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 D4.9: 3rd year report on Liaison with Stakeholders

**Abstract:** This document describes CONCORDIA's activities related to the establishment of liaisons with cybersecurity stakeholders in Europe during Year 3 of the project. The CONCORDIA newsletters have been delivered quarterly. The stakeholders' groups are growing, especially the NSG counts now 14 members in the NSG from 11 EU member states (Austria, Cyprus, Czech Republic, Germany, Greece, Italy, Luxembourg, the Netherlands, Romania, Spain, and Sweden). The CONCORDIA Open Door event 2021 was successfully delivered as an online event (due to the pandemic situation) counting 193 registrants, of which 100 were from non-Concordia partner organizations.

| | |
|---|---|
| Contractual date of delivery | *M36* |
| Actual date of delivery | *22.12.2021* |
| Deliverable dissemination level | *Public* |
| Editors | *Antonio Ken Iannillo* |
| Contributors | *SnT* |
| Quality assurance | • *Dimitra Stefanatou (Arthur's Legal)*<br>• *Filipe Campos (EFACEC)*<br>• *Christos Papachristos (FORTH) (review lead)*<br>*Stefan Katzenbeisser (University of Passau)* |

[†] 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 |
| SURF | SURF 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 BV. | 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~~ |
| NCSA | Ministry of Digital Governance - National Cyber | Greece |

| | | |
|---|---|---|
| | Security Authority | |
| 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 |
| FER | University of Zagreb, Faculty of Electrical Engineering and Computing | Croatia |

# Document Revisions & Quality Assurance

**Internal Reviewers**

1. Christos Papachristos (FORTH) (review lead)
2. Dimitra Stefanatou (Arthur's Legal)
3. Filipe Campos (EFACEC)
4. Stefan Katzenbeisser (University of Passau)

**Revisions**

| Ver. | Date | By | Overview |
|---|---|---|---|
| *0.1* | *12/11/2021* | *Antonio Ken Iannillo* | *First Draft* |
| *0.2* | *7/12/2021* | *Antonio Ken Iannillo* | *Advanced Draft* |
| *1.0* | *15/12/2021* | *Antonio Ken Iannillo* | *Final Version* |
| | | | |

# Executive Summary

Work Package 4 (WP4) is named *Policy and the European Dimension* and EIT Digital leads it. 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. For the 3rd year of the project, deliverable D4.9 (this document, 3rd year report on the liaison with stakeholders) reports the output of this task.

In the third year of CONCORDIA, the T4.6 team expanded CONCORDIA's pool of stakeholders. In 2021, T4.6 kept issuing the stakeholders' newsletters, one every three months. The CONCORDIA network, regularly receiving this newsletter, consists of 549 members from 270 different organisations. Furthermore, T4.6 held the first meeting of the NSG (National Cybersecurity Competence Centres and Agencies Stakeholders Group) with 32 participants from 14 member states. T4.6 also simplified the process to join the OSG (Observer Stakeholders Group), reaching 63 people from 57 organisations.

The T4.6 team organised the third event of the CONCORDIA Open Door series, namely COD2021, as a virtual event due to the COVID-19 pandemic. 100 out of 193 registrants were from organisations that are not part of the CONCORDIA consortium.

Regarding the stakeholders' type:

- 26 registrants were from national authorities, national agencies, or national public entities;
- 12 registrants were from European authorities, European agencies, or European public entities;
- 90 registrants were from companies;
- 65 registrants were from universities or research centres.

Regarding gender distribution, 130 registrants were male while 63 were female, 67% male against 33% female.

# Contents

# 1. Introduction

WP4 has the following objectives:

- Create and operationalise 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;
- Formalise the research and other outcomes into a Cybersecurity Roadmap for Europe;
- Surface the necessity to address the social aspects linked to the effective operationalisation 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 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 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, T4.6 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.

During the second year, T4.6 faced the current pandemic and noted a substantial slow-down in the stakeholders' organisations' bureaucratic processes. The virtualisation of the meetings, including COD2020, had its advantages: significant expansion of the network and more meaningful feedback for the CONCORDIA consortium.

While initially aiming for a physical, or at least hybrid, Open Door event in 2021, the event was eventually held remotely, due to COVID restrictions in different member states, including Romania, which was supposed to be the COD2021 hosting country. COD2021 was held virtually with a reduced audience than the 2020 edition but with more offline interactions (i.e. through the CONCORDIA YouTube channel[1]).

[1] https://www.youtube.com/c/CONCORDIAH2020

## 1.2. Structure of the Document

Chapter 2 presents the updates for each service in the service catalogue. Chapter 3 presents COD2021, including its planning activities, its program, and its results. Chapter 4 consists of final remarks on the overall year and a plan for T4.6's activities in 2022. The appendix contains the program of COD2021.

# 2. CONCORDIA Service Catalogue

CONCORDIA's primary interface with external stakeholders is its service catalogue, presented in a previous deliverable[2]. The service catalogue of CONCORDIA is modelled as a path-to-follow to become a "booster" of cybersecurity competencies for Europe and strengthen the European digital sovereignty on this matter.

All the deliverables referred to in this document are available on the project's website[3].

