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 4: Policy and the European dimension Deliverable D4.7: Year 1 report on the liaison with stakeholders

Abstract: The purpose of this deliverable is to show the progress toward the objectives of task 4.6 (*T4.6 - Liaison with Stakeholders*) performed by CONCORDIA during the first year of the project. The stakeholder engagement strategy is first described followed by the explanation of the strategy implementation activities. In particular, the methodology used to create the first dataset of CONCORDIA's stakeholders is presented and exploited to identify the entities involved and their needs. The CONCORDIA service catalog is defined as the main access point for external stakeholders to engage with CONCORDIA and is extensively described. Finally, selected success stories of the first year of the project are presented, such as the extension of the original consortium with new CONCORDIA partners, the first CONCORDIA Open Door event, and some preliminary outcomes of task 4.5 (*Women in Cybersecurity*) activities.

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

Contractual Date of Delivery	*M12*
Actual Date of Delivery	*Actual Date*
Deliverable Dissemination Level	Public
Editors	Antonio Ken Iannillo (SnT) Barbara Carminati (UI) Felicia Cutas (EIT DIGITAL) Olivier Festor (UL) Thibault Cholez (UL)
Contributors	All CONCORDIA's partners
Quality Assurance	Argyro Chatzopoulou (TUVA) Daniela Friedl (SBA) Luis Barriga (Ericsson) Radu State (SnT)

The CONCORDIA Consortium

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

ISI	ATHINA-ISI	Greece
UNI PASSAU	University of Passau	Germany
RUB	Ruhr University Bochum	Germany

Document Revisions & Quality Assurance

Internal Reviewers

1. Argyro Chatzopoulou (TUVA)
2. Daniela Friedl (SBA)
3. Luis Barriga (Ericsson)
4. Radu State (SnT)

Revisions

Ver.	Date	By	Overview
0.01	3/12/2019	*Thibault Cholez (UL)*	First consolidated version for internal review
0.02	8/12/2019	*Radu State (SnT)*	Document revised
0.03	12/12/2019	*Antonio Ken Iannillo (SnT)*	New structure and changes on contents
0.04	13/12/2019	*Thibault Cholez (UL)*	Rev1 taking into account all comments from the 1st round of internal review
0.05	22/12/2019	*Thibault Cholez (UL)*	Rev2 taking into account all comments from the 2cd round of internal review

Executive summary

Work package 4 (WP4) is named *Policy and the European Dimension* and it is led by EIT Digital. WP4 creates working groups in the research domains of CONCORDIA and establishes liaisons with the relevant European stakeholders to develop and implement a cybersecurity roadmap for Europe. In the frame of WP4, task 4.6 (T4.6) *Liaison with stakeholders* is led by SnT, University of Luxembourg.

T4.6's main objective is to establish liaisons and collaborate closely with the relevant European stakeholders in order to achieve the following goals: (1) the continuity of CONCORDIA's results (by disseminating them to the key players in Europe in the domain of cybersecurity); and (2) the collection and integration of concrete feedback linked to various activities performed under the project. The output of this task is reported in deliverable 4.7 (D4.7) *Year 1 report on the liaison with stakeholders*.

In this first year of CONCORDIA, T4.6 identified and analyzed a first set of stakeholders in the European cybersecurity landscape. T4.6 produced the service catalog that includes all the services provided by CONCORDIA. The service catalog is available online[1] and it is the main entry point for a stakeholder to engage with CONCORDIA. T4.6 organized the first event of the CONCORDIA Open Door (COD) events series in Luxembourg in October 2019, involving around 100 stakeholders. The event's presentations and poster are also available online[2].

T4.6 completed all its activities in the first year according to plan. Among other things, the following should be highlighted: 13 new partners joined the project during the first year, great exchanges took place during the panel of the COD, and the important subject of *Women in Cybersecurity* has already shown significant advances with the organization of a dedicated workshop resulting in the launch of *Women in Cyber - a Manifesto for TODAY*.

[1] https://www.concordia-h2020.eu/concordia-service-catalog/
[2] https://opendoor.concordia-h2020.eu/

Contents

1 Stakeholders Engagement Strategy

CONCORDIA aims at taking the lead in connecting the European cybersecurity competencies[3] and to overcome future challenges in cybersecurity to guarantee Europe's digital sovereignty. In line with the initial call[4], CONCORDIA aims to unify the fragmented European cybersecurity landscape which will lead to better cooperation between cybersecurity experts, better dissemination of research results, and the affirmation of Europe's digital sovereignty[5][6][7].

The stakeholders of CONCORDIA are any person, group or organization that has interest or concern in the project and can affect or be affected by the project's objectives, actions and policies toward the construction of a rich and structured European cybersecurity network. **In other words, a CONCORDIA stakeholder is any entity that shares the same interests in cybersecurity innovation, propagation, and application.** Activities performed within this Task have two main goals: first, the continuity of CONCORDIA results by transferring them to the key players in Europe in the domain of cybersecurity; and second, the collection of concrete feedback linked to the various activities performed under the project.

To create and exploit liaisons and reach the above goals, a stakeholder engagement strategy was defined consisting of 4 main steps as shown in Figure 1. These steps are:

- Definition of the stakeholders for CONCORDIA;
- Analysis of the defined stakeholders;
- Planning and implementation of actions in order to engage with the stakeholders, and finally;
- Review of the whole process according to results and feedbacks.

