



Horizon 2020 Program (2014-2020)
Cybersecurity, Trustworthy ICT Research & Innovation Actions
Security-by-design for end-to-end security
H2020-SU-ICT-03-2018



Cyber security cOmpeteNCe fOr Research and InnovAtion^{1†}

Deliverable D3.1: 1st year report on community building and sustainability

Abstract: D3.1 provides an overview of the key WP3 achievements in Y1 of CONCORDIA. We present a high-level overview of the results we attained in each of the five tasks, our lessons learned, and our way forward for Y2.

Contractual Date of Delivery	Dec 31, 2019
Actual Date of Delivery	Dec 23, 2019
Deliverable Dissemination Level	Public
Editors	Marco Caselli (T3.1) Cristian Hesselman (T3.2, D3.1) Reinhard Gloger (T3.3) Felicia Cutas (T3.4) Aljosa Pasic (T3.5)
Contributors	Siemens SIDN CODE/MUNI/BADW-LRZ EIT Digital ATOS
Quality Assurance	Jakub Cegan (MUNI) Daniel Tovarnak (MUNI) Detlef Houdeau (IFAG) Thibault Cholez (UL)

1

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

The CONCORDIA Consortium

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

BMW	BMW	Germany
GSDP	Ministry of Digital Policy, Telecommunications and Media	Greece
RISE	RISE Research Institutes of Sweden AB	Sweden
Ericsson	Ericsson AB	Sweden
SBA	SBA Research gemeinnutzige GmbH	Austria
IJS	Institut Jozef Stefan	Slovenia

Document Revisions & Quality Assurance

Internal Reviewers

1. Jakub Cegan (MUNI)
2. Daniel Tovarnak (MUNI)
3. Detlef Houdeau (IFAG)
4. Thibault Cholez (UL)
5. Christian Keil (DFN-CERT)

Revisions: we continually updated drafts of D3.1 on Confluence

Executive summary

The goal of WP3 is to reinforce Europe's cybersecurity leadership by developing and evaluating building blocks for a European cross-sector cybersecurity infrastructure, specifically for collaborative threat handling, technology and service experimentation, training and education, and starting up new businesses. WP3 utilizes WP1's technology developments and WP2's industry pilots and this inter-WP cooperation has been successfully initiated in Y1.

The overall Year 1 WP3 achievements include the following:

- Task 3.1 has successfully met Y1 targets to establish the groundwork for information sharing of cyber threats. The Threat Intelligence Platform is under development and utilizes the MISP open source threat intelligence platform that was successfully validated at DFN-CERT. Testing with WP2's Telecom and Finance pilots has commenced.
- Task 3.2 is on track for developing the high-level architecture for the DDoS Clearing House, running a first version of the pilot, and its associated usability "cookbook". A significant achievement was the establishment of the legal data sharing agreement for the pilot in the Netherlands. This will form the blueprint for the broader agreement needed for effective deployment at the EU level.
- Task 3.3 is on track to create a cyber security ecosystem to validate and demonstrate CONCORDIA's results and to foster cyber security trainings. A steadily growing inventory of tools, cyber range platforms, and training offerings have been created. Task 3.3 also researched the possibility of sharing testing and training content across cyber range platforms in CONCORDIA.
- Targeting the development of an EU-wide cybersecurity educational ecosystem, Task 3.4 has successfully conducted the assessment of the EU's educational portfolio to develop the initial methodology for creating cybersecurity courses and an associated certification schema.
- Task 3.5 addressing of community building activities to support startups is on track. The background tasks of identifying startup stakeholder motives, challenges, influence factors and the establishment of performance indicators has been completed.

Contents

1	Introduction.....	6
2	Building a threat intelligence platform for Europe (T3.1).....	7
2.1	Task objective	7
2.2	Status	7
2.3	Key achievements Y1.....	7
2.4	Further Contributions and Outlook for Y2.....	9
3	Piloting a DDoS clearing house for Europe (T3.2)	9
3.1	Task objective	9
3.2	Status	10
3.3	Key achievements Y1.....	10
3.4	Outlook Y2.....	14
4	Developing CONCORDIA's ecosystem (T3.3).....	15
4.1	Task objective	15
4.2	Status	15
4.3	Key achievements Y1.....	15
4.4	Outlook Y2.....	18
5	Establishing a European education ecosystem for cybersecurity (T3.4)..	19
5.1	Task objective	19
5.2	Status	19
5.3	Key achievements Y1.....	19
5.4	Outlook Y2.....	24
6	Community building, support and incentive models (T3.5)	24
6.1	Task objective	24
6.2	Status	24
6.3	Key achievements Y1.....	25
6.4	Outlook Y2.....	28
7	Conclusions and outlook.....	28
8	References	28
	Annex A: Assessing the courses for Cybersecurity professionals already developed by CONCORDIA partners (T3.4).....	29
A.1	Executive summary.....	29
A.2	The Landscape	31
A.3	CONCORDIA ecosystem.....	42
A.4	Conclusions.....	51
A.5	Annexes	54
	Annex B: Startup scene (T3.5)	62

1 Introduction

The goal of CONCORDIA's WP3 is to develop building blocks for a *European cross-sector ("horizontal") cybersecurity infrastructure*, specifically for:

- Collaborative threat handling (T3.1, T3.2),
- Developing and evaluating new technologies and services (T3.3),
- Training and education (T3.3, T3.4), and
- Starting up new businesses (T3.5)

Table 1 provides an overview of the key building blocks that WP3 provides and the tangible forms that they take:

- *Technical designs (TD)*, such as for cybersecurity platforms (e.g., for threat intelligence), labs, testbeds, and tools (e.g., simulating adversary behaviour)
- *Methodologies (M)*, for instance for setting up pan-European cybersecurity courses, trainings, and start-ups.
- *Use cases (UC)* of the technical designs and methodologies, for instance through actual cybersecurity courses and technical pilots.

For example, the DDoS clearing house (T3.2) consists of a technical design that we will use twice through a pilot in the Netherlands and in Italy and that will also result in a "cookbook" (methodology) that discusses how to develop, setup, and govern a DDoS clearing house. Similarly, CONCORDIA's educational actions (T3.4) focus on developing methodologies and frameworks to design, certify, and teach courses for cybersecurity professionals, mid-managers, executives, and teachers as well as describe processes for using them.

Table 1. Key building blocks of CONCORDIA's cross-sector cybersecurity infrastructure.

WP3 key building block	Output	Task
An <i>intelligent decision support system</i> for incident response teams using a shared threat intelligence platform	TD, M, UC	T3.1
A <i>DDoS clearing house</i> for proactively and collaboratively handling DDoS attacks using DDoS fingerprints	TD, M, UC	T3.2
A <i>virtual lab</i> for other CONCORDIA WPs, trainings, and (smaller) European cybersecurity companies in a post-CONCORDIA era	TD, M, UC	T3.3
Hands-on <i>trainings for operational teams</i> , for instance based on the concept of "cyber ranges"	TD, M, UC	T3.3
Cybersecurity <i>educational instruments</i> such as courses and curriculums for professionals and teachers (as part of the EEEEC)	M, UC	T3.4
A " <i>factory</i> " for starting new cybersecurity businesses (start-ups), for instance in terms of IPR management and data sharing	M, UC	T3.5

The rest of this report provides an overview of the main results and lessons learned of WP3 in 2019, with a separate section for each of WP3's tasks (Sections 2 through 6). We conclude with the overall status of WP3 and an outlook for 2020 in Section 7.

2 Building a threat intelligence platform for Europe (T3.1)

2.1 Task objective

The aim of Task 3.1 is to build and operate the CONCORDIA Threat Intelligence Platform, a logically centralized system that enables players from different sectors to share a wide variety of threat indicators in a trusted way. The platform will be able to automatically analyze threat information and seamlessly distribute appropriate event notifications. Its implementation will be based on existing components, such as the Malware Information and threat Sharing Platform (MISP) [1] and the Incident Clearing House developed in the project “Advanced Cyber Defence Centre” (ACDC) [2].

2.2 Status

Task 3.1 is on track and fulfilled the envisioned targets for Y1. The work carried out in Y1 prepared the ground for the comprehensive development of all activities related to threat intelligence information sharing in the next years of the project.

2.3 Key achievements Y1

Technology scouting

Task 3.1 started in January 2019 with a seminal discussion among all project partners with the goal of defining requirements and objectives for Threat Intelligence (TI) sharing. Later on, the collected feedback guided the search for TI platforms available on the market that could fulfill CONCORDIA’s needs. The TI platform of choice, MISP, was selected not just because of its comprehensive set of features but also for its maturity and its already-established wide-spread usage around Europe.

Created in 2011, MISP is an open source threat intelligence sharing platform supported by the Computer Incident Response Center Luxembourg (CIRCL). CIRCL is a partner of the SPARTA project, which increases the probability that MISP will become a standard in Europe.

Originally developed cooperatively by CIRCL and NATO, MISP emerged as an effective and efficient solution to share Indicators of Compromises (IoCs) which, at that time, were exchanged only by email as unstructured textual data (e.g., PDF documents). With the increase of cyberattack sophistication and the consequent need for collaborative analysis operated by distributed teams of security experts, the advantages of using MISP became clear and the project expanded to support a growing number of users: from individuals to world-wide private organizations as well as national and supranational CERTs (e.g., CERT-EU).

CONCORDIA platform for threat intelligence

Within CONCORDIA, the central MISP instance, represents the core of the envisioned CONCORDIA Platform for threat intelligence sharing. MISP was deployed at DFN-CERT in June 2019 and is currently managed cooperatively by Siemens AG (principal and formal responsible) and DFN-CERT itself. A selected number of CONCORDIA participants (mostly related to the CONCORDIA “Telecom” and “Finance” pilots)

started testing and interacting with the central MISP instance in November 2019 paving the way to the official roll-out face in 2020.

In the second half of Y1, Task 3.1 focused on aligning activities and contributions of the involved partners. Those include topics such as: the role and actions of the Incident Clearing House (ICH) of DFN-CERT, the definition of a reference architecture for the CONCORDIA platform, the identification of the kind of information that will be shared among all stakeholders, the techniques for gaining knowledge on top of the available data (e.g., machine learning).