## 2.1. Notitia Level

The *Notitia* level is the first level of the catalogue. 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 organisations and individuals. While the main activities on social media are carried by T5.2 (Dissemination and Communication Activities) and presented in deliverable D5.4, task 4.6 released four **stakeholders' newsletters** in March 2021, June 2021, September 2021, and December 2021. All the issues are also available online at https://www.concordia-h2020.eu/concordia-service-cybersecurity-updates/.

The newsletter has the same objectives as T4.6: present CONCORDIA's results to stakeholders and request feedback on CONCORDIA's activities. Starting from September 2021, the PECS-UP community newsletter merged with the stakeholders' newsletter.

When writing this document, the CONCORDIA mailing list contains 549 members from 270 different organisations (large companies, national and European entities, SMEs, research centres, financing bodies, and more). Figure 1 shows the distribution of these stakeholders across Europe. There is a stakeholder for each member state except Malta and Slovakia. 257 stakeholders belong to international organisations, and they were not associated with any member state in Figure 1.

### 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. It lists 90 experts, and T4.6 is opening discussion with EU CyberNet[4], another European project that provides a similar service, to merge our efforts in creating such a pool for the European community. We may also explore a possible linking of the experts in the CONCORDIA website with the ATLAS EC system that has been developed deployed and supported by the JRC team.

[2] 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
[3] https://www.concordia-h2020.eu/deliverables/.
[4] https://www.eucybernet.eu/about-project.

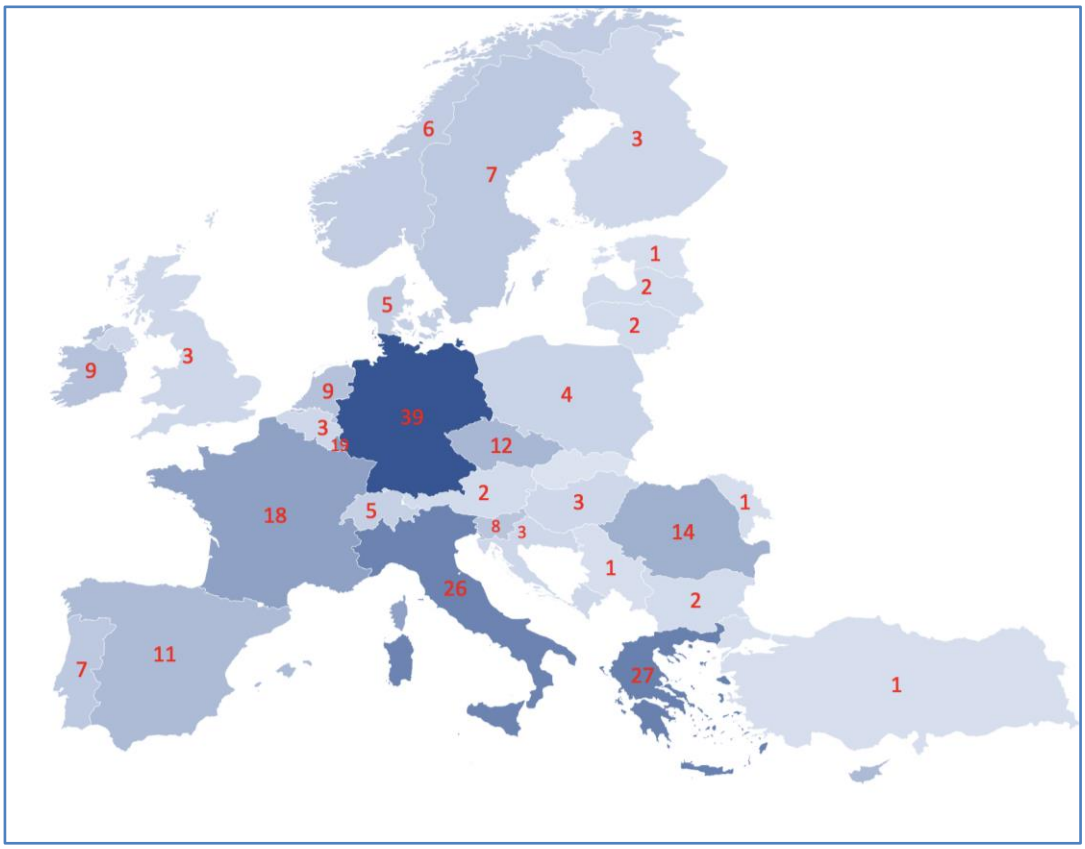



Figure 1: Members of the stakeholders' mailing list, or CONCORDIA stakeholders' network, split by country of origin (46 stakeholders are not considered in this visual analysis because it was not possible to extract the country of origin).

### 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 organisations and individuals can be updated on the latest scientific progress in the cybersecurity landscape. In 2021, CONCORDIA published and made available 71 publications at https://www.concordia-h2020.eu/concordia-service-cybersecurity-research/. Further details are in Deliverable D1.3 (3rd 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 organisations 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 provides organisations and individuals information about cybersecurity courses, training, and cyber ranges in Europe. This service corresponds to 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 D3.3 (3rd-year report on community building and sustainability). The service is available at https://www.concordia-h2020.eu/concordia-service-cybersecurity-skills/.