These steps are analysed in detail in the following sections.

1.1 Definition of the stakeholders

The first step of the selected stakeholder engagement strategy is the identification of the CONCORDIA stakeholders.

[3] Individuals, companies or any organization with theoretical or practical skills in cybersecurity.

[4] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/su-ict-03-2018

[5] https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-netwo

[6] https://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf

[7] http://aegis-project.org/wp-content/uploads/2019/01/AEGIS-Cybersecurity-and-Privacy-landscape-in-Europe.pdf

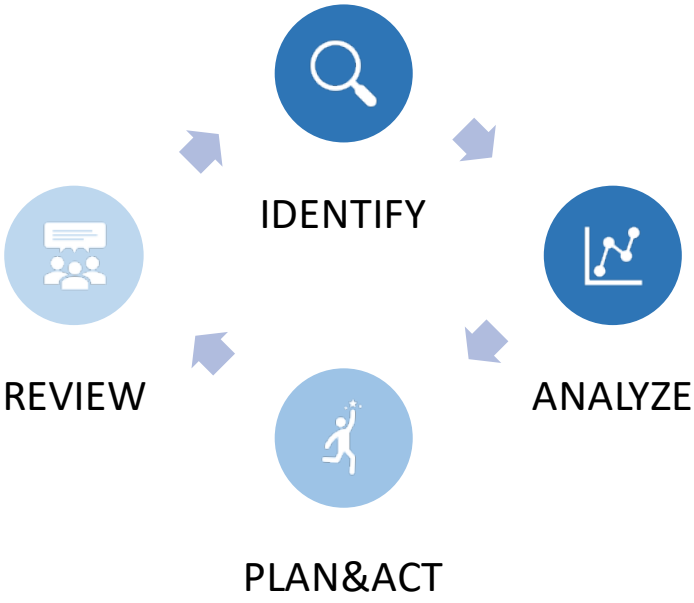

Figure 1: The CONCORDIA stakeholder engagement strategy

Stakeholders in the European cybersecurity landscape are unquantified and very heterogeneous. CONCORDIA wants to support the EU retain and develop the cybersecurity technological and industrial capacities necessary to secure its Digital Single Market through the formation of a cybersecurity competence community where academia, industries, and public bodies cooperate in a trustworthy network.

Different stakeholders have different objectives and needs. Because the potential stakeholders are plentiful and cover different actors of the society, a classification based on six classes was established as follows:

SC1 national authorities, national agencies, and national public entities;

SC2 European authorities, European agencies, and European public entities;

SC3 companies or consortiums of companies;

SC4 research networks, research communities, universities, and research centers;

SC5 project consortia funded by EC or mostly by EU member states;

SC6 other stakeholders.

These classes resulted from the clustering of potential stakeholders individual entities, performed by brainstorming sessions among experts within task 4.6. The main idea was to create coarse-grained groups with different interests and objectives concerning cybersecurity and the European landscape.

1.2 Analysis of the stakeholders

As the second step, we wanted to identify each stakeholder previously defined and to understand how CONCORDIA can engage with them effectively.

First, the liaisons already existing from every CONCORDIA partner were exploited. CONCORDIA partners are well-established members of the different cybersecurity communities and they become the point of contact for these communities' members to CONCORDIA. This provided CONCORDIA the first set of stakeholders to analyze. This analysis is detailed in Section 2.

The results reflected the heterogeneity of the stakeholders and of their respective interests. The results of this analysis guided the plan and the actions to take for engaging with stakeholders.

The next subsection presents a complete service list that can be easily accessed by any type of stakeholder and the preparation of our first public event to advertise the services to the stakeholders.

1.3 Plan and Actions for the stakeholders

The third step was the definition and implementation of a campaign for engaging and communicating with the CONCORDIA stakeholders (cf communication activities in *D5.2 - 1st year report on exploitation, dissemination, certification and standardization*). While D5.2 primarily focuses on communication activities with stakeholders, D4.7 presents other engagement activities.

The approach to engage with stakeholders consists of two key elements:

- a catalog of heterogeneous services to start collaboration in different areas of the CONCORDIA project;
- the organization of events to create a constructive dialogue with stakeholders.

The CONCORDIA service catalog is fully presented in Section 3. Once a stakeholder is reached, the entry point to engage with CONCORDIA is through its exposed services. Every stakeholder, due to its different characteristics, may be interested in different services of the catalog, where each of them creates and fosters a liaison with them. The services have been designed to mirror the interests of the analyzed stakeholders and the internal activities of the CONCORDIA project.

The first iteration of the series of events created by CONCORDIA, namely CONCORDIA Open Door (COD) events, is presented in Section 4. The CONCORDIA open door will be used as an enabler of an open and constructive dialogue about the whole spectrum of cybersecurity, from research to technology, from legal to business. This dialogue will be used to align CONCORDIA activities with the needs of the cybersecurity community.

1.4 Review of the stakeholder engagement strategy

As the last step, the review process is critical to evolve the plan and the actions taken to engage with stakeholders.

The considered outputs consisted of the participation at the CONCORDIA Open Door event and other success stories from the already active services in the CONCORDIA catalog, as presented in Section 5.

In particular, we want to become more attractive to stakeholders by addressing their specific needs and, thus, we plan to use even more features in the classification of the stakeholders to better understand them, each one having specific needs in terms of cybersecurity competences. Furthermore, we noticed difficulties in interacting and engaging with some eastern countries of Europe. Thus, we are evaluating the idea to organize our next COD in one of these countries.

