **A1:** Set-up innovation and exploitation steering sub-committee: meet twice/year to review potential of technology, pilots, and technical progress made by each partner.
- **A2:** Guide and support partners to develop business plan to formalize exploitation strategy based on tech results & IPR and protection. The sub-committee will identify novel ideas worthy of support, patentability, promotion of top candidates, etc.
- **A3:** Set-up protected *knowledge management area* in Concordia website for controlled dissemination and exploitation.
- **A4:** Perform commercial exploitation based on strong Concordia industry, outcomes used internally in consortium and externally in incubators and new start-ups.
- **A5:** Create environment for deployment and validation of prototypes before large-scale roll-outs.
- **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.
- **A7:** Support and guide partners in EU data sharing with workshops, events, and interaction with stakeholders
- **A8:** Provide support of services related to incentive models for threat intelligence data sharing.

Regarding the merging of the two tasks, in effect, during the last month of this year and in the future, activities such as continuous "scouting" of "start-up community" stakeholders will continue to function under the name of "Pan-European Cybersecurity Start-up Community (PECS-UP)". All results of T3.5, such as PECS-UP mailing list, quarterly newsletters, and work on data sharing incentives, will continue in the task T5.1, now much better integrated and aligned with the exploitation strategy and roadmaps. However, for the current year, since the majority of T3.5 work was carried out in WP3, this work will be reported in D3.2.

2.2. Strategy to achieve Task Objectives

The overall strategy of the project for achieving the new T5.1's objectives has been to put effort during the second year of the project in the following steps:

- Form the Industrial Strategy 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 stakeholders outside the project. 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, available or reachable incubators and accelerators, 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, as well as communicate potential avenues for knowledge sharing in events with key stakeholders Related activities: A3, A7, and further discussed in Section 2.2.3.
- Consult with outside key stakeholders for extracting new insights and capturing important trends outside the project, as well as incentives for knowledge sharing on threat intelligence. Related activities: A6, A7, A8 and further discussed in Section 2.2.4.

2.2.1. Industrial Strategy Committee

The project, earlier in Y2, formed the Industrial Strategy Committee to take-on, among others, the responsibilities of the exploitation and innovation subcommittee as defined in the new task T5.1 of the GA.

This committee is due to meet twice per year to review the potential of technology built within the project's technical work packages and use case pilots, and assess technical progress made from the partners towards the exploitation of the technology built. Furthermore, the committee is due to identify novel ideas worthy of support by the consortium in different ways. For example, some projects may need help with patenting and other IPR protection, PR and other media support, guidance in developing business plans, etc. The committee is also responsible for formalizing the exploitation strategy based on these technology results.

The committee's initial formation has 22 members (1 from each industrial partner at the time) and 1 chair (from ACS partner). The first meeting of the committee was in July 2020. This formation will be re-assessed when new industrial members join CONCORDIA.

Among the first tasks of the committee were the following:

1) Redefine what Exploitable Results (ERs) are, as explained in subsequent subsection (done).
2) Redefine the important dimensions that should be collected from partners regarding ERs (done).
3) Redefine the important dimensions that should be collected from partners regarding the incubators and accelerators available within or associated with the consortium (done).

4) Perform assessment and ranking of collected ERs, to select Key ERs with high ROI (in progress).
5) Open channels of communication with said entities (in progress).

Furthermore, the committee had its second meeting in early December 2020, and discussed several aspects related to innovation management in CONCORDIA, ERs declared by partners so far (as explained next), and different dimensions related to each ER. During its meeting, the committee assessed innovation potential, market readiness, technical maturity and community/network effect for each of a subset of 12 ERs. Based on these assessments, it will prepare a ranked list of Key ERs (KERs) and will prepare recommendations and consultations for the partners that proposed them, so that they can define successful business models, how to transition from innovative idea to market, how to take advantage of the full potential of CONCORDIA's network of stakeholders, etc.

2.2.2. Strategy in collecting and ranking partner input

In order to collect and rank input provided from the partners, the committee followed the below strategy. However, and if necessary, 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 [1], various criteria can be used to rank exploitable results declared by the partners:

- Type of result (product, process, software, service, etc.)
- Innovation and differentiation of ER from state of art
- Unique value proposition of ER
- Completeness in terms of features, functionalities, references, etc.
- Target audience and user type of ER
- Stakeholder interest
- Technical maturity (e.g., size and scope of verification and validation, type of environment used for testing, Technical Readiness Level (TRL), etc.)
- Contribution to or positioning in a specific market
- Relation to specific industry sector / pilot / etc.
- Delivery, execution and transfer capability
- Protection and IPR issues
- Benefits to customers, collaboration of partners, public, etc.
- Exploitation path (internal, public, etc.)

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

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 to be reached by an exploitable result, before assessing if the exploitable result is worth to be considered or not. Methodologies outlined already on the web for assessing the achievement of each criterion will be considered[2], and applied when partners 1) report completion of these exploitable results, and 2) readiness to push them to the market.

2.2.3. Results sharing

The material collected from partners using these surveys, after it is sanitized, it is ranked and shared with the partners of the consortium, so that they are aware of all the exploitable efforts in the project. Each partner is also 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 is requested at least every six months. In fact, this process has been performed 4 times during the first 23 months of the project, by frequent surveys and circulation and analysis of updated ER collection during General Assembly and other board meetings.

Furthermore, the results are 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 is used for announcing exploitable results and for dissemination purposes to external public stakeholders.

By the end of Y2, exploitable results were shared with the partners through presentations and accessible documents on project’s online common workspace (Confluence[3]). Overall, we have already 30 exploitable results declared by consortium partners (detailed in Section 2.3). This number has increased by almost threefold since the end of Y1. In this second year of the project, the partners were requested to define more details per result, and declared results are more mature, have better differentiation from the state-of-art, and exploitation path. There were also more collaborative exploitable results defined, that is, results that are designed and implemented by one (or more) partners and have a target audience of one or more other consortium partners, or even external companies and general industry sectors.

2.2.4. Strategy to communicate results to key stakeholders

We perform constant monitoring of the sector via participation to key events in industrial and academic meetings and other types of relevant events. This activity is executed in collaboration with partners in T3.4 and T3.5. 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 second CONCORDIA Open Door event (COD) online, at the end of October 2020. At COD, we presented the project for collection of key exploitation 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

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

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

stakeholders engaged with the project and involved in the CONCORDIA ecosystem. Details on these events are given in the next Section 3.3.5.

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)[4] encoding to declare the maturity of the ER. The list of collected ERs is reviewed by the committee every six months, during the regular biannual meetings.

The last round of input received from 27 partners revealed 30 ERs, up from 11 ERs declared at the end of Y1. A brief analysis of the declared items follows. As probably expected, the majority of ERs declared are software and services (~70%), with other ERs such as events, labs, process, etc., completing the other ~30%.

In general, we had the following breakdown on eight types of ERs declared:

- Software: 12
- Service: 9
- Event: 3
- Standardization: 2
- (virtual) Lab: 2
- Report: 2
- Process: 1
- Course: 1

In particular, we had software ERs being declared such as the following:

1. MISP to Flowmon ADS integration
2. Passwordless Authentication and Identity Verification Solution - KYC Solution
3. Pipeline for Privacy vs. Utility Tradeoff Assessment
4. Threat Intelligence Platform (TIP)
5. Detection of IoT models behind a home NAT
6. ML techniques for identifying file-less attacks and malicious documents
7. KYPO Cyber Range Platform (CRP)
8. Financial Threat Intelligence Platform
9. Path Computation Element (PCE)
10. DDoS clearing house
11. Library-based access control
12. (Blockchain) Payment Channel as a Service

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

13. CONCORDIA TI Sharing Platform

Furthermore, we had services ERs being declared such as the following:

1. CONCORDIA TI Sharing Platform[5]
2. CCH Service
3. Federated Learning Modeling Service
4. Telenor MISP platform
5. Patient data platform
6. Labs and Cyber Ranges
7. Security architecture for UAS
8. Financial Threat Intelligence Platform

Finally, we had other types of ERs being declared such as the following:

1. Capture The Flag event
2. Cyber-Range Training (1)
3. Cyber-Range Training (2)
4. Pilot course / associated skills certification scheme for cybersecurity consultant profile
5. Cybersecurity Threat Landscape (technical aspects)
6. Stakeholders group creation process
7. OASIS standardization for cyber intelligence
8. Virtual lab: 5G Lab
9. Cyber Range Scenario Interoperability
10. Virtual lab: Open-Source Analytics (OSA)
11. Cybersecurity Consultant Profile

These ERs collected were from 16 industrial and 11 academic partners. Interestingly, and perhaps expectedly, the majority (60%) of ERs are in their early stages of maturity, covering different industrial sectors and pilot tasks. Next, we outline some interesting breakdowns on maturity, industry involved, and CONCORDIA task related to their definition and applicability.

Partners defined the technical maturity of their ERs using the following list of Technical Readiness Levels (TRLs) published by the EU:

- TRL 1 – basic principles observed
- TRL 2 – technology concept formulated
- TRL 3 – experimental proof of concept
- TRL 4 – technology validated in lab
- TRL 5 – technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies)

[5] declared both as a software and service

- TRL 6 – technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies)
- TRL 7 – system prototype demonstration in operational environment
- TRL 8 – system complete and qualified
- TRL 9 – actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies; or in space)

Technical Maturity:

- TRL 1-4: 18
- TRL 5-7: 4
- TRL 8-9: 5

Industries involved:

- Several declared relevance to many/all industrial sectors
- Finance
- Telecommunications / networks
- Health

CONCORDIA Tasks involved / applicable:

- T2.1, T2.2, T2.4, T2.5
- T3.1, T3.2, T3.3
- All pilot tasks (i.e., ER was declared as relevant to all pilot tasks)

Furthermore, some of the defined ERs requested for support with IPR protection (7 ERs) and some requested help in PR promotion (10 ERs). Finally, the majority of ERs (16/30) were declared that they will have a version (preliminary or final) by M24. Furthermore, 4 ERs have such a deadline at M36. Interestingly, 8 ERs have a delivery deadline by end of the project, i.e., M48.

2.4. Incubators and Accelerators

From our earlier efforts, it became clear that CONCORDIA (and any EU project for that matter) 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 Industrial Strategy Committee 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. These are entities that were contacted by the consortium partners and made aware of our collection effort, so that they are positive to reach out to them. 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 inputs:

Overall, the collection of incubators and accelerators provided by the consortium partners, as it was first collected by end of Y1, and also re-collected and information-updated by end of Y2, 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.

Given that the new Task 5.1 has been expanded to include the activities of old T3.5, this allowed us work on developing and supporting the community of 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. Towards this goal, we started reaching out to the collected entities, in order to expose them and engage them to our exploitation activities.

Survey structure:

The input requested by the consortium partner 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 have increased from 19 (declared by M12) to 26 (declared by M24):

1. Wayra
2. Pier01
3. La Salle Technova
4. Univ. of Luxembourg Incubator
5. EIT Digital Accelerator
6. EIT Digital Venture Program
7. Cybersecurity incubator London
8. JIC
9. Bayern startup
10. Filarete Servizi
11. Tovarna Podjemov
12. CEDRA SPLIT
13. Incubateur Lorrain
14. BGN Technologies Ltd
15. Health Hub Vienna
16. INiTS
17. weXelerate
18. ABC Accelerator
19. Primorski Tehnološki Park
20. Ljubljanski Univerzitetni Inkubator
21. Pos4work
22. Ericsson ONE
23. Cube5
24. eCapital Cybersecurity
25. Scaler
26. FIWARE iHubs and accelerator

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, 100M 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 small and medium-sized, with up to 10-100 startups supported, but in some cases, the identified accelerators / incubators support up to 500 startups.

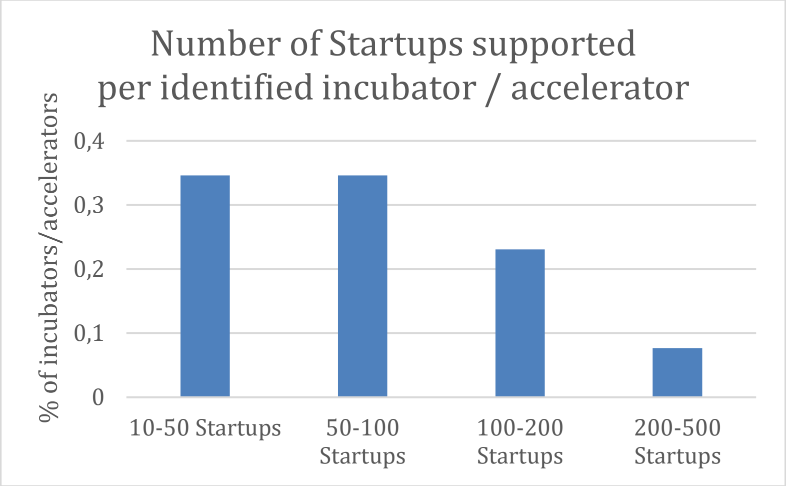


Figure 1: Number of startups supported per identified incubator / accelerator

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: 27%
- IT specific: 35%
- Cybersecurity:38%

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

Geographical coverage:

Most entities identified (~85%) focus on EU-based start-ups, and in some cases only in start-ups that operate in specific countries. Some exceptions exist which support startups in a worldwide arena (~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:	25%
Partner has knowledge/relation:	40%
Partner is aware of the entity:	35%

The above breakdown shows that 65% of the incubators/accelerators identified are either directly linked to a partner, or the partner has some knowledge or loose ties with the entity. The other 35% of entities are not directly linked to the project, but in fact, reveals potential space for effort to be placed in the next years to establish such relationships. We note that from M12, there has been a total increase of 9% in entities that partners have direct or loose relationships with, demonstrating in action the earlier statement.

Channels of communication:

We have already started to communicate our exploitation strategy and results to these entities and other key stakeholders (more than 35 entities and key individuals). In fact, we have invited them to join our Pan-European Cybersecurity Start-Up Community (PECS-UP), which is a community established in CONCORDIA project with a vision of agility in technology transfer and market adoption, as well as interconnecting external initiatives and stakeholders of relevance to the community. Our communications will be with them via direct emails, the quarterly newsletter on exploitation and community efforts, as well as virtual and face-to-face meetings and events throughout the year.

2.5. Impact from COVID-19

The pandemic affected or even interrupted the work of several CONCORDIA teams, either academic or industrial, and reduced or even stopped their technical progress (as it is explained in the corresponding deliverables due in M24). Therefore, there was a marked slowdown in getting closer to exploitable results that are demonstrable to key stakeholders, or even worthy of pushing to an incubator / accelerator to hit the market.

Indeed, the CONCORDIA partners were able to react to the Task 5.1 calls for defining (or adapting) their exploitable results, provide more information about their novelty and value, and help T5.1 with assessing the landscape of technology built within the project. Due to these efforts, we succeeded in collecting almost 2 times more exploitable results than last year, and several more incubators and accelerators in reach of the consortium.

However, there were several efforts impacted by COVID-19 regarding Task T5.1, which were planned for execution during Y2, but COVID-19 has severely slowed them down. They are now being planned for execution in the upcoming year.

One effort will be to push potential Key Exploitable Results from academic and industrial partners, as identified by the Industrial Strategy Committee, into the cybersecurity market. Furthermore, there needs to be more concrete processes in place, to facilitate closer collaboration with respect to the academic partners solving problems the industrial partners are facing, via true knowledge transfer between them.

Another effort will be at the business model definition part, so that more exploitable results are properly defined with competitive business models, and then these models being exposed to reachable incubators and accelerators from our collection. Furthermore, the

Industrial Strategy 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. Such sessions are already being designed and underway to be executed in the next few months of the project.

2.6. Next Steps on Exploitation and Incubators

CONCORDIA has deep reach into large accelerators and incubators across Europe and worldwide. This means great potential for the startups that are being initiated within the consortium based on technology built during the CONCORDIA project, as well as afterwards.