### 2.1.6. Women in Cybersecurity

The "Women in Cybersecurity" service aims to provide organisations and individuals information about CONCORDIA activities on promoting workforce diversity in the field of cybersecurity. It corresponds to activities in T4.5 (Women in Cybersecurity). The service is available at https://www.concordia-h2020.eu/concordia-service-women-in-cybersecurity/.

### 2.1.7. Cybersecurity Tools

The "Cybersecurity Tools" service aims to provide organisations and individuals with 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 50 tools available at https://www.concordia-h2020.eu/concordia-service-cybersecurity-tools/.

### 2.1.8. Career Opportunities

The "Career Opportunities" service aims to provide organisations and individuals information about open positions in academia and industry for cybersecurity-related jobs. Seven CONCORDIA partners published 18 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 provides new-born and growing organisations (such as startups) guidance to develop and implement business models. It corresponds to activities in task T3.5 (Community Building, Support, and Incentive Models) presented in deliverable D3.3 (3rd-year report on community building and sustainability). The service is available at https://www.concordia-h2020.eu/concordia-service-start-up-guidance/.

### 2.1.10. Instruments Guidance

The "Instruments Guidance" service provides organisations technical, legal, and economic guidance to design and implement new cybersecurity policies. It corresponds to activities in WP4 (Policy and the European Dimension), but no external stakeholders specifically asked for this service. The service is available at https://www.concordia-h2020.eu/concordia-service-intruments-guidance/.

## 2.2. Pacta Level

The *Pacta* level is the second level of the catalogue. 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 organisations and individuals with a way to promote their courses, training, cyber ranges, tools, and open positions on the CONCORDIA website. T4.6 dispatched this kind of requests to the task T3.4 team (Establishing a European Education Ecosystem for Cybersecurity). The service is available at https://www.concordia-h2020.eu/concordia-service-promotion-pact/.

### 2.2.2. Research Pact

The "Research Pact" service aims to provide academic organisations with a way to engage with CONCORDIA partners and start research collaboration. Deliverable D1.3 (3rd year report on designing a European Secure, Resilient, and Trusted Ecosystem) provides further details. The service is available at https://www.concordia-h2020.eu/concordia-service-research-pact/.

### 2.2.3. Industrial Pact

The "Industrial Pact" service aims to provide industrial organisations with a way to engage with CONCORDIA partners and start a collaboration. Deliverable D6.6 (3rd year management report) provides further details. The service is available at https://www.concordia-h2020.eu/concordia-service-industry-pact/.

### 2.2.4. Community Pact

The "Community Pact" service aims to provide organisations with a way to engage with CONCORDIA partners and start a discussion on cybersecurity-related topics. The service is available at https://www.concordia-h2020.eu/concordia-service-community-pact/.

Last year T4.6 launched three stakeholder groups:

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

A previous deliverable (D4.8) reports the three group descriptions (as distributed to potential members).

In 2021, T4.6 reached 14 members in the NSG from 11 EU member states (Austria, Cyprus, Czech Republic, Germany, Greece, Italy, Luxembourg, the Netherlands, Romania, Spain, and Sweden). Last year, NSG consisted of only 5 members from 5 country.

On the 21st of April 2021, T4.6 held the first meeting of the NSG. 31 participants from 14 EU Member states (Austria, Croatia, Cyprus, Czech Republic, Finland, Germany, Greece, Italy, Luxembourg, Romania, Slovenia, Spain, Sweden, the Netherlands) and 2 participants from Norway (as EEA country) joined the meeting. The meeting was moderated by Arthur van der Wees (Arthur's Legal) that proposed to each of the participants two main questions:

1. **What would you expect from this group (NSG), CONCORDIA, and the European cybersecurity community? What would you like to contribute?**

**Consider the following four perspectives (at your discretion, you can address one or two):**
   a. **Digital Sovereignty;**
   b. **Economic Development & Competition;**
   c. **Research & Innovation, and;**
   d. **Education & Skills.**

2. **What would your 'top 3' priorities in cybersecurity and related domains that the European society should focus on (short term, mid-term, or longer-term)?**

While for the first question, T4.6 received similar answers from the participants that showed interest in all the four domains, T4.6 noted interesting priorities for the second one. The focus areas as per April 2021 are:

- Functional capacity building and operation;
- Digital sovereignty;
- Trusted and trustworthy information sharing;
- Societal cybersecurity awareness, training, and accountable behaviour;
- Situational awareness and scenario plotting;
- Cybercrime fighting and cyber defence;
- Education, skills, training and jobs;
- Building Interdisciplinary NCC, community, and ecosystems;
- Reinforce cybersecurity (SME) industries, (PPP) research and innovation;
- Building secure trusted digital infrastructure;
- Building societal trust and collaborative resilience;
- Implementation of risk-based standards.

Then, the participants were presented (offline via email) with the preliminary version of the CONCORDIA *Cybersecurity Roadmap for Europe*[5], with links between the roadmap's chapters and the afore-mentioned priorities. T4.6 envisions to have further interactions in the course of 2022 to discuss any more advanced version of the roadmap and of the priorities captured therein.

Regarding the OSG, T4.6 realised that a lighter onboarding process was necessary. T4.6 established a simple form[6] where a representative of the organisations can register by specifying the topic of interest. These labels will target specific subgroups of the OSG while organising CONCORDIA workshops on a well-defined topic. So far, OSG has 63 people from 57 organisations (last year, OSG had only 7 affiliations).

Information on the community pact and the stakeholders' group can also be found in deliverable D6.6 (3rd year management report).

## 2.3. CONCORDIA Level

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

[5] https://www.concordia-h2020.eu/roadmap/
[6] https://www.concordia-h2020.eu/observers-stakeholder-group-osg-registration/

### 2.3.1. CONCORDIA Partnership

The "CONCORDIA Partnership" service aims to provide organisations with a means to join the CONCORDIA consortium as a full partner. In 2021, two new partners joined CONCORDIA consortium, namely, the University of Zagreb (FER) and Innovation Center Nikola Tesla (ICENT) from Croatia. They will represent a new Member State in the consortium (no previous member is from Croatia), chosen due to their expertise and activities in cybersecurity. CONCORDIA is now a consortium of 54 partners from 21 European countries (17 member states, 3 Horizon 2020 associated countries, and UK).

# 3. CONCORDIA Open Door Event 2021

The CONCORDIA Open Door (COD) event series brings a significant number of cybersecurity stakeholders in a single event, and it provides an environment to fulfil the goals of task T4.6 (Liaison with stakeholders). This series aims to connect all the cybersecurity stakeholders to create valuable exchanges between academia, industry, public bodies, and policymakers.

The specific objective of COD2021 was to deliver a networking event that could bring together different sub-groups of the European cybersecurity community despite the pandemic situation and the limitation of virtual events.

## 3.1. Organisation

At the beginning of the year, T4.6 selected BitDefender among CONCORDIA's partners as a local host to organise COD2021 in Bucharest due to the impossibility to host it in 2020. After the first quarter of 2021, it was clear that a purely physical event was not possible due to the ongoing pandemic. Thus, T4.6 decided to make COD2021 a hybrid event meaning that participants could join the physical event in Romania or watch it online through a streaming platform.

Once again, T4.6 chose the *Tame* platform[7] 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.

Unfortunately, in September 2021, Romania was hit by another wave of COVID cases and due to the restrictions that followed, COD2021 had to be essentially held solely remotely.

## 3.2. Program

COD2021 took place on the 20th and 21st of October, during the European Cybersecurity Month[8]. The selected topics were "Cybersecurity Threats and Certification" on the first day and "European Cybersecurity Competence Centre and the Community" on the second day. Each day started with a keynote to introduce the topic, continued with two panels, and ended with a brief demo of two CONCORDIA outputs. On the first day, it also hosted the Women's Awards Ceremony. In the appendix, Figures 3 and 4 illustrate the program, including the speakers' names and affiliations.

## 3.3. Registrations

COD2021 opened registration on the 6th of September 2021 and counted 193 registrations. Figure 4 demonstrates the diversity of COD2021 registrants in Europe. Overall, 100 out of 193 registrants were from organisations that are not part of the CONCORDIA consortium.

[7] https://tame.events/
[8] 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

More specifically:

- 26 registrants were from national authorities, national agencies, or national public entities;
- 12 registrants were from European authorities, European agencies, or European public entities;
- 90 registrants were from companies;
- 65 registrants were from universities or research centres.

Regarding the gender distribution, 130 registrants were male while 63 were female, meaning that 67% of the participants were male, where 33% were female.

Notably, a participation in this year's event was decreased compared to COD2020. The decreased level of participation could be due to the pandemic situation as well as due to the nature of virtual events. In this respect, even before the event, T4.6 received several emails asking whether the videos of the event would be available online after the event itself. Other requests arrived after the events. Thus, only part of the community joined the live event because it was willing to interact with the speakers and panelists. Most of them were only interested in the content of the sessions and exploited the virtuality of COD2021.

## 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 CONCORDIA's YouTube channel[9].

### 3.4.1. Panel "Bridging the gap between next generation cybersecurity, cloud edge system, and machine learning/artificial intelligence"

The discussion panel had representatives of ENISA, CONCORDIA's task 4.1 (Working group in technology domains of interest), Bitdefender, and STMicroelectronics. The topic was the cybersecurity gaps and challenges when cloud-edge systems meet big data, machine learning, and artificial intelligence. It focused on how current cybersecurity approaches are expected to evolve to support this novel ecosystem with security and privacy requirements in mind.

The main notable takeaways can be summarised as follows:

- Technology is moving into a world with substantial pipelines where the computations are distributed on devices at the edge of the network.
- Machine learning models became the target of many attacks because they are the core of many autonomous systems.
- There is a need for machine learning methods to fight cybersecurity attacks because there may be up to tens of thousands of malicious events per hour that are impossible for a human to handle.
- A big issue is still the presence of software vulnerabilities because it is challenging to write a device software that is protected by any kind of attacks.
- Practitioners must assume zero trust and implement continuous verification of both collected data and corresponding data sources.

[9] https://www.youtube.com/concordia-h2020

- There is a need for new certification techniques for environments that have no fixed topology and are based on non-deterministic behaviours.
- On-chip AI/ML is the new frontier of edge systems and hardware vendors.

### 3.4.2. Panel "Cybersecurity Product Certification - insights, challenges, and ways forward"

Cybersecurity Certification is mandated by the EU CSA for ICT products, Services and Processes. During this panel discussion, there was the opportunity to exchange ideas regarding Cybersecurity Certification from different perspectives. ECSO presented the various developments from a policy perspective and the ongoing work about the Cybersecurity Certification of ICT products. CYRENE project introduced a novel cybersecurity certification scheme developed to address the cybersecurity certification of supply chain services. CETIC presented how standard criteria and DevOps should be integrated to bypass some of the obstacles imposed by ICT products' current methodologies and certification schemes. TÜV Trust IT explained the process of testing and certification from the practical viewpoint of a Lab and Certification Body, with a focus on IoT certification.

All panelists commented on the obstacles and challenges regarding cybersecurity certification and presented their next steps.

The main notable takeaways can be summarised as follows:

- There are many standards that, if used (as a basis) in certification, would lead to a multitude of certification schemes and labels that would fragment and confuse the market. For each specific case, there should be a consensus on the standard to be acknowledged and used for implementation as a basis for certification.
- The work regarding the first cybersecurity certification schemes is still ongoing. Important decisions should be made regarding the schemes and their functioning before the market can utilise them.
- There is an astonishing amount of certification schemes to be developed, stakeholders should be involved, and the processes expedited to cover the market's needs.
- Several topics need to be addressed in the emerging schemes, including how the testing/inspection/auditing is to be carried out because of changes and updates to the product, service, or process.
- When talking about cybersecurity certification of ICT products, it should be considered that processes are a part of the development and should be incorporated in the certification schemes.
- An organisation may use several suppliers to facilitate the provisions of a process or service. This supply chain has an immediate effect on cybersecurity and should be taken into consideration.
- IoT standardisation and certification should be considered in the near future.

### 3.4.3. Panel "How can the community help the ECCC"

The panel was introduced by Mr. Miguel GONZALES-SANCHO from the European Commission and temporary director of the European Cybersecurity Competence Center that opened the second day of COD2021 by presenting the ECCC. The panel consisted of representatives from the European Commission, CONCORDIA, the Swedish Civil Contingencies Agency, the German Federal Office for Security in Information Technology,

and the Romanian National Cyber Security Directorate discussing the relationships between the ECCC, the network of a national coordination centre, and the community.

The main notable takeaways can be summarised as follows:

- The ECCC needs input from the community, such as creative ideas and stakeholders' views for the investment priorities.
- It's essential to connect to create a fast information loop between the coordination centres and the communities (provide a communication platform).
- The community needs to know what the framework of the debates with the ECCC is.
- The community should have a balance of supply and demand-side.
- To be part of the community is a commitment to cooperation.

### 3.4.4. Panel "Code of Engagement for the Trusted Threat Intelligence Sharing Platform"

The panel discussion focused on the Code of Engagement (CoE) for the Trusted Threat Intelligence Sharing Platform, drafted by legal partner of CONCORDIA (Arthur's Legal) with the support of CONCORDIA technical partners, responsible for the actionable components of CONCORDIA Platform, namely, MISP, ICH-CH and DDoS-CH .

In terms of main notable takeaways, considering the challenge to share data in the first place and to define workflows and policies even within the CONCORDIA community and, certainly, beyond, the discussion highlighted the necessity for a dynamic framework of principle-based arrangements that would be easy for the community of cybersecurity stakeholders to read, understand, and commit to. In this context, the CoE aims to create a reliable framework for data sharing pertinent to threat intelligence sharing, initially addressed to CONCORDIA partners. It is envisioned that CoE is taken up by other cybersecurity stakeholders beyond CONCORDIA consortium, therefore, creating an impact even after the end of CONCORDIA.

The latest stable version of CoE will become publicly available as part of D4.3: 3rd Year Report on the Threat Landscape, due in December 2021.

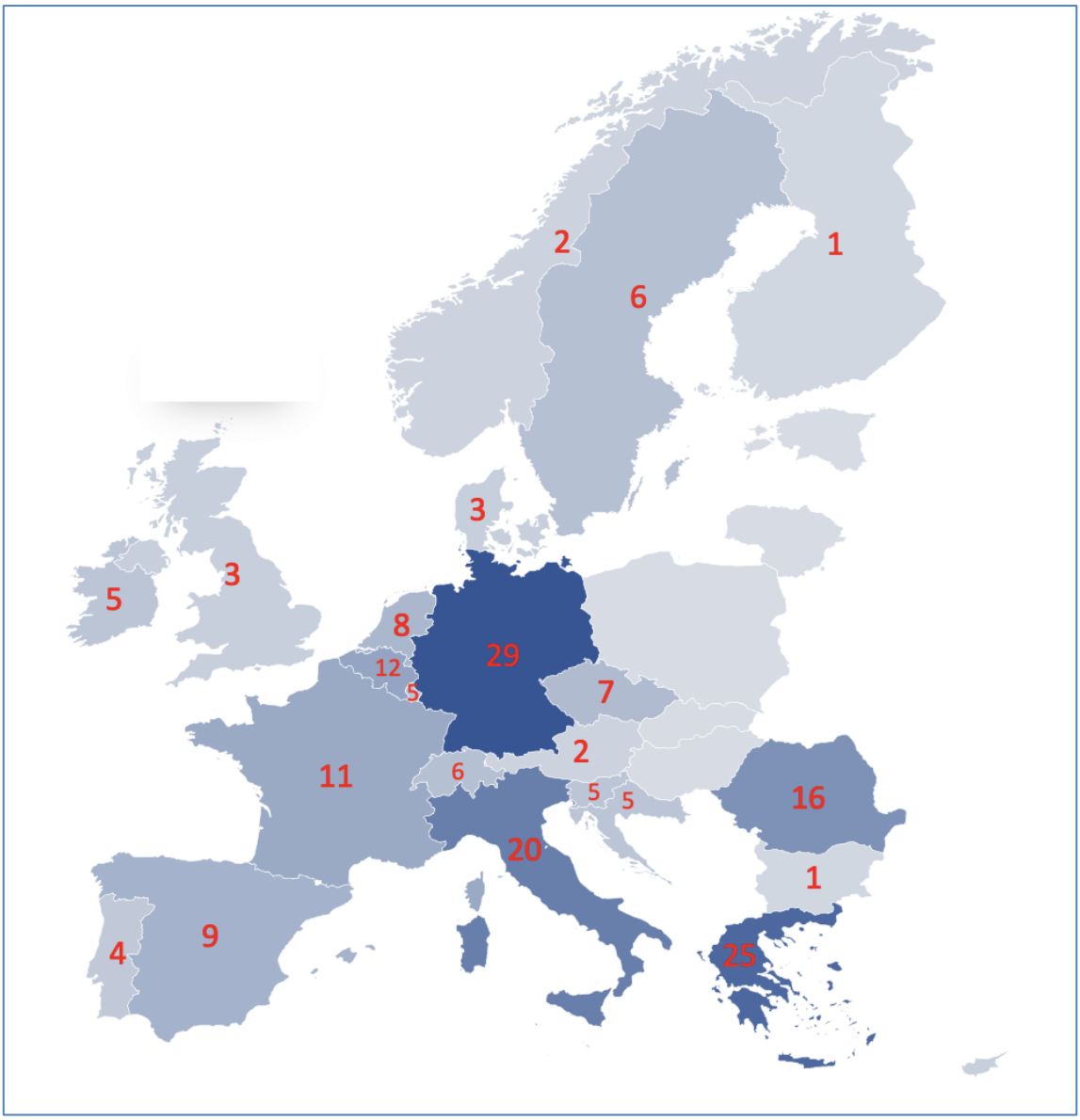



Figure 2: Distribution of COD2021 registrants

# 4. Conclusions

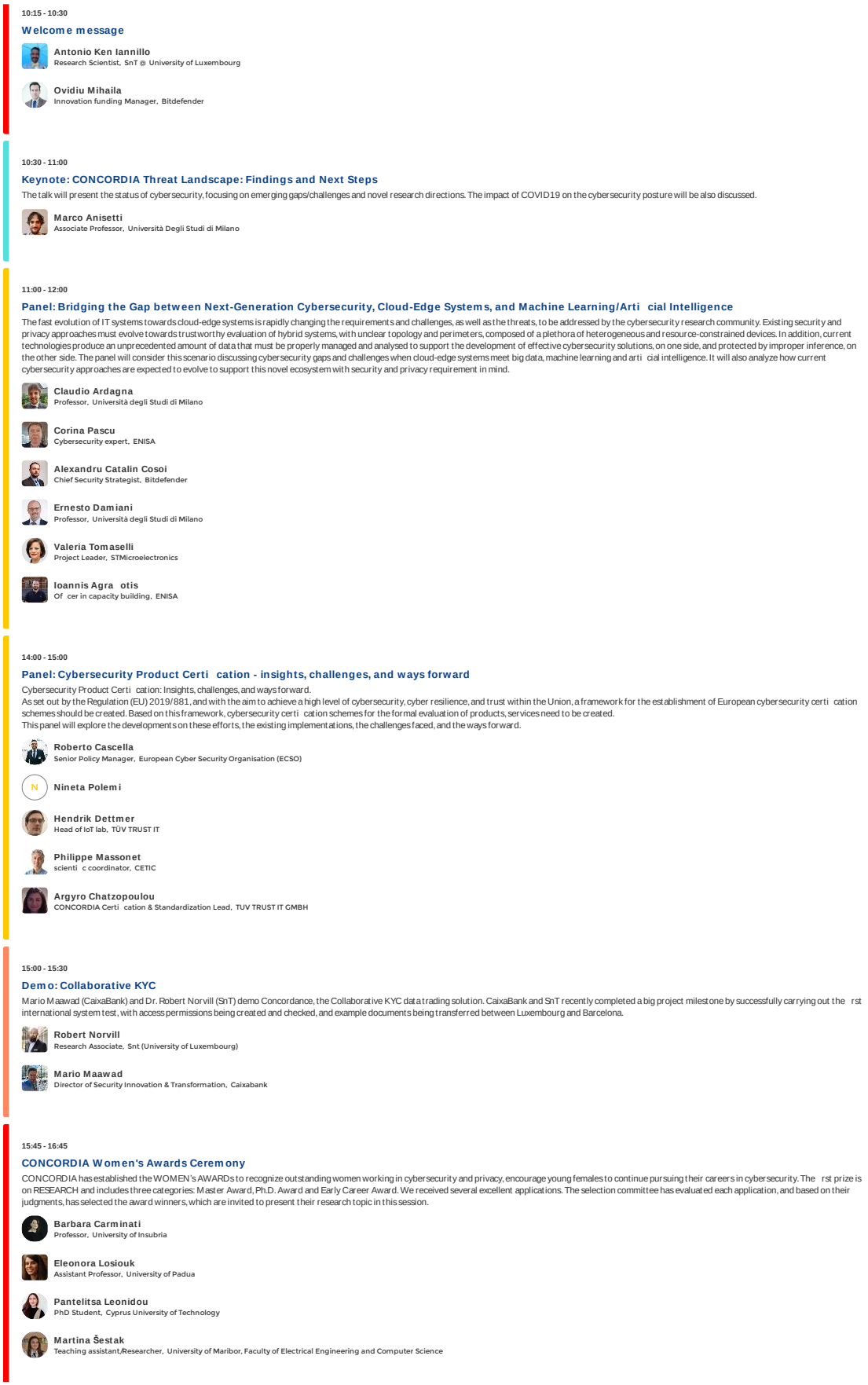
T4.6's main objective is to establish liaisons and collaborate closely with the relevant European stakeholders. T4.6 reached this objective in 2021 by extending our stakeholders' network to 549 members from about 270 different organisations, issuing stakeholders' newsletters, and delivering a two-day virtual event (COD2021) with 193 registrants.

Activities in T4.6 were unfortunately affected by the COVID19 pandemic. In particular, CONCORDIA did not hold the COD2021 event in Bucharest as initially planned and moved to a virtual event. However, T4.6 managed to have a first meeting of the NSG virtually.

T4.6 is directly contributing to several KPIs in CONCORDIA. COD2021 is already the third 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, 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). More than 10 H2020 projects affiliated with CONCORDIA in the OSG (KPI-DC-11: Liaisons with other projects: At least three (3) collaborations with projects in H2020).

Our plan for 2022 is to extend our stakeholders' network further and have a second meeting with the NSG at the beginning of 2022. COD2022 will be again a physical or 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.

# Appendix



10:15 - 10:30

**Welcome message**

**Antonio Ken Iannillo**
Research Scientist, SnT @ University of Luxembourg

**Ovidiu Mihaila**
Innovation funding Manager, Bitdefender

10:30 - 11:00

**Keynote: CONCORDIA Threat Landscape: Findings and Next Steps**

The talk will present the status of cybersecurity, focusing on emerging gaps/challenges and novel research directions. The impact of COVID19 on the cybersecurity posture will be also discussed.

**Marco Anisetti**
Associate Professor, Università Degli Studi di Milano

11:00 - 12:00

**Panel: Bridging the Gap between Next-Generation Cybersecurity, Cloud-Edge Systems, and Machine Learning/Arti cial Intelligence**

The fast evolution of IT systems towards cloud-edge systems is rapidly changing the requirements and challenges, as well as the threats, to be addressed by the cybersecurity research community. Existing security and privacy approaches must evolve towards trustworthy evaluation of hybrid systems, with unclear topology and perimeters, composed of a plethora of heterogeneous and resource-constrained devices. In addition, current technologies produce an unprecedented amount of data that must be properly managed and analysed to support the development of effective cybersecurity solutions, on one side, and protected by improper inference, on the other side. The panel will consider this scenario discussing cybersecurity gaps and challenges when cloud-edge systems meet big data, machine learning and arti cial intelligence. It will also analyze how current cybersecurity approaches are expected to evolve to support this novel ecosystem with security and privacy requirement in mind.

**Claudio Ardagna**
Professor, Università degli Studi di Milano

**Corina Pascu**
Cybersecurity expert, ENISA

**Alexandru Catalin Cosoi**
Chief Security Strategist, Bitdefender

**Ernesto Damiani**
Professor, Università degli Studi di Milano

**Valeria Tomaselli**
Project Leader, STMicroelectronics

**Ioannis Agra otis**
Of cer in capacity building, ENISA

14:00 - 15:00

**Panel: Cybersecurity Product Certi cation - insights, challenges, and ways forward**

Cybersecurity Product Certi cation: Insights, challenges, and ways forward.
As set out by the Regulation (EU) 2019/881, and with the aim to achieve a high level of cybersecurity, cyber resilience, and trust within the Union, a framework for the establishment of European cybersecurity certi cation schemes should be created. Based on this framework, cybersecurity certi cation schemes for the formal evaluation of products, services need to be created.
This panel will explore the developments on these efforts, the existing implementations, the challenges faced, and the ways forward.

**Roberto Cascella**
Senior Policy Manager, European Cyber Security Organisation (ECSO)

**Nineta Polemi**

**Hendrik Dettmer**
Head of IoT lab, TÜV TRUST IT

**Philippe Massonet**
scienti c coordinator, CETIC

**Argyro Chatzopoulou**
CONCORDIA Certi cation & Standardization Lead, TUV TRUST IT GMBH

15:00 - 15:30

**Demo: Collaborative KYC**

Mario Maawad (CaixaBank) and Dr. Robert Norvill (SnT) demo Concordance, the Collaborative KYC data trading solution. CaixaBank and SnT recently completed a big project milestone by successfully carrying out the rst international system test, with access permissions being created and checked, and example documents being transferred between Luxembourg and Barcelona.

**Robert Norvill**
Research Associate, Snt (University of Luxembourg)

**Mario Maawad**
Director of Security Innovation & Transformation, Caixabank

15:45 - 16:45

**CONCORDIA Women's Awards Ceremony**

CONCORDIA has established the WOMEN'S AWARDs to recognize outstanding women working in cybersecurity and privacy, encourage young females to continue pursuing their careers in cybersecurity. The rst prize is on RESEARCH and includes three categories: Master Award, Ph.D. Award and Early Career Award. We received several excellent applications. The selection committee has evaluated each application, and based on their judgments, has selected the award winners, which are invited to present their research topic in this session.

**Barbara Carminati**
Professor, University of Insubria

**Eleonora Losiouk**
Assistant Professor, University of Padua

**Pantelitsa Leonidou**
PhD Student, Cyprus University of Technology

**Martina Šestak**
Teaching assistant/Researcher, University of Maribor, Faculty of Electrical Engineering and Computer Science

Figure 3: COD2021 - program of day 1

10:25 - 10:30

**Welcome message**

**Antonio Ken Iannillo**
Research Scientist, SnT @ University of Luxembourg

10:30 - 11:00

**Keynote: First steps of ECCC**

**Miguel GONZALEZ-SANCHO**
Head of Unit, European Commission

11:00 - 12:00

**Panel: How can the community help ECCC?**

**Martin Übelhör**
Head of Sector, European Commission

**Sirko Höer**
IT-Security Expert, Bundesamt für Sicherheit in der Informationstechnik

**Gabi Dreo**
Executive Director, Research Institute CODE

**Christoffer Karsberg**
Senior Advisor, Swedish Civil Contingencies Agency, MSB

**Sabin Popescu**
Head of Analysis, Policies and Cooperation, Romanian National Cyber Security Directorate

13:30 - 14:30

**Panel: Code of Engagement for the Trusted Threat Intelligence Sharing Platform**

Imagine you want to become a member of a sports team, a musical ensemble, an innovation hub, or interest group, to contribute, learn and otherwise engage. With that, you want to become part of a certain community, each with its speci c habits, codes and rules to set clear expectations of the members of such community as well as protect the interests of both the community and each of the members separately, as well as society and the ecosystems within the community is operating. Imagine this is possible regarding sharing of threat intelligence and related trusted data sharing and engagement.

Welcome to the world of CONCORDIA Platform for Threat Intelligence and its Dynamic Code of Engagement.

The dynamics of cybersecurity, threat intelligence, clearing houses and the various cybersecurity communities in general, and the CONCORDIA Platform for Threat Intelligence (with its three core actionable components: MISP, ICH-CH and DdoS-CH and its communities) in particular, deserve a dynamic framework of principle-based arrangements that are easy to read, understand, become part of and commit to. This, in order to be able to better collaborate, orchestrate and share data based on trust, transparency, appreciation, clear governance and co-accountability.

Why join, how to engage, and what can you do with this novel instrument? Learn more during this panel!

**Dimitra Stefanatou**
Senior Legal Counsel, Arthur's Legal

**Marco Caselli**
Senior Key Expert, Siemens AG

**Christian Keil**
Principal Researcher, DFN-CERT

14:30 - 15:00

**Demo: Demonstrating the DDoS Clearing House testbed**

We have created a distributed testbed on which we can pilot the DDoSClearing House ef ciently and independently of non-technological aspects. In this talk, I discuss the motivation for developing the testbed, its implementation, and show how it is used in a pilot of the DDoSClearing House.

**Thijs van den Hout**
Research Engineer, SIDN

Figure 4: COD2021 - program of day 2

# Acronyms

| | |
|---|---|
| **CA** | Consortium Agreement |
| **COD** | CONCORDIA Open Door |
| **CoE** | Code of Engagement |
| **DoA** | Description of Action |
| **DDoS** | Distributed Denial of Service |
| **DDoS-CH** | DDoS Clearing House |
| **EC** | European Commission |
| **EU** | European Union |
| **GA** | Grant Agreement |
| **ICH** | Incidence Clearing House |
| **LSG** | Liaison Stakeholders Group |
| **MISP** | Malware Information Sharing Platform |
| **MS** | Member State |
| **NSG** | National Cybersecurity Competence Centres and Agencies Stakeholders Group |
| **OSG** | Observer Stakeholders Group |
| **WP** | Work package |