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 D4.8: 2nd year report on Liaison with Stakeholders

Abstract: This document describes CONCORDIA's activities during its second year related to the liaisons with cybersecurity stakeholders in Europe. It presents the stakeholders' newsletter and the stakeholders' groups, among the other CONCORDIA services, and the CONCORDIA Open Door event of 2020.

Contractual date of delivery	*M24*
Actual date of delivery	*30.12.2020*
Deliverable dissemination level	*Public*
Editors	*Antonio Ken Iannillo*
Contributors	*SnT*
Quality assurance	*Michael Sirivianos (Cyprus University of Technology)* *Anja Majstorovic (eesy-innovation)* *Georgia Anousaki (National Cyber Security Authority of Greece)* *Nils Gruschka (UIO)*

[†] 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 a 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 a 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	Greece

	Media	
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. Michael Sirivianos (Cyprus University of Technology) (review lead)
2. Anja Majstorovic (eesy-innovation GmbH)
3. Georgia Anousaki (GSDP)
4. Nils Gruschka (UIO)

Revisions

Ver.	Date	By	Overview
0.01	*30/11/2021*	*Antonio Ken Iannillo*	*First version*
0.02	*18/12/2021*	*Antonio Ken Iannillo*	*Final version*

Executive Summary

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

This task's main objective is to establish liaisons and collaborate closely with the relevant European stakeholders to achieve the following goals: (1) the sustainability of CONCORDIA's outcomes (by disseminating them to the key cybersecurity stakeholders in Europe); and (2) the collection and integration of concrete feedback, linked to various activities performed in the project. The output of this task, during the 2nd year of the project, is reported in deliverable 4.8 (D4.8): Year 2 report on the liaison with stakeholders.

In the second year of CONCORDIA, T4.6 team engaged with more stakeholders and established mutual trust among them. T4.6 updated the service catalog in collaboration with the other related tasks. In particular, in 2020, we started issuing the stakeholders' newsletters, and three issues have already been published. The CONCORDIA network regularly receiving this newsletter, consists of 297 members from 165 different organizations. Furthermore, the stakeholders' groups, within the scope of the proposed regulation for the European cybersecurity competence center and network, have six member states in the NSG and seven affiliations for the OSG.

The T4.6 team organized the second event of the CONCORDIA Open Door series, namely COD2020, as a virtual venue due to the COVID-19 pandemic. 162 out of 278 registrants were from organizations that are not part of the CONCORDIA consortium.

Regarding the stakeholders' type:

- 21 registrants were from national authorities, national agencies, or national public entities;
- 20 registrants were from European authorities, European agencies, or European public entities;
- 154 registrants were from companies;
- 83 registrants were from universities or research centers.

Regarding gender distribution, 207 registrants were male while 71 were female, that is 74% male against 26% female.

The outcome of COD2020 discussions highlighted, among others, that European digital sovereignty is a shared responsibility and should be approached from different domains; that teaching practical skills in cybersecurity is essential; and that synergy between SMEs, big industries and academia has demonstrated its utility but needs further funding and cooperation to develop marketable research and innovation.

Contents

1. Introduction

WP4 has the following objectives:

- Create and operationalize working groups in the research domains of interest of CONCORDIA
- Identify future and emerging threats in the domains of interest identified;
- Define scenarios and produce threat reports for each of the threats identified above;
- Examine the economic and legal considerations involved;
- Establish liaisons and collaborate closely with the relevant European stakeholders;
- Formalize the research and other outcomes into a Cybersecurity Roadmap for Europe;
- Surface the necessity to address the social aspects linked to the effective operationalization of a cybersecurity competence network;
- Promote workforce diversity in cybersecurity in an appropriate manner for the Digital Single Market's particular needs.

In particular, T4.6 focuses on establishing and fostering liaisons with cybersecurity stakeholders by establishing an open, constructive dialogue. This communication will give feedback to the activities of WP4 and of the whole consortium, enhancing the roadmap and other deliverables available to the broader cybersecurity community.

1.1. Stakeholders Engagement Strategy

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 sustainability of CONCORDIA results by transferring them to the critical cybersecurity stakeholders in Europe; and second, the collection of concrete feedback from stakeholders, linked to the various activities performed in the project.

Recollecting the 1st year activities report, we defined a stakeholders' engagement strategy to create and exploit liaisons reaching the above goals, which consists of 4 main steps:

- Definition of the stakeholders.
- Analysis of the defined stakeholders.
- Planning and implementation of actions to engage with the stakeholders.
- Review of the whole process according to results and feedback.

This year, we set off based on last year's results by focusing on our stakeholders' lists and our engagement deriving from COD2019. We noticed that Eastern countries were underrepresented and needed to be more involved in the CONCORDIA network. We first advertised the service catalog in collaboration with CONCORDIA's communication team. Still, the primary engagement activity remains COD, as demonstrated during its first edition. Originally, the COD2020 event was to take place in Romania, in partnership with a startup networking event, namely the *how-to-web* conference. The specific location of venue served to improve our engagement with stakeholders in the Eastern Europe and focus on startups. Unfortunately, due to the pandemic situation in 2020, we had to re-think of COD2020 as a virtual event. Furthermore, regarding the stakeholders' groups, we noted a substantial slow-down in the bureaucratic processes within the stakeholders' organizations, which eventually slowed down. This virtualization of the meeting had its pro and cons, as presented later in

this deliverable. Still, there was significant expansion of the network and more meaningful feedback for the CONCORDIA consortium was received.

1.2. Structure of the Document

Chapter 2 presents the updates for each service in the service catalog, referring to other deliverables, where most of these services and their results are extensively described. However, this deliverable provides exclusive content for the following services: Cybersecurity Updates (stakeholders' newsletter), Cybersecurity Experts, and Community Pact (stakeholders' groups).
Chapter 3 presents COD2020, including its planning activities, its program and its results.
Chapter 4 consists of some final remarks on the overall year and a plan for T4.6's activities in 2021.
Appendix A includes the description of the stakeholders' groups, as presented to the potential members.

2. CONCORDIA Service Catalog

CONCORDIA's primary interface with external stakeholders is its service catalog, presented in a previous deliverable[1]. The service catalog of CONCORDIA is modelled as a path-to-follow to become a "booster" of cybersecurity competencies for Europe and strengthen the European sovereignty on this matter.

All the deliverables referred to in this document are available at https://www.concordia-h2020.eu/deliverables/.

2.1. Notitia Level

The *Notitia* level is the first level of the catalog. It includes all services where CONCORDIA provides information. External stakeholders can receive this information on-demand or subscribe to feeds. Currently, it consists of 10 services.