2 Inventory of the stakeholders

2.1 Methodology

To identify the CONCORDIA stakeholders and to understand their needs, an inventory of initial stakeholders has been produced collaboratively by all CONCORDIA partners. This data set consists of particular stakeholders who already have a direct relationship with at least one CONCORDIA members and, thus, are well known to us. We consider this first circle of privileged stakeholders being at a one step distance from CONCORDIA because there is no need of other intermediates outside the consortium to interact with them.

Every data point in such a data set contains the following information:

- the name of the stakeholder;
- the class of the stakeholder (including a SC6 class "others" for those stakeholders that do not fit in any of the defined classes);
- the county, or countries, where the stakeholder operates;
- one of the stakeholders class (as enumerated below);
- the website of the stakeholder;
- the full name of the direct CONCORDIA contact person (potentially, for disseminating information or organizing a meeting);
- the email of the above person;
- the cybersecurity needs of the stakeholder as known by the above person (updated with any further information acquired in meetings and communication with the stakeholders)
- any other interesting piece of information on the stakeholder in relation to CONCORDIA's objectives as known by the above person (updated with any further information acquired in meetings and communication with the stakeholders)

This data set was initially populated through a survey conducted for two months (April and May 2019). All the initial partners of CONCORDIA replied to the survey. After every amendment the project went through, the survey was extended to the new partners as well. The full dataset is stored internally in CONCORDIA's repositories, with limited access to the management board and T4.6. Whoever within the consortium wants to access this dataset, may do so after authorization by T4.6. Persons outside the consortium cannot access this dataset due to privacy and confidentiality issues. In the following section, we are going to present synthetic results of the previously mentioned processed data. This and further analyses will support strategic decisions for the upcoming years of the project.

2.2 Synthetic results

The dataset consists of 206 stakeholders by the end of 2019. Because some of the stakeholders are consortia or network, we can potentially reach a greater number of individual stakeholders. The first esteem is about 350 single stakeholders. The distribution of the stakeholders according to the six classes, shown in Figure 2, reassured that CONCORDIA is well positioned in different cybersecurity communities since different people have different contacts with different classes of stakeholders.

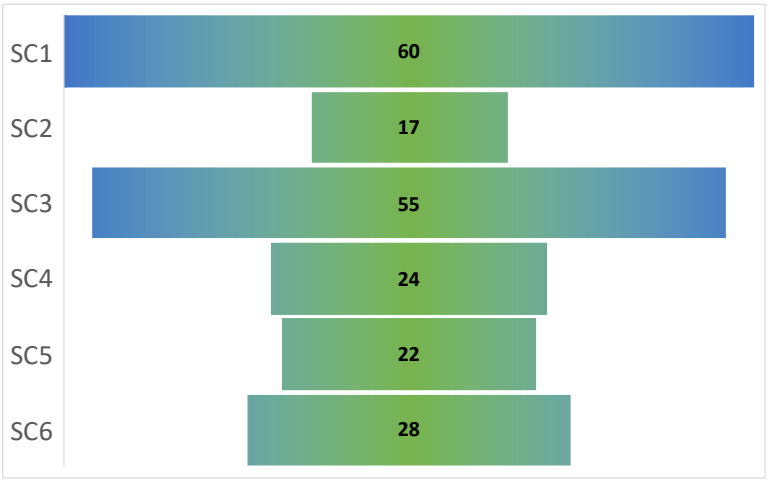

Figure 2: The initial set of CONCORDIA stakeholders

At the national level, 21 European countries are represented as illustrated in Figure 3. This includes national stakeholders from most of the member states, but also from Switzerland and Norway. For the next year, we will consolidate the list of national stakeholders for missing European countries, especially focusing efforts on the Eastern European countries that are currently missing from the inventory. Our first points of contact in these countries will be the Ministry of Foreign Affairs, Ministry of Interior, Ministry of Education and Research, and the national CERT as prominent stakeholders. Furthermore, we are elaborating the idea to organize our next CONCORDIA event in Eastern Europe to facilitate participation. We will also include the results of previous surveys made by the European Commission such as the ”Cybersecurity competence survey” [8] that will be updated in the following months.

Figure 4 shows the potential needs or interests of the different stakeholders regarding the CONCORDIA outcomes. As expected, they are well distributed and cover all areas of the project, confirming the relevance of our proposal regarding the current cybersecurity challenges that need strong research results, real case sce-

[8] https://ec.europa.eu/jrc/en/research-topic/cybersecurity/cybersecurity-competence-survey