While the ICH reactively informs resource owners of actual problems in their networks (e.g., bots detected connecting to their command and control server) and thus forwards incidents to the affected parties, the DDoS Clearing House (presented in Section 3) proactively shares fingerprints of detected DDoS attacks with other parties to facilitate easy mitigation once the attack comes their way. Since the already operational ICH requires established third parties as trust anchors to manage access to the ICH for the different classes of organizations (e.g., Trusted Introducer for CERTs), terms of access to the ICH as part of the CONCORDIA project were developed and shared with the consortium. The overall integration of the ICH within the CONCORDIA platform was preliminary examined but will be more thoroughly discussed in the upcoming months.

At the time of writing, a basic set of interactions related to the CONCORDIA Platform has been identified. This is shown in both Figure 1 and Figure 2. Figure 1 emphasizes activities involving CONCORDIA stakeholders with either the central MISP instance or the ICH. Such situation describes the status of threat intelligence sharing in CONCORDIA for the whole of Y1.

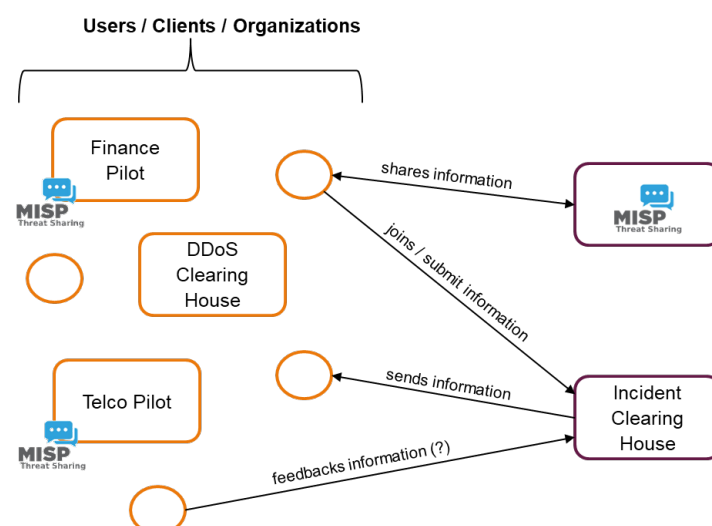


Figure 1. CONCORDIA Platform in Y1.

Figure 2, on the other hand, shows the intention of providing to the project a virtual single point of contact for all threat intelligence related activities. Components within

the CONCORDIA platform will interact with one another to organize available threat intelligence information and thus transparently improve their services to all users.

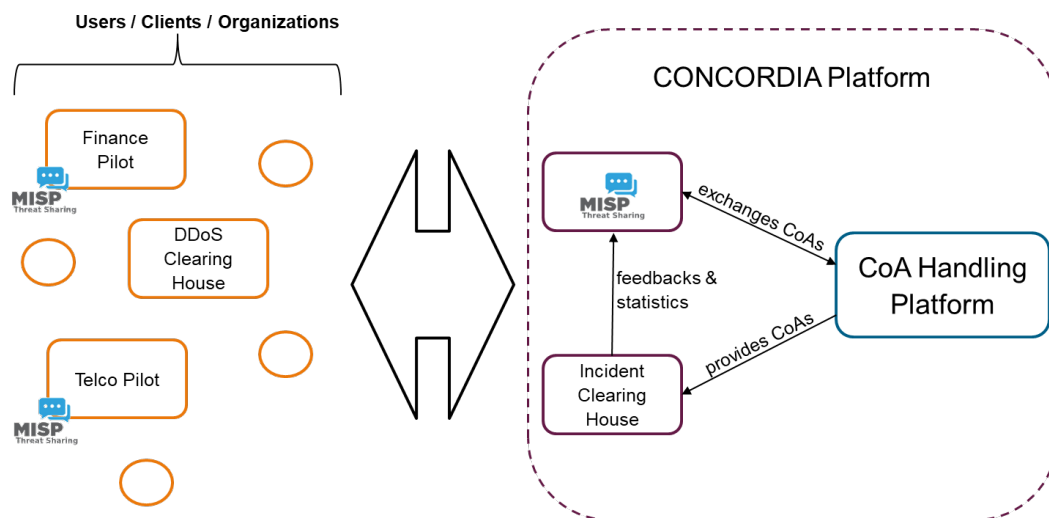


Figure 2. CONCORDIA Platform Vision.

2.4 Further Contributions and Outlook for Y2

In the upcoming years, in order to populate the CONCORDIA Platform, all interested partners will work on generating threat intelligence indicators (e.g., FORTH is working on customizing and deploying state-of-the-art honeypot solutions for this purpose). These indicators will be eventually pushed to the central MISP instance and, thus, shared within the consortium.

Finally, an important contribution of T3.1 relies on the handling of “Course of Action” (CoA) data, namely, information on response actions to be performed to counteract cyberattacks and security breaches.

Within the CONCORDIA Platform, a specific component named “CoA Handling Platform” will be designed to fulfill this task. The CoA Handling Platform will not just collect CoAs but also evaluate them, make correlation and contextualize the information to make it “ready to use”. These activities will pave the way for automated deployment of CoAs with the ambition of boosting computer emergency response teams’ efficiency and, thus, their capabilities to quickly respond to the upraising number of cyberthreats.

3 Piloting a DDoS clearing house for Europe (T3.2)

3.1 Task objective

The objective of Task 3.2 is to pilot a DDoS Clearing House with European industry for Europe to proactively and collaboratively protect European critical infrastructure against DDoS attacks.

The tasks key deliverables are a pilot in the Netherlands and in Italy and a DDoS clearing house “cookbook” that enables other sets of service providers to set up and operate their own clearing house.

3.2 Status

Task 3.2 is on track towards its goal, but we made more progress on the cookbook (e.g., in terms further developing the clearing house concept) than on the pilot in the Netherlands itself, which we had not anticipated. The main cause is that the development of the draft data sharing agreement had a long lead time, partly because of staffing issues and partly because it took a while for the legal and tech experts to understand each other’s problem space and agree on a common approach. To tackle the latter, we will set up a permanent Legal working group for the pilot in the Netherlands (see lessons learned in Section 3.3).

3.3 Key achievements Y1

Experimental setup

We set up the first iteration of the DDoS clearing house pilot in the Netherlands, which focuses on creating and sharing DDoS fingerprints through `ddosdb.nl`, a central instance of DDoS-DB [3] that runs on the network of SIDN Labs. The NL pilot is a collaboration of 10 different organizations (e.g., ISPs, Internet exchange points, and government agencies), three of which are CONCORDIA partners (SIDN, SURFnet, and the University of Twente).

Data sharing agreement

We developed a simple data sharing agreement for the first phase of the pilot, covering basic legal aspects like objectives, liability, security, personal identifiable information (PII), and governance. The data sharing agreement is valid for a fixed but extensible duration of 6 months and is currently being reviewed by the pilot partners in the Netherlands. For simplicity, the DDoS fingerprints we share currently only include metadata and no packet captures (PCAPs).

The development of the data sharing agreement had a long lead time, partly because of staffing issues and partly because it took a while for the legal and tech experts to understand each other’s problem space and agree on a common approach.

Draft overall architecture

We developed the high-level architecture of the clearing house (Figure 3), which revolves around three key components: the dissector (generates fingerprints from DDoS traffic), DDoS-DB (distributes fingerprints and provides a searchable fingerprint history), and a converter (maps fingerprints to traffic filtering rules). Figure 3 shows an example in which service provider SP2 handles DDoS attack A and shares the attack’s fingerprint FP(A) with service providers SP1 and SP3. The operations teams of SP1 and SP3 use the fingerprint to reconfigure their infrastructure (e.g., by loading appropriate filtering rules into their routers), thus proactively preparing for attack A should it come their way as well. We refer to [5] for a discussion on how the Dissector works.

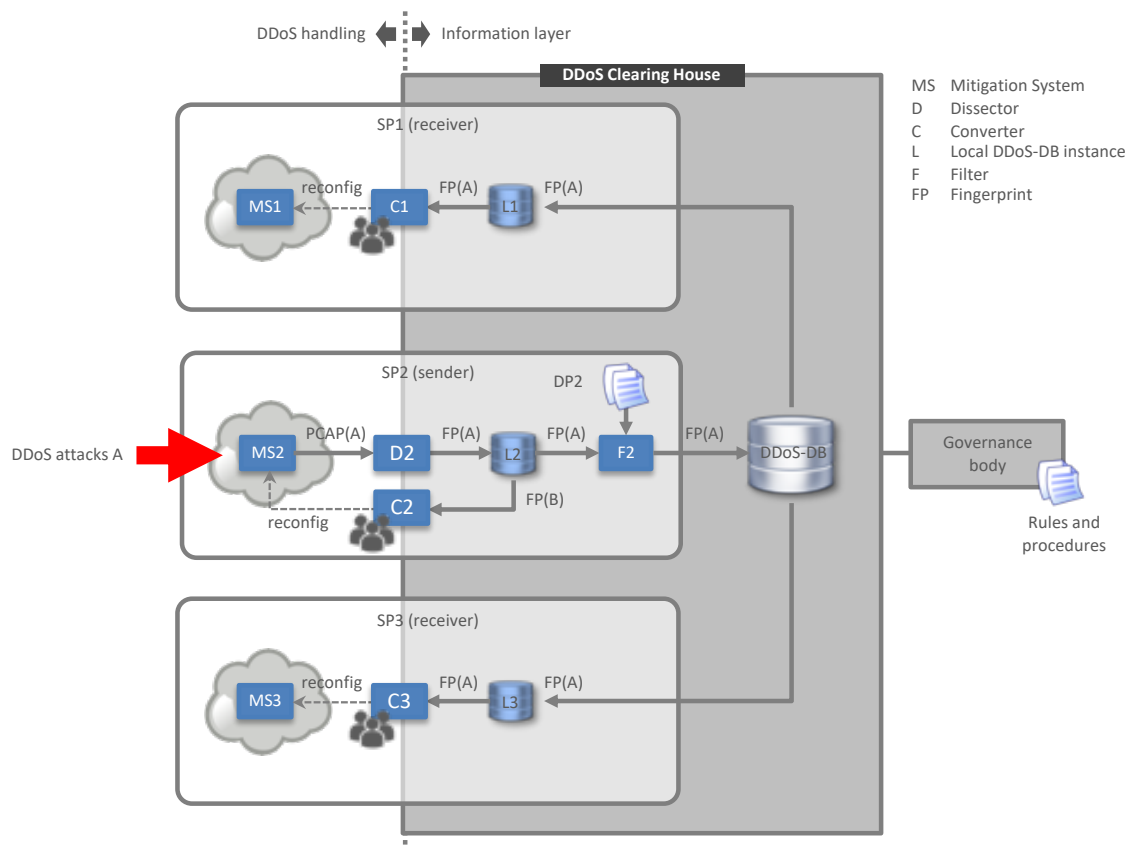


Figure 3. Service providers SP1, SP2, and SP3 using a clearing house.