2.1.1. Cybersecurity Updates

The "Cybersecurity Updates" service aims to provide the latest updates and news in the landscape of cybersecurity to organizations and individuals. While the main activities on social media are carried by T5.2 (Dissemination and Communication Activities) and presented in deliverable D5.3, task 4.6 launched the **stakeholders' newsletter** in May 2020, followed by the second issue in September 2020 and the third one in December 2020.

The newsletter has the same objectives as T4.6: present CONCORDIA’s results to stakeholders and request feedback on CONCORDIA’s activities.

Besides, the newsletter contains pointers to articles and not full-text articles, better serving the network's heterogeneity, as some readers are interested in the research legal, economic, or technical aspects of cybersecurity-related news. Others can altogether skip this. Readers will be lightly informed on news across different domains, including CONCORDIA’s results, with the possibility to explore each topic. Eventually, they will land on our feedback request page to participate actively in the network.

All the issues are also available online at https://www.concordia-h2020.eu/concordia-service-cybersecurity-updates/.

Starting from COD2019, every CONCORDIA event requests the participants to subscribe to the CONCORDIA network and receive periodic information about cybersecurity.

[1] Deliverable D 4.7: Year 1 report on the liaison with stakeholders; available at https://www.concordia-h2020.eu/wp-content/uploads/2020/05/D4.7-Year1ReportOntheLiaisonwithStakeholders.pdf

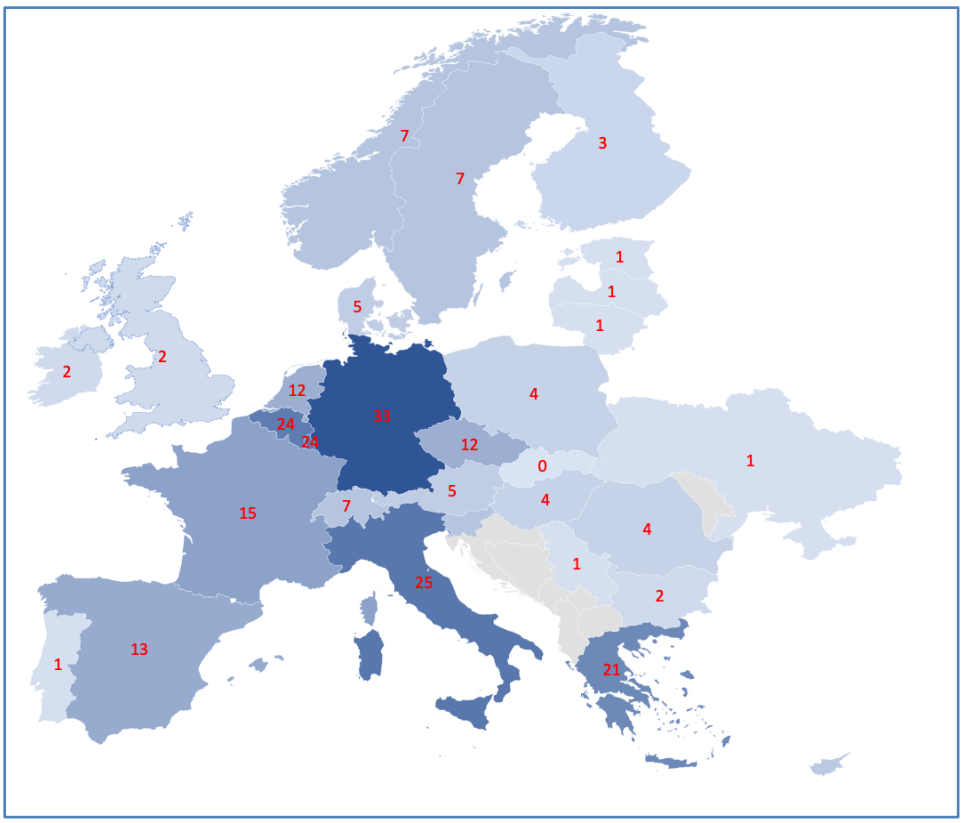

Figure 1: Members of the stakeholders' mailing list, or CONCORDIA stakeholders' network, split by country of origin (46 stakeholders are not considered in this visual analysis because it was not possible to extract the country of origin).

At the time of writing this document, the CONCORDIA mailing list contains 297 members from about 165 different organizations (large companies, national and European entities, SMEs, research centers, financing bodies, and more). Figure 1 shows the distribution of these stakeholders across Europe. There is a stakeholder for each member state but Croatia, Malta, and Slovakia. However, some member states still have a low number of representatives (less than five subscribers).

2.1.2. Cybersecurity Experts

The "Cybersecurity Experts" service aims to provide information on the experts in the CONCORDIA consortium, available at https://www.concordia-h2020.eu/concordia-service-cybersecurity-experts/. Thus, external stakeholders can contact them according to their expertise. We list 90 experts, among which 20 also have a dedicated web page on the CONCORDIA website with a short biography. In collaboration with T5.2 (Dissemination and Communication Activities), we add and advertise full profiles every week.

2.1.3. Cybersecurity Research

The "Cybersecurity Research" service aims to provide access to all the scientific publications written in the CONCORDIA project so that organizations and individuals can be updated on the latest scientific progress in the cybersecurity landscape. In 2020, CONCORDIA published and made available 107 publications at https://www.concordia-h2020.eu/concordia-service-cybersecurity-research/. Further details are in Deliverable D1.2 (2nd year report on implementing a European Secure, Resilient, and Trusted Ecosystem).

2.1.4. Cybersecurity Improvements

The "Cybersecurity Research" service aims to provide access to all the public documents of the CONCORDIA project so that organizations and individuals can be informed on the latest cybersecurity progress by CONCORDIA. They are all available at https://www.concordia-h2020.eu/concordia-service-cybersecurity-improvements/.

2.1.5. Cybersecurity Skills

The "Cybersecurity Skills" service aims to provide organizations and individuals information about cybersecurity courses, training, and cyber-ranges in Europe. This service matches activities in tasks T3.3 (Developing the CONCORDIA's Ecosystem: Virtual Lab, Services, and Training) and T3.4 (Establishing a European Education Ecosystem for Cybersecurity). These activities are presented in Deliverable D3.2 (2nd-year report on community building and sustainability).

2.1.6. Women in Cybersecurity

The “Women in Cybersecurity" service aims to provide organizations and individuals information about CONCORDIA activities on promoting workforce diversity in the field of cybersecurity. It matches activities in T4.5 (Women in Cybersecurity), presented in Deliverable D4.5 (1st report on cybersecurity workforce diversity).

2.1.7. Cybersecurity Tools

The "Cybersecurity Tools" service aims to provide organizations and individuals information about the latest software tools in the field of cybersecurity. In collaboration with task T3.3 (Developing the CONCORDIA's Ecosystem: Virtual Lab, Services, and Training), there are 47 tools available at https://www.concordia-h2020.eu/concordia-service-cybersecurity-tools/.