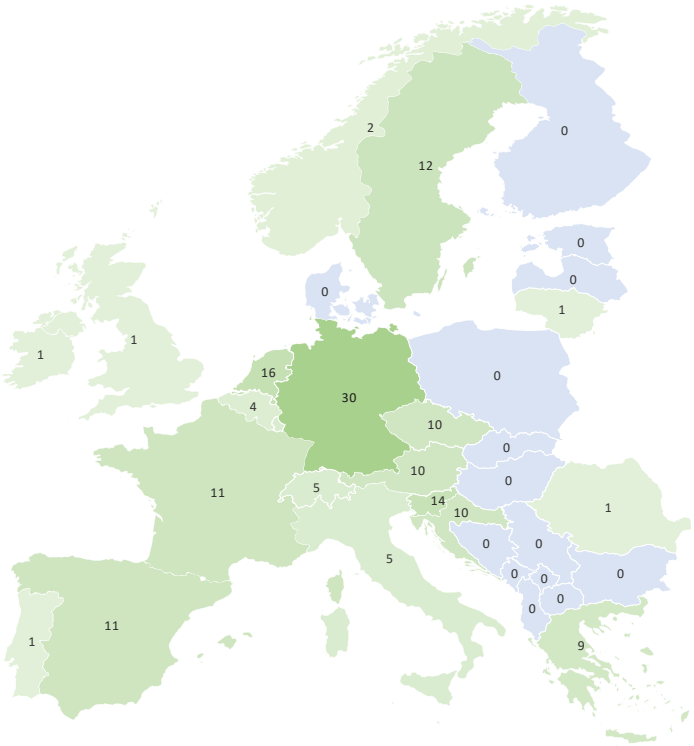

Figure 3: Map of the distribution of the national-level stakeholders over Europe

narios as industrial pilots and new collaborative tools to be addressed. In particular, some key proposals of CONCORDIA to federate the exchanges of cybersecurity information are awaited like the Threat Intelligence platform or the DDoS clearing house.

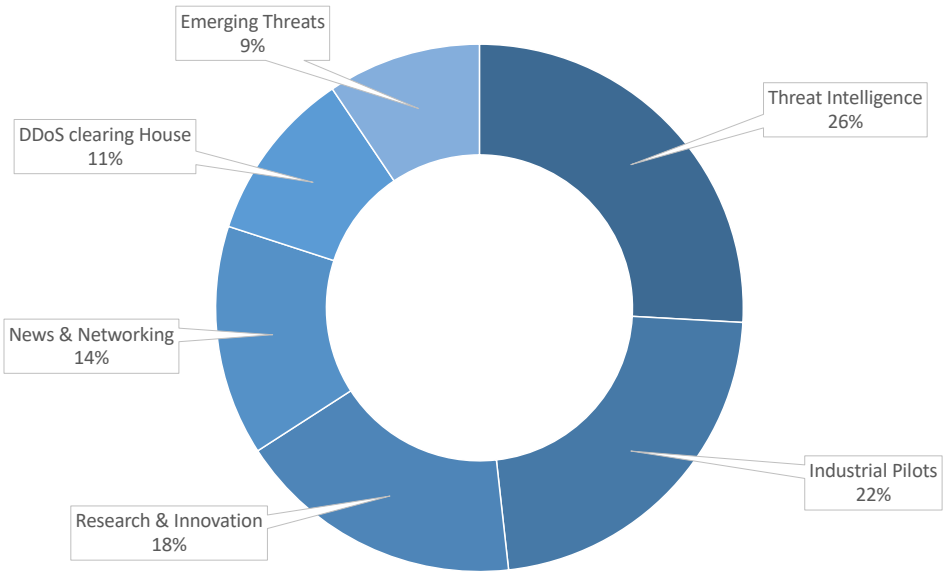

Figure 4: Stakeholders' interests in CONCORDIA activities

3 CONCORDIA Service Catalog

CONCORDIA's main interface with external stakeholders is its service catalog presented in this section. The service catalog of CONCORDIA is modeled as a path-to-follow to become a "booster" of Cybersecurity competencies for Europe and strengthen the European sovereignty on this matter.

The catalog is split in three levels, where each level implies a higher level of interaction with CONCORDIA. The first level is called *Notitia*[9] and consists of a passive interaction where the stakeholders receive or subscribe to the information provided by CONCORDIA. The second level is called *Pacta*[10] and consists of an active interaction where the stakeholders actively collaborate with CONCORDIA partners on a common topic of interest. The third and last level is *Concordia*[11] and consists in a full partnership with the stakeholders. As new partners of the consortium, the stakeholder collaborates internally to increase the value of CONCORDIA and take the lead on a specific aspect of the cybersecurity landscape.

The service catalog is accessible on the CONCORDIA website[12] and it has been introduced, explained, and advertised in the CONCORDIA Open Door event 2019.

[9] from Latin, news
[10] from Latin, agreements
[11] from Latin, harmony
[12] https://www.concordia-h2020.eu/concordia-service-catalog

The following subsections will provide a comprehensive descriptions of the 15 services (10 *Notitia*, 4 *Pacta*, 1 *Concordia*) composing the catalog. Table 2 presents the services, their targets, and the involved parts.

3.1 Notitia level

The *Notitia* level is the first level of the catalog and includes all services where information is provided by CONCORDIA and external stakeholders can receive this information on demand or by subscribing to feeds. It consists of 10 services.

3.1.1 Cybersecurity Updates

The "Cybersecurity Updates" service aims to provide the latest updates and news in the world of cybersecurity to organizations and individuals. Task 5.2 (T5.2 - Dissemination and Communication Activities) periodically retrieves updates from each task leader and from the management board, and pushes them through CONCORDIA media channels, such as Twitter, LinkedIn, Facebook, Instagram, the CONCORDIA blog, and the CONCORDIA newsletter. The external stakeholders can subscribe to any media channel and receive cybersecurity contents in their feeds including references to the latest facts on international research, EU laws, economic aspects, and funding opportunities.