Figure 3 also illustrates how the DDoS clearing house differs from the Incident Clearing House (see Section 2): the DDoS clearing house proactively shares fingerprints of detected DDoS attacks, whereas the incident Clearing House reactively informs resource owners of actual problems in their networks (e.g., bots detected connecting to their command and control server).

System requirements

The partners in the Dutch pilot have also developed a report that provides an overview of the technical requirements and use cases to improve the clearing house's key components (dissector, DDoS-DB, and converter). Examples of requirements include that the dissector must not include any sensitive information about the victim of a DDoS attack in a fingerprint (e.g., destination IP or MAC addresses) and that the DDoS-DB must allow an authenticated user to perform searches on the index of fingerprints and download them.

The requirements specification also contains a breakdown in different 4 dev-ops phases, with the first phase focusing on improvements to set up a stable “clearing house cycle”: from generating fingerprints using the dissector, to distributing them through DDoS-DB, and using the fingerprints in non-production routers.

The development of the requirements was a collaborative effort of the 10 partners in NL, using a system architect jointly funded by the Netherlands' National Cyber Security Center (NCSC-NL), NBIP and SURFnet.

Dissemination

We presented the DDoS clearing house at 9 different conferences and workshops (see Table 2), including the key security conference in the Netherlands (the One Conference) and the CONCORDIA Open Door Event. All presentations are available at www.concordia-h2020.eu/publicity/.

Table 2. Task 3.2 presentations in Y1.

Date	Event
26-Nov-2019	C. Hesselman and J. Santanna, “Fighting DDoS attacks together on a national scale”, SNIc 2019 ResiliIT conference (national conference for student associations in computer science), Amersfoort, NL
05-Nov-2019	C. Hesselman and J. Latour, “The DNS and the IoT: security and stability opportunities, risks, and challenges (for ccTLDs)”, ICANN66, Montréal, Canada
17-Oct-2019	C. Hesselman, “Piloting a DDoS Clearing House for Europe”, CONCORDIA Open Door Event, Luxembourg City, Luxembourg
02-Oct-2019	C. Hesselman and J. Santanna, “Fighting DDoS attacks together on a national scale”, One Conference, The Hague, NL
02-Sep-2019	C. Hesselman, C. Hesselman, “Mitigation of IoT-based DDoS attacks”, APTLD76, Malaysia (remote presentation)
16-Jun-2019	C. Hesselman, “Increasing trust in the digital infrastructure through a national DDoS clearing house”, Africa Internet Summit (AIS2019), Kampala, Uganda (remote presentation)
28-May-2019	C. Hesselman, “Increasing the resilience of the Netherlands’ digital infrastructure together”, ISC2NL Cyber Resilience Event, Amersfoort, The Netherlands
17-May-2019	C. Hesselman, “Mitigating DDoS attacks from botnets through a national DDoS clearing house”, BotLeg Workshop, co-located with TILting Perspectives 2019, Tilburg, the Netherlands
23-Feb-2019	C. Hesselman, “Collaboratively increasing the resilience of critical services in the Netherlands through a national DDoS clearing house”, Internet Infrastructure Security Day at APRICOT2019, Daejeon, South Korea (remote presentation)

Lessons learned

Our key lessons learned are:

The need for a DDoS clearing house is widely recognized. Based on the positive feedback we received on our talks, we conclude that the need for a DDoS clearing house is widely acknowledged. This is also illustrated by the Dutch partners’ investments in the clearing house pilot, both in-kind and in-cash. For example, all partners are putting in person months (both technical and legal experts) and NCSC-NL, NBIP, and SURFnet jointly funded a systems architect to further flesh out the overall architecture of Figure 3.

The DDoS clearing house needs to be part of a wider “anti-DDoS coalition”. The DDoS clearing house is an operational facility that needs to be supported by an active

community, which we call an “anti-DDoS coalition” (in the Netherlands: the Dutch anti-DDoS coalition). Member organizations organize themselves into various working groups to provide continuity, for instance to develop and maintain work products such as iterations of the clearing house’s data sharing agreement, procedures and waiver agreements for DDoS exercises, and the rules of engagement for coalition members (e.g., membership rules).

The Dutch partners in the pilot also expressed the need to carry out large-scale DDoS exercises together and actually ran one in the fourth quarter of 2019. As a result, we think of an anti-DDoS coalition as in terms of two core operational tasks: running the DDoS clearing house and carrying out DDoS exercises.

We also learned that an anti-DDoS coalition should consist of two types of members: a core of organizations that have a joint operational relationship (sharing fingerprints and carrying out DDoS exercises) and a group of affiliated members that focus on sharing expertise and experiences (rather than operational activities). The objective of the entire coalition should be to further improve the protection of members’ critical services by sharing expertise, experiences, and operational data on DDoS attacks.

Anti-DDoS coalitions need a legal working group. The development and operation of the clearing house requires a working group of legal experts that collaboratively develop and maintain legal documents for various iterations of the pilot, such as the data sharing agreement, the waiver agreements for DDoS exercises, and the clearing house’s evolving governance structure. A legal working group speeds up the development and deployment of the clearing house because the people on the working group are closely involved in the topic and provide continuity when people are temporarily unavailable or change jobs (we experienced the latter first-hand in the Dutch pilot). In addition, a legal working group uses the combined expertise of its members, which will help aligning the legal documents with the different iterations of the pilot. We are currently setting up a legal working group for the Dutch coalition.

Personal trust is crucial at early stages. Personal trust between the 10 partners in the Netherlands was crucial to make progress in this early stage of the clearing house. For example, people were confident that they could reach consensus in the working group that develops the DDoS clearing house, which is why we opted for unanimous decision making in our current “governance model” (formalized as part of the data sharing agreement).

Keep data sharing agreement simple and scalable. The data sharing agreement needs to clearly articulate the purpose of the first iteration of the pilot, which is to experiment with exchanging DDoS fingerprints across different organizations to assess the usefulness and effectiveness of the clearing house. It also needs to cover other legal aspects (e.g., liability, security, PII, and governance), but only the bare minimum. This is important to keep the data sharing agreement simple and scalable and fit for experimentation.

A future challenge is to evolve the data sharing agreement so that its level of simplicity and scalability continues to align with next pilot iterations.

Combining tech and legal expertise early on is a must. The data sharing agreement requires close collaboration between legal and technical experts from the start. For example, the tech folk need to provide guidance for legal experts on the concept of a DDoS fingerprint and highlight the purpose and nature of the data exchange (collaboration and experimentation). This is important to reduce legal uncertainty, which helps avoiding conservative legal constructs (cf. [4])

Combining research and operational expertise early on is a must. Early discussions with the operational teams who will work with the clearing house is important to get their requirements. For example, they need to be in control of installing filtering rules on their network infrastructure, which means that the clearing house should not install these rules automatically. Another example is that systems might fail under a DDoS attack, which means that ops teams also need the possibility to create fingerprints by hand through a UI or a command line tool and share whatever information they learned about the attack (e.g., suspected origin, protocol type).

CONCORDIA partners play a bridging role. SIDN, UT, and SURFnet play a bridging role between two different workstreams: the development of the DDoS clearing house pilot in the Netherlands with 7 non-CONCORDIA partners and the more research type of work in CONCORDIA (T3.2 and T1.2). To enable the two workstreams to advance more in parallel, we will create a separate experimental setup for CONCORDIA partners (ddosdb.eu) and share the results across the two workstreams.

3.4 Outlook Y2

Our next steps for the NL pilot are to sign the data sharing agreement, start sharing DDoS fingerprints, and use the fingerprints to configure non-production routers. In addition, we have started fleshing out the requirements for the next iterations of the pilot and improve the dissector, DDoS-DB, and converter software.

Our other plans for 2020 include writing a blog on our lessons learned in the NL pilot (starting point for the DDoS clearing house cookbook), setting up an instance of the clearing house at SIDN Labs specifically for T3.2 (ddosdb.eu), and run experiments such as fingerprinting based on cross-VM DDoS traffic, clustering of fingerprints, and automatic generation of mitigation rules. We'll also translate the data sharing agreement from Dutch to English to accommodate this activity and make it available within CONCORDIA (e.g., for T3.5).

Finally, we aim to increase cooperation within T3.2 and with other WP3 tasks, specifically:

- T3.1: to develop a technical design on how to share DDoS fingerprints through the CONCORDIA threat intel platform (in addition to through DDoS-DB)
- T3.3: to run ddosdb.eu in the CONCORDIA virtual lab (or first run it at SIDN Labs, then migrate it)
- T3.5: to provide input for the “start-up factory” and guidance on data sharing based on the first version of the DDoS clearing house cookbook.

4 Developing CONCORDIA's ecosystem (T3.3)

4.1 Task objective

The objective of T3.3 is to establish the CONCORDIA cybersecurity ecosystem with virtual labs, services and training activities. *Virtual Lab* activity aims to develop an ecosystem that would support validations and demonstrations of CONCORDIA's results on large IT infrastructures and in smaller cybersecurity labs. *Services* activity aims to create a curated portfolio of public and proprietary tools and available cybersecurity labs to create a cutting-edge advantage for the partners to speed up research and development of cybersecurity systems. *Training* activity aims to develop and continuously evolve cyber range trainings to achieve better automated and custom- tailored training that correspond to the evolving cyber threat landscape.

4.2 Status

Task 3.3 is on track towards its goal. The main focus was on Cyber Training and the inventory of Cyber Ranges and Trainings is already available online (website: <https://www.concordia-h2020.eu/map-courses-cyber-professionals> and on confluence for project-internal use). The first steps for exchanging scenarios were done as well as the cooperation with other H2020 projects and pilots has started. The visibility in Services was better than expected. The concept of a Virtual Lab, which relies on Services and Trainings, will need to be discussed further within the WP3 in the future (lesson learned).