Overall, 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, 2) defining appropriate and profitable business models, 3) reaching out to venues and entities that can help said technology to hit the market, 4) exposing key stakeholders to CONCORDIA technology. 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 dissemination and communication strategy of CONCORDIA project. The reported effort is organized in three sections, namely:

1. The description of goals and objectives of this Task (Section 3.1).
2. The strategy to achieve these goals (Section 3.2).
3. The description of communication and dissemination activities performed in the second year of the project (Section 3.3).

3.1. Objectives of this Task (T5.2)

Dissemination and communication activities are essential for the CONCORDIA project and a dedicated task was designated for their implementation. The purpose of T5.2 and also, its main challenge, is to boost the impact of CONCORDIA project through dissemination and communication. In order to address this challenge effectively, the T5.2 uses the strategic approach based on the following logic (**Figure 2**). Firstly, the general communication and dissemination goals were defined. These goals are aligned to the project goals and they serve as the main guiding principles for our dissemination and communication. Secondly, specific communication and dissemination objectives were defined in order to implement the general goals. Thirdly, the communication and dissemination strategy was built in order to achieve the objectives.

D&C GOALS
D&C OBJECTIVES
D&C STRATEGY

Figure 2: CONCORDIA dissemination and communication logic

Whereas the general dissemination and communications goals remain the same during the whole project, dissemination and communication objectives can be updated in order to react on evaluations, reviewers' recommendations, phase of the project or the context in general. Dissemination and communication objectives of the project were focused especially on publicity and branding during the first year of the project. The objectives were updated for the second year of the project in order to reflect the dissemination phase of the project (see Table 4) and also the reviewers' recommendations. The main difference is our shift to content marketing tactics. This is described in the section which deals with communication objectives. Involvement in communication activities and work on the communication goals of the project is a common task of all partners. A communication group is in charge of coordinating and implementing strategic communication activities. The group is led by Masaryk University (MUNI) and has three members who deal with the communication activities and three members from other tasks who provide insight and help with coordination.

The group has no budget available for the use of external services (creation of multimedia content, PR services, etc.).

Dissemination and communication goals:

We defined four general dissemination and communication goals, which are aligned with the CONCORDIA objectives. These goals are aligned to the project goals and they serve as the main guiding principles for our dissemination and communication. They remain the same during the whole project.

Table 2: 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).

Dissemination and communication objectives:

In order to achieve the aforementioned goals, we defined specific objectives that will be executed by the project. These communication objectives defined below in Table 3 can be updated during the project in order to support communication goals appropriately.

Table 3: CONCORDIA Dissemination and Communication Objectives (DCO)

DCO	Name	Description	When
1	Project 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	Content Marketing	We will focus on the preparation of our own unique content with the purpose to show what we do and enhance the impact of our results. Especially we will focus on producing blog posts, newsletters, infographics, videos and webinars. 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

3	Social Media	We will actively use social media channels (Twitter, LinkedIn and Facebook) to promote our results, increase trust and build community. The activity will be monitored based on the total number of views and likes (15,000 as KPI-DC-10).	M1-M48
4	Campaigns	We will lead communication campaigns – planned and coordinated communications activities focused on boosting the impact of concrete outcome (e.g. event, software, deliverable).	M15-M48
5	Events	We will participate in relevant events in order to build our brand and share our results.	M1-M48
5	Publicity	We will exploit all relevant communication opportunities which will occur during the project to support our communication goals. We will focus on media relations and we will also engage in cybersecurity initiatives, education activities, targeted focus groups with EU officials, policymakers, ECSO and cPPP officials and other stakeholder organizations.	M1-M48
6	CCN communication activities	We will participate in coordinated communication activities with the other pilots (ECHO, SPARTA, CyberSec4Europe) 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)
7	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
8	Offline activities	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-M48
9	Publicity	We will exploit all relevant communication opportunities which will occur during the project to support our communication goals. We will focus on media relations and we will also engage in cybersecurity initiatives, education activities, targeted focus groups with EU officials, policymakers, ECSO and cPPP officials and other stakeholder organizations.	M1-M48

10	Internal communication	We will spread knowledge within the consortium, and we will actively foster the consortium members and our partners to engage in dissemination and communication activities. We will provide regular internal instructions for our partners which accurately describe what to do to support our goals while keeping communications consistent.	M1-M6 preparation, M6-M48 regularly updates and reminders

Communication phases:

CONCORDIA communication and dissemination activities are, in general, divided into five distinctive phases, as explained in Table 3: 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. In every phase, we adjust our dissemination and communication objectives in order to reflect the phase specifics.

Table 4: CONCORDIA communication phases.

Phase	Description	Time	Dependencies
I. 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	
II. 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
III. 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
IV. 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

V. 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?

Therefore, our dissemination and communication strategy consists of three parts which are interconnected and based on our dissemination and communication goals and objectives.

- CONCORDIA narrative, key messages and content
- Target audiences
- Dissemination and Communication tactics

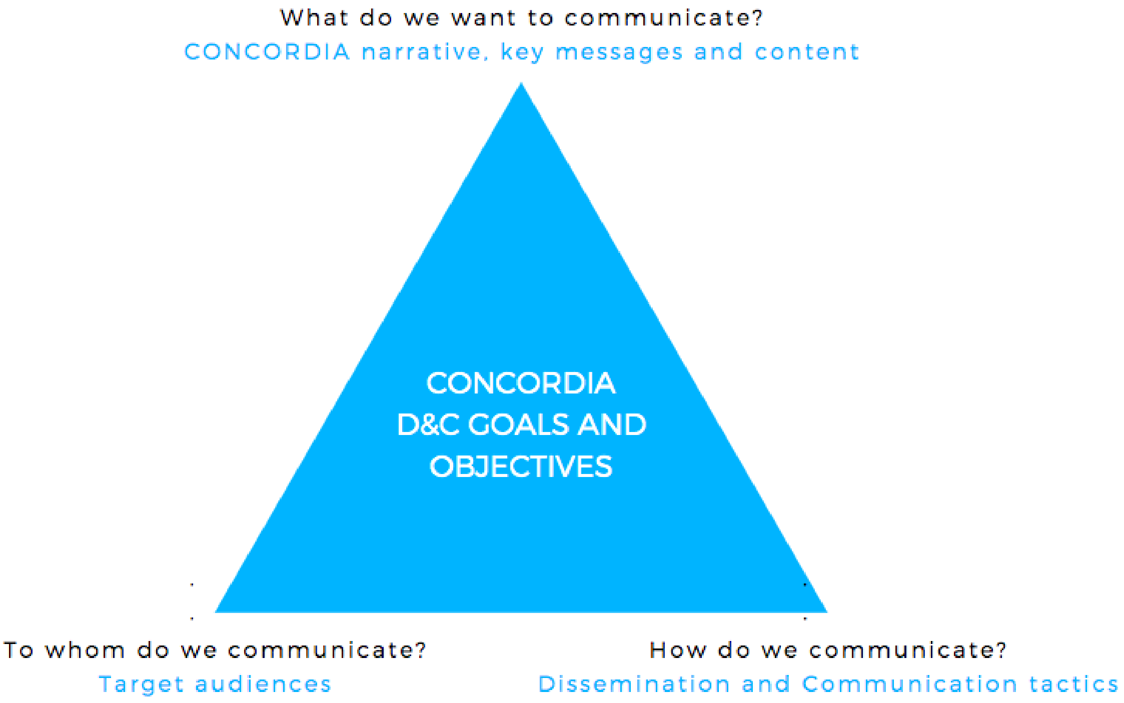

What do we want to communicate?
CONCORDIA narrative, key messages and content
CONCORDIA D&C GOALS AND OBJECTIVES
To whom do we communicate?
Target audiences
How do we communicate?
Dissemination and Communication tactics

Figure 3: CONCORDIA dissemination and communication strategy

3.2.1. CONCORDIA narrative, key messages and content

This section describes what we will communicate. The core of this part is our narrative which summarizes the brand story of our project, this narrative is then delivered in key messages and in our content. The simple scheme of this hierarchy represents Figure 4.

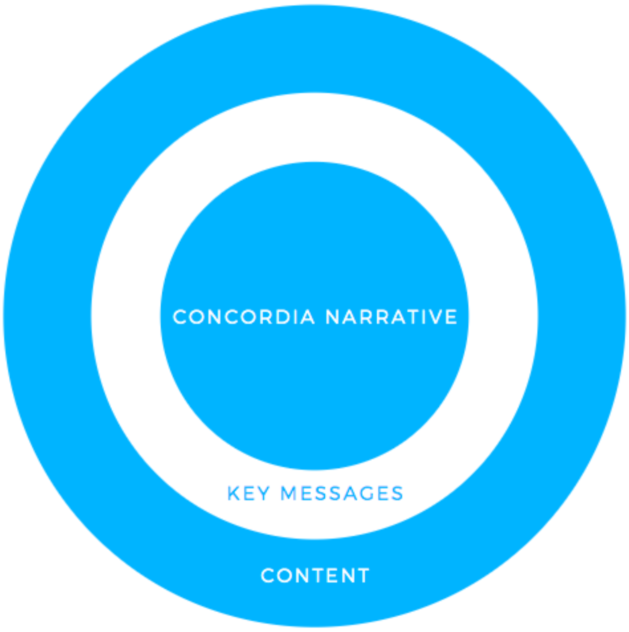


Figure 4: Hierarchy of CONCORDIA dissemination and communications outputs

<u>CONCORDIA narrative:</u>

CONCORDIA narrative is the overreaching leitmotiv for our dissemination and communication activities. Its purpose is to maintain brand identity consistency in our communications. It is based on the theory of archetypes, in specific the leader archetype. It can be summarized by this: European cybersecurity competencies are fragmented. Our mission is to lead their integration to build the European Trusted, Secure and Resilient Ecosystem for Digital Sovereignty of Europe.

<u>Key messages:</u>

CONCORDIA communications group uses two types of key messages. The first type is key messages which are coined for every communication campaign according to its audience and the objective of the campaign (e. g. call to participation/action or messages to raise awareness). These key messages are not listed here. The second type is key messages about the project itself. Their purpose is consistency in communication about the project identity. These key messages are listed in the Table 5.

Table 5: CONCORDIA key messages

Topic	Message
Who we are and what is our purpose	We are a dedicated consortium of more than 50 partners. 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?	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/

Content:
Three main categories of content were identified for CONCORDIA. These categories consist of topics on which we focus in our communications.

Table 6: CONCORDIA content

Category	Topics
Facts about the project	This covers many topics which are not directly related to our results. For example, our successes, introducing of project partners, “backstage” information, planned actions, consortium internal events, etc.
Project results	Most of our content is focused on the results of work from WP1, WP2, WP3, WP4, WP5 and W6.
Reactions to context	In addition to the planned content of the first two categories, we will focus on production of content that will react to ongoing events relevant to the CONCORDIA project.

3.2.2. Target audiences

This section describes our target audiences. Since CONCORDIA project has a large scope the simplification of segmentation is needed. The most relevant target audiences were defined in relation to project objectives.

Community of cybersecurity professionals
Cybersecurity community at European level is the crucial target audience for CONCORDIA. Whether decision-makers or practitioners, they can benefit from CONCORDIA multidisciplinary approach to cybersecurity since it deals with a wide range of tasks (technical, legal, societal, economical). We will focus on building trust with the cybersecurity community and sharing of our results.

CONCORDIA stakeholders
The subsystem of the cybersecurity community is CONCORDIA stakeholders – that means cybersecurity subject who have already some form of relation with CONCORDIA. This audience requires more targeted communications. Tasks 4.6 is focused on this audience.

Scientific community:
We address the scientific community to enhance the impact of CONCORDIA’s multidisciplinary research outcomes. Targeted dissemination and communication activities are performed by the traditional means (conferences, workshop, papers) and communication group also disseminate the results to the cybersecurity community and to other relevant audiences.

Private sector
The private sector is one of the end costumers of CONCORDIA. Whether it's start-ups, SMEs or big industries, they all can strongly benefit from CONCORDIA outcomes. Targeted communication will be achieved via cooperation with specialized tasks (e. g. T5.1 Exploitation and Incubators). Communication with the private sector will build on existing relationships and informal communication channels. It will also be supported by media relations, social media, content marketing and printed materials.

Public bodies and cybersecurity initiatives

Our goal is to establish cooperation with public bodies and cybersecurity initiatives at European level in order to become CONCORDIA stakeholders. As in the private sector, we want to present our results to these entities and at the same time, we want to participate in their communication activities. National cybersecurity authorities, ENISA, ECSO, ECHO, SPARTA, CyberSec4Europe, Cyberwatching, etc. are particularly relevant.

Media and the general public

Media are mainly intermediary for reaching other target audiences. Of course, in a world where journalists fight every day with the overload of press releases is challenging to get into the media with media relation tools. In order not to become banal, our approach to the media is based on a careful selection of the most promising outcomes with a strong story. We will share them with specialized media at first. If relevant we will also address the mainstream media at European and national level to reach the general public in order to demonstrate the benefits of our project for everyday life.

Consortium members

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.

3.2.3. Dissemination and communication tactics

This section describes which communication tactics (channels, methods and materials) we use to deliver our messages to the defined target audiences. Of course, not all communications tactics are relevant to all audiences in every case. Therefore, they need to be carefully chosen in order to fulfil the objective of the concrete communication action.

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.

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/

Media

Media are in general powerful channel for reaching our audiences. We will prepare a media list of the specialized media and we will use press releases to inform these media about our most promising outcomes.

Channels of cybersecurity initiatives and projects:
These channels are very relevant for CONCORDIA since they have an audience which is important for our project. Therefore, we will actively ask for support by other projects and initiatives.

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.

Cyber Competence Network pilots coordinated channels:
CCN communication channels (website, Twitter, media relations, materials, etc.) are important tools for coordinated communications about CCN and they can also boost the communication activities of each pilot.

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).

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.

Visual identity:
Visual identity is an essential tool for brand building, as it represents one of its most visible external representations. Together with our narrative and key messages, visual 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.

Content marketing forms:
We will use different forms to deliver our content. Especially relevant are blog posts, news items, social media posts, videos, infographics, white papers, deliverables, presentations and webinars. This list is not restrictive. On the contrary, we can use also other content form if it makes sense in given context.

Communication campaigns:
Communication campaigns are important communication tactic of CONCORDIA project. Coordinated communication activities in given period of time will boost a concrete topic much better than individual promotional acts. Our approach is based on using various forms of contents and all relevant channels to promote selected topic (e.g., event invitation, software release, important article).

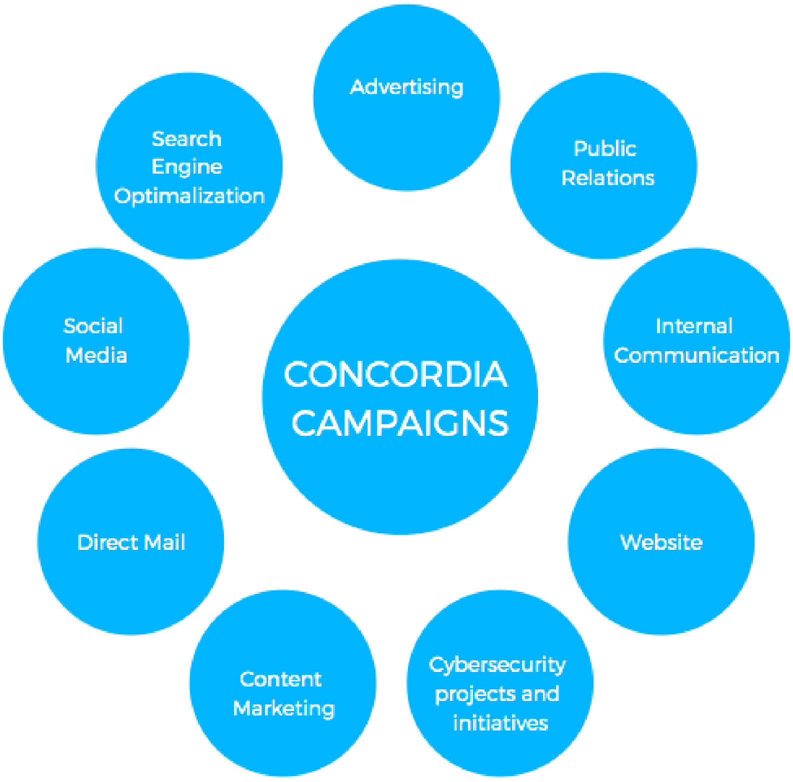


Figure 5: CONCORDIA campaigns approach

3.3. Disemination & Communication Activities

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

3.3.1. CONCORDIA website

The CONCORDIA website (www.concordia-h2020.eu) is the main 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. During the second year of the project, we redesigned the homepage of the website to better reflect the project targets and results and also improve the look and feel of the website. The website has been regularly updated with new content. The current version of the homepage is presented in Figure 6.