2.1.8. Career Opportunities

The "Career Opportunities" service aims to provide organizations and individuals information about open positions in academia and industry for cybersecurity-related jobs. Seven CONCORDIA partners published 16 job opportunities in both academia and industry. An external stakeholder can access them through the service page at https://www.concordia-h2020.eu/concordia-service-career-opportunities/.

2.1.9. Startup Guidance

The "Startup Guidance" service aims to provide new-born and growing organizations (such as startups) guidance to develop and implement business models. It matches activities in task T3.5 (Community Building, Support, and Incentive Models) presented in deliverable D3.2 (2nd-year report on community building and sustainability).

2.1.10. Instruments Guidance

The "Instruments Guidance" service aims to provide organizations technical, legal, and economic guidance to design and implement new cybersecurity policies. It matches activities in WP4 (Policy and the European Dimension), but no external stakeholders specifically asked for this service.

2.2. Pacta Level

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

2.2.1. Promotion Pact

The "Promotion Pact" service aims to provide organizations and individuals a way to promote their courses, training, cyber ranges, tools, and open positions on the CONCORDIA website. In 2020, we received several requests regarding the possibility to advertise courses. We dispatched these requests to the task T3.4 team (Establishing a European Education Ecosystem for Cybersecurity).

2.2.2. Research Pact

The "Research Pact" service aims to provide academic organizations a way to engage with CONCORDIA partners and start research collaboration. No request was dispatched for this service. However, CONCORDIA researchers are highly active in different research communities, continuously creating a connection with other researchers. Deliverable D1.2 (2nd year report on designing a European Secure, Resilient, and Trusted Ecosystem) provides further details.

2.2.3. Industrial Pact

The "Industrial Pact" service aims to provide industrial organizations a way to engage with CONCORDIA partners and start a collaboration. Several industries have contacted CONCORDIA to discuss new cybersecurity use cases. Deliverable D6.5 (2nd year management report) provides further details.

2.2.4. Community Pact

The "Community Pact" service aims to provide organizations a way to engage with CONCORDIA partners and start a discussion on cybersecurity-related topics. A (draft) regulation proposed to strengthen the (development, build-up, and deployment of) competitiveness and capacities in cybersecurity, at EU and national levels. It also proposed to support research to facilitate and accelerate standardization and certification processes while reducing digital dependence. This service inclusively and comprehensively engages diverse competencies/stakeholders to result in a high-impact EU-wide cybersecurity ecosystem. Recognizing that different stakeholders (national or institutional) represent different levels of competencies and with associated differing levels of engagement, CONCORDIA has established dedicated processes to engage the initial set (to be expanded as needed) of stakeholders to the consortium as:

- The National Cybersecurity Competence Centres and Agencies Stakeholders Group (NSG);
- The Liaison Stakeholders Group (LSG);
- The Observer Stakeholders Group (OSG).

The three group descriptions (as distributed to potential members) are reported at the end of this subsection. It is essential to note the differences with already established stakeholders' groups in Europe. Some aim to build cybersecurity (ECSO working groups, FIC

Observatory[2]), some promote operational cooperation (CSIRTs network), and some others facilitate the exchange of information on specific domains (NLO network[3], the ENISA Advisory Group, and SCCG[4]). Other cybersecurity pilots include stakeholders to receive feedback from them on the cybersecurity roadmap and to provide them a preview of products and services (SPARTA friends and associates [5] and ECHO participants [6]). However, the three CONCORDIA stakeholders' groups mimic the structure proposed by the European Commission for the European cybersecurity competence center and network to detect the challenges and functionalities of such a structure before the Regulation entering into force.

In 2020, we sent out the first round of invitations for the NSG. Besides the two entities that already showed interest in 2019, five national entities from five countries signed the affiliation letters. However, we encountered several difficulties obtaining signatures, even from interested entities, due to other priorities raised by this year's pandemic.

Similarly, we also accepted the first affiliation letters for the OSG. We collected seven affiliations, all but one being H2020 consortia. By nature, these consortia are temporary, but we believe that single entities will eventually enrol in the group after their H2020 projects end. They are SPIDER, THREAT-ARREST, C4IIOT, CyberSANE, CyberWiser, and cyberwatching.eu. The last one is MoveToDigital: a digital innovation hub for the south region in France.

Information on the community pact and the stakeholders' group can also be found in deliverable D6.5 (2nd year management report).

2.3. CONCORDIA Level

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

2.3.1. CONCORDIA Partnership

The "CONCORDIA Partnership" service aims to provide organizations with a means to join the CONCORDIA consortium as a full partner. In 2020, we introduced two new partners: Eötvös Loránd University (ELTE) from Hungary and Utimaco Management GmbH (Ultimaco) from Germany. The first one represents a new member state in the consortium. At the same time, the latter is a strong industrial partner in the field of hardware security. CONCORDIA is now a consortium of 52 partners from 20 European countries.

[2] https://observatoire-fic.com/en/dna/
[3] https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office
[4] https://ec.europa.eu/digital-single-market/en/stakeholder-cybersecurity-certification-group
[5] https://www.sparta.eu/partners/
[6] https://echonetwork.eu/join-echo/echo-participants/

3. CONCORDIA Open Door

The CONCORDIA Open Door (COD) event series designed embraces a significant number of cybersecurity stakeholders in a single event and provides the environment to fulfil the goals of task T4.6 (Liaison with stakeholders). This series has the general objective of connecting all the cybersecurity stakeholders to create useful exchanges between academia, industry, public bodies, and policymakers.

The specific objectives of COD2020 were:

- To maximize the number of external people joining COD2020;
- To involve stakeholders from more member states than COD2019, especially with a focus on eastern Europe, which is underrepresented;
- To facilitate the discussions during the event.

3.1. Reaction to the pandemic

At the beginning of the year, T4.6 selected BitDefender among CONCORDIA's partners as a local host to organize COD2020 in Bucharest. We connected with HowToWeb[7], a large conference for startups, and defined the first actions towards a successful combined event.

Once Italy detected the first cases of COVID-2019, T4.6 started entertaining the idea to have a virtual event and discussed it with the HowToWeb organizing team that was having the same doubts. In May 2020, the T4.6 team officially decided to move COD2020 to a virtual format due to the various restrictions.

We looked for a virtual conference platform with enough functionalities to resemble a physical event in the spirit of connecting stakeholders and make them discuss with each other. We opted to filter out all the platforms not compliant with GDPR and not based in Europe, in line with Europe's digital sovereignty objective.
After demos with several companies, we chose the *Tame* platform[8] that included:

- A main virtual room (main stage) for the speakers to join with camera and microphone and broadcasted to all attendees;
- The opportunity to create other virtual rooms (tame sessions) for coffee breaks and open discussions where attendees can join with camera and microphone;
- A virtual exhibition area where attendees can visit booths and discuss with the people in charge of the booth in private virtual rooms.