4.3 Key achievements Y1

Lessons learned: focus on cyber ranges

The idea along the lines of a common "live" testing lab must undergo a further discussion due to security, trust and privacy issues. Because of these reasons, emulation and simulation approaches are usually used in this context.

After several rounds of information-gathering within the consortium we have learned that at the present time the most commonly reported manifestation of a cybersecurity lab is either a cyber range or a cyber range platform and related trainings. Our further efforts in Y1 was therefore focused on this very complex area.

Cyber range (CR) is a multipurpose environment to execute complex cybersecurity scenarios in an isolated and safe manner – essentially a cyber space counterpart to military testing and training ranges. Cyber range platforms, on the other hand, allow to create multiple instances of cyber range environments on demand.

Virtual Lab

One of the goals of the Virtual Lab is to grant access to cybersecurity labs to partners and possibly also to certification bodies. This goal is very tightly connected to the Services and Training activities where several potential labs and solutions were mapped.

Threat Intelligence (TI) platform and Central Clearing House (CCH) are currently hosted in the related tasks T3.1 and T3.2, respectively.

Services

In order to fulfil the objective of providing curated portfolio of tools and services to CONCORDIA and the wider community, we integrated cybersecurity ecosystem content into the CONCORDIA website: <https://www.concordia-h2020.eu/map-courses-cyber-professionals/> (see Figure 4). Thereby, all information is in one place and can easily be found.

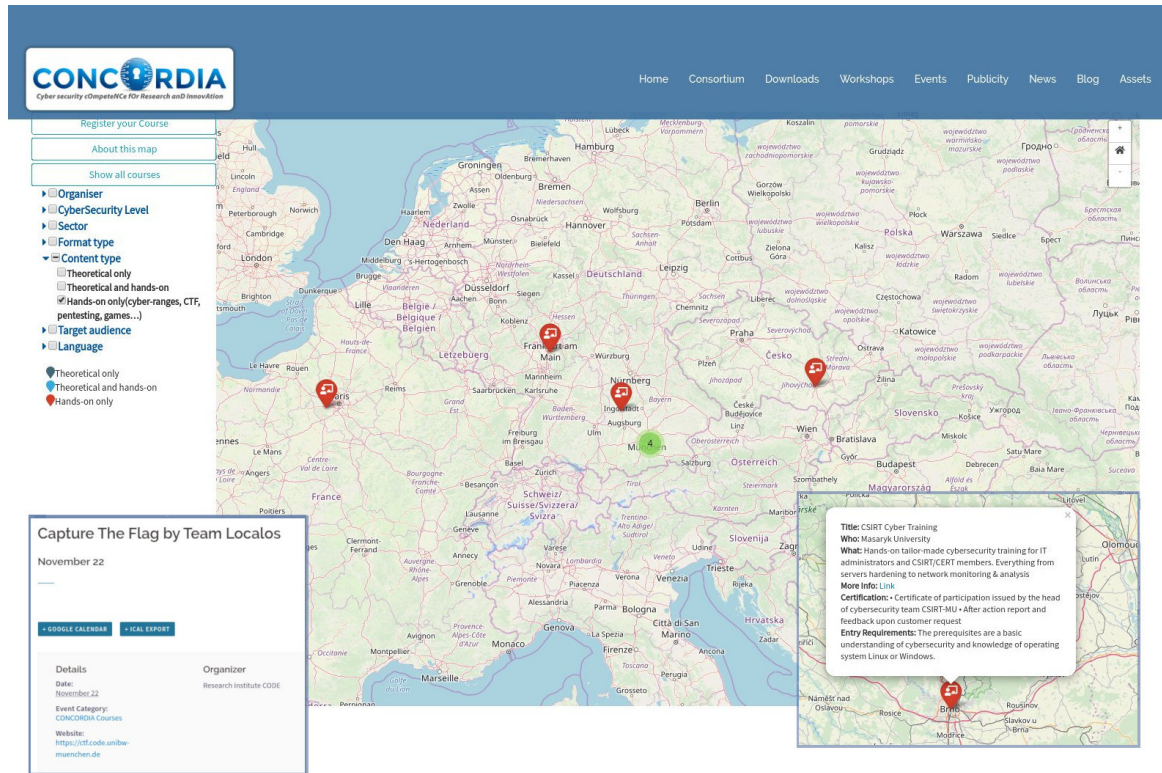


Figure 4. Cyber Ranges and CTF Events within the CONCORDIA map² and calendar³.

As a first step, we gathered several information about cyber ranges and training possibilities from CONCORDIA partners. More than 10 cyber ranges and cyber range platforms are either running or being created/set-up within CONCORDIA, for example at CODE, UL, ACS, RISE, and MUNI. These cyber ranges as well as Capture the Flag (CTF) events are already shown in the CONCORDIA map² (see Figure 4), which is a joint cooperation with T3.4. The map includes, for example, information about the place, security area (related to the research tasks in WP1), sectors (related to WP2), and additional information. In order to see the different cybersecurity events during the year, we are currently working together with different tasks to include them into the CONCORDIA calendar³, as shown in Figure 4 as well.

In a second step, recommended tools, like Chizpurple (has a focus on testing vendor-specific system services of Android OS) and Frida (dynamic instrumentation toolkit for developers), are currently being collected internally and they are going to be displayed in the service catalog¹ in Y2. Further helpful information, like existing

¹ <https://www.concordia-h2020.eu/concordia-service-cybersecurity-tools/>

cybersecurity labs, will be available via the service catalog at the CONCORDIA website as well.

Training

Cyber range platforms, CR-based trainings, and related tools are the main focus of the Training activity. Initial discussions were started with technical topics such as technical federation, exchange of scenarios, automatic execution of attack scenarios, scoring mechanisms and network simulation/emulation. Actual status and development at CODE, UL, ACS, RISE, MUNI, and other cyber range partners was taken into account. A joint workshop was held at CODE in order to broaden collaboration between CODE and MUNI.

A broader consensus was reached regarding technical federation of cyber ranges and CR platforms. At the present time CONCORDIA does not have ambitions to pursue this direction, as opposed to other pilots, for example. Instead, we are currently focused on researching the possibility of interchanging testing and training content (e.g. base virtual images, network topologies, SW configurations, and scenario descriptions) between cyber range platforms (e.g., MUNI Cyber Range, CODE Cyber Range, and UL Cyber Range). This will enable the partners to combine and share effort in the area of training creation via (partial) scenario exchange.

CODE, UL, and MUNI have their CR platforms in an operational state and as academic partners they are able to share details about their internal workings. MUNI created a first draft of a minimal network topology description format with the goal of sharing topology description between task partners. MUNI also started legal and technical procedures to release their Cyber Range Platform as open source in Y2, which is based on the KYPO cyber range concept developed at Masaryk University.

Six major events were held with CONCORDIA's participation (see Table 3) that are directly related to the project¹ measurable KPI-DC-5 "More than four (4) Capture-the-Flag (CTF) competitions, training seminars, and training courses."

Table 3. Training events in Y1.

<i>CODE - CTF and CTF qualification</i>	<i>22.-23. 11. 2019</i>	<i>120 participants</i>
CODE's Jeopardy-style CTF involved multiple categories of challenges for which the teams had a limit of 18 hours to solve. The teams had to go through an online qualifying CTF, where 29 out of 56 teams (6 from CONCORDIA) got qualified. URL: https://ctf.code.unibw-muenchen.de/ctf-2019---the-5th-element-results.html		
<i>UL - Security Management Course</i>	<i>18-22. 11. 2019</i>	<i>25 participants</i>

² <https://www.concordia-h2020.eu/map-courses-cyber-professionals/>

³ <https://www.concordia-h2020.eu/cybersecurityevents/>

⁴ <https://www.concordia-h2020.eu/concordia-service-cybersecurity-tools/>

The UL course provided an overview of methods and tools related to security management in an integrated manner, the different practical exercises being performed over the cyber range platform.		
URL: http://telecomnancy.univ-lorraine.fr/fr/security-management		
UL - Cyber Range Launch Event	24. 09. 2019	150 participants
The UL Cyber Range Launch Event included an overview of CONCORDIA activities related to the cyber range, demonstrations of the cyber range.		
URL: https://telecomnancy.univ-lorraine.fr/fr/inauguration		
MU – KYPO Summer School on CS	13-15. 08. 2019	20 participants
Hands-on tutorials and cybersecurity (CS) games for training of the Czech national team participating in joint venture with CyberSec4Europe.		
URL: https://www.europeancybersecuritychallenge.eu. J		
CODE - Workshop at CODE 2019	10. 06. 2019	40 participants
The aim of the workshop was to discuss the best practices and technologies required to simulate real systems. Furthermore, it was discussed how cyber ranges could provide a broader portfolio of scenarios for efficient training.		
URL: https://www.unibw.de/code/jahrestagungen		
MU - Cyber Czech Exercise	21-22. 05. 2019	24 participants
The exercise was chosen to demonstrate cyber range platform capabilities to CONCORDIA representatives. The exercise trained technical skills, ability to collaborate, communicate, and share relevant information with management.		
URL: https://www.concordia-h2020.eu/blog-post/cyber-training-defence-exercise/		

T3.3 initiated cooperation with the other pilots (ECHO, SPARTA, CyberSec4Europe) and H2020 projects (THREAT-ARREST) in the area of cyber range platforms and CR-based trainings. With ECHO, SPARTA, and THREAT-ARREST, points of contact were established. With CyberSec4Europe, joint collaboration is already underway in the form of summer schools (executed and planned). Also, panel discussion Cyber Ranges in H2020 Pilots at IEEE NOMS 2020 conference was proposed to foster the idea of cooperation.

4.4 Outlook Y2

Our plans for T3.3 in Y2 are:

Virtual Lab

- Collaborate with tasks T3.1 and T3.2 in terms of testing IT infrastructure.
- Gather more information in the context of existing cybersecurity labs.

Services

- Include more specific tools and training offerings into the CONCORDIA portfolio.
- Incorporate more Training events in CONCORDIA calendar.

- Provide a more fine-grained mechanism of filtering and search in the available CONCORDIA items.

Training

- Continue to work on a minimal network topology description format. Further pursue the idea of scenario exchange.
- If legally and technically possible, release KYPO Cyber Range Platform as open source.
- Participation on “IFIP summer school on Privacy and Identity Management” in collaboration with CyberSec4Europe.

5 Establishing a European education ecosystem for cybersecurity (T3.4)

5.1 Task objective

This task will contribute to the development of a European Education Ecosystem for Cybersecurity through a number of targeted actions addressing mainly the cybersecurity industry and its professionals (technicians, mid-level management, executives) and teachers.

5.2 Status

The task 3.4 is progressing as planned. The work performed in the first year on pooling, assessing and disseminating existing courses in Concordia consortium, the communication activities around them set solid grounds for developing a European Education Ecosystem for Cybersecurity. The findings of the feasibility study for a Cybersecurity Skills Certification Scheme will help further in closing the work on developing the framework for a CONCORDIA certificate and on the methodology for the creation of new courses already started in year 2019.

5.3 Key achievements Y1

In year 1, under task T3.4 we started working on four of the six task actions listed in the project plan, namely Actions 1. Pooling, assessing and disseminating existing courses, Action 2. Design and develop a Cybersecurity specific Methodology for the creation of new courses and/or teaching materials, Action 4. Develop a framework for a CONCORDIA certificate to be attached to the courses produced by the consortium and Action 6. Contribute to building a European Education Ecosystem for Cybersecurity (Figure 5. Structure of the T3.4 actions and progress).



Figure 5. Structure of the T3.4 actions and progress.

Overview of cybersecurity courses offered by CONCORDIA partners

Action 1's initial effort was allocated to collecting information on the existing courses offered by the CONCORDIA consortium to different categories of industry professionals in Cybersecurity within Europe such as technologists, mid-level managers, executives. The partners were invited to provide details via the EU Survey platform on the content of the course, target audience, delivery format, language, certification, alumni, but also on the linkage of the course to the five pillars of the data-centric approach to Cybersecurity advocated by CONCORDIA, and on their association to the five core industrial pilots that CONCORDIA is focusing on, namely Telecom, Finance, Transport e-mobility, e-Health and Defense sectors.

In view of disseminating the CONCORDIA courses, we have plotted them on a [dynamic map¹](https://www.concordia-h2020.eu/map-courses-cyber-professionals/) on the project website. We also made available different filters which can be used to help professionals identify the trainings which best suit their needs for upskilling, reskilling or simply learning about cybersecurity. We also used the [events calendar²](https://www.concordia-h2020.eu/cybersecurityevents/) as an additional channel for dissemination of the CONCORDIA courses by providing concrete dates where available (see Figure 6. CONCORDIA dynamic map of courses and excerpt from the calendar).

¹ <https://www.concordia-h2020.eu/map-courses-cyber-professionals/>

² <https://www.concordia-h2020.eu/cybersecurityevents/>

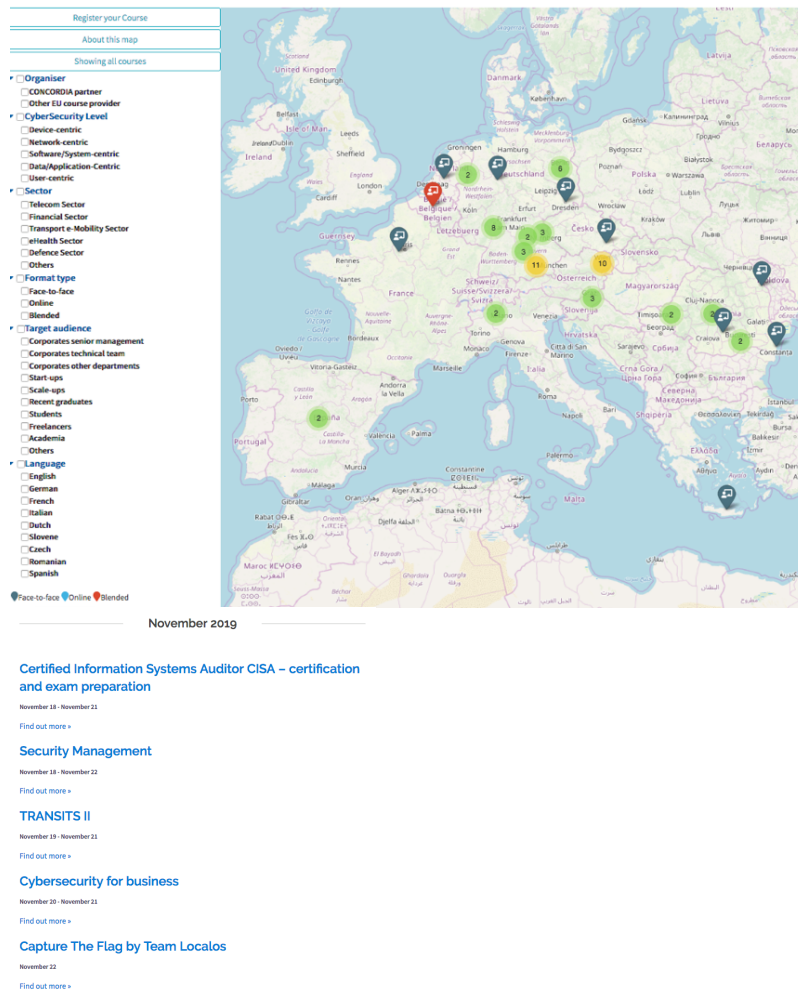


Figure 6. CONCORDIA dynamic map of courses and excerpt from the calendar.

By November 2019, non-less than 33 courses organised by the CONCORDIA partners were plotted on the map. To these, a number of 27 external courses were added as we opened the map for external submissions. This endeavour is part of the task Action 6 as it helps contribute to building the European Education Ecosystem for Cybersecurity. The map will be updated on a continuous basis and aim at becoming the main source of information on available courses for cybersecurity professionals and of professionals interested in cybersecurity.

The courses were disseminated online via the CONCORDIA website (the courses map and the calendar), social media posts, and offline during events (Brussels – ECSO meetings; Rome – Women in cyber; Heraklion – ENISA summer school; Luxembourg - CONCORDIA Open Door 2019) – the links are:

- Launch the dynamic map on courses (during the GA 5/06):
 - <https://www.concordia-h2020.eu/map-courses-cyber-professionals/>
 - <https://www.concordia-h2020.eu/news/towards-a-european-education-ecosystem-for-cybersecurity/>
- Promote the dynamic map on social media:
 - <https://twitter.com/FLCutas/status/1138378020094402560>
- News item (calendar of courses) created on CONCORDIA website:

- <https://www.concordia-h2020.eu/news/concordia-calendar-courses/>
- Dissemination activities on social media:
 - <https://twitter.com/FLCutas/status/1166285862381989890>
 - <https://twitter.com/FLCutas/status/1159012919230849024>
 - <https://twitter.com/concordiah2020/status/1158762987454377984>
 - <https://twitter.com/BCarminati/status/1154070421379190784>
 - https://twitter.com/Fl_CODE/status/1158998271651713024
 - <https://twitter.com/FLCutas/status/1154000779906150400>
 - <https://twitter.com/FLCutas/status/1151404667332694016>
 - <https://twitter.com/concordiah2020/status/1151396260793987072>
 - <https://twitter.com/concordiah2020/status/1151396260793987072>
 - https://twitter.com/EIT_Digital/status/1166247733780471808
 - https://www.linkedin.com/posts/felicia-cutas-18212332_concordia-calendar-for-cybersecurity-courses-activity-6564787038250377216-04jB
 - https://www.linkedin.com/posts/felicia-cutas-18212332_we-are-part-of-concordia-ecosystem-h2020-activity-6559706731482497024-LcQe
 - https://www.linkedin.com/posts/concordia-h2020_concordia-calendar-for-cybersecurity-courses-activity-6564528922619334656-AcEG
 - https://www.linkedin.com/posts/concordia-h2020_cybersecurity-skills-europe-activity-6557161779615539200-kUCt
 - https://www.linkedin.com/posts/eit-digital_cybersecurity-incidents-cost-businesses-40b-activity-6572017256409112576-Lfng
- News item to promote the updates linked to the courses
 - <https://www.concordia-h2020.eu/news/concordia-map-60-cybersecurity-courses-collected-in-6-months/>
- Promotion of the calendar and courses on Twitter:
 - <https://twitter.com/FLCutas/status/1202154413940494336>
 - <https://twitter.com/FLCutas/status/1191642813647278080>
 - <https://twitter.com/FLCutas/status/1204348141052538880>

Assessment of CONCORDIA courses

A significant work part of Action 1. Pooling, assessing and disseminating existing courses was devoted to assessing the existing CONCORDIA courses (Annex A: Assessing the courses for Cybersecurity professionals already developed by CONCORDIA partners (T3.4)). In view of doing so, we first outlined the key Cybersecurity needs and challenge areas, looked into the different Cybersecurity competencies needed and some of the relevant courses offerings, explored the market needs in terms of cybersecurity skills and presented existing models in support of matching the companies needs with the skills offers.

We then asked the CONCORDIA industry partners about their needs in terms of skills and technical people and check to which extent they are addressed by the actual CONCORDIA professional education offer. The conclusions were captured in Annex A: Assessing the courses for Cybersecurity professionals already developed by CONCORDIA partners (T3.4) and was/will be further used in developing the methodology for the creation of new courses and in feeding the CONCORDIA cybersecurity roadmap Education chapter. Content wise, the courses are various but

not necessarily industry specific, especially the ones addressed to middle managers and executives. Besides, they cover mainly academic and technical knowledge and to a lesser extent business aspects and hands-on components for which part of the industry partners are looking for.

Methodology for the creation of new courses

Based on the observations drawn in Annex A: Assessing the courses for Cybersecurity professionals already developed by CONCORDIA partners (T3.4) assessing the existing CONCORDIA courses and the education environment for professionals, we have stated developing as part of the task Action 2, a methodology for the creation of new courses and teaching materials. The proposed methodology will have a business approach in the sense that it will start from the industry needs in term of upskilling their personnel and/or hiring skilled workers. The document is structured in ten chapters as depicted in the Figure 7. We plan at building it as a practical guide by providing under each chapter a check lists and referring to some best practice cases. The structure was validated internally with the partners contributing to the development of this action and is in the process of being developed. The methodology paper will be made available to the consortium partners at the beginning of year 2020.



Figure 7. CONCORDIA structure of the Methodology for creation of courses.