3.1.2 Cybersecurity Experts

The "Cybersecurity Experts" service gives access to experts from the CONCORDIA. For example, they can join events organized by some stakeholders as speakers or panelists. Stakeholders can request academic, industrial, legal, and technical experts from CONCORDIA. The management board receives the requests and identifies the right person inside the consortium to join the event or the panel.

3.1.3 Cybersecurity Research

The "Cybersecurity Research" service aims to provide access to all the scientific publications written in the frame of the CONCORDIA project, so that organizations and individuals can be updated on the latest scientific progress in the cybersecurity landscape. Members publish scientific publications and notify Task 5.2 (Dissemination and Communication Activities) that uploads them on the website. Most of scientific publications will be produced by Work Package 1 (European Secure, Resilient and Trusted Ecosystem), but the other work packages may also produce scientific content (for instance, results of field trials from WP2, education or economic aspects of cybersecurity from WP3, etc.).

Service Name	Target	Involvements
Cybersecurity Updates	Organizations and Individuals	T5.2, Management Board, all tasks
Cybersecurity Experts	Organizations	Management Board
Cybersecurity Research	Organizations and Individuals	WP1, T5.2
Cybersecurity Improvements	Organizations and Individuals	all tasks, Management Board, T5.2
Cybersecurity Skills	Organizations and Individuals	T3.4, T3.3, T5.2
Women in Cybersecurity	Organizations and Individuals	T4.5, T5.2
Cybersecurity Tools	Organizations and Individuals	T3.3, T5.2
Career Opportunity	Individuals	T5.2
Startup Guidance	New-born and Growing Organizations	T3.5
Instruments Guidance	Organizations	WP4
Promotion Pact	Organizations and Individuals	T5.2, T3.3, T3.4, T4.5
Research Pact	Academic Stakeholders	WP1
Industry Pact	Industrial Stakeholders	WP2
Community Pact	National Centers, International Organizations, and Standardization and Certification Entities	Management Board
Concordia Partnership	Organizations	Management Board

Table 2: List of services in the CONCORDIA service catalog. Service Name is the name of the service as found in the catalog. Target indicates the features of the stakeholder that the service is targeting. The last columns Involvements show the Work Packages (WP), Tasks (T), and other CONCORDIA projects entities that are involved for the realization of the service.

3.1.4 Cybersecurity Improvements

The ”Cybersecurity Research” service aims to provide access to all the public deliverables of the CONCORDIA project, so that organizations and individuals can be informed on the latest progress in preparation of the European Cybersecurity Competence Network. All the CONCORDIA partners prepare the deliverables of the project and, upon acceptance, Task 5.2 (Dissemination and Communication Activities) uploads them on the website.

3.1.5 Cybersecurity Skills

The ”Cybersecurity Skills” service aims to provide organizations and individuals information about cybersecurity courses, trainings, and cyber-ranges in Europe. Task T3.4 (Establishing an European Education Ecosystem for Cybersecurity) collects all these data from Task T3.3 (Developing the CONCORDIA’s Ecosystem: Virtual Lab, Services and Training) and all the partners of CONCORDIA.

3.1.6 Women in Cybersecurity

The ”Women in Cyberscurity” service aims to provide organizations and individuals information about CONCORDIA activities on promoting workforce diversity in the field of cybersecurity. Task T4.5 (Women in cybersecurity) organizes such public activities and initiatives.

3.1.7 Cybersecurity Tools

The ”Cybersecurity Tools” service aims to provide organizations and individuals information about the latest software tools in the field of cybersecurity. Task T3.3 (Developing the CONCORDIA’s Ecosystem: Virtual Lab, Services and Training) collects all the cybersecurity tools, informs Task 5.2 (Dissemination and Communication Activities) that uploads their references on the website.

3.1.8 Career Opportunities

The ”Career Opportunities” service aims to provide organizations and individuals information about open positions in academia and industry for a cybersecurity-related job. Task 5.2 (Dissemination and Communication Activities) collects all the open positions and uploads their references on the website.

3.1.9 Startup Guidance

The ”Startup Guidance” service aims to provide new-born and growing organizations (such as startups) guidance to develop and implement business models. Stakeholders send an email to CONCORDIA asking for guidance and Task T3.5 (Community Building, Support and Incentive Models) get in touch with them.

3.1.10 Instruments Guidance

The ”Instruments Guidance” service aims to provide organizations technical, legal, and economic guidance to design and implement new cybersecurity policies. Stakeholders send an email to CONCORDIA asking for guidance and Work Package 4 (Policy and the European dimension) gets in touch with them.

3.2 Pacta level

The *Pacta* level is the second level of the catalog and includes all the services where a collaboration between CONCORDIA and the stakeholder is built. External stakeholders can start this interaction on demand. It consists of 4 services.

3.2.1 Promotion Pact

The ”Promotion Pact” service aims to provide organizations and individuals a way to promote their courses, trainings, cyber-ranges, tools, and open positions on the CONCORDIA website. External stakeholders send an email or fill a form, depending on the service to promote, Task 5.2 (Dissemination and Communication Activities) receives it and dispatches it to the right service holder.

3.2.2 Research Pact

The ”Research Pact” service aims to provide academic organizations a way to engage with CONCORDIA partners and start a research collaboration. Stakeholders send an email presenting their idea of collaboration on a cybersecurity-related research, Work Package 1 (European Secure, Resilient and Trusted Ecosystem) gets in touch with the stakeholders and start a discussion with them on the new potential research topic.

3.2.3 Industrial Pact

The ”Industrial Pact” service aims to provide industrial organizations a way to engage with CONCORDIA partners and start a collaboration. Stakeholders send an email presenting their use case or idea of collaboration for solving a cybersecurity-related challenge, Work Package 2 (Industrial Domains and Sector-Specific Pilots) gets in touch with the stakeholders and starts a discussion on the new potential collaboration.

3.2.4 Community Pact

The ”Community Pact” service aims to provide organizations a way to engage with CONCORDIA partners and start a discussion on cybersecurity-related topic. CONCORDIA set up three stakeholders groups: the Observer group with standardization and certification entities, the Liaison group with international institutions

(such as ENISA, EDA, and the World Economic Forum), and the National Centres group with national cybersecurity agencies. Stakeholders send an email with a will to join one of the stakeholders groups, the management board gets in touch with the stakeholders and, eventually, include them in the associated stakeholder group. Stakeholders groups are meant to meet regularly, virtually or physically, to discuss and promote collaboration for the definition of needs and actions that European players have to take in the field of cybersecurity.

3.3 Concordia level

The *Concordia* level is the third and last level of the catalog and consists of the single service for joining the CONCORDIA consortium. External stakeholders can start this interaction on demand.

3.3.1 Concordia Partnership

The ”Concordia Partnership” service aims to provide organizations a mean to start the process of joining the CONCORDIA consortium as full partner. Stakeholders send a request introducing themselves, the management board gets in touch and discusses a potential partnership with CONCORDIA.

4 CONCORDIA Open Door

CONCORDIA Open Door (COD) events series has been designed with the purpose of embracing the greatest numbers of cybersecurity stakeholders in a single event and provide the environment to fulfill the goals of the liaisons with the stakeholders task (see Section 1). The logo of the events series is depicted in Figure 5.

Figure 5: Logo for the CONCORDIA Open Door events series

In May 2019 (M5), the organization of the first edition of COD started. It was decided what are the main narrative of the event, its location and dates: COD2019 was primarily a presentation of the newborn CONCORDIA consortium, of its objectives, of its activities, but especially of its services (cfr Section 3). Therefore COD2019 was the first public handshake with external stakeholders and took place in the heart of Europe in Luxembourg. Due to its central position, Luxembourg was the ideal choice to ease the participation of stakeholders from all the other member states.

The date of October 2019 was chosen since October is the European Cybersecurity Month[13]. Furthermore, we decided to organize the event in the frame of the Luxembourgish Cybersecurity Week[14], a national advocacy-campaign week in line with CONCORDIA's objectives. We confirmed the 16th and 17th of October 2019 as the dates for COD2019.

Meanwhile, an active communication campaign performed by the whole consortium was launched to attract the stakeholders identified in the previous phase of the stakeholders engagement strategy (cfr. Section 2). The communication campaign consisted of messages to be transmitted by the partners to their stakeholders via e-mails, phone calls, meetings, or other means. The messages and timings were the following:

[13] COD2019 is listed as an event of the European Cybersecurity Month on the official website: https://cybersecuritymonth.eu/ecsm-countries/luxembourg/concordia-open-door-2019

[14] https://www.cybersecurityweek.lu/

- Save the date (June 2019): a generic message with the location and date of the event, and the main contents of the event[15];
- Registrations are open (July 2019): a message with the registration link and the fees[16];
- Remind to register (September 2019): a gentle reminder after the summer holiday for the registration presenting also the program and speakers of the event[17]
- Last days to register (October 2019): the last message before closing the registrations on the 8th of October.

The campaign was accompanied by the creation of a dedicated website[18] and ad-hoc posts and tweets on our media channels (see D5.2).

The program of the event was split into two parts: a policy-oriented day and a technical day. The full program can be found online [19]. together with links to the slides and posters presented.

The first day focused on the service catalog of CONCORDIA, the economic and legal aspects of cybersecurity, the *Women in Cyber - a Manifesto for TODAY*, and the panel "What can the community offer to the future European Cybersecurity Competence Center?". The panel, moderated by Arthur van der Wees (Arthur's Legal), consisted of:

- 1 panelist from CONCORDIA: Gabi Dreo Rodosek (CODE);
- 1 panelist from SPARTA: Thibaud Antignac (CEA);
- 2 panelists from industry: Christophe Bianco (Excellium Services) and Maria Dolores Perez (KBL Group);
- 1 panelist from national public bodies: Sheila Becker (ILR);

The second day consisted of flash talks on industrial use cases, presentations on CONCORDIA research topics, Threat Intelligence for Europe and DDoS Clearing House for Europe. The main session consisted of a poster exposition where more than 30 research posters were presented together with three industrial demos and the CONCORDIA service desk presenting the CONCORDIA ecosystem in detail.

[15] https://opendoor.concordia-h2020.eu/save-the-date.html
[16] Early registration fee was 150 euros until September 13th, 2019. The full registration fee was 250 euros. Academics and public bodies were exempt from the registration fee.
[17] https://opendoor.concordia-h2020.eu/program.html
[18] https://www.concordia-h2020.eu/concordia-open-door-event/
[19] https://opendoor.concordia-h2020.eu/program.html

5 Success Stories

In the next subsections, we are going to present the success achieved in the task 4.6 *Liaison with stakeholders* during the first year. They are the following contributions: the outcomes of COD2019, the services for Women in Cybersecurity, the Community Pacts, and the new partners that joined the project.

However, many other CONCORDIA's success stories are included in other deliverables that further describe the services and the interaction with stakeholders. In particular, some of the services outcome not presented here are presented in the following deliverables: D3.1 (1st year annual report on community building), D5.1 (Website and Social Media presences), D5.2 (1st year report on exploitation, dissemination, certification and standardization), and D6.3 (Innovation strategy plan).

5.1 COD2019 outcomes

COD2019 was held at Hotel Parc Alvisse, Luxembourg on the 16th and 17th of October 2019.

CONCORDIA established itself as a central player, and sponsor, of the Luxembourgish Cybersecurity Week (LCW) for discussions on the European landscape. The CONCORDIA logo was present on the LCW website, social media, printed materials, and events, such as the Gala dinner that closed the week.

COD 2019 counted 100 participants, consisting of

- 79 participants from CONCORDIA's partner organizations, whereof 55 from academia, 23 from industries, and 1 from a public entity.
- 21 participants from external organizations, whereof 3 from academia, 14 stakeholders from industries, and 4 from public entities.

Besides numbers, important feedback was given during the perfectly gender-balanced panel of the first day, namely "What can the community offer to the future European Cybersecurity Competence Center?", that saw the audience participating as well with interesting questions and follow-ups. Conclusions derived from the panel may be summarized as follows.

- Stakeholders in the EU need to jointly build collaborative competences, capabilities, and communities together in order to get to "Europe fit for the digital age".
- Digital and cyber-physical ecosystems need to be built in a resilient manner and with a collaborative approach as no one can do this alone.
- Keeping the data will neither solve the issues in digital ecosystems nor bring a competitive edge, but the power and value is in trusted data sharing;

- Sharing information about known or new vulnerabilities is quite important, also for communication and engagement purposes. However, these information-sharing structures can not sustain themselves without a cycle of giving and receiving. It is therefore important to discuss and assess together which values can be identified and distributed in order for each to contribute and get something out of it.

- Taking cybersecurity measures cost money, time and other resources, where cybersecurity expertise is hard to employ. Responsibility can not be outsourced, but the right teams of practical expertise is a way to expedite on making systems more resilient.

- Cybersecurity is still considered as an activity without return on investment (ROI). Efforts should be done to make people and organizations more aware of the risks, get them on board and make them feel co-accountable of the global security. Cybersecurity needs and can also be explained and "sold" as an enabler and facilitator of trust and trustworthiness between economic actors. This can boost the opportunities in society and economy, and can even give the EU a competitive edge in the digital age.

These outcomes confirmed the right direction taken by CONCORDIA to create a community around all the different stakeholders of the cybersecurity landscape. Furthermore, they highlight that there is a need to inform and educate individuals and organizations that cybersecurity is a solution and an enabler, not a problem.

Next year, we have the intention to focus more on the discussion and the creation of this community. In alignment of what was reported in the inventory of the stakeholders (cfr. Section 2), COD2020 will be held in one of the Eastern European countries to facilitate the participation of all the European member states in such event.

5.2 Women in Cybersecurity

Task 4.5 (T4.5 - Women in Cybersecurity) is devoted to incentivize women to join the field of Cybersecurity. This was originally planned to start at M20, however, during the first year, we actively worked with the aim of analyzing the actual situation and design a proper roadmap of actions to be implemented during CONCORDIA lifetime. These activities are advertised and accessed by the homonymous service in the service catalog.

During the first year, we organized the workshop *Women in Cyber - a Manifesto for TODAY*, in collaboration with ECSO Women4Cyber.[20]. The workshop was intended to provide a supportive environment to fertilize the collaboration among relevant stakeholders, aiming to develop a common vision to support women engagement in the cybersecurity area and to coordinate the work across different

[20] https://ecs-org.eu/working-groups/news/women4cyber

communities. The workshop outcome was the definition of the *Manifesto for TODAY*, a document intending to highlight the main objectives of CONCORDIA's gender gap strategy. To achieve this goal, the manifesto adopted a holistic approach considering the gender gap from different perspectives, namely: education/skills, entrepreneurship, industry, investment, legal/strategy, research.

The workshop format was designed to promote a lively discussion among participants to collect their feedback and to converge on the final version of the Manifesto. The audience was invited to join focus groups where the discussions, driven by moderators, aimed at identifying objectives, as well as, a set of actions to achieve them. Focus groups and respective moderators were as follows:

- education/skills: Nina Hasratyan (ECSO Women4Cyber);
- entrepreneurship: Sara Colnago (Swascan);
- industry: Madalina Baltatu (Telecom Italia);
- investment: Regina Llopis (Women Angels for STEM);
- legal/strategy: Dimitra Stefanatou (Arthur's Legal);
- research: Tatjana Welzer Druzovec (University of Maribor).

The workshop was collocated at the 6th *ACM Celebration of Women in Computing: womENcourage 2019* conference, 17th September in Rome. It gave the opportunity to engage with about 40 representatives of the cybersecurity industry, education, research, entrepreneurship and investment areas. They all brought their contribution to the discussion with real cases and innovative ideas that could incentivise, especially, young professionals to join the domain of Cybersecurity.

The outcome of the workshop is contained in the final Manifesto available online [21] and it has been officially launched at COD2019 (cfr. Section 4).

5.3 Stakeholders groups

The idea behind the stakeholders groups, presented as the"Community Pact" in the service catalog, is to interconnect different European stakeholders to promote discussion and ensure the European sovereignty in the digital single market. The stakeholders group of national cybersecurity centers and agencies is already being formed. Two entities already signed the affiliation to this group, namely the Federal Chancellery of Austria and the Federal Office for Information Security of Germany, but many more already expressed their intentions to join. We envision to reach a critical mass next year and organize the first workshop of the stakeholder group of national cybersecurity centers and agencies.

[21] https://www.concordia-h2020.eu/wp-content/uploads/2019/09/WomenInCyberMANIFESTO.pdf

Similarly, also for the observer (standardization and certification entities) and the liaison (international institutions) groups, CONCORDIA is moving forward to invite and include all stakeholders of interest (such as ENISA, EDA, the World Economic Forum). Again, we envision the first meeting of this group next year.

5.4 New Partners

CONCORDIA started as a consortium of 42 partners, but it rapidly grew since more and more organizations wanted to be part of the activities of the project, as described in the *Concordia* level of the service catalog in Section 3. After two amendments, the consortium now counts 51 partners, 27 academic and 24 industrial, from 19 countries.

Initially, Sweden was not part of any of the pilots for a European Cybersecurity Competence Network funded by the EC. RISE, together with Ericsson, analyzed the four pilots and then approached CONCORDIA to join the consortium. RISE, among other topics, works on cybersecurity for the Internet of Things (IoT) and Artificial Intelligence (AI), and with Ericsson's involvement, security for telecoms and 5G also falls within their remit. CONCORDIA also offered RISE a sit on the management board to bring Swedish perspectives into European work. Furthermore, Sweden is contributing by almost 1.7 million on funding.

Austria was another member state missing in the consortium, and SBA with its competencies properly fits in the CONCORDIA research efforts pool. SBA got in touch with the management board and joined the project. Similarly, IJS approached CONCORDIA during one of the European cybersecurity events and it joined the consortium because of the extensive research activities conducted in IJS. UiO approached CONCORDIA during one of the European working group events on cybersecurity and expressed its will to join the consortium. Due to its valuable research activities, it became a partner of CONCORDIA as the first partner from Norway. ISI contacted CONCORDIA to join and, as a major research center in Greece with multiple institutes and locations, they joined through their Industrial Systems Institute bringing in the consortium their links to the Greek industry. Another university with high profile researchers on smart device cybersecurity that joined CONCORDIA this year was RUB.

A completely different story applies to two new partners, namely ULANC and UNI PASSAU, who joined the consortium because some key people changed affiliation during this first year. To preserve the activities plan, the management board of CONCORDIA promptly started a discussion with these two universities and included them in the consortium.

Meanwhile, CONCORDIA has already been contacted by several other organizations and a discussion is ongoing between them and the management board. Some of them are already in the process of signing the non-disclosure agreement, the grant agreement, and the consortium agreement and they will be hopefully presented early next year. Currently, we mainly prioritize those requests from big industrial organizations that can extend our sector-specific pilots in work pack-

age 2 (WP2 - Industrial Domain and Sector-Specific Pilots) and ensure the two main goals of the liaisons with the stakeholders. These are, again, the continuity of CONCORDIA's results by transferring them to the key players in Europe in the domain of cybersecurity and the collection of concrete feedback linked to the various activities performed under the project.

6 Conclusion

This document presented the work conducted during the first year of the CONCORDIA project regarding the liaisons with the stakeholders. We described the stakeholders engagement strategy we put in place, in particular how we defined and identified the stakeholders and how we planned concrete actions to get engaged with them. An inventory of a first-circle of close stakeholders was conducted by the consortium and resulted in 206 identified stakeholders of different nature, from different European countries, and with different potential interests in CONCORDIA, highlighting the diversity of the stakeholders and the challenge addressed by the present task to get involved with each of them. To that end, we proposed CONCORDIA's service catalog which is the cornerstone of our strategy to work with stakeholders. It already includes 15 services that are organized into 3 levels of engagement. The services have been extensively described and are already available to be used by our stakeholders from our website. To advertise this service catalog and more generally to encourage our stakeholders to discover CONCORDIA, the first edition of our annual CONCORDIA Open Door event took place in Luxembourg and was very successful.

Among the success stories of this first year, we can note very interesting outcomes of the CONCORDIA Open Door event which confirmed the right direction taken by CONCORDIA to create a trustful community around all the different stakeholders of the cybersecurity landscape. We also welcomed 9 new partners that joined the project through the highest engagement level of the service catalog. CONCORDIA also organized a specific workshop on the important topic of Women in cyber that resulted in the creation of the *Manifesto for TODAY*.

The next year will pursue the different actions described in this deliverable. We will, in particular, extend our inventory of the stakeholders by taking into consideration recent surveys in the topic but also consolidate our first circle of stakeholders, in particular in eastern countries. To that end, we are currently evaluating the idea to host the next edition of the CONCORDIA Open Door in the east of Europe. Another important step in the second year will be to finalize the stakeholders' groups and initiate specific meetings with them. To measure the progress of our liaison task, we expect a higher number of external stakeholders to participate in the next edition of the CONCORDIA Open Door event, and an increasing level of interaction with our service catalog that we will closely monitor. This will prove that the community-building process is successful and validate our global strategy.