3.2. Program

COD2020 took place on the 28th and 29th of October, in the European Cybersecurity Month[9]. The selected topics were "European digital sovereignty and education" on the first day and "European policy, startups, and SMEs" on the second day. Each day started with a keynote to introduce the topic, continued with two panels, and ended with a brief presentation of the related CONCORDIA services.

[7] https://www.howtoweb.co/
[8] https://tame.events/
[9] COD2020 is listed as an event of the European Cybersecurity Month on the official website: https://cybersecuritymonth.eu/countries/world/concordia-open-door-2020-online

The program is illustrated in Figures 2 and 3, including the speakers' names and affiliations.

Figure 2: COD2020 program - day 1

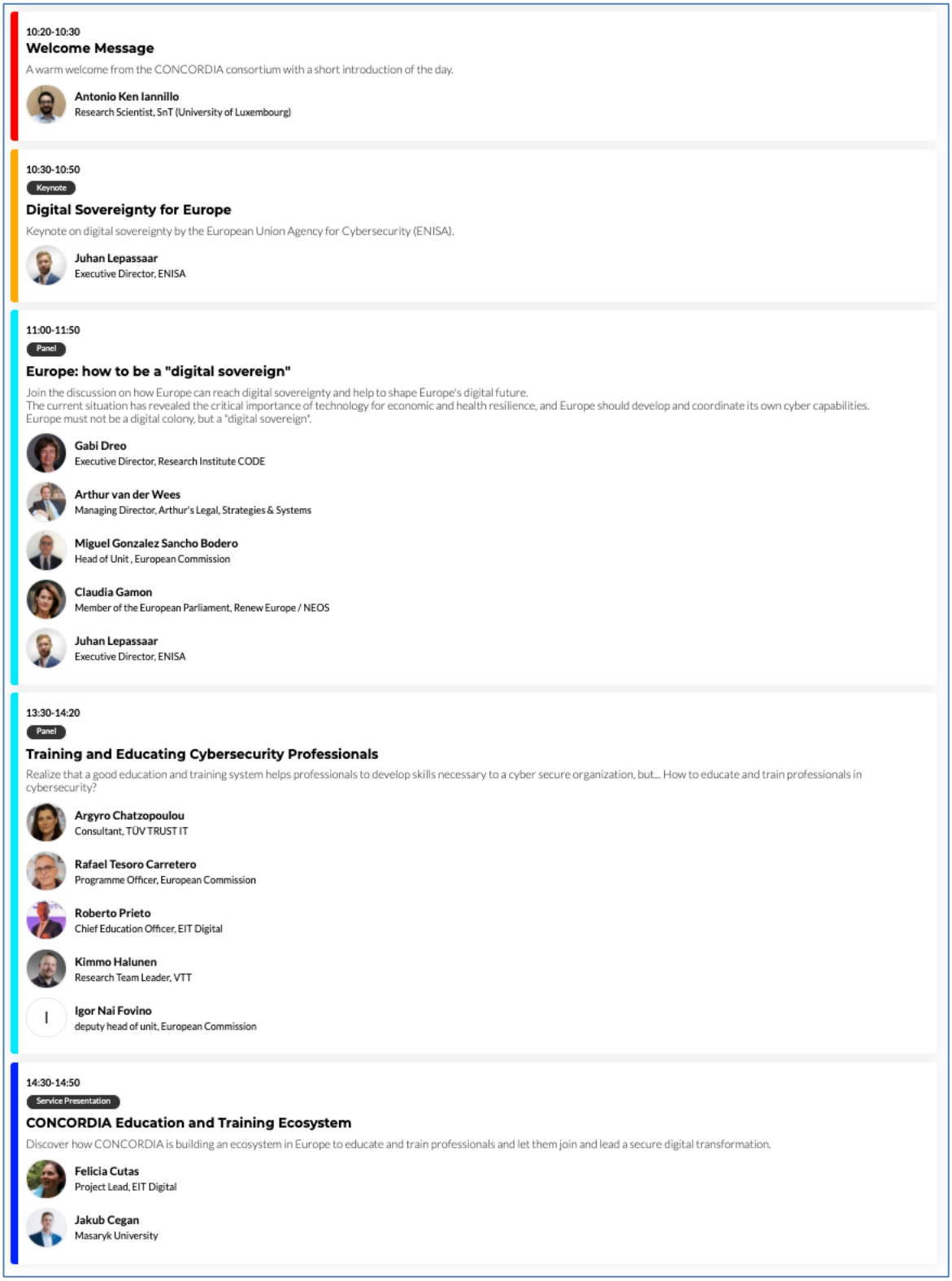

Figure 3: COD2020 program - day 2

Moreover, COD2020 accounted for 12 exhibitors: four startups, six H2020 projects, the Women4Cyber booth (a collaboration between Task T4.5 and ECSO), and the CONCORDIA service booth (where members of the consortium provided information about the CONCORDIA services).

3.3. Registrations

COD2020 opened the registrations on the 1st of September and counted 278 registrations. Registrants were from all the member states but Croatia, Finland, Malta, and Slovakia, as shown in Figure 4.

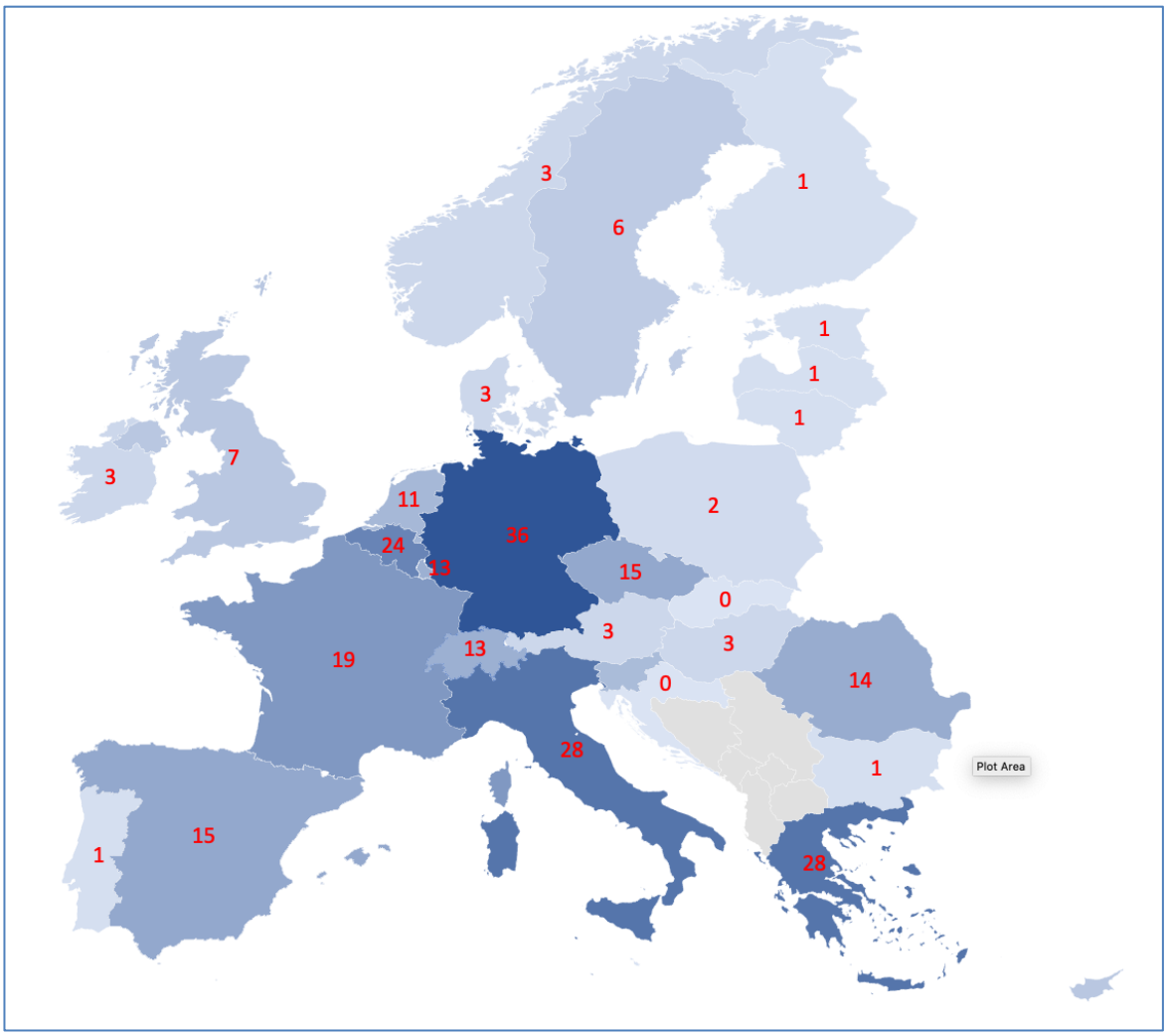

Figure 4: Distribution of COD2020 registrants in Europe.

Out of 278 registrants, 162 were from organizations that are not CONCORDIA partners.

Regarding the stakeholders' type

- 21 registrants are from national authorities, national agencies, or national public entities;
- 20 registrants are from European authorities, European agencies, or European public entities;
- 154 registrants are from companies;
- 83 registrants are from universities or research centers.

Regarding the gender, 207 registrants were male while 71 were female, that is 74% male against 26% female.

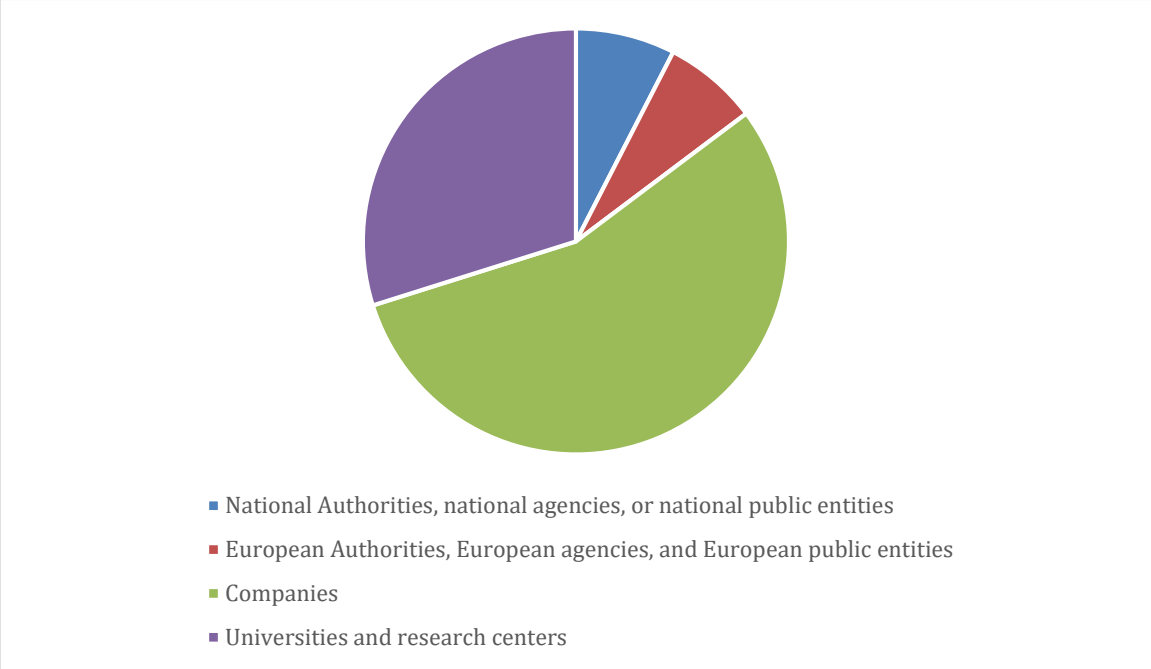

Figure 5: COD2020 registrants grouped by the stakeholders' type

3.4. Outcome

This subsection presents the outcome of the discussions held during the four panels. The recordings of all the sessions are available online on the CONCORDIA's YouTube channel https://www.youtube.com/concordia-h2020.

3.4.1. Panel "Europe: how to be Digital Sovereign"

The discussion panel had representatives of the European Commission, European Parliament, ENISA and CONCORDIA. The topic was about how the European Union can avoid becoming a digital colony and instead can reach digital sovereignty, develop and coordinate its cyber capabilities, and shape Europe's digital future.

There was an unmistakable consensus in the panel on the reasons w*hy* to support building, achieving, and sustaining European digital sovereignty, but in general terms also on the *How* to do so. To elaborate on the *How*, the panel discussed both the current state of play (even from policy and implementation perspectives), state of the art (including where we should go and what we should do), as well as the GAP (how to get there and what it takes). The issues raised by the current COVID-19 pandemic were also discussed.

Some notable takeaways points were:

- **Cybersecurity and digital sovereignty are shared responsibilities**;
- The Cybersecurity Competence Centers and Network are a missing piece of the puzzle;
- The fact that about 95% of cybersecurity incidents arise from known vulnerabilities again proved that regarding trusted, timely, and efficient data sharing, we are only "scratching the surface" at this moment;

- The European Union community needs to pull in resources, including the necessary fostering and incentivizing of private and other investments in the domain of digital sovereignty;
- The cybersecurity policy and coordination pipeline are stepping up to the occasion, with the Cybersecurity Strategy soon anticipated, and are focusing on implementing and updating existing and new policy instruments on numerous topics and in multiple domains, while improving capacity building and enabling capabilities and harmonization.

3.4.2. Panel "Training and Educating Cybersecurity Professionals"

Rafael Tesoro Carretero from the European Commission started the panel outlining the current challenges in cybersecurity skills for professionals in the European Union. Then, the representatives of EIT Digital, VTT, TUV TRUST IT, and JRC outlined their activities in this context. Roberto Prieto highlighted the importance of educating professionals in the industry. Kimmo Halunen advocated for the role of MOOCs as a teaching tool. Argyro Chatzopoulou presented the joint work of the four cybersecurity pilots on skill certification. Igor Nai Fovino presented the Cybersecurity Atlas. The main highlight of the discussion was the awareness of the need for practical skills, besides theoretical knowledge, in cybersecurity.

3.4.3. Panel "Startups, SMEs, and the future European Cybersecurity Competence Center and Network"

The panel session started with introducing Europe's Cybersecurity expertise and implementing European Cybersecurity Competence Center and Network. The new structure described in the legislative proposal – an EU-level Competence Centre with its network of national-level competence centers, but also a wider community – needs to pay special attention to startups and SMEs.

The first panelist Jean Diederich (Wavestone) gave an overview of the current cybersecurity startup landscape and mentioned that there are segments, such as cloud security, which are not addressed by startups. Another issue is that many non-EU investors start cybersecurity businesses in Europe and officially count as EU startups, even if they only have resell or commercial office. The challenge lies, as all panelists agreed, with how to coordinate what is useful for the EU in the emerging startup landscape (e.g., what strategic segments are), how to move from proof of concept to the next stage that involves real operational deployment, as well as how to keep startups in Europe, after their initial success.

The next panelists mentioned more gaps, such as lack of growth capital and specialized cyber investors and business development skills, among young graduates with technical knowledge. The funding gap was already covered in the EIB presentation. Still, it was stressed that EIB could not act like private equity since they must keep political balance and, for example, support all member states equally. Concerning critical mass needed for cybersecurity specific incubators, there was an opinion expressed that, even if some member states might have this mass, others do not. Finally, it was also mentioned that the EU must be more receptive to talent coming from outside the EU.

José Ruiz Gualda from jtsec and the CONCORDIA startup community stressed the importance of choosing the best solution and not limiting the selection to the member states.

Some examples of services and functions that have been mentioned in the CONCORDIA startup community were also highlighted. Regarding gaps, one point where the future community could contribute, is to increase the credibility of startups, by organizing the EU and not MS champions.

Victoria Villanyi from ELTE addressed the entrepreneurship gap but also linked it to the cultural factors. In Hungary, for example, students prefer to work for a large company, so they often search for internships instead of taking risks.

Finally, Danilo D'Elia from ECSO presented several initiatives of this organization, such as a startup award and letter of intent to initiate dialogue on creating a cybersecurity-specific investment fund.

In the final round of questions, panelists addressed the future European Cybersecurity Competence Center and how it should act towards startups and small/medium enterprises. Besides addressing already mentioned gaps (funding, growth, territorial, and educational), the conclusion was that **the EU needs better, not more** in the cybersecurity startup and SME landscape and that everyone cannot be a champion.

3.4.4. Panel "Big vs. Small Industries: Approach to Cybersecurity"

The panel focused on better understanding the real-life context of how the European startups, SMEs, and large enterprises are approaching the cybersecurity challenges.

Despite a growing interest in cybersecurity in 2020, many startups and SMEs are not aware of the impact of cyber breaches and threats on their businesses. This lack of awareness was confirmed by independent statistics and the panel guests Georgiana and Christopher.

Some of the main challenges are:

- lack of awareness on the external threats and attacks (facing the pressure of business digitalization and the pandemic effects, the vast majority of SMEs is dealing with remote collaboration and embracing workforce mobility alternatives without a secure infrastructure);
- low cybersecurity literacy regarding the internal processes (quite often the startups and SMEs are meeting the cybersecurity challenge by fighting first with their employees, as the vast majority is not fully aware of the risks their organizations are facing when going online);
- low cybersecurity budgets (even in 2020, the SMEs decision-makers are considering cybersecurity as an IT issue, rather than an organizational governance issue and consequently, they are setting-up smaller budgets compared to the real needs);
- lack of designated resources (inadequate staff cannot support the necessary, increasing activities to preserve the businesses' cyber-integrity).

These challenges are encountered by large corporations as well, but on a different scale, as big enterprises' representatives confirmed.

There is still a strong need to further encourage the actions and impact of joint cybersecurity initiatives, such as the CONCORDIA project, where European academia and industry are working together to develop marketable research and innovations. **This synergy must be backed up by policy development, more consistent funding available for cybersecurity tech adoption and standardization measures**, which will boost the way cybersecurity

could become a significant pillar of the European innovation landscape with a concrete impact on society and businesses.

4. Conclusions

T4.6's main objective is to establish liaisons and collaborate closely with the relevant European stakeholders. We reached this objective in 2020 by extending our stakeholders' network to 297 members from about 165 different organizations, introducing a stakeholders' newsletter, and delivering a two-day event (COD2020) with 278 registrants from 28 European countries.

Activities in T4.6 were unfortunately affected by the COVID19 pandemic. In particular, we had to not hold the COD2020 event in Eastern Europe and move to a virtual event. Furthermore, official affiliations in the National cybersecurity coordination center Stakeholders' Group (NSG) were delayed, and we are now forecasting the consolidation of such a group in 2021.

However, T4.6 is directly contributing to several KPIs in CONCORDIA. COD2020 is already the second edition of the event series (KPI-DC-8: Organization of workshops and conferences. At least one major event and three satellite or special events). The stakeholders' groups, and especially the NSG, are increasingly aggregating European stakeholders to establish discussion and synergy (KPI-DC-9: Targeted focus groups with EU officials, policymakers, ECSO, and cPPP officials). Thanks to the OSG, six H2020 projects affiliated with CONCORDIA (KPI-DC-11: Liaisons with other projects: At least three (3) collaborations with projects in H2020).

The activities CONCORDIA is performing to link the cybersecurity stakeholders can be easily adapted to further accommodate the European strategy. The CONCORDIA Open Door events proved to be the right forum where stakeholders from different backgrounds can discuss cybersecurity, focusing on helping each other while helping Europe grow. This derived synergy among experts should be exploited into a lasting European community, to support the European Cybersecurity Competence Center and Network, as proposed by the European Commission. It is important to understand that different stakeholders have different interests in joining these events and meetings. It is important to individually address every class of stakeholders; on the other hand, it is fundamental to find an optimal approach that can get the most from them, which cannot be simplistic. T4.6 activities, such as stakeholders' newsletters, a combination of panels and presentations in COD, and focused discussion groups, are attempting such an optimal resolution.

Our plan for 2021 is to extend our stakeholders’ network further and have a first meeting with the NSG. COD2021 will be again a live or a hybrid event, if the conditions allow it, even if a current trend is to always allow for virtual participation of those who cannot be present in person.

Acronyms

CA	Consortium Agreement
COD	CONCORDIA Open Door
DoA	Description of Action
EC	European Commission
EU	European Union
GA	Grant Agreement
LSG	Liaison Stakeholders Group
MS	Member State
NSG	National Cybersecurity Competence Centres and Agencies Stakeholders Group
OSG	Observer Stakeholders Group
WP	Work package

Appendices

A Descriptions of the stakeholders' groups

NSG

CONCORDIA

Cyber security cOmpeteNce FOr Research anD Innovation

CONCORDIA NSG

The National Cybersecurity Competence Centres and Agencies Stakeholders Group

Introduction

Cybersecurity does not offer the luxury to be just a localized national interest concern. The inter-linked digital world necessitates a community solution. In this context, CONCORDIA1 is developing an EU-wide Cybersecurity community and matching ecosystem to exchange and collate EU competences to become a potent coordinated force to address current and upcoming cyber threats at the EU level.

For this, a (draft) regulationi is proposed to strengthen the (development, build-up and deployment of) competitiveness and capacities in cybersecurity at EU and national level, and support research to facilitate and accelerate standardisation and certification processes, this all while reducing digital dependence.

In lieu of the above, a key objective for CONCORDIA is to inclusively and comprehensively engage diverse competencies/stakeholders to result in a high-impact EU-wide Cybersecurity ecosystem. Recognizing that different stakeholders (national or institutional) represent different levels of competencies and with associated differing levels of engagement, CONCORDIA has established dedicated processes to engage the initial set (to be expanded as needed) of stakeholders to the consortium as:

A. The National Cybersecurity Coordination Centres and Agencies Stakeholders Group (NSG);
B. The Liaison Stakeholders Group (LSG), and;
C. The Observer Stakeholders Group (OSG).

The Purpose of NSG

The NSG concerns current, upcoming and future National Cybersecurity Coordination Centres ('NCCCs') in each member state, including the discrete National Cybersecurity Competence Centres and Agency that currently exist in the individual member states. The purpose of the NSG is support the development of the proposed network (including both the NCCCs and the Cybersecurity Competence Community) including without limitation interconnecting existing, developing or to be developed ecosystem in and across the member states with the other stakeholders of this evolving network.

Based on the (draft) Regulation, and recognizing that cybersecurity is a broad dimension where various domains and stakeholders – also within the various public sector perspectives in each member state and the European Union – should be identified in order to enable and facilitate each member state to work on, build and foster cybersecurity capabilities, competences and sources, in consultation with the Commission we have made the distinction between four (4) main domains:

[1] https://www.concordia-h2020.eu/

CONCORDIA project receiving funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 830927.

A. Sovereignty, CERT & NIS;
B. Economic Development & Competition;
C. Research & Innovation, and;
D. Education & Skills.

The NSG is envisioned to have three main tasks, based on the main mission to help build a platform for trustworthy exchange of ideas, approaches, topics of joint actions and collaborations:

1. Build and maintain a trusted zone of dialogue and collaboration, including without limitation sharing, develop and sustain good practices and other information regarding the various objectives of each NCCC, the network, the proposed Regulation, and the Cybersecurity Atlas, including without limitation mapping common state of play and state of the art and addressing relevant gaps;
2. Discuss how to coordinate, operationalize and sustain the various domains set forth above within scope of the proposed Regulation, including addressing both the numerous engagements as well as preconditions, also with the aim to add to the actual functioning of the Cybersecurity Competence Community of which NCCCs will become part of;
3. Cooperate in the field of cybersecurity innovation, research, economic and societal implications encouraging cross-borders and other collaboratives programs, projects and event-driven developments

Participation

The NSG is an invite-only Stakeholders Group.
CONCORDIA, also under the suggestions of the EC, will invite national entities to join the NSG and where relevant a specific domain.

During the membership process we would request you to sign the form attached to this document to become officially part of the NSG.

We envision the stakeholders groups to primarily communicate via electronic means. The periodic meeting (as agreed by the members with a maximum of twice a year) will be coordinated by CONCORDIA with an invitation to attend the yearly physical meeting organized by CONCORDIA for all the stakeholders groups. We are looking forward to engaging.

[i] https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2018/0328(COD)&l=en. EUR-Lex status quo: https://eur-lex.europa.eu/procedure/EN/2018_328. Proposal 2018/0328 (COD): https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-centres-regulation-630_en.pdf. Commission Staff Working Paper to 2018/0328 (COD): https://ec.europa.eu/transparency/regdoc/rep/10102/2018/EN/SWD-2018-403-F1-EN-MAIN-PART-1.PDF

CONCORDIA project receiving funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 830927.

LSG

CONCORDIA LSG

The Liaisons Stakeholder

Introduction

Cybersecurity does not offer the luxury to be just a localized national interest concern. The inter-linked digital world necessitates a community solution. In this context, CONCORDIA[1] is developing an EU-wide Cybersecurity community and matching ecosystem to exchange and collate EU competences to become a potent coordinated force to address current and upcoming cyber threats at the EU level.

For this, a (draft) regulation[i] is proposed to strengthen the (development, build-up and deployment of) competitiveness and capacities in cybersecurity at EU and national level, and support research to facilitate and accelerate standardisation and certification processes, this all while reducing digital dependence.

In lieu of the above, a key objective for CONCORDIA is to inclusively and comprehensively engage diverse competencies/stakeholders to result in a high-impact EU-wide Cybersecurity ecosystem. Recognizing that different stakeholders (national or institutional) represent different levels of competencies and with associated differing levels of engagement, CONCORDIA has established dedicated processes to engage the initial set (to be expanded as needed) of stakeholders to the consortium as:

A. The National Cybersecurity Coordination Centres Stakeholder Group (NSG);
B. The Liaison Stakeholder Group (LSG), and;
C. The Observer Stakeholder Group (OSG).

The Purpose of LSG

The purpose of LSG is to engage European institutions such as for instance potentially the European Union Agency for Cybersecurity (ENISA), the European Defence Agency (EDA), the Europol or European Central Bank (ECB), World Economic Forum (WEF) and the Munich Security Conference (MSC) and others for coordinated coverage across such European agencies. These institutions are involved in cybersecurity issues from different perspectives of policy, governance and financial oversight among others.

The main mission of the LSG is support the development of the proposed network (including both the National Cybersecurity Coordination Centres ('NCCCs') and Cybersecurity Competence Community) including without limitation interconnecting existing, developing or to be developed ecosystem in and across the member states with the other stakeholders of this evolving network. The LSG will focus on the Cybersecurity Competence Community.

Based on the (draft) Regulation, and recognizing that cybersecurity is a broad dimension where various domains and stakeholders – also within the various sectors' perspectives in each member state and the European Union – should be identified in order to enable

[1] https://www.concordia-h2020.eu/

CONCORDIA project receiving funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 830927.

and facilitate each member state to work on, build and foster cybersecurity capabilities, competences and sources, in consultation with the Commission we have made the distinction between four (4) main domains:

A. Sovereignty, CERT & NIS;
B. Economic Development & Competition;
C. Research & Innovation, and;
D. Education & Skills.

The LSG is envisioned to have three main task, based on the main mission to help build a platform for trustworthy exchange of ideas, approaches, topics of joint actions and collaborations:

1. Build and maintain a trusted zone of dialogue and collaboration, including without limitation sharing, develop and sustain good practices and other information regarding the various objectives of the Cybersecurity Competence Community, the network, the proposed Regulation, and the public Cybersecurity Atlas, including without limitation mapping common state of play and state of the art and addressing relevant gaps;

2. Discuss how to coordinate, operationalize and sustain the various domains set forth above within scope of the proposed Regulation, including addressing both the numerous engagements as well as preconditions, also with the aim to add to the actual functioning of the Cybersecurity Competence Community of which the respective liaisons may or swill become part of;

3. Cooperate in the field of cybersecurity innovation, research, economic and societal implications encouraging cross-borders and other collaboratives programs, projects and event-driven developments.

Participation

The LSG is an invite-only Stakeholder Group. CONCORDIA, also under the suggestions of the EC and our NSG members, will invite organisations to join the LSG and where relevant a specific domain.

During the membership process we would request you to sign the form attached to this document to become officially part of the LSG.

We envision the stakeholder groups to primarily communicate via electronic means. The periodic meeting (as agreed by the stakeholder members with a maximum of twice a year) will be coordinated by CONCORDIA with an invitation to attend the yearly physical meeting organized by CONCORDIA for all the stakeholder groups. Only public information will be made available. We are looking forward to engage.

[i] https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2018/0328(COD)&l=en. EUR-Lex status quo: https://eur-lex.europa.eu/procedure/EN/2018_328. Proposal 2018/0328 (COD): https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-centres-regulation-630_en.pdf. Commission Staff Working Paper to 2018/0328 (COD): https://ec.europa.eu/transparency/regdoc/rep/10102/2018/EN/SWD-2018-403-F1-EN-MAIN-PART-1.PDF

CONCORDIA project receiving funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 830927.

OSG

CONCORDIA OSG

The Observer Stakeholders Group

Introduction

Cybersecurity does not offer the luxury to be just a localized national interest concern. The inter-linked digital world necessitates a community solution. In this context, CONCORDIA[1] is developing an EU-wide Cybersecurity community and matching ecosystem to exchange and collate EU competences to become a potent coordinated force to address current and upcoming cyber threats at the EU level.

For this, a (draft) regulation[i] is proposed to strengthen the (development, build-up and deployment of) competitiveness and capacities in cybersecurity at EU and national level, and support research to facilitate and accelerate standardisation and certification processes, this all while reducing digital dependence.

In lieu of the above, a key objective for CONCORDIA is to inclusively and comprehensively engage diverse competencies/stakeholders to result in a high-impact EU-wide Cybersecurity ecosystem. Recognizing that different stakeholders (national or institutional) represent different levels of competencies and with associated differing levels of engagement, CONCORDIA has established dedicated processes to engage the initial set (to be expanded as needed) of stakeholders to the consortium as:

A. The National Cybersecurity Coordination Centres and Agencies Stakeholders Group (NSG);
B. The Liaison Stakeholders Group (LSG), and;
C. The Observer Stakeholders Group (OSG).

The Purpose of OSG

The OSG concerns current, upcoming and future stakeholders of the Cybersecurity Competence Community, not being national governmental bodies (who generally will be part of the NSG) or European institutions (who generally will be part of the LSG).

The purpose of the OSG is to support the development of the proposed network (including both the National Cybersecurity Coordination Centres ('NCCCs') and Cybersecurity Competence Community) including without limitation interconnecting existing, developing or to be developed ecosystem in and across the member states with the other stakeholders of this evolving network. The OSG will focus on the Cybersecurity Competence Community.

Based on the (draft) Regulation, and recognizing that cybersecurity is a broad dimension where various domains and stakeholders – also within the various sectors' perspectives in each member state and the European Union – should be identified in order to enable and facilitate each member state to work on, build and foster cybersecurity capabilities,

[1] https://www.concordia-h2020.eu/

CONCORDIA project receiving funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 830927.

competences and sources, in consultation with the Commission we have made the distinction between four (4) main domains:

A. Sovereignty, CERT & NIS;
B. Economic Development & Competition;
C. Research & Innovation, and;
D. Education & Skills.

The OSG is envisioned to have three main tasks, based on the main mission to help build a platform for trustworthy exchange of ideas, approaches, topics of joint actions and collaborations:

1. Build and maintain a trusted zone of dialogue and collaboration, including without limitation sharing, develop and sustain good practices and other information regarding the various objectives of the Cybersecurity Competence Community, the network, the proposed Regulation, and the public Cybersecurity Atlas, including without limitation mapping common state of play and state of the art and addressing relevant gaps;

2. Discuss how to coordinate, operationalize and sustain the various domains set forth above within scope of the proposed Regulation, including addressing both the numerous engagements as well as preconditions, also with the aim to add to the actual functioning of the Cybersecurity Competence Community of which the respective liaisons may or swill become part of;

3. Cooperate in the field of cybersecurity innovation, research, economic and societal implications encouraging cross-borders and other collaboratives programs, projects and event-driven developments.

Participation

The OSG is an invite-only Stakeholder Group. CONCORDIA, also under the suggestions of the EC and our NSG members, will invite organisations to join the OSG and where relevant a specific domain.

During the membership process we would request you to sign the form attached to this document to become officially part of the OSG.

We envision the stakeholder groups to primarily communicate via electronic means. The periodic meeting (as agreed by the stakeholder members with a maximum of twice a year) will be coordinated by CONCORDIA with an invitation to attend the yearly physical meeting organized by CONCORDIA for all the stakeholder groups. Only public information will be made available. We are looking forward to engaging.

[i] https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2018/0328(COD)&l=en. EUR-Lex status quo: https://eur-lex.europa.eu/procedure/EN/2018_328. Proposal 2018/0328 (COD): https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-centres-regulation-630_en.pdf. Commission Staff Working Paper to 2018/0328 (COD): https://ec.europa.eu/transparency/regdoc/rep/10102/2018/EN/SWD-2018-403-F1-EN-MAIN-PART-1.PDF

CONCORDIA project receiving funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 830927.