Towards a Cybersecurity Skills Certification Scheme

Progress has been made also in the task Action 4. Develop a framework for a CONCORDIA certificate to be attached to the courses produced by the consortium linked to the development of a framework for a CONCORDIA Certificate. We are currently finalizing the Feasibility study for a Cybersecurity Skills Certification Scheme assessing the need for the creation of such a certification scheme, and identifying specific profiles not currently covered by any certification scheme. The study looks mainly into the existing initiatives for cybersecurity careers and studies, cybersecurity body of knowledge, existing Cybersecurity skills certification schemes, and mapping existing certification schemes to competencies and levels. Based on the conclusions of the Feasibility study we will develop a Certification framework to provide the necessary information regarding the process of the skills certification

specific to certain profiles - from the submission of the application to the achievement and the preservation of their certification, to describe the examination mechanisms proposed by CONCORDIA for the certification of knowledge, skills and other competences of the related professionals, and to look into the type of supporting technology to be used in the implementation of the framework.

5.4 Outlook Y2

In Year 2 we will continue updating the information on the cybersecurity courses for professionals with respect to the dates and new content and will promote them online and offline. The methodology for the development of new cybersecurity courses for professionals will be finalized and made available to the consortium in Q1-2020. The methodology will be afterwards applied to the Action 3 of T3.4 by developing new courses targeting industry mid-level management and executives. We also plan to finalize the work on the Feasibility study for the Cybersecurity skills certification scheme and on the Framework for the Certificate. The intention would be to test the Framework for the Certificate by applying it to a specific profile identified via the Feasibility study.

6 Community building, support and incentive models (T3.5)

6.1 Task objective

Task 3.5 has two objectives. The first is related to early stage startups and services that CONCORDIA could deliver to these stakeholders, including creation of future startups (e.g. today's CONCORDIA researchers) and definition of support services that they might need. The second objective of the task is to develop and evaluate incentive models for data sharing, which will start in Year 2. In both objectives, collection of best practices and drafting of guidelines are examples of activities to be executed.

Task 3.5 contributes to CONCORDIA overall project objective O2, which states that "CONCORDIA addresses this with a governance model that combines the agility of a startup with the sustainability of a large center".

Task T3.5 is closely related to task T5.1, which focuses on "startup incubators". We therefore jointly carry out information gathering activities.

6.2 Status

We are on track for the first objective of task T3.5. In Y1, we developed a first description of the concept of a "startup factory" and shared our preliminary results within CONCORDIA and with the larger cybersecurity community in Europe. These results are based on a set of research questions we articulated, a literature study, and interviews of several startup cybersecurity companies and researcher-entrepreneurs.

We captured the results of Y1 in an internal deliverable (see Appendix B), which was distributed to the partners involved and to the management board, as well as external advisors. The feedback was collected and discussed at the CONCORDIA Open Door Event in Luxembourg, with several alternative options for the further development of services for CONCORDIA startup community.

We observe that starting cybersecurity business off the ground is slightly different than starting other IT business, given the market specificities (for more details see deliverable D6.3). The services and business model may vary due to the location or physical presence, but in some cases not entirely. A cybersecurity startup that targets SME customers, for example, might choose a local go-to-market strategy, while niche solution could only use online sales channels. There are some guidelines and best practices available on the Internet¹ and entrepreneurship has been added to certain curricula, such as EIT Digital Master School², but the difficulty lies in approaching the demand side customers, which are often reluctant to work with the freshly established companies.

The second part of task T3.5 on data sharing incentives will start in Y2 because it depends on other CONCORDIA activities, such as T3.1, T3.2, and the WP2 pilots.

6.3 Key achievements Y1

Research questions articulated

Our first work product consisted of a set of research questions, which we articulated based on a literature study that covered topics such as cybersecurity-specific contexts, different kinds of financing options for startups, stakeholder motivations, and success factors.

The research questions we focus on are:

- What are the motives for different stakeholders in “startup factory” schemes and services?
- How is the performance measured and how does it relate to cybersecurity key performance indicators in general?
- What are the external factors that shape or influence “startup factory” landscape for cybersecurity entrepreneurs in Europe?

We also interviewed selected spin-offs and startups to gain insight into these questions from their experiences, as well as with some investors and other stakeholders. In parallel, we have carried out a literature study on services for early stage startups in other IT sectors. Finally, collection and analysis of data included comparison of findings from literature and public sources, in order to find specific challenges and gaps in the cybersecurity startup situation in Europe.

Startup factory proposition

We developed a first description of the concept of a “startup factory”, for instance in terms of its service definition, value proposition, and positioning. This is the main result of phase 1 (see Figure 8) that is establishing vision and, after all feedback is gathered from the management board, it will be also reflected in the strategy.

¹ So You Want to Run a Cybersecurity Startup, available at <https://static1.squarespace.com/static/551468e4e4b0bd427144c108/t/560af216e4b053ff51a6e0d6/1443557910287/FullSiteSol-article-V4.pdf/>

² <https://masterschool.eitdigital.eu/programmes/sap/>

The concept is based on reconciliation of innovation push and pull paradigms in a cybersecurity ecosystem such as CONCORDIA. Demand side customers, as well as large system integrators or consultants already present on the market, are able to better identify real business needs and derive or connect to innovative ideas coming from supply side academia or startups. Inside CONCORDIA these ideas could be tested before or in parallel to the business modelling or start of startup revenues. The mechanism that could be used could be Open Call (already described in the description of work) or as a part of the WP2.

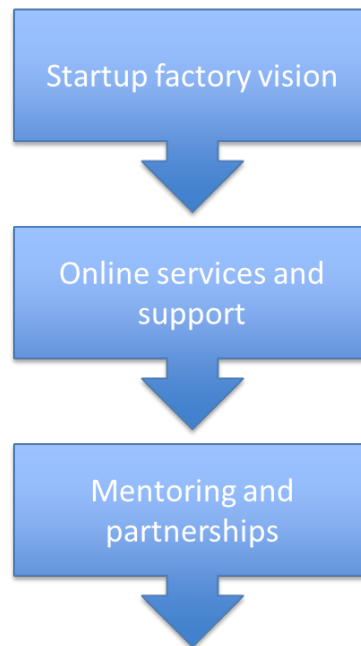


Figure 1. Implementation of early stage startup services in 3 phases

Our definition is based on interviews with researchers-entrepreneurs and early stage startups, which are the startup factory's main target groups. We for instance discussed other similar services with them (e.g., in terms of their gaps), the specificities of cybersecurity markets, and the relationships between the target audience of the startup factory and other stakeholders.

We drew up a first set of conclusions, which we presented at several events, such as Concordia Open Door event in Luxembourg or Cybersec4europe concentration event in Toulouse. Some examples are:

- Community building through networking and brokerage is fine, but startups would not pay for it.
- Support for skills and education including mentoring is highly welcomed and some startups are willing to pay for it, if organised at the regional level
- The concept of cybersecurity-specific incubators received positive feedback and these could be pan-European
- Startup vouchers (e.g. for use of testing facilities, or certification) are also seen as a good idea.

- At the moment there is no problem with access to finance, but startups have difficulty to reach customers without partnerships with trusted and established large companies. Partner matchmaking could be a good idea.
- Business development support in CONCORDIA is welcomed and KPIs should be related to “access to final customer” instead of pure financing

Participation in other events (e.g., ECSO Cyber Investor days and South Summit) had the objective of gathering opinions from early stage startups, in order to understand their needs as well as further promote the CONCORDIA startup community.

Startup challenges

Based on our literature study and the interviews we conducted, we identified four key challenges for cybersecurity startups:

Access to early adopter customers, which is critical for any new company, but in the case of cybersecurity it is much more problematic, since the business is based on trust. Customers do not want to be the first client and they often prefer well-known providers or brands, even if these established players lack agility or innovative products. This is even more the case for operators providing essential services or operating specific market segments such as defence, which are experienced in working with startups, for instance in the form of subcontractors of large companies.

Access to funds and financing, which seems to be rather satisfactory because startups have several alternative funding mechanisms at their disposal (e.g. incubators, open challenges or hackatons, cyberinvestor events etc), which is unlike a few years ago when the set of options was more limited and bank credits or “friends and family” financing models were predominant. However, solving finance issues does not solve all the problems for the startup. Investments from seed funds, for example, do not bring references and is not a guarantee for the solution deployment. Customers do not trust some existing references that come from research or innovation projects, and often ask for references from the operational environment with customers that are similar to them in terms of size and market segment. Here again, financing that mixes partnership with larger companies, or some sort of vouchers or incentive for first time deployment, was mentioned as one of the possible solutions.

Keeping up with the quickly changing cybersecurity landscape, which forces all stakeholders to continuously monitor technology and markets, as well as to implement internal innovation processes to maintain appropriate level of security. While this is an important activity for any company, it is more complicated for early stage startups because they often do not have resources for this kind of tasks. Similar concerns were expressed for future certifications, labelling and compliance tasks.

Developing business support services for startups, which is important because cybersecurity companies will be collaborating with many parties in many different ways in the future, including jointly entering the market and subcontracting. This translates to specific business model challenges, including cybersecurity startup value networks. Knowledge sharing and best practice exchange is expected with similar companies operating in other regions, universities, corporates, startups and

other Member States. Support services, such as mentoring or business partnership building, will thus play a vital role.

6.4 Outlook Y2

In Y2, we will be comparing regional differences, such as the investments in different Member States, the ratio venture capital available, cultural and institutional factors, risk appetite.

We will also look to join parts of this task with those from T5.1, which deals with more mature startups. Based on best practices we plan to publish a “Guide for young cybersecurity entrepreneurs”. The work on data sharing incentives will also start in year 2, with stronger collaboration between pilot activities and tasks T3.1 and T3.2.

7 Conclusions and outlook

As a community building and sustainability activity, WP3 has fully met its objectives for Year 1 and proactively explored enhancements beyond the baseline activities scoped in the DoA. All WP3 activities are currently on track and all tasks have outlined their Y2 work.

8 References

- [1] MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing. (<https://www.misp-project.org/>)
- [2] The “Advanced Cyber Defence Centre” project - Information Sharing Platform/Central Clearing House. (<https://acdc-project.eu/software/information-sharing-platformcentral-clearing-house/>)
- [3] DDoS-DB homepage, <https://github.com/ddos-clearing-house>
- [4] K. e Silva, “Mitigating botnets: Regulatory solutions for industry intervention in large-scale cybercrime”, Ph.D. thesis, Tilburg University, Dec 2019
- [5] J. Conrads, “DDoS Attack Fingerprint Extraction Tool: Making a Flow-based Approach as Precise as a Packet-based”, M.Sc. Thesis, University of Twente, Aug 2019

Annex A: Assessing the courses for Cybersecurity professionals already developed by CONCORDIA partners (T3.4)

Abstract: This document is part of the deliverable D3.1 and is providing insights on the courses for Cybersecurity professionals already developed by CONCORDIA partners while placing them in the larger landscape of cybersecurity. The findings reflect the period of assessment between January – October, 2019, and will be further used as a basis for establishing a European Education Ecosystem for Cybersecurity.