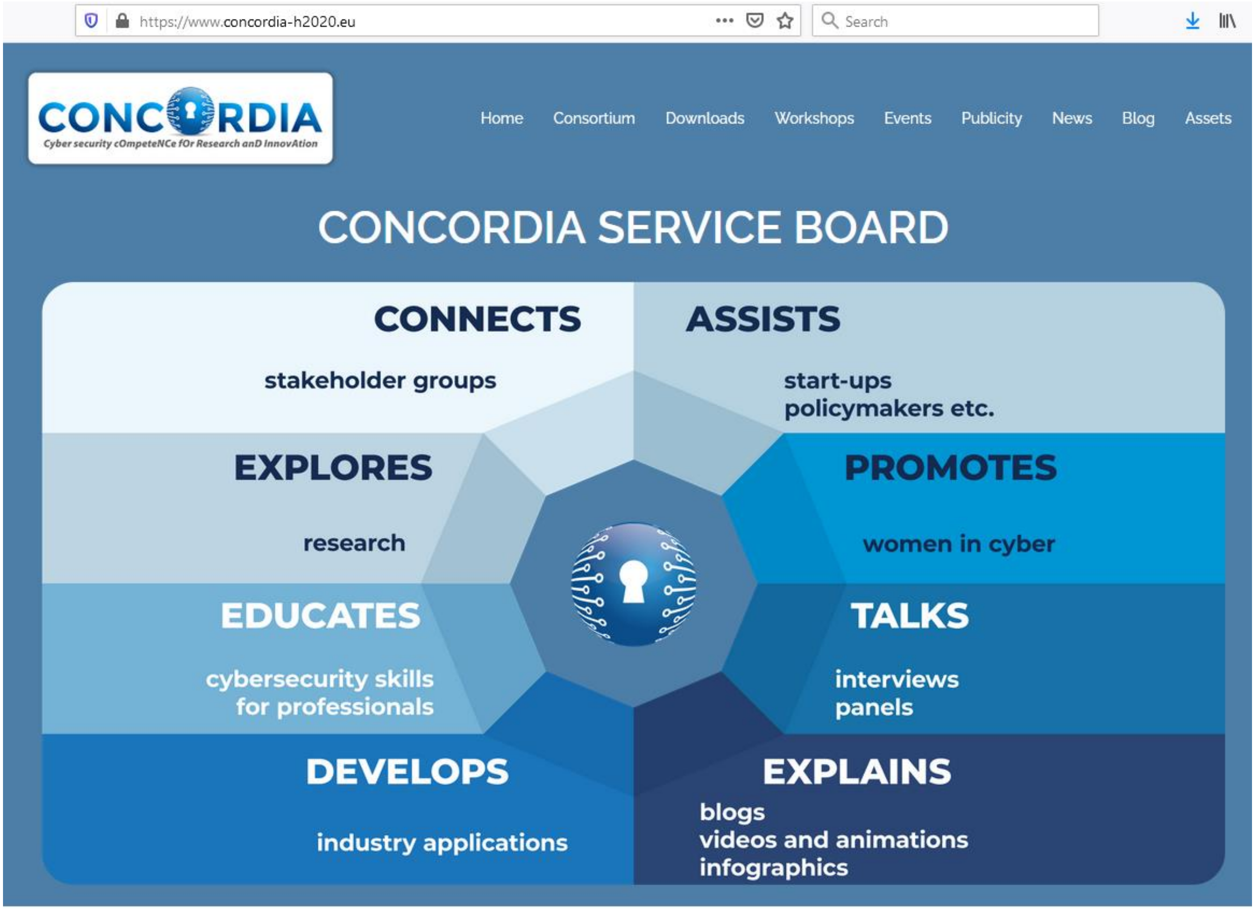
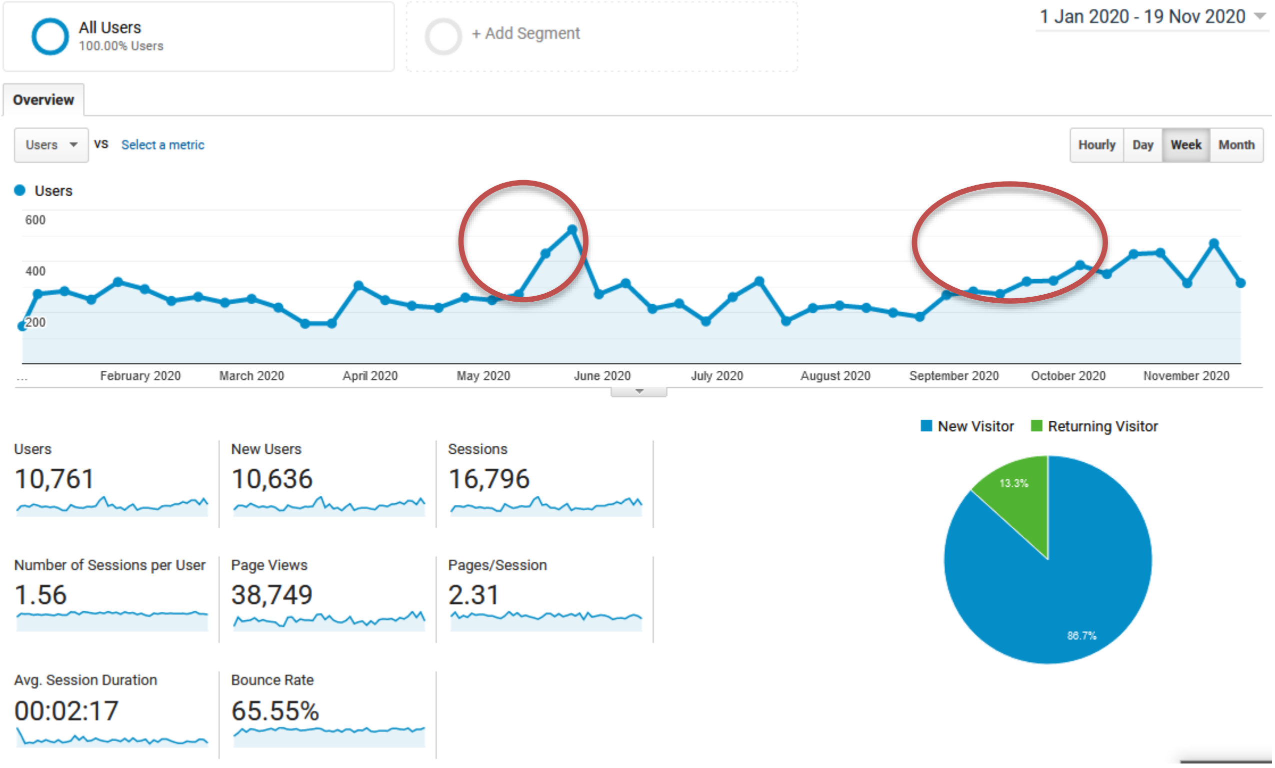


Figure 6: CONCORDIA website (homepage)

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 some statistics for the second year of the project (2020).

Website Visitors and Trend:

The users that were served by the CONCORDIA website per week during the second year of the project can be seen in the Figure 7. We can see that more than 10000 users were recorded in this period. This means that we had an approximate of more than 30 visits per day. The spike during June is probably due to the traffic produced from the CONCORDIA workshop on Education for Cybersecurity professionals, while the increase that is visible from September till October due to the dissemination activities related to COD2020 event that took place online at the end of October. The figure also presents that these visitors created 16K sessions against the website which resulted in 38K served webpages. This is about 100 webpages per day.



All Users 100.00% Users

1 Jan 2020 - 19 Nov 2020

Users vs Select a metric

Users 10,761

New Users 10,636

Sessions 16,796

Number of Sessions per User 1.56

Page Views 38,749

Pages/Session 2.31

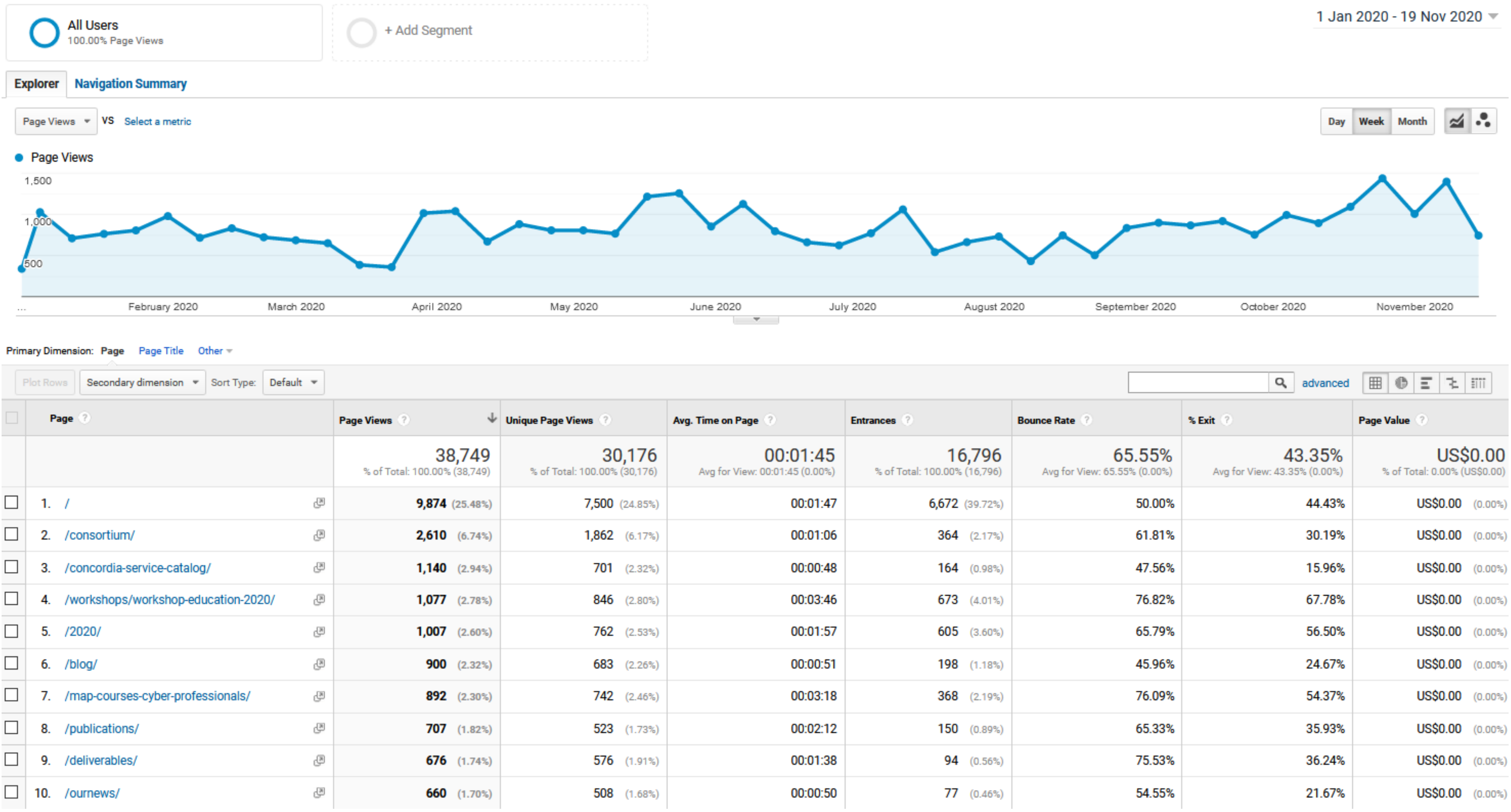
Avg. Session Duration 00:02:17

Bounce Rate 65.55%

Figure 7: Users per week that visited the CONCORDIA website. With red circles we marked the CONCORDIA workshop on Education for Cybersecurity professionals and the COD2020 event

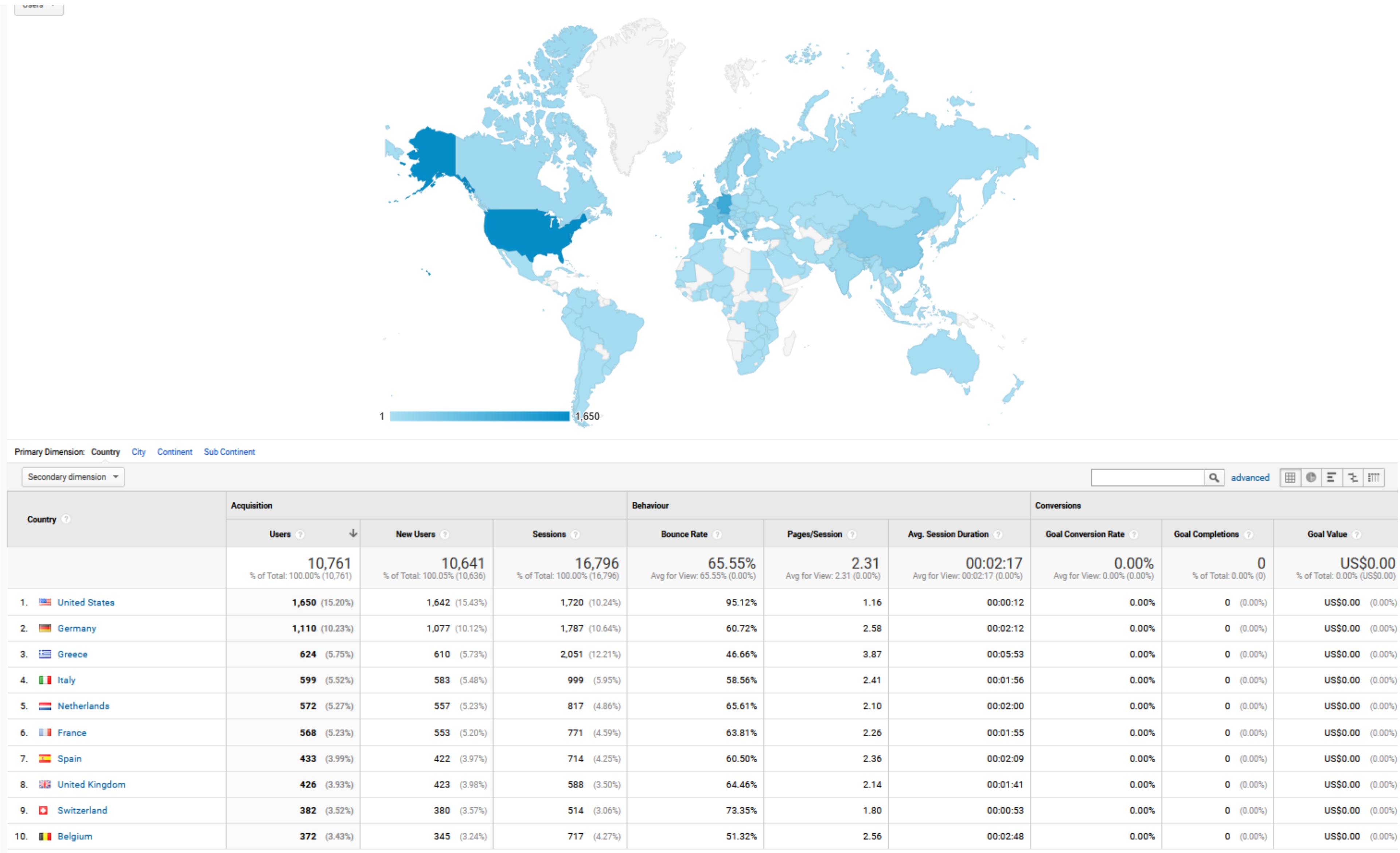
Figure 8 presents the most popular pages of the website during the reporting period. Naturally, the most visited page is the welcome page followed by the Consortium page, the service catalogue, the workshop on education page for Cybersecurity professionals and the COD2020 event page. It seems that the visitors where interested to learn more about the CONCORDIA consortium (who are they?) and what are their latest activities, news and events. Moreover, we can see that visitors are also interested in the CONCORDIA courses map and the publications produced by the consortium.

Additionally, in Figure 9 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, Netherlands, France and Spain.



	Page	Page Views	Unique Page Views	Avg. Time on Page	Entrances	Bounce Rate	% Exit	Page Value
		38,749 % of Total: 100.00% (38,749)	30,176 % of Total: 100.00% (30,176)	00:01:45 Avg for View: 00:01:45 (0.00%)	16,796 % of Total: 100.00% (16,796)	65.55% Avg for View: 65.55% (0.00%)	43.35% Avg for View: 43.35% (0.00%)	US$0.00 % of Total: 0.00% (US$0.00)
□	1. /	9,874 (25.48%)	7,500 (24.85%)	00:01:47	6,672 (39.72%)	50.00%	44.43%	US$0.00 (0.00%)
□	2. /consortium/	2,610 (6.74%)	1,862 (6.17%)	00:01:06	364 (2.17%)	61.81%	30.19%	US$0.00 (0.00%)
□	3. /concordia-service-catalog/	1,140 (2.94%)	701 (2.32%)	00:00:48	164 (0.98%)	47.56%	15.96%	US$0.00 (0.00%)
□	4. /workshops/workshop-education-2020/	1,077 (2.78%)	846 (2.80%)	00:03:46	673 (4.01%)	76.82%	67.78%	US$0.00 (0.00%)
□	5. /2020/	1,007 (2.60%)	762 (2.53%)	00:01:57	605 (3.60%)	65.79%	56.50%	US$0.00 (0.00%)
□	6. /blog/	900 (2.32%)	683 (2.26%)	00:00:51	198 (1.18%)	45.96%	24.67%	US$0.00 (0.00%)
□	7. /map-courses-cyber-professionals/	892 (2.30%)	742 (2.46%)	00:03:18	368 (2.19%)	76.09%	54.37%	US$0.00 (0.00%)
□	8. /publications/	707 (1.82%)	523 (1.73%)	00:02:12	150 (0.89%)	65.33%	35.93%	US$0.00 (0.00%)
□	9. /deliverables/	676 (1.74%)	576 (1.91%)	00:01:38	94 (0.56%)	75.53%	36.24%	US$0.00 (0.00%)
□	10. /ournews/	660 (1.70%)	508 (1.68%)	00:00:50	77 (0.46%)	54.55%	21.67%	US$0.00 (0.00%)

Figure 8: CONCORDIA pages with the most page views



Primary Dimension: Country City Continent Sub Continent

Country	Acquisition			Behaviour			Conversions		
	Users	New Users	Sessions	Bounce Rate	Pages/Session	Avg. Session Duration	Goal Conversion Rate	Goal Completions	Goal Value
	10,761 % of Total: 100.00% (10,761)	10,641 % of Total: 100.05% (10,636)	16,796 % of Total: 100.00% (16,796)	65.55% Avg for View: 65.55% (0.00%)	2.31 Avg for View: 2.31 (0.00%)	00:02:17 Avg for View: 00:02:17 (0.00%)	0.00% Avg for View: 0.00% (0.00%)	0 % of Total: 0.00% (0)	US$0.00 % of Total: 0.00% (US$0.00)
1. United States	1,650 (15.20%)	1,642 (15.43%)	1,720 (10.24%)	95.12%	1.16	00:00:12	0.00%	0 (0.00%)	US$0.00 (0.00%)
2. Germany	1,110 (10.23%)	1,077 (10.12%)	1,787 (10.64%)	60.72%	2.58	00:02:12	0.00%	0 (0.00%)	US$0.00 (0.00%)
3. Greece	624 (5.75%)	610 (5.73%)	2,051 (12.21%)	46.66%	3.87	00:05:53	0.00%	0 (0.00%)	US$0.00 (0.00%)
4. Italy	599 (5.52%)	583 (5.48%)	999 (5.95%)	58.56%	2.41	00:01:56	0.00%	0 (0.00%)	US$0.00 (0.00%)
5. Netherlands	572 (5.27%)	557 (5.23%)	817 (4.86%)	65.61%	2.10	00:02:00	0.00%	0 (0.00%)	US$0.00 (0.00%)
6. France	568 (5.23%)	553 (5.20%)	771 (4.59%)	63.81%	2.26	00:01:55	0.00%	0 (0.00%)	US$0.00 (0.00%)
7. Spain	433 (3.99%)	422 (3.97%)	714 (4.25%)	60.50%	2.36	00:02:09	0.00%	0 (0.00%)	US$0.00 (0.00%)
8. United Kingdom	426 (3.93%)	423 (3.98%)	588 (3.50%)	64.46%	2.14	00:01:41	0.00%	0 (0.00%)	US$0.00 (0.00%)
9. Switzerland	382 (3.52%)	380 (3.57%)	514 (3.06%)	73.35%	1.80	00:00:53	0.00%	0 (0.00%)	US$0.00 (0.00%)
10. Belgium	372 (3.43%)	345 (3.24%)	717 (4.27%)	51.32%	2.56	00:02:48	0.00%	0 (0.00%)	US$0.00 (0.00%)

Figure 9: Top 10 countries visiting the CONCORDIA website

3.3.2. Content marketing

During this year we changed our communication focus from publicity and brand building to production of our own unique content. The purpose is to show what we do and enhance the impact of our results. However, we did not resign from our communication goals since content production is effective way how to build reputation in organic way.

Blog posts:

We regularly deliver blog posts to our target audience. Our blog posts cover wide range of topics since they are written by CONCORDIA partners with different backgrounds in cybersecurity. While during the first year of the project were our blog post primally focused on building awareness about the project, during the second year we focus more on what we do and where are the benefits. The blog posts are intended for cybersecurity professionals in general. During this year we published 39 blog posts and we have 55 blog posts in total on our website.

Table 7: CONCORDIA Blog posts

Topic	Link
Fast, interoperable and secure mobile network made in Switzerland	https://www.concordia-h2020.eu/blog-post/fast-interoperable-and-secure-mobile-network-made-in-switzerland/
Cybersecurity threats: trends	https://www.concordia-h2020.eu/blog-post/cybersecurity-threats-trends/
Improving Quality Assurance and Situational Awareness for CONCORDIA's incident clearing house	https://www.concordia-h2020.eu/blog-post/improving-quality-assurance-and-situational-awareness-for-concordias-incident-clearing-house/
Security Playbook Automation through CONCORDIA	https://www.concordia-h2020.eu/blog-post/security-playbook-automation-through-concordia/
"Cyber Threat Intelligence": what should I share?	https://www.concordia-h2020.eu/blog-post/cyber-threat-intelligence-what-should-i-share/
CONCORDIA visiting patients at Smart Home	https://www.concordia-h2020.eu/blog-post/concordia-visiting-patients-at-smart-home/
Let's talk about Education in cyber	https://www.concordia-h2020.eu/blog-post/lets-talk-about-education-in-cyber/
First lessons learned from setting up a national anti-DDoS initiative	https://www.concordia-h2020.eu/blog-post/increasing-the-netherlands-ddos-resilience-together/
Increasing the Netherlands' DDoS resilience together	https://www.concordia-h2020.eu/blog-post/setting-up-a-national-ddos-clearing-house/

Dutch Anti-DDoS Coalition: lessons learned and the way forward	https://www.concordia-h2020.eu/blog-post/dutch-anti-ddos-coalition-lessons-learned-and-the-way-forward/
Data as an Enabler	https://www.concordia-h2020.eu/blog-post/data-as-an-enabler/
Can we trust Huawei? The need for Open Networking!	https://www.concordia-h2020.eu/blog-post/can-we-trust-huawei-the-need-for-open-networking/
Enhancing Hardware Security in IoT/Embedded Systems	https://www.concordia-h2020.eu/blog-post/enhancing-hardware-security-in-iot-embedded-systems/
Online User Tracking in Extreme Right and Left-Leaning Websites	https://www.concordia-h2020.eu/blog-post/online-user-tracking-in-extreme-right-and-left-leaning-websites/
COVID-19 crisis and cybersecurity: Transforming the threat to an opportunity	https://www.concordia-h2020.eu/blog-post/covid-19-crisis-and-cybersecurity-transforming-the-threat-to-an-opportunity/
Stay secure during Home Office	https://www.concordia-h2020.eu/blog-post/stay-secure-during-home-office/
A few words about EuroSec2020	https://www.concordia-h2020.eu/blog-post/a-few-words-about-eurosec2020/
The causal loops of online trust, user behavior and misinformation	https://www.concordia-h2020.eu/blog-post/the-causal-loops-of-online-trust-user-behavior-and-misinformation/
Cybersecurity in the financial sector: knowing your enemy	https://www.concordia-h2020.eu/blog-post/cybersecurity-in-the-financial-sector-knowing-your-enemy/
COVID-19, Telecommuting and Threat Intelligence	https://www.concordia-h2020.eu/blog-post/covid-19-telecommuting-and-threat-intelligence/
Securing Machine Learning	https://www.concordia-h2020.eu/blog-post/securing-machine-learning/
Boosting the CONCORDIA’s Cyber Security Ecosystem: Virtual Lab, Services and Training	https://www.concordia-h2020.eu/blog-post/boosting-the-concordias-cyber-security-ecosystem-virtual-lab-services-and-training/
Threat Intelligence and Operation Resilience	https://www.concordia-h2020.eu/blog-post/threat-intelligence-and-operation-resilience/
Securing the sky	https://www.concordia-h2020.eu/blog-post/securing-the-sky/
How to build a Next Generation Intrusion Detection System: Who has the answer?	https://www.concordia-h2020.eu/blog-post/how-to-build-a-next-generation-intrusion-detection-system-who-has-the-answer/
SURF’s TAO approach to Cybersecurity	https://www.concordia-h2020.eu/blog-post/surfs-tao-approach-to-cybersecurity/
Opportunistic Cyber Threats in a Time of Pandemic	https://www.concordia-h2020.eu/blog-post/opportunistic-cyber-threats-in-a-time-of-pandemic/
Preparing to fight Cyber Threats – The Human aspect	https://www.concordia-h2020.eu/blog-post/preparing-to-fight-cyber-threats-the-human-aspect/
Integration of MISP into Flowmon ADS	https://www.concordia-h2020.eu/blog-post/integration-of-misp-into-flowmon-ads/
Make Digital Work, not just Function	https://www.concordia-h2020.eu/blog-post/make-digital-work-not-just-function/
How 5G can leverage Cyber Threat Intelligence	https://www.concordia-h2020.eu/blog-post/how-5g-can-leverage-cyber-threat-intelligence/
Cybersecurity in the financial sector – part II	https://www.concordia-h2020.eu/blog-post/cybersecurity-in-the-financial-sector-part-ii/

Work in Progress: the CONCORDIA Platform for Threat Intelligence	https://www.concordia-h2020.eu/blog-post/a-concordia-platform-for-threat-intelligence/
Malware analysis: a successful cooperation between Cyber-Detect and Lorraine University	https://www.concordia-h2020.eu/blog-post/malware-analysis-a-successful-cooperation-between-cyber-detect-and-lorraine-university/
False Flags in Cyber Threat Intelligence Operations	https://www.concordia-h2020.eu/blog-post/false-flags-in-cyber-threat-intelligence-operations/
(Emerging) digital identity models and their impact on user-centric security	https://www.concordia-h2020.eu/blog-post/emerging-digital-identity-models-and-their-impact-on-user-centric-security/
Do you need a cyber range? The KYPO Cyber Range Platform is now available for free	https://www.concordia-h2020.eu/blog-post/do-you-need-a-cyber-range-the-kypo-cyber-range-platform-is-now-available-for-free/
CONCORDIA OPENED THE DOOR IN CYBERSPACE	https://www.concordia-h2020.eu/blog-post/concordia-opened-the-door-in-cyberspace/
CODE 2020: “European Digital Sovereignty – Road to Success?”	https://www.concordia-h2020.eu/blog-post/code-2020-european-digital-sovereignty-road-to-success/

<u>Videos:</u>

During this year we started with video production. We also launched CONCORDIA YouTube channel, prepared introductory animation and jingle. We produced then 19 videos this year and the overall number of views is 2 149. Most of the videos are from "CONCORDIA stories" series. Stories are short and simple videos in which CONCORDIANS describe their work and their results.

#CONCORDIACONNECTS

We are working for you even if you don't know it yet – CONCORDIA Stories

Figure 10: CONCORDIA Stories Example (https://www.youtube.com/watch?v=rIcFsW_yUbM)

We also produced animated video with the goal to simply communicate who we are and what we do. The video is focused on introduction of CONCORDIA Service Board concept.

Our mission is to lead their integration into the cyber competence network.

#cybersecurity
CONCORDIA Service Board

Figure 11: CONCORDIA Service Board video (https://www.youtube.com/watch?v=zgZa_htdv_0)

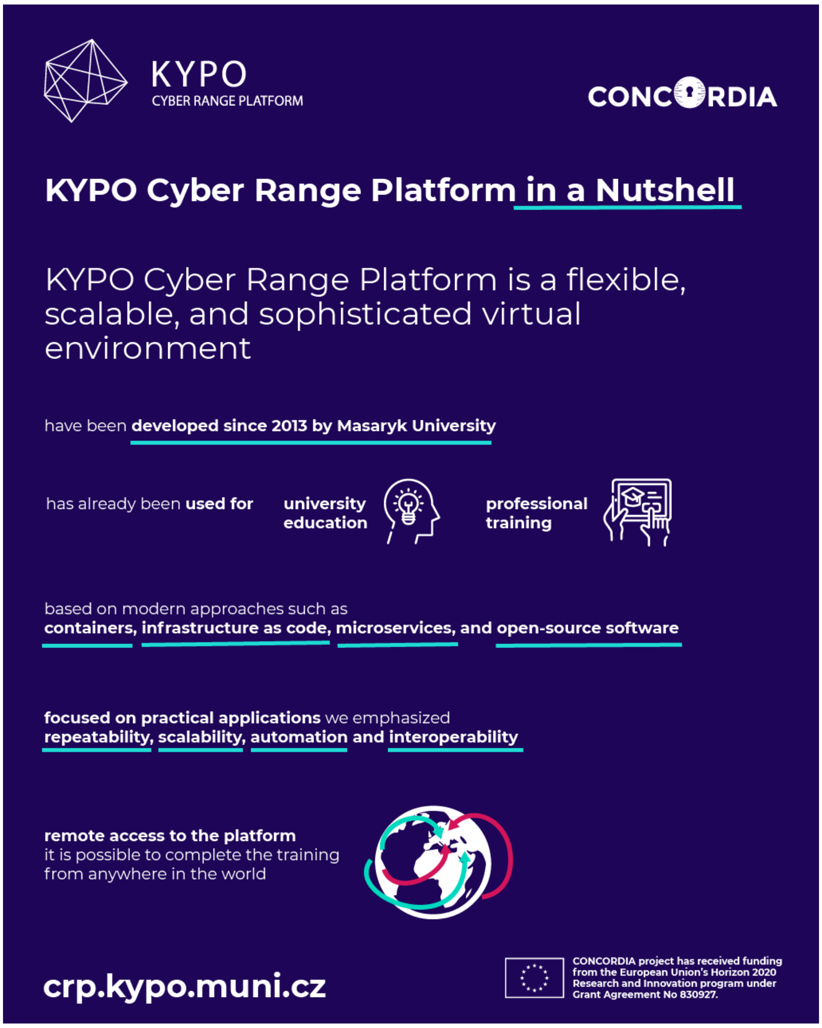
Finally, we produced a general branding video about CONCORDIA, where Gabi Dreo, the CONCORDIA project coordinator, introduces the whole project.

#CyberSecurity #H2020
CONCORDIA project – all you need to know

Figure 12: All you need to know about CONCORDIA project video (https://www.youtube.com/watch?v=5Ex1YVMVcm0)

Infographics:

We created 16 infographics during the last year. They cover various topics which are relevant for CONCORDIA project. The infographics can be found on CONCORDIA website (https://www.concordia-h2020.eu/dissemination-material/).



KYPO
CYBER RANGE PLATFORM

CONCORDIA

KYPO Cyber Range Platform in a Nutshell

KYPO Cyber Range Platform is a flexible, scalable, and sophisticated virtual environment

have been **developed since 2013 by Masaryk University**

has already been **used for** **university education** **professional training**

based on modern approaches such as
containers, infrastructure as code, microservices, and open-source software

focused on practical applications we emphasized
repeatability, scalability, automation and interoperability

remote access to the platform
it is possible to complete the training from anywhere in the world

crp.kypo.muni.cz

CONCORDIA project has received funding from the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 830927.

Figure 13: CONCORDIA infographics example

Meet CONCORDIA women:

In cooperation with task 4.5 (Women in Cybersecurity) we regularly promote women in CONCORDIA. We published 14 role model postcards during this year.

DIVERSITY BRINGS BENEFITS

"Cybersecurity is a diverse and interdisciplinary field of research. It is important to emphasize that diversity and interdisciplinarity in general make a major contribution to finding new approaches – let's replace the image of the white-haired male researcher."

#CONCORDIA**PROMOTES**

Stephanie Jakoubi

- Project Manager, Strategic Innovation & Communication at SBA
- CONCORDIA participant

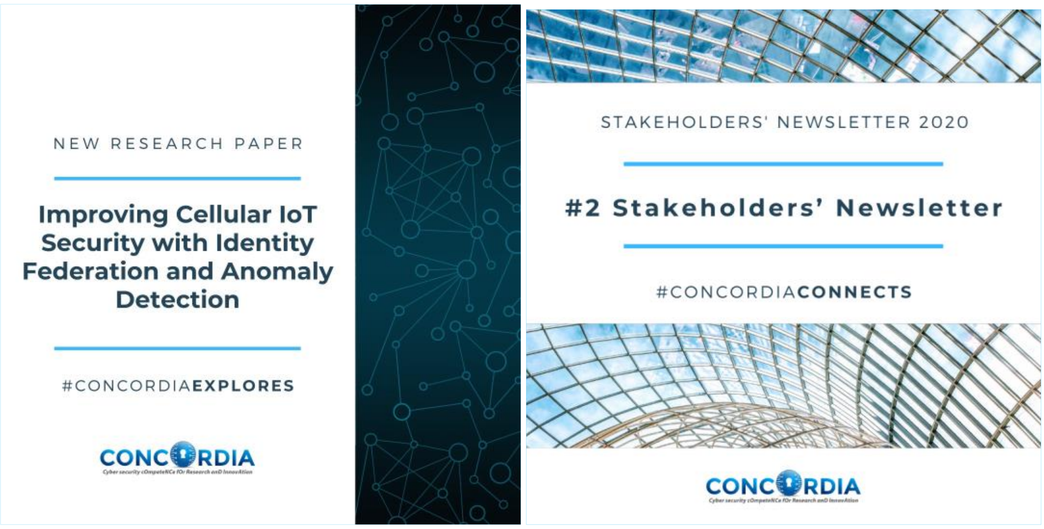
WOMEN IN CYBER

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

Figure 14: Role model postcard example

Promotional content:

We support CONCORDIA outputs by the production of promotional content. We regularly promote CONCORDIA research papers (this year we promoted 24 research papers), but we also focus on other outputs (e.g., CONCORDIA map, Service catalog or our newsletters).



NEW RESEARCH PAPER

Improving Cellular IoT Security with Identity Federation and Anomaly Detection

#CONCORDIA**EXPLORES**

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

STAKEHOLDERS' NEWSLETTER 2020

#2 Stakeholders' Newsletter

#CONCORDIA**CONNECTS**

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

Figure 15: Examples of CONCORDIA promotional content

We also started with the specific promotional activity which is focused on CONCORDIA experts. We want to show how diverse are our experts and also support networking since the project is after all about building a network. This content is then connected with the database of our experts on CONCORDIA website (https://www.concordia-h2020.eu/concordia-service-cybersecurity-experts/).

Luis Barriga

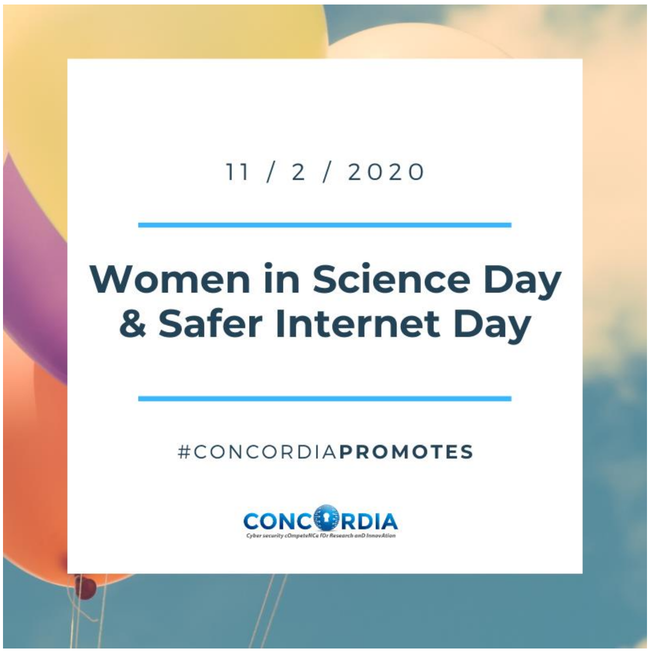
ERICSSON RESEARCH
Principal Researcher

Luis is Ericsson's delegate in CONCORDIA where his main focus is to participate in the Telco working group which designs and develops a Telco pilot showcasing the latest Threat Intelligence and Machine Learning technologies for IoT security, automated threat analysis and privacy preservation.

Figure 16: Example of CONCORDIA experts activity

Ad hoc content:

Finally, we produced various types of ad hoc content in order to raise awareness about relevant events (international days, surveys, competitions etc.). We have 15 outputs of this type during the last year.



11 / 2 / 2020

Women in Science Day & Safer Internet Day

#CONCORDIAPROMOTES

Figure 17: Example of ad hoc content output

3.3.3. Social media

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”. In this section we will provide only the report on the social media activity for the second year of the project (2020). 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. Communication group does not have access to any type of social media management software. Therefore, we are limited in reporting and analysis only to very basic tools which are offed by platforms for free.

LinkedIn:

Our LinkedIn network grew significantly during the second year of the project. It enlarged from 440 connected accounts to 1371. We have also 1443 followers on LinkedIn. We published 236 posts on our LinkedIn channel and they in total achieved 3337 likes and 132222 views. The data were obtained using the LinkedIn site for posts and activity management.

Table 8: LinkedIn activity

Months	Posts	Likes	Views
M12-M24	281	3337	132222

Twitter:

Currently, we have 1237 followers on our profile. There were 248 original posts published, which had in total 13 994 engagements and 455224 impressions. The data were obtained via Twitter Analytics.

Table 9: Twitter activity

Months	Posts	Engagements	Impressions
M12-M24	248	13 994	526524

Facebook:

Currently, we have 339 followers on our project profile. There were 269 posts published which, in total, achieved 4404 reactions and achieved a reach of 33465. The data were obtained via Facebook Insights.

Table 10: Facebook activity

Months	Posts	Reactions	Reach
M12-M24	269	4404	33465

3.3.4. Campaigns

We started with the concentrated communication activities on different topics during the second year of the project. In every campaign, we use our website, social media channels and content marketing. We also use direct mails, internal communications, media relations and cooperation with other subjects if it is relevant. The following table contains a list of our communication campaigns.

Table 11: CONCORDIA Campaigns 2020

Name	Date	Goal
Women in Cyber – A Manifesto for Today	1. 3. – 8. 3. 2020	To increase awareness about the Manifesto
CONCORDIA Service Board	22. 4. – 30. 4. 2020	To introduce CONCORDIA Service Board concept
Workshop on Education 2020	21. 5. – 3. 6. 2020	To motivate cybersecurity professionals to participate
CCN webinar on Cyber Ranges	21. 5. – 3. 6. 2020	To motivate people to participate
#CONCORDIAEDUCATES	9. 9. – 30. 9.	To attract as many relevant people as possible to CONCORDIA Education Ecosystem
CONCORDIA Open Door 2020	September – October	To motivate people to participate
Zooming-in on the Service Catalogue	October (CyberSecMonth)	To increase awareness of CONCORDIA services
KYPO Open-Source release	16. 11. – 30. 11.	To support the use of KYPO CRP
Cybersecurity & Diversity – webinar series	26. 11. – 14. 12.	To motivate people to participate

3.3.5. Events

The following table includes a list of 46 events – 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. The lower number of events is of course result of the COVID-19 pandemic. Scientific events for representation of research papers are listed in Deliverable D1.2. Communication group also cooperated on preparation on CONCORDIA Open Door event 2020. More information about this event can be found in deliverable D4.8.

Table 12: CONCORDIA Events 2020

Title	Event	Date	Place
Management in the Age of Softwarization, Artificial Intelligence, and Cybersecurity	IEEE/IFIP NOMS 2020	2020-04-23	online
Seminars on Security Testing	Seminar	Jan 4-7, 2020	Lisbon
Seminar on Cloud Threat Modelling	Seminar	Jan 28, 2020	Austria
Consistency in a Cloudy World	Seminar	Feb 3-4, 2020	US
Seminars on Threat Modelling	Seminar	Feb 10-11,2020	UK
Seminar on Security Metrics	Seminar	Feb 24-25,2020	Finland
CONCORDIA Roadmap	Meetings	Feb 28	US
Seminars on Threat Modelling	Seminar	March 2-3,2020	US
Seminars on Threat Modelling	Seminar	March 4-5,2020	US
Security Testing	Meetings	March 16-17,2020	Germany
Data Security	Seminar	April 20, 2020	UK
Decentralized Runtime Monitoring Approach Relying on the Ethereum Blockchain Infrastructure	IC2E Conference	April 21-22, 2020	Australia
Eurosys Conference	Eurosys Conference	April 28, 2020	Greece
Trace Sanitizer: Eliminating the Effects of Non-Determinism of Error Prop. Analysis	DSN Conference	Jun 28, 2020	Spain
Threat Models	Meetings	Jun 29, 2020	France
The perspective of the Cybersecurity Competence Network (4 pilots) and future collaboration opportunities	H2020: SEREN4 Cybersecurity Workshop	April 28th, 2020	Austria
Free and Open Source Software Communities Meeting	FossComm 2020	21-22 November 2020	Greece
Can Exploration and Exploitation Co-Exist in the Same Innovation Ecosystem	R&D performance management conference	26-27 Nov	Germany, Online
Smart Security	Digital Show	23 Nov 2020	Spain, Online
Startups, SMEs, and the future European Cybersecurity Competence Center and Network	COD2020	29 Oct 2020	Online
CONCORDIA Financial Sector use cases	Cybersecurity in Finance	30 Oct 2020	Online
CONCORDIA's Cross-sector Cybersecurity Infrastructure (tentative title	Cyber Competence Network Concertation Event	Dec 10, 2020	Online
Threat Intelligence in the Financial Services sector	Cyber Competence Network Concertation Event	Dec 11, 2020	Online
Financial Sector Cybersecurity and Regulatory Challenges	Workshop	Dec 14, 2020	Online

IoT security and the DDoS Clearing HouseDDoS Clearing House	INTERSCT kickoff	Oct 2020	Online
DDoS Clearing House: technical updates	Plenary Session of the Dutch Anti-DDoS Coalition	Sep 2020	Online
DDoS Clearing House: setup and updates	Dutch ISPs Plenary	Sep 2020	Online
YouTube Channel with instructions on how to run the Clearing House	How to run the Clearing House	Sep 2020	Online
Internet of Things: kansen, keerzijdes én oplossingsrichtingen (in Dutch)	SIDN webinar series	Sep 2020	Online
The DNS & the Internet of Things: Opportunities, Risks & Challenges	High Interest Plenary Session, ICANN68	Jun 2020	Online
DDoS Clearing House for Europe Cross-sector Pilot	Council of European National Top-Level Domain Registries (CENTR) Jamboree	May 2020	Online
The IoT and the DNS	ETNO Working Group Meeting	Feb 2020	Online
Increasing the Netherlands' DDoS resilience together	SURF Security and Privacy Conference, Tilburg University, Netherlands	Feb 2020	Netherlands
Privacy and Safety in Cyberspace today	Seminar in Cyprus University of Technology	July 2020	Limassol, Cyprus
Civility in Online Discourse	The Web Conference 2020	April 2020	Online
The Challenges and Opportunities in Online Safety	International Conference on Web and Social Media 2020	May 2020	Online
Privacy & Safety in the Cyberspace Today	Wayra Talks	May 2020	Online
Vulnerability Propapagtion	Meetings	27-28 July 2020	France, Germany
Dagstuhl Seminar, Software/Security Testing	Seminar	17-21 Aug 2020	Germany
Data Centric Security	Meetings	1-2 Sept 2020	UK
Threat Models	Meetings	Oct 8 2020	Germany
Software/Security Testing	Meetings	Oct 22 2020	Germany
CONCORIDA: A Cybersecurity Competence Network with leading research, technology, industrial and public compete	IFIP SEC 2020	21-23 September 2020	Slovenia
CONCORDIA H2020 booth setup and presentation	IFIP SEC 2020	21-23 September 2020	Slovenia
Women in cyber – CONCORDIA H2020 contribution	IFIP SEC 2020	21-23 September 2020	Slovenia

3.3.6. Publicity

This section describes publicity results and activities during the second year of the project. Even though that publicity is not the main goal during the dissemination phase of the project it is still important part of project communication activities.

Publicity outputs:

These communication activities helped to increase the publicity of the project. Last year we had 34 publicity outputs, as summarized in the next table.

Table 13: Publicity outputs

Publicity date	Publicity info	Type
14-11-2020	Airbus Cybersecurity brochure	Brochure
14-11-2020	Airbus Cybersecurity website entry	Website entry
10-11-2020	Europa moet ook digitaal van zich kunnen afbijten	Article
10-11-2020	Dutch MoD minister acknowledging data-centric and data-supported collaboration, engagement & digital sovereignty	Article
26-10-2020	Secretary of State of the Dutch Ministry of Economic Affairs and Climate Policy, Monica Keijzer refers to CONCORDIA	Interview
06-10-2020	Cyber Information Sharing: Building Collective Security – World Economis Forum	Report
21-09-2020	Sotiris Ioannidis: A Cybersecurity Competence Network with leading research, technology, industrial and public compete @35th International Conference on ICT Systems Security and Privacy Protection – IFIP SEC 2020	Conference Presentation
21-09-2020	Barbara Carminati: Women in cyber – CONCORDIA H2020 contribution @ 35th International Conference on ICT Systems Security and Privacy Protection – IFIP SEC 2020	Conference Presentation
11-09-2020	Gabi Dreo leitet ein europäisches IT-Forschungsprogramm	German Newspaper
31-08-2020	Universität der Bundeswehr München video.	Facebook Video
29-06-2020	Lancaster University: CONCORDIA T1.3/T4.4 discussions – Airbus, Thales	Discussions
28-06-2020	Lancaster University: CONCORDIA T1.3 DSN paper presentation	Paper Presentation
23-06-2020	The DNS and the Internet of Things: Opportunities, Risks, and Challenges	Presentation
11-06-2020	The national anti-DDoS coalition launches website	News and Blog
11-06-2020	The national anti-DDoS coalition launches website	Article
14-05-2020	Access to market in Concordia project, Cyberinvestor days	Presentation
13-05-2020	CONCORDIA: Universität Passau verstärkt europäische Cyber-Strategie	Article

28-04-2020	Lancaster University: Eurosys Conf Panel/Session	Conference
22-04-2020	SMS - Schwanke meets Science Wie die Digitalisierung unsere Sicherheit verändert	TV program
21-04-2020	Lancaster University: CONCORDIA T1.3 IC2E paper presentation	Paper Presentation
20-04-2020	Lancaster University: CONCORDIA TI discussions: GCHQ, EPSRC	Discussions
03-04-2020	Assessing the courses for Cybersecurity professionals already developed by CONCORDIA partners	Report
16-03-2020 - 17-03-2020	Lancaster University:T1.3 discussions: Deutsche Bahn, Thales	Discussions
04-03-2020 - 05-03-2020	Lancaster University: T1.3 Seminars – Microsoft, SAP	Seminars
02-03-2020 - 03-03-2020	Lancaster University: T1.3 Seminars – CMU, SMU-SEI, CMU-CERT	Seminars
28-02-2020	Lancaster University: CONCORDIA Roadmap Discussion: NIST, NSF	Discussion
24-02-2020 - 25-02-2020	Lancaster University: T1.3 Seminar: Finnish National Academy	Seminars
02-11-2020	Conservative News Sites Track You Lots More Than Left-Leaning Ones	Article
10-02-2020 - 11-02-2020	Lancaster University: T1.3 Seminars: University College London, Cambridge, BT	Seminars
07-02-2020	C. Hesselman, Increasing the Netherlands' DDoS resilience together, SURF Security and Privacy Conference, Tilburg University, Netherlands	Talk
03-02-2020 - 04-02-2020	Lancaster University: T1.3 Distinguished Seminar: Univ of Massachusetts, MIT	Seminar
28-01-2020	Lancaster University: T1.3 Seminar Austrian Institute of Technology	Seminar
13-01-2020 - 15-01-2020	Lancaster University: CONCORDIA Intl Engagement Mtg: US-NSF, US-NIST	Meeting
04-01-2020 - 07-01-2020	Lancaster University: CONCORDIA Seminars – SAP & University of Lisbon	Seminars

Cooperation activities:

The project and its activities gained a lot of publicity thanks to the support of other entities during the second year of the project. Within social media, there is regular cooperation of entities dealing with cybersecurity in Europe (especially ENISA, ECSO, Sparta, ECHO, CyberSec4Europe, Cyberwatching, CyberSane, Cyberwiser and other H2020 projects). Of course, CONCORDIA also supports the communication activities of these entities.

It is essential to emphasize our cooperation with the EC communication team. In addition to supporting social media and coordinating communication activities within the Cyber Competence communication group, it is a particularly important Cybersecurity and digital privacy newsletter. It has a large audience which is very relevant for CONCORDIA. We send inputs for this newsletter regularly.

Announcements:

This section summarizes CONCORDIA announcements (website news items, press releases etc.) during the second year of the project.

Table 14: CONCORDIA announcements

Topic	Link
Cybersecurity in High-school – a Survey	https://www.concordia-h2020.eu/news/cybersecurity-in-high-school-a-survey/
Becoming Cybersecurity Consultant	https://www.concordia-h2020.eu/news/becoming-cybersecurity-consultant/
CONCORDIA Strategic EU Cybersecurity Competence Network Project Based in Munich	https://www.concordia-h2020.eu/news/concordia-strategic-eu-cybersecurity-competence-network-project-based-in-munich/
#4 PECT-UP Newsletter 2020 (Pan-European Cybersecurity Start-Up Community)	https://www.concordia-h2020.eu/news/4-pect-up-newsletter-2020-pan-european-cybersecurity-start-up-community/
Diversity & Cybersecurity: Women Entrepreneurship Webinar	https://www.concordia-h2020.eu/news/diversity-cybersecurity-women-entrepreneurship-webinar/
Financial Sector Infrastructure Cyber-Physical Security and Regulatory Standards Workshop	https://www.concordia-h2020.eu/news/financial-sector-infrastructure-cyber-physical-security-and-regulatory-standards-workshop/
Joint Pilots CONVERGENCE event	https://www.concordia-h2020.eu/news/joint-pilots-convergence-event/
CONCORDIA releases an open-source Cyber Range platform!	https://www.concordia-h2020.eu/news/concordia-releases-an-open-source-cyber-range-platform/
KYPO Open Source – Press Release	https://www.concordia-h2020.eu/wp-content/uploads/2020/11/KYPO_CRP_Press_Release.pdf
#3 PECT-UP Newsletter 2020 (Pan-European Cybersecurity Start-Up Community)	https://www.concordia-h2020.eu/news/3-pect-up-newsletter-2020-pan-european-cybersecurity-start-up-community/
CONCORDIA Open Door Event 2020	https://www.concordia-h2020.eu/news/concordia-open-door-event-2020/
#2 Stakeholders‘ Newsletter	https://www.concordia-h2020.eu/news/2-stakeholders-newsletter/
Cybersafety workshops in school	https://www.concordia-h2020.eu/news/cybersafety-workshops-in-school/
#2 PECT-UP Newsletter 2020 (Pan-European Cybersecurity Start-Up Community)	https://www.concordia-h2020.eu/news/2-pect-up-newsletter-2020-pan-european-cybersecurity-start-up-community/
Interim Assistant Professorship	https://www.concordia-h2020.eu/news/interim-assistant-professorship/
CONCORDIA Workshop on Education for cybersecurity professionals post workshop report	https://www.concordia-h2020.eu/news/concordia-workshop-on-education-for-cybersecurity-professionals-post-workshop-report/
CCN webinar on Cyber Ranges	https://www.concordia-h2020.eu/news/ccn-webinar-on-cyber-ranges/
Threat Landscape Validation Survey	https://www.concordia-h2020.eu/news/threat-landscape-validation-join-our-new-survey/
#1 Stakeholders’ Newsletter	https://www.concordia-h2020.eu/news/1-stakeholders-newsletter/
CONCORDIA workshop on Education for Cybersecurity professionals	https://www.concordia-h2020.eu/news/workshop-education-2020/
Lessons from COVID-19: Connectivity matters in a time of crisis	https://www.concordia-h2020.eu/news/lessons-from-covid-19-connectivity-matters-in-a-time-of-crisis/

Participate in the definition of the European Cybersecurity Consultant profile	https://www.concordia-h2020.eu/news/participate-in-the-definition-of-the-european-cybersecurity-consultant-profile/
SPARTA’s 5th Podcast – Everyone matters	https://www.concordia-h2020.eu/news/spartas-5th-podcast-everyone-matters/
#1 PECT-UP Newsletter 2020 (Pan-European Cybersecurity Start-Up Community)	https://www.concordia-h2020.eu/news/1-pect-up-newsletter-2020-pan-european-cybersecurity-start-up-community/
Invitation to CYBERWISER.eu Webinar – Free Cybersecurity Training with customised Learning Paths	https://www.concordia-h2020.eu/news/invitation-to-cyberwiser-eu-webinar-free-cybersecurity-training-with-customised-learning-paths/
International Day of Women and Girls in Science	https://www.concordia-h2020.eu/news/international-day-of-women-and-girls-in-science/
PHD Candidate on path verification in future internet infrastructures	https://www.concordia-h2020.eu/news/phd-candidate-on-path-verification-in-future-internet-infrastructures/
The Industrial Systems Institute joined CONCORDIA system The Industrial Systems Institute joined CONCORDIA system	https://www.concordia-h2020.eu/news/the-industrial-systems-institute-joined-concordia-system/
Lectureship in Cyber Security x 2 posts	https://www.concordia-h2020.eu/news/view-all-vacancies-lectureship-in-cyber-security-x-2-posts/
One postdoc position available at University of Insubria-Varese, Italy	https://www.concordia-h2020.eu/news/one-postdoc-position-available-at-university-of-insubria-varese-italy/
First Review Meeting	https://www.concordia-h2020.eu/news/first-review-meeting/
Open PhD Positions at Lancaster University	https://www.concordia-h2020.eu/news/open-phd-positions-at-lancaster-university/
Open Positions at Ericsson	https://www.concordia-h2020.eu/news/open-positions-at-ericsson/

3.3.7. CCN communication activities

CONCORDIA participated in coordinated activities of Cyber Competence Network communication group (consists of CONCORDIA, ECHO, SPARTA and CyberSec4Europe). That means in particular realization of CCN communication plan which includes usage of shared social media, websites and events. We also collaborated with DG CNECT on activities such as the European Cybersecurity Month and the monthly newsletters. We met regularly (at least once a month) during whole year. Our face-to-face meeting in Lisbon was cancelled due to COVID-19 situation.

CONCORDIA specific contribution to the CCN communication activities was the preparation of CCN Webinar on Cyber Ranges which took place in June. The purpose of the webinar was to present the achievements of the four pilots — CONCORDIA, CyberSec4Europe, ECHO, and SPARTA in the domain of cyber ranges. We prepared the infrastructure for the webinar and we also led the communication campaign for the webinar, which was also supported by other pilots. The webinar was quite successful since we had 109 registered participants, 78 unique visitors and 65 visitors on average during the webinar.

Figure 18: CCN Webinar on Cyber Ranges visual style example

A significant coordinated activity was preparation of the CONVERGENCE event. The purpose of the event was to highlight to the European cybersecurity stakeholder community the progress that is being made in harnessing European expertise and resources in the broader context of the proposed legislation relating to a European Cybersecurity Industrial, Technology and Research Competence Centre and a Network of National Coordination Centres. CyberSec4Europe, SPARTA, CONCORDIA and ECHO organized a two-day concertation event which took place from 9-11 December and was hosted online with the friendly support of the Representation of the State of Hessen to the EU.

9–11 December
Online
CONVERGENCE
Making the European Cybersecurity
Competence Network a Reality

Figure 19: CONVERGENCE visual

CyberSec4Europe, CONCORDIA, SPARTA and ECHO organized a two-day concertation event which took place from 9-11 December and was hosted online with the friendly support of the Representation of the State of Hessen to the EU. Each pilot had the opportunity to demonstrate their achievements. CONCORDIA prepared a dynamic presentation with multiple speakers for its section. I addition we participated in the program of several focus groups, in specific: Communications, Education, Governance, Roadmapping and Threat intelligence in the financial sector.

The chair of the CCN communication group is held by one of the pilots, rotating every six months. The first six month of 2021 will be the group chaired by CONCORDIA. We will aim to maintain the level of coordinated communications and work on the group strategic objectives.

3.3.8. Visual identity

During the second year of the project, we made several iterations of current templates and visuals. We also create many new visual outputs in order to support CONCORDIA activities during the second year of the project. Usually we prepare banners, headers, apply our logo, icons, etc. – these are small, but necessary applications. Specifically, we would like to mention two applications of our visual identity. First one is creation and application of CONCORDIA Service Board Concept and the second is creation of visuals for the CONCORDIA Open Door 2020 event. The CONCORDIA Service Board is a concept that reacts to the complexity of the CONCORDIA project. It was really hard to describe briefly what we do since the scope of the project is wide.

The visual representation of the CONCORDIA Service Board allowed us to simplify the entire answer into one image. The creative process was performed in close cooperation with the management board of the project. In addition, 8 defined categories are further used on our website and also on other channels. Although the categories may change during the project, the visual representation will remain because it is a very effective way of how we can communicate what we do.

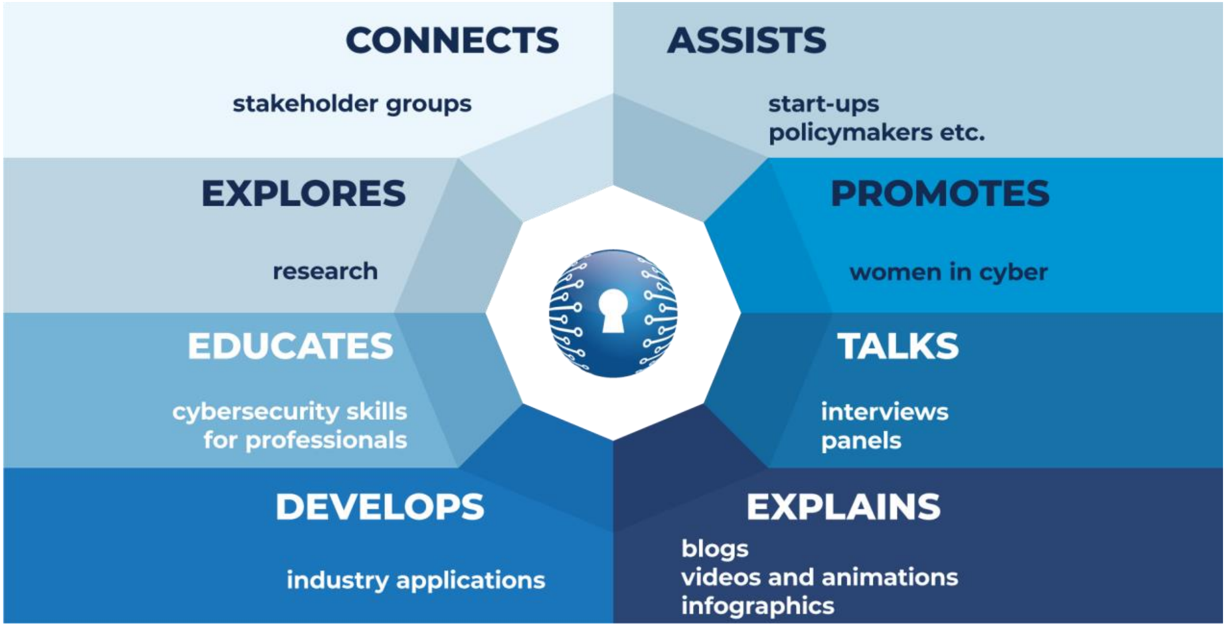
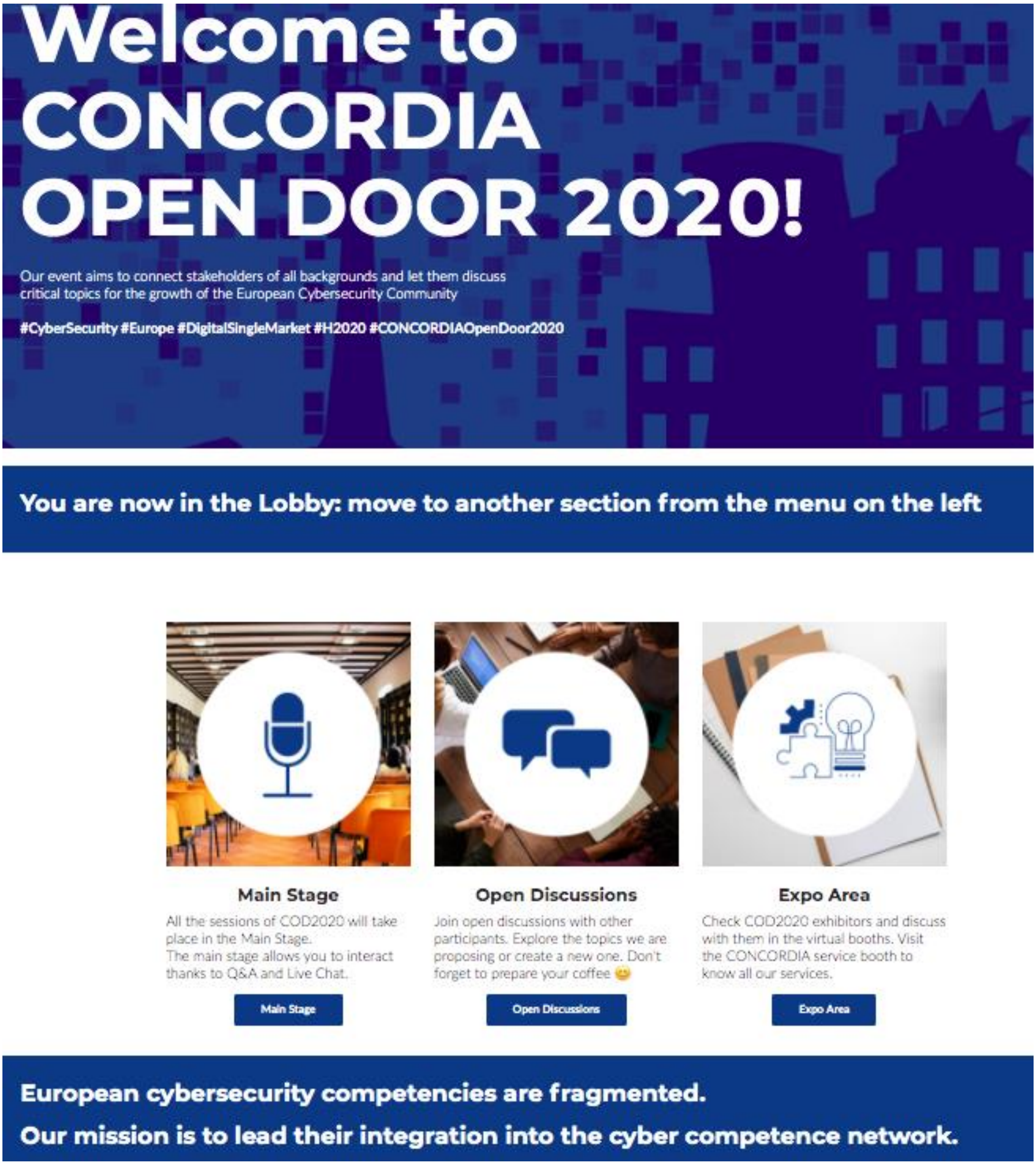


Figure 20: CONCORDIA Service Board concept



Welcome to CONCORDIA OPEN DOOR 2020!

Our event aims to connect stakeholders of all backgrounds and let them discuss critical topics for the growth of the European Cybersecurity Community

#CyberSecurity #Europe #DigitalSingleMarket #H2020 #CONCORDIAOpenDoor2020

You are now in the Lobby: move to another section from the menu on the left

Main Stage

All the sessions of COD2020 will take place in the Main Stage.
The main stage allows you to interact thanks to Q&A and Live Chat.

Open Discussions

Join open discussions with other participants. Explore the topics we are proposing or create a new one. Don't forget to prepare your coffee 😊

Expo Area

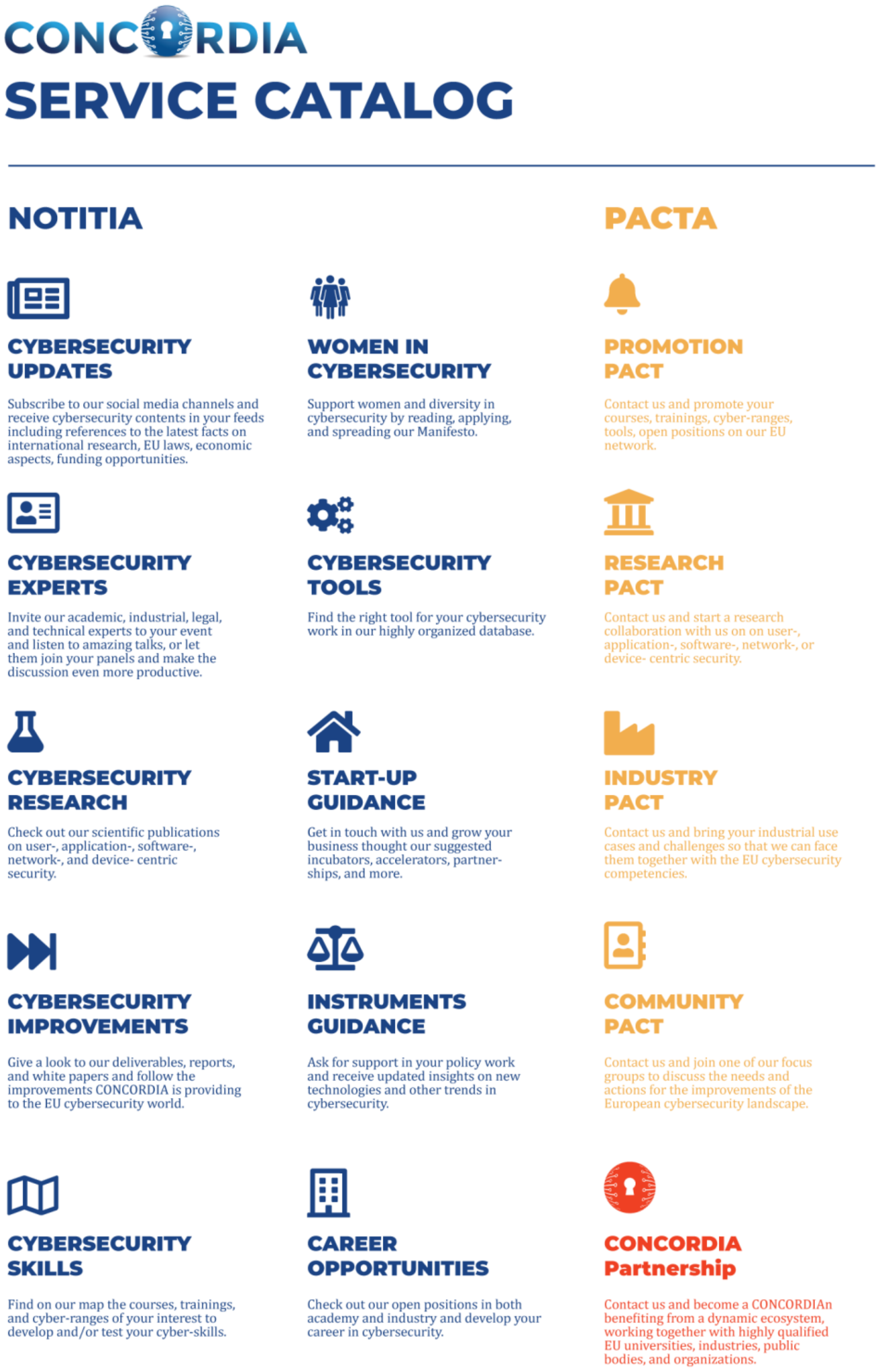
Check COD2020 exhibitors and discuss with them in the virtual booths. Visit the CONCORDIA service booth to know all our services.

European cybersecurity competencies are fragmented.
Our mission is to lead their integration into the cyber competence network.

Figure 21: Part of the CONCORDIA Open Door 2020 website

3.3.9. Offline activities

Offline activities were influenced by COVID-19 situation since usage of printed materials is usually connected with the events participation. However, we prepared a graphics for banner focused on CONCORDIA Service Catalog.



CONCORDIA
SERVICE CATALOG

NOTITIA

CYBERSECURITY UPDATES

Subscribe to our social media channels and receive cybersecurity contents in your feeds including references to the latest facts on international research, EU laws, economic aspects, funding opportunities.

CYBERSECURITY EXPERTS

Invite our academic, industrial, legal, and technical experts to your event and listen to amazing talks, or let them join your panels and make the discussion even more productive.

CYBERSECURITY RESEARCH

Check out our scientific publications on user-, application-, software-, network-, and device- centric security.

CYBERSECURITY IMPROVEMENTS

Give a look to our deliverables, reports, and white papers and follow the improvements CONCORDIA is providing to the EU cybersecurity world.

CYBERSECURITY SKILLS

Find on our map the courses, trainings, and cyber-ranges of your interest to develop and/or test your cyber-skills.

WOMEN IN CYBERSECURITY

Support women and diversity in cybersecurity by reading, applying, and spreading our Manifesto.

CYBERSECURITY TOOLS

Find the right tool for your cybersecurity work in our highly organized database.

START-UP GUIDANCE

Get in touch with us and grow your business thought our suggested incubators, accelerators, partner-ships, and more.

INSTRUMENTS GUIDANCE

Ask for support in your policy work and receive updated insights on new technologies and other trends in cybersecurity.

CAREER OPPORTUNITIES

Check out our open positions in both academy and industry and develop your career in cybersecurity.

PACTA

PROMOTION PACT

Contact us and promote your courses, trainings, cyber-ranges, tools, open positions on our EU network.

RESEARCH PACT

Contact us and start a research collaboration with us on on user-, application-, software-, network-, or device- centric security.

INDUSTRY PACT

Contact us and bring your industrial use cases and challenges so that we can face them together with the EU cybersecurity competencies.

COMMUNITY PACT

Contact us and join one of our focus groups to discuss the needs and actions for the improvements of the European cybersecurity landscape.

CONCORDIA Partnership

Contact us and become a CONCORDIAn benefiting from a dynamic ecosystem, working together with highly qualified EU universities, industries, public bodies, and organizations.

Figure 22: Graphics for CONCORDIA Service Catalog banner

3.3.10. Internal communication

Communication group was also focused on internal communication during the second year of the project. We regularly share any important news with the consortium and we also build a "CONCORDIA Months" website in Confluence in order to provide centralized source information about our communication outputs which can be then used in activities by task leaders (e.g., as an input for newsletters).

We also provide instructions to make our communication consistent. During the last year we produced updated version of “CONCORDIA’s communication cheat sheet” – a simple internal document which purpose is to equip all members of the consortium with the necessary knowledge about our communication strategy and their involvement into communication activities. We also produced a manual for preparing CONCORDIA stories videos. Internal communication activities are also performed in cooperation with task 6.1 (more information is available in deliverable D6.5).

3.3.11. Dissemination and communication activities performed by other tasks

It is important to highlight that activities which were reported in previous paragraphs are not the only communication and dissemination activities performed by the CONCORDIA project. Communication group (T5.2) leads the communication and dissemination and it is responsible for its coordination and planning. Below table that provides an overview of the dissemination and communication activities of other project tasks. All tasks cooperate with the communication group. We only list dissemination communication activities which use formal channels in the following table.

Table 15: Dissemination and communication in consortium

Task	Activity
WP1 tasks	Produce scientific papers and deal with dissemination to the scientific community. More information is available in Work Package 1 in Deliverable D1.2.
T3.5	Deals with communication activities targeted to start-ups. It creates a community mailing list, produces his own newsletter.
T4.5	Focuses on communication activities related to workforce diversity. It produces various types of content, including webinars. Communication group closely cooperates with the task 4.5. More information is available in Deliverable D4.5.
T4.6	Deals with communication activities targeted to CONCORDIA stakeholders. Among other things, it creates a community mailing list, produces his own newsletter and organizes the CONCORDIA Open Door Event. More information is avaible in Deliverable D4.8.
T6.1	Deals with governance of the project which is connected with the internal communication activities. More information is avaible in Deliverable D6.5.

3.4. Impact from COVID-19

The impact of a pandemic on CONCORDIA dissemination and communication can be assessed in three ways.

Firstly, the pandemic affected or even interrupted the work of several CONCORDIA teams, either academic or industrial, and reduced or even stopped their technical progress (as it is explained in the corresponding deliverables due in M24). Technical and scientific achievements of the project are an important input for the communication group (see Table 6 – CONCORDIA content) therefore dissemination and communication activities which should boost some project results are rescheduled to the next year of the project.

Secondly, the pandemic also influenced the usage of our communication tactics. It is obvious that events opportunities were significantly reduced during this year. This also means that there was no demand for offline communication materials. However, the demand moved to digital activities which were even more important for us. This was also demonstrated by the organization of CONCORDIA main event –CONCORDIA Open Door 2020 which took place virtually. Communication group significantly supported this activity which was led by tasks T4.6 (more information can be found in the deliverable D4.8).

Finally, the pandemic situation was also an opportunity for discussing the importance of cybersecurity. We supported communication activities performed by ENISA and the European Commission which deal with the relation of pandemic and cybersecurity. In addition, we also produced several blog posts which were focused on this topic.

3.5. Next Steps on Dissemination and Communication

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 second 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 goals of the project. The purpose of communication and dissemination will always be to boost the impact of CONCORDIA project.

Our plans for the next year are evident from the communication phases of the project (described in in Table 3). We are currently in the dissemination phase of the project which focuses primarily on sharing project results and increasing their impact. We expect that more significant output will be produced during the third year of the project. Our aim is to support these outputs with performance communication campaigns which will use all relevant channels, demonstrate added value and influence concrete actions. The communication tactics which will be more relevant are media relations and webinars. We will also chair the CCN communication group for the first six months of 2021 where we will aim to maintain the level of coordinated communications and work on its strategic objectives. However, in addition to the plans, we remain ready to use all the opportunities that we have in this area to support our dissemination and communication 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.

Finally, Section 4.5 contains information regarding the next steps that will be undertaken for the Certification and Standardization task of the project.

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.

Cross-pilot collaboration on certification

"All EU CCN pilot projects share many common focus areas and there is a risk that much work is being duplicated by them"[7]. One of these common focus areas is certification and standardization.

Although an overall plan is not yet completed but several collaboration activities have been put in place, individual activities for collaboration have started.

Initial exploratory discussions were conducted within the activities of the Cyber Competence network Group for Education. These discussions revealed a cooperation potential between two pilots: CONCORDIA and CyberSec4Europe.

More specifically, CyberSec4Europe has created a list of quality assurance criteria for MOOCs with an emphasis on Cybersecurity whereas CONCORDIA has already implemented a certification scheme for Cybersecurity Skills and is in the process of finalizing a Cybersecurity Certification Framework.

Taking these into consideration, the two projects have decided to collaborate in order to implement the following actions:

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

[7] JRC Technical Report, Summary of Recommendations and Guidelines for the Competence Network Pilot Projects, 2020

Action 1: Conduct Survey on refined requirements for a Certification Scheme for the MOOC and Cyber ranges needed in Education and Training. [until 12.2020]

Action 2: Based on the results of the surveys, decisions regarding the implementation of a joined scheme certification will be taken. [during 12.2020]

Action 3: Design and implement advanced Certification Schemes. [until 07.2021]

At the time of the implementation of this report, action 1 is in progress. Specifically, a survey with the subject “Cybersecurity MOOCs certification survey” has been created and is expected to be published during the second week of December 2020.

Making Certification more proactive

During the 2nd review of the CONCORDIA project, it was pointed out that “Certification and standardization is key but can be tricky in fast-developing sector. So, the recommendations of the project for a more granular approach (such as maturity models or best practice) that accounts for fast developments, would be particularly useful.”

To address this comment, the Certification and Standardization Stakeholder group function is currently being redesigned in order to act as a catalyst to the relevant task. More specifically, the project team is designing a way to incorporate more stakeholders in order to gain more feedback and connection to the certification market.

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.”[8]
- **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 [9].

Considering the above definitions, for the CONCORDIA project, some of the types of documents referred to as Standards are [10]:

- **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.

[8] 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

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

[10] 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

- **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. [11] 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.[12]
- **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.[13]

Data Collection:

The effort regarding the collection of data on standardization efforts relevant to the CONCORDIA project has started from the previous year and is in progress. More specifically, as described in the 1st year report on exploitation, dissemination, certification and standardization, a survey was conducted involving all partners in order to collect the following information, per Work Package, per Task and per Partner:

- 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.

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

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

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

This survey was conducted again this year and the related results are included in Section 4.3.2.

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 overall activities that are planned to be implemented are depicted below along with their respective status:

- **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. The document contains an analysis of the market situation, of the available skills frameworks and concludes with the identification of possible gaps in Cybersecurity Skills Certification Schemes. The document of the feasibility study has been published in the CONCORDIA website: https://www.concordia-h2020.eu/wp-content/uploads/2020/06/CONCORDIA-SkillsFeasibilityStudy-forpublication.pdf.
- **Select a Cybersecurity Skills Certification Scheme for implementation**: The feasibility study mentioned above revealed gaps in Cybersecurity Skills Certification Schemes. Moreover, the project team conducted an online survey, to retrieve the opinion of the CONCORDIA partners regarding their implementation preference. The results of these two actions led the project team to select the role of the Cybersecurity Consultant. The Role Profile of the Cybersecurity Consultant had not been formulated before. To create the role profile, an analysis of existing guidance and a specialized workshop was conducted (https://www.concordia-h2020.eu/news/participate-in-the-definition-of-the-european-cybersecurity-consultant-profile/). The combined results of these actions produced a document called "Cybersecurity Consultant Role Profile" which is currently in its final stages of implementation.
- **Create Supporting material for the implementation of the Scheme**: A certification scheme for skills, based on the international best practices of ISO 17024, comprises of the following documents: The certification scheme, the examination databank, a code of conduct for the certified professionals and various templates of required documents e.g. certificate, affirmation etc. At the point that this report is being drafted, the certification scheme is at the final stages of implementation and the examination databank for the theoretical part of the assessment is underway.
- **Create a Certification Framework**: The purpose of the Certification Framework is to define the rules under which the Certification Scheme will operate. The Certification Framework will contain the best practices regarding certification in the area of Cybersecurity based on the knowledge and experience of the CONCORDIA partners. The final version of the Certification Framework will be issued after the evaluation of the results of the pilot certification scheme (Cybersecurity Consultant).

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 and inform accordingly the partners of the CONCORDIA project. This activity was carried out in the beginning of the project (and the results were included in the previous yearly report) and was repeated this year (and the results are included within this report).

Number of identified:

- Standards Developing Organizations: 31
- Standards: 368
- Standards in preparatory stages (Draft, Pending, etc): 57

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 Appendix A.

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.

The total number of subjects found was 98 (increased from the respective number of last year - 64).
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 396 entries (last year's respective value was 295). A table containing the Standards Developing Organizations and the number of identified standards is contained in Appendix A.

Number of identified:

- Standards Developing Organizations: 37
- Standards: 396
- Standards in preparatory stages (Draft, Pending, etc): 61

Furthermore, in some cases, assistance in the identification of related standardization efforts was requested by the respective CONCORDIA partners from the Standardization task leader.
For all the areas where assistance was requested, a research was conducted and where possible suitable standards were identified, and the partners were notified.
Moreover, to further structure the standards related information for all partners, an analysis was conducted on the identified standards, and categories (related also to the key topics mentioned above) were assigned.

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

Table 16: Standardization efforts that CONCORDIA partners are participating.

Standardization Organization	Title of committee or standard	Type of participation
3GPP	SA3	Participation in its security activity
CEN/CENELEC CWA	Workshop on "Requirements and Recommendations for Assurance in Cloud Security (RACS)".	Contributor
Cloud Security Alliance financial Sector WG		
CORD	OpenCORD	Member of the Technical Steering Team for CORD
DKE AK 351.0.6	IT-Sicherheit im Bahnsystem	member
DKE AK 351.3.7	Security Anforderungen an signaltechnische Einrichtungen	member
ENISA's Financial experts Working Group		
ESBG Cloud Certification Working Group		
ETSI	Cloud Standard Coordination	Contributor
ETSI	NFV ISG	Chair
ETSI	Smart Card Platform	Participant

ETSI	TC CYBER	Contributions to the TC
ETSI	TC CYBER	Observer
ETSI	WG: SEC	Participation
FI-ISAC		
GSMA	Fraud and security Architecture Group	Contributor
IETF	6TiSCH WG - Robust Scheduling against Selective Jamming in 6TiSCH Networks	Author
IETF	6TISCH Working Group RFC draft Zero - Touch Secure Join Connect, 6TiSCH secure minimal architecture	Observer
IETF	ACE WG - Additional OAuth Parameters for Authorization in Constrained Environments (ACE)	Author
IETF	ACE WG - Authentication and Authorization for Constrained Environments (ACE) using Oauth 2.0 Framework (ACE-OAuth)	Author
IETF	ACE WG - CBOR Profile of X.509 Certificates	Author
IETF	ACE WG - Datagram Transport Layer Security(DTLS) Profile for Authentication and Authorization for Constrained Environments (ACE)	Author
IETF	ACE WG - EST over secure COaP (EST-coaps)	Author
IETF	ACE WG - Key Management for OSCORE Groups in ACE	Author
IETF	ACE WG - Key Provisioning for Group Communication using ACE	Author
IETF	ACE WG - OSCORE profile of the Authentication and Authorization for Constrained Environments Framework	Author
IETF	ACE WG - Proof-of-Prossession Key Semantics for CBOR Web Tokens (CWTs)	Author
IETF	ACE WG - Protecting EST payloads with OSCORE	Author
IETF	CoRE WG - Discovery of OSCORE Groups with the CoRE Resource Directory	Author
IETF	CoRE WG - Group Communication for the Constrained Application Protocol (CoAP)	Author
IETF	CoRE WG - Group OSCORE - Secure Group Communication for CoAP	Author
IETF	CoRE WG - Object Security for Constrained RESTful Environments (OSCORE)	Author
IETF	DNSOP WG	Contributor
IETF	NETCONF/YANG	contributing to WG documents
IETF	Network Working Group - ACE Clients in Disadvantaged Networks	Author
IETF	RATS	contribution to WG discussions

IETF	RFC 7744	Author
IETF	SUIT	following WG progress
IETF	TEEP	following WG progress
IETF	WG: TEEP, PANIC, I2NSF	Participation
IRTF	Extending IP Flow-Based Network Monitoring with Location Information	Co-Author
IRTF	Network Management Research Group NMRG	Chair
ISO/IEC	ISO/IEC JTC 1/SC 42 - Artificial intelligence - ISO	Contributor
NGMN	Security Competence Team	Observer
OASIS	CACAO TC	Member
OASIS	eXtensible Access Control Markup Language (XACML)	Contributor
OASIS	OpenC2 TC	Member
OASIS	STIX	Member
OASIS Open (oasis-open.org)	Collaborative Automated Course of Action Operations (CACAO) for Cyber Security TC	Secretary
OASIS Open (oasis-open.org)	Open Command and Control (OpenC2) TC	Voting Member
Open Daylight (ODL)	open-source SDN framework	Contibutor, member of the Advisory Board
OSM	Open Source MANO	TID leads this open source community, which provides a practical implementation of the reference architecture for NFV Management & Orchestration
Payment Security Support Group and Card Fraud Prevention (EPC)		

4.4. Impact from Covid-19

The activities and objectives of the standardization and certification task have not been influenced by the COVID-19 pandemic. The related meetings and workshops were carried out remotely within the predetermined timeframes.

4.5. Next Steps in Certification and Standardization

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

Certification

- Finalization of the design of the Certification Stakeholder Group
- Initiation and operation of the Certification Stakeholder Group
- Implementation of the Certification scheme of the Cybersecurity Consultant (pilot phase) – Impelementation of the relevant exams and issue of the first related certificates
- Review of the results of the pilot phase and finalization of the CONCORDIA Skills Certification Framework.

- Review the results of the Survey on MOOCs and MOOC Certification implemented in collaboration with CyberSec4Europe and decide on the next implementation steps.
- Investigate further activities aligned with the EU CSA and related to the activities depicted within the Roadmap.

Standardization

- Support the CONCORDIA partners in their needs regarding standardization
- Investigate the areas proposed during the last communications with the partners on the subject (feedback of October 2020)
- Investigate further actions and synergies regarding standardization

5. Conclusions

CONCORDIA project has defined in its main activities the Work Package 5 (WP5), whose purpose is to boost the impact of the project through strategic activities in exploitation, dissemination, and standardization.

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 second year of the project.

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

- Efforts on Exploitation (Section 2):
    - 26 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
    - 30 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):
    - 10 761 users visited the CONCORDIA website from around the world during the first year of the project.
    - 39 blog posts published on CONCORDIA website or in prominent technology websites, written by CONCORDIA partners explaining technology they built, their services offered, etc.
    - 19 videos about our work, especially focused on demonstrating the value.
    - 16 infographics to which covers various project outputs and lots of other different form of content.
    - 46 events / conferences / invited talks / seminars held or attended by the consortium partners and its members.
    - 248 Twitter posts / 269 Facebook posts / 281 LinkedIn posts.
    - 21700+ of total engagements across social media platforms.
    - 9 communication campaigns focused on different topics.
    - 34 announcements posted on the CONCORDIA website.
    - 36 news and other web articles published providing high publicity to the project’s activities.
    - Cooperation with other subjects and active participation in CCN communication group.
- Efforts on Certification and Standardization (Section 4)
    - 37 Standards Developing Organizations have been identified from the consortium partners as organizations developing standards that are relevant to the work performed within the CONCORDIA project.
    - 396 standards to be studied from the consortium partners for their relevance in their activities in the cyber security sector.
    - CONCORDIA partners have declared that they participate in the activities of 18 Standards Developing Organizations and Stakeholder Groups

  - CONCORDIA partners have declared that they participate in 48 activities of these organizations or groups

Conclusion & Future Plans:

All objectives set in the project's WP5 have been so far achieved or exceeded even despite of the impact of COVID-19. 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, communicating and disseminating to its target audiences, as well as helping its partners have impact on standardization in cybersecurity.

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. Overall, CONCORDIA is committed to strong exploitation of all results that are exploitable from its industrial and academic partners. As already identified by the innovation and exploitation managers of the project, for this to happen, the consortium needs to dedicate resources and attention to its partners that need help with identifying novel pieces of technology that they built and how they can patent them (if needed), defining appropriate and profitable business models that will allow them to hit the market in the upcoming years of the project and beyond, reaching out to venues and entities that can help said technology to hit the market, and of course, exposing CONCORDIA's key stakeholders to our novel and innovative technology.

CONCORDIA communication and dissemination activities will be focused on sharing project results and increasing their impact. Although CONCORDIA is a fairly large consortium dealing with a number of areas of the cybersecurity domain, its communications team is relatively small and has no additional resources to use external services (in comparison to what is standard in communication services). This means that the available resources of time and energy must be invested in communication and dissemination activities that will have the greatest possible impact in terms of project objectives. Only such activities are really strategic.

We expect that more significant output will be produced during the third year of the project. From the point of view of communication, these outputs will be crucial for us, as they will enable us to demonstrate clearly the value which we bring to the cybersecurity community. The position of thought leadership cannot be achieved only by branding activities. It must be underpinned by real "hard outputs" that bring value. Our aim is to support these outputs with performance communication campaigns which will use all relevant channels, demonstrate added value and influence concrete actions.

Regarding certification and standardization, the following can be further mentioned:

The project team is already implementing various steps regarding certification and standardization. (Information has already been provided in the previous sections). At the same time, considerable work and collaboration has taken place in these specific subjects but from the viewpoint of the Cybersecurity Roadmap for Europe (Deliverable D 4.4). Standards play a paramount role in the dispersion of knowledge, in innovation, development as well as in sustainability. Certification is a powerful tool that builds on an agreed basis (provided through standardization) and provides for transparency, comparability, consumer protection and cross border acceptance and circulation of products, processes and services. Within the Cybersecurity Roadmap for Europe, specific actions regarding standardization and certification are proposed taking into consideration the relevant context (the EU CSA, the existing policies and plans, the NIS etc).

Although at this time, Deliverable D 4.4 is in a draft state and is expected to be finalized with the project completion, it is the plan of the project team to review the proposed actions and collaborate with the CONCORDIA partners in order to produce (where possible) some initial recommendations.

Especially for the certification efforts, the proposals regarding the subject as depicted within the Cybersecurity Roadmap for Europe, will be reviewed along with the Certification Stakeholder Group, in order to get valuable feedback and validation. (As mentioned previously, the Certification Stakeholder Group is planned to operate within 2021).

At the same time, the collaboration efforts with the various partners will continue, in order to produce tangible and needed results in the areas of Standardization and Certification.

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
WP	Work package

Appendix A

As described in Section 4 regarding standardization, the topics researched or dealt with within CONCORDIA, were collected. These topics were used as a starting point for the research of relevant Standards.

The key topics identified based on the inputs from CONCORDIA partners are depicted in the following table:

Table 17: Key topics and areas dealt with within the CONCORDIA project

Business / Project related topics
Accelerators
Attestation
Business plan
Cybersecurity roadmap
Exploitation strategy
Incubators
Ipr
Know your customer
Knowledge management
Start-ups
Tech-transfer
Sector specific - Health
E-health
Medical devices
IOT
Firmware updates (IoT)
Full stack IoT security
Generic PKI for IoT
IoT devices
IoT security
Secure zero touch deployment of industrial IoT devices in low-power lossy network (LLN)
Smart home
Software security for IoT
Machine Learning
Deep learning
Information sharing (federated machine learning over a common model)
Machine learning techniques for learning utility of data of users
Machine learning techniques for protection
Privacy
Anonymity of data
Monitoring and analysis of encrypted traffic preserving user privacy
Personal data leakage detection
Privacy and data protection
Security-by-design and privacy preservation (anonymization)
Risk
Hardware security assessment

Vulnerabilities

Technical Implementation Controls

Client identification and authentication (physically and virtually)
Cryptography primitives and cryptography operation in embedded system environment
Device security based on TrustZone
End-to-end security architecture for 5g-controlled drone
Hardware security
Hardware security tokens
Identity management
Identity related information discovery
Network device configuration
Secure communication
Tactical ad hoc networks
Tactical software defined networks
Trusted execution environment for ARM Cortex M3
Trusted execution environments

Cyber Threats

Cyber threat analysis
Cyber threat assessment
Cyber threat intelligence
Cyber threat intelligence platform (for cybersecurity technical IOC and financial IOC)
Cyber threat landscape
Cyber threat reporting
Cyber threat training models
Cyber threat visualization
Cyber threat/intrusion detection system - AI based
Data-centric threat Modelling
Detection of indicators of compromise in telco environment
Development of intel sharing platform
Emerging threats
Honeypots
Metrics for situational awareness based on sharing platform data
Sharing of infected and vulnerable systems with owners of systems

Table 18: Number of Standards per SDO after the CONCORDIA partners provided their contribution for 2020

Standards Developing Organization	Number of Identified Standards
ACDC project (www.acdc-project.eu)	1
Alliance for Telecommunication Industry Solutions	2
ANSI	3
APTA	1
ASTM	3
CENELEC	1
CSA	1
csrc.nist.gov	61
DIN	1
Ecma	1
ETSI	33
https://cybersecurity.ieee.org/center-for-secure-design/	5
https://www.openchargealliance.org	1
IEC	1
IEEE	17
IETF	31
International Association of Drilling Contractors	2
International Telecommunication Union-T	3
ISA	1
ITU	9
MITRE	2
NASA	1
NATO Cooperative Cyber Defence Centre of Excellence (ccdcoe.org)	2
Naval Aviation	2
NEMA	1
psacertified.org	1
SAE	2
UL	9
w3.siemens.com	1
www.fda.gov	11
www.iec.ch	43
www.isa.org	6
www.iso.org	51
www.nccoe.nist.gov	61
www.nerc.com	17
www.oasis-open.org	7
X-arf community (xarf.org)	1
Total	396