Editors	<i>Felicia Cutas</i>
Contributors	<i>EIT Digital – Felicia Cutas UMIL – Claudio Ardagna UOP – Kostas Lampropoulos UT – Mattijs Jonker TUDA – Neeraj Suri</i>

A.1 Executive summary

Cybersecurity as a concept in industrial and business environment was considered in the past as an after-thought of the design and operation of Informational Technology systems process. This had to do with the lack of proper training and security awareness of the business/industrial professionals involved in such environments. Under the light of many cybersecurity attacks that have caused havoc at European and International level and produced considerable risks and damages, this attitude has considerably changed. Thus, nowadays, there is a growing need by the industrial professional community for learning basic but also advanced cybersecurity concepts. This is reflected in the considerable amount of offered cybersecurity courses by various European and international organizations. However, despite the plethora of options to learn there is a profound lack of coherency and holistic planning in this training and awareness effort since each offered course (or series of courses) is designed with different criteria from other courses (by another organization). Hence, in several cases this approach is confusing the trainee on what and how he should perceive cybersecurity concepts, as well as how to use them to cover his professional needs. In Concordia, we acknowledge the problem and try to address it by developing a European Education Ecosystem for Cybersecurity that will include a broad range of courses presented in a consistent and coherent manner, that will take into account the actual needs of both the industry and the industry professionals, and that will indicate the roadmap on how to design new course serving the professionals in the best possible manner.

This document presents the portfolio of courses offered by the CONCORDIA consortium to different categories of industry Cybersecurity professionals within Europe such as technologists, mid-level managers, executives. This endeavor, along with other actions to be developed under WP3, aims at contributing to the development of a European Education Ecosystem for Cybersecurity.

The findings presented in this paper will be further used in developing a Cybersecurity specific methodology for the creation of new courses and teaching materials for Cybersecurity professionals, and for potentially identify unmet needs in terms of courses. It will also contribute to developing a Cybersecurity Roadmap for Europe as part of the WP4.

The document is organized as a progression of 3 chapters that cover the following:

Chapter A2: outlines the major educational/competence building challenges related to the Cybersecurity sector while also introducing a non-exhaustive collection of available Cybersecurity courses for professionals, both online and offline. The chapter overviews trends in needs of European companies in terms of cybersecurity types/profiles of jobs openings on LinkedIn over the period April – October 2019 and closes by pointing to different models aiming at helping (future) Cybersecurity professionals in developing the needed skills to build their career within the sector. The intent is to contribute, as viable, to match the “demand and supply” for talent in term of skills development.

Chapter A3: presents the currently available pool of Cybersecurity relevant courses already developed by the CONCORDIA partners. The data on these courses was collected as to reflect their linkage to the five pillars of the data-centric approach to Cybersecurity advocated by CONCORDIA, and also their association to the five core industrial pilots that CONCORDIA is focusing on, namely Telecom, Finance, Transport e-mobility, e-Health and Defense sectors. Furthermore, the CONCORDIA industry partners were queried on their needs in terms of cybersecurity skills and people, in an attempt to get a better understanding of the general skills gap challenge.

Chapter A4: closes with some recommendations on the characteristics of courses needed to be offered on the Cybersecurity skills marketplace as to face the current challenges and to support the increasing demand for Cybersecurity professionals.

A.2 The Landscape

What are the key Cybersecurity needs and challenge areas?

The digitization of industries, the constant increase in number of interlinked IoT devices, the dramatic rise in the data volumes and the pervasive use of ICT technologies in all walks of life are expanding the list of Cybersecurity risks.

A [survey conducted by TUV Rheinland](#)¹ lists 8 main trends in Cybersecurity for 2019. Relevant to our assessment exercise it's worth mentioning the following trends. Trend 1: Cybersecurity has become a board-level issue, Trend 5: The Cybersecurity skills shortage will distort the labor market, and Trend 8: Cybersecurity will define digital economy winners and losers.

Indeed, it is important to acknowledge that Cybersecurity it is not strictly an "IT matter" any longer, but it impacts all levels of the businesses and turned into a business risk. Cybersecurity strategies should address horizontally all departments of an organization and would need to be allocated reasonable funding, both for investing in technologies and in people at different levels. Thus, it becomes paramount to increase the trained workforce pool and to upskill the existing one, both in general knowledge but also in very technical ones.

According to the Varonis' infographics [The future of Cybersecurity budgeting](#)², most C-level executives (60%) interviewed consider that the current solutions they have implemented in their organizations keep them safe from cyber threats, thus do not prioritize investment in information security products and services. The disagreement over priorities between the senior management and the Cybersecurity experts contributed to exposing the companies to data breaches. Nevertheless, the importance of cyber protection is more and more acknowledged and 75% of the organizations studied have increased their Cybersecurity investments in the past 12 months. It is not clear though to which extent, part of this budget is allocated to skills development within the organization.

[More than 40% of cyberattacks](#)³ are targeting small businesses. Besides, to date, 60% of small companies go out of business within six months of a cyber-attack. The skills shortage estimated to reach 1.5 million globally by 2020 will lead to an increase in salaries, making it challenging for the small organizations to attract talent so as to protect their organization. Consequently, if little investment in developing Cybersecurity skills within the organization is made, the cyber risk will turn into the main business risk.

¹ <https://img06.en25.com/Web/TUVRheinlandAG/%7B72babaf7-4989-4086-a89b-2536d75429b5%7D TÜV Rheinland Cybersecurity Trends 2019 EN.pdf>

² <https://techaeris.com/2019/05/11/infographic-the-future-of-cybersecurity-budgeting>

³ <https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html>

The Cybersecurity sector has a strong annual growth rate, as the worldwide market for information security is expected to reach €145 billion by 2020. Part of this growth is generated by startups and young companies from the Network and Information Security sector, those innovative and agile way of acting bring an added value to the sector. An ENISA analysis on [Challenges and opportunities for EU Cybersecurity startups](https://www.enisa.europa.eu/publications/challenges-and-opportunities-for-eu-cybersecurity-start-ups)¹ confirmed that the start-ups are as well impacted by the skills shortage because of the scarcity of the appropriate profiles and the cost of sourcing, which reduce their chances to scale-up. The same analysis identifies that on top of the category of investment and funding channels for the NIS start-ups are the following: investors specialized in Cybersecurity (eg. accelerators); investors non-specialized in Cybersecurity; private stakeholders that provide support other than funding to NIS start-ups, such as private incubators, private accelerators and corporate open innovation in large companies. Some of these categories could be also looking into developing knowledge and be kept updated in the Cybersecurity area for the benefit of the startups they are investing in, and of the European Cybersecurity industry as a whole.

But the investors are not the only “un-conventional” category of professionals those activities would benefit from acquiring knowledge on cybersecurity. Following the trend of digitization, the cyberattacks are threatening an increased range of industries, thus forcing a shift in skills needed to perform traditional tasks. For instance, in the health sector, physicians would not only need to take care of the patients but also to protect their data. The cybersecurity threats and some of the associated vulnerabilities that currently affect the health sector are well described in the publication [Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients](https://healthsectorcouncil.org/wp-content/uploads/2018/12/HICP-Main-508.pdf)² which also recommend [cybersecurity practices for small organizations](https://healthsectorcouncil.org/wp-content/uploads/2018/12/tech-vol1-508.pdf)³ and for [medium and large organizations](https://healthsectorcouncil.org/wp-content/uploads/2018/12/tech-vol2-508.pdf)⁴. Same goes in the legal area where the practitioners would not only need to understand cybersecurity field if interested to become a cybersecurity lawyer but also to protect the information they are working with as a significant amount of data is collected during the process. Universities are expanding their offers as to prepare the new generations, but the practitioners should also get an understanding of the cyber domain and develop basic security skills.

When it comes to the IT professionals, the [Tripwire Skills gap survey 2019](https://www.tripwire.com/misc/skills-gap-survey-2019/)⁵ revealed not only that the skills gap is growing and it is getting harder for the companies to hire skilled security professionals, but also the fact that the skills required to be a great IT security professional are changing at a faster pace.

¹ <https://www.enisa.europa.eu/publications/challenges-and-opportunities-for-eu-cybersecurity-start-ups>

² <https://healthsectorcouncil.org/wp-content/uploads/2018/12/HICP-Main-508.pdf>

³ <https://healthsectorcouncil.org/wp-content/uploads/2018/12/tech-vol1-508.pdf>

⁴ <https://healthsectorcouncil.org/wp-content/uploads/2018/12/tech-vol2-508.pdf>

⁵ <https://www.tripwire.com/misc/skills-gap-survey-2019/>

Both higher education industry and the professional training providers are working to address the increase skills need. But, as reflected in the ECSO paper [Gaps in European Cyber Education and Professional training](#)¹ there is a need for a transformation in the area. Cybersecurity is to be viewed as an emerging meta-discipline and not just an academic discipline. The academic education system approaches Cybersecurity from a holistic perspective whereas the professional training is usually focused on specific skills. As are addressing different learning needs, they should both be part of a career development path. Besides, they should not work in isolation but cooperate and exchange knowledge.

One of the challenges the organizations are facing today when looking for Cybersecurity specialists, is the difficulty in matching the recruitment criteria with the studies and the qualifications listed in the CVs of the applicants because of the use of non-standard terminology. The [adoption of a standard lexicon, including cyber role responsibilities](#)² will help on the one hand companies identifying the right talent for the job, and on the other hand the education providers better shape their curriculum to match the cyber workforce needs.

Finally, as the cyber threats an organization is facing are diverse and would require different type of skills and perspectives, a [diverse team](#)³ should be built. The diversity within the team would require different backgrounds and personalities (techies, creative people, problem solvers, communicators, ...) but also different age and gender. It will bring the advantage of reaching better outcomes as will help assessing situations from different perspectives and providing different approaches to problem solving.

What are the different Cybersecurity competencies needed?

In the context of the CONCORDIA project and for the purpose of this analysis we use the term “**Cybersecurity professionals**” as including academia thought mostly the broad group of industry representatives such as IT technical team members and experts, middle managers leading IT or non-IT technical departments, and executives of the companies.

Since Cybersecurity is a horizontal issue impacting all digitized industries, the needs in terms of competencies might differ but the following elements could be considered generally valid:

- IT Technical team members – are looking for acquiring new knowledge, developing new skills, and to upskill the existing ones. This category could

¹ <https://www.ecs-org.eu/documents/publications/5bf7e01bf3ed0.pdf>

² [https://niccs.us-cert.gov/sites/default/files/documents/pdf/cybersecurity talent identification and assessment.pdf?trackDocs=cybersecurity%20talent%20identification%20and%20assessment.pdf](https://niccs.us-cert.gov/sites/default/files/documents/pdf/cybersecurity_talent_identification_and_assessment.pdf?trackDocs=cybersecurity%20talent%20identification%20and%20assessment.pdf)

³ <https://www.forbes.com/sites/extrahop/2019/07/19/how-to-combat-the-security-skills-shortage/#27db2e464eae>

incorporate also the recent graduates and the students coming back to the universities to follow only specific Cybersecurity related modules.

- IT Technical experts and freelancers – are looking for expanding their Cybersecurity knowledge, or to test their skills in different scenarios.
- Middle-managers leading IT departments – are looking into learning about new techniques and/or solutions to identify, protect, detect, react fast and recover from a cyberattack.
- Middle-managers leading non-IT departments – are looking into understanding the general cyber related risks, and into practical techniques to be implemented as to avoid a cyberattack, and to recognize and know how to react in case such an event occurs. This category could include also non-traditional categories such as physicians, lawyers.
- Executives – are looking into having a general understanding of the Cybersecurity area and its impact on the business, investment and insurance wise included, as Cybersecurity is becoming a business risk. Cybersecurity Auditors within companies are also part of this group. This category incorporates also the startups and scaleups which do not afford having a specialized IT department to protect their business thus need to cover all the aspects of the business.
- Investors looking into in developing knowledge and be kept updated in the Cybersecurity area, in view of placing funding in different cyber or non-cyber related businesses.
- Academia – are looking for enriching their theoretical knowledge with information on new protocols, techniques, products, services developed by the industry
- Non-IT employees – not necessarily actively looking into developing Cybersecurity skills but being asked by the company procedures to have a basic knowledge in the field in order to prevent and/or react properly in case of a possible cyber-attack. This category could include also the users in general.

Besides, in order to build a career in Cybersecurity one should be aware that apart of technical skills, soft skills such as analytical-, communication-, writing-, leadership skills should ideally be developed.

These needs are backed by the findings of the International Information System Security Certification Consortium (ISC)² in their [2018 \(ISC\)² Cybersecurity workforce](#)

[study¹](#) in which Cybersecurity experts identified common challenges that could be addressed at the company level such as: the lack of security awareness among end-users; a lack of funding; not enough skilled staff available; a general lack of support/awareness from management about the urgency of Cyber- security initiatives overall.

Furthermore, the (ISC)² study also depicts different skills areas identified by Cybersecurity professionals as important to be improved or enhanced in the future.

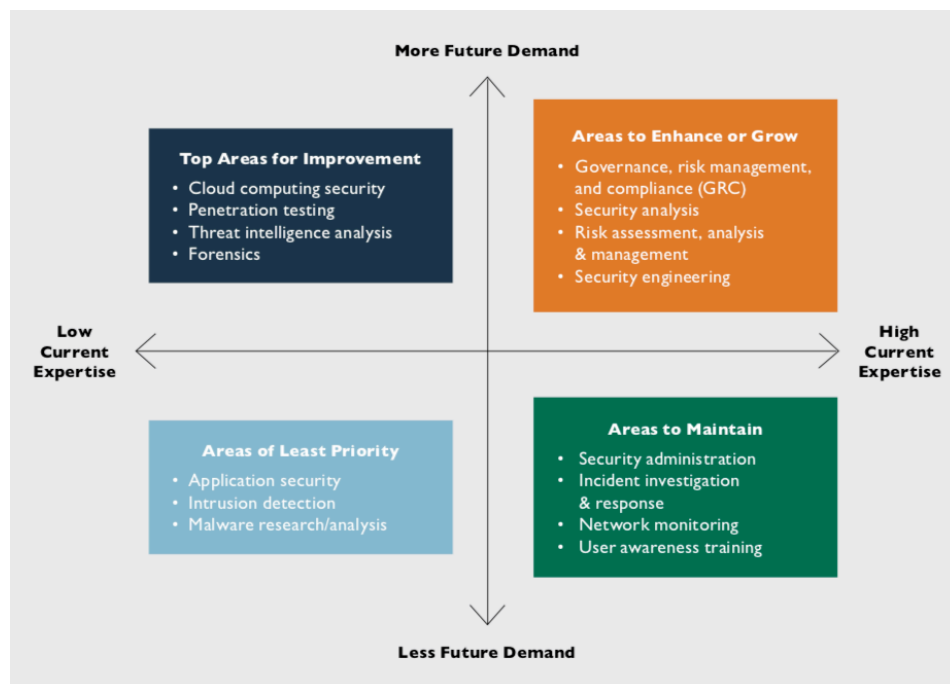


Figure A1. Credits: (ISC)²

It is important to note that, in today data-driven environment and data-driven economy, a cyber-security professional must have competences in the area of data analysis. The latter in fact is of paramount importance for guaranteeing and verifying cybersecurity in modern architectures. Even more, the role of the data scientist is fundamental to get rid of novel threats and attacks. In fact, security is moving from application security to data security, meaning that cybersecurity depends on data security and the capabilities of correctly interpreting the data at our disposal. Today, many Artificial Intelligence approaches are applied for guaranteeing cybersecurity, while, in turn, cybersecurity techniques are applied to artificial intelligence to prove some security properties on them. The need of data analysis for cybersecurity is clear in all above boxes in Figure A1. and especially in the dark blue box – “top areas for improvement”, where a huge amount of data is collected every day (e.g., Cloud) and the ability of correctly analyzing them become fundamental (e.g., forensics). This is also true in the orange box – “areas to enhance and growth” pointing to the new effort

¹ <https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0>

supported by the European Commission in the definition of the [EU Cybersecurity Certification Framework](#)¹.

A look into the available course offerings

In the context of CONCORDIA, we consider the **courses/trainings for Cybersecurity professionals** as the courses to which a Cybersecurity professional can have direct access without being constrained to be enrolled in a full programme. These could be organized online, face-to-face, or could be blended.

A search on the Internet reveals that there is a plethora of courses addressing Cybersecurity professionals. The online courses are convenient to professionals as they offer full control on organizing peoples' time for studying thus helping them to cope both with the professional business life and the needs for upskilling or reskilling. These could be doubled by face-to-face courses for middle and senior managers or executives, or by specific competitions such as cyber-ranges for technical experts.

When it comes to the online courses, we identified the main platforms from the viewpoint of the users and of the Cybersecurity related content as being the following:

- [Coursera](#)² – has 33 million users and it has in its portfolio about 50 courses on Cybersecurity, most of them addressing introductory topics.
- [edX](#)³ platform – has 14 million users to which it offers only around 30 Cybersecurity related courses
- [LinkedIn Learning](#)⁴ - a learning platform with 9.5 million users, hosts around 120 courses on Cybersecurity, half of them addressing intermediate skill level, closely followed by courses aimed at developing basic skills levels
- [Cybrary platform](#)⁵ offers to its 2 million users about 500 cyber specific video courses for professionals as to develop their careers, but also for businesses in view of workforce development.
- [IASACA](#)⁶ (Information Systems Audit and Control Association) provides online, offline and mixed courses of different levels (foundation, practitioner) both for information security and Cybersecurity, including courses for Cybersecurity auditors. The courses are sanctioned by certifications. IASACA is a nonprofit global association that serves 140,000 professionals in 180 countries
- [Udacity platform](#)⁷ – has 8 million users but has only a small (9) number of security/Cybersecurity courses

Although they are addressing the same market, each platform is structuring the information based on its own model, and without making a reference to any common

¹ <https://www.enisa.europa.eu/news/enisa-news/the-european-union-agency-for-cybersecurity-a-new-chapter-for-enisa>

² <https://www.coursera.org/>

³ <http://www.edx.org/>

⁴ <https://www.lynda.com/>

⁵ <https://www.cybrary.it/>

⁶ <https://www.isaca.org/pages/default.aspx>

⁷ <https://www.udacity.com/>

competence framework. Thus, it makes difficult to compare the different offers and their attractiveness.

In an attempt to measure the reaction of the market to the risks the cyberattacks are bringing within the different industries, we used the public statistics offered by LinkedIn Learning platform over a period of 6 months and monitored the number of “views” of different Cybersecurity related courses. The figures confirmed for instance a reaction to the increased Cybersecurity risk for the business by registering a raise in number of “views” from one month to another (between 7-15%) on courses for managers such as “Reasonable Cybersecurity for business leaders”, “Cybersecurity for executives”, “Microsoft Cybersecurity: shutting down shadow IT”, “Cybersecurity for SMEs: essential training”, all launched in late 2018 or early 2019. The biggest increase in views (19-20%) is registered for the course “Transitioning to a career in Cybersecurity”, and the newly launched (June 2019) “Cybersecurity for IT professionals” and “The Cybersecurity threat landscape”.

With respect to the cyber-ranges, information is very scarce thus difficult to assess at this stage. cyberwiser.eu¹ – the “Civil Cyber Range Platform for a novel approach to Cybersecurity threats simulation and professional training” newly launched end of 2018 and benefiting from H2020 funding, aims at providing a set of innovative tools to generate highly detailed exercise scenarios simulating ICT infrastructures to be used for Cybersecurity professional training, together with tools and solutions to simulate cyberattacks and defensive countermeasures. Cyberwiser.eu offers a “[Behind the scenes: an in-depth look at the technology behind the CYBERWISER.eu Platform](#)”²

The [European Union Agency for Network and Information Security](#)³ (ENISA) put at the disposal of interested professionals a comprehensive set of training materials in support of developing skills in the Incident Response and in the field of Operational Security. In May 2019, the [ENISA CSIRT training material](#)⁴ list was comprised of 42 titles, covering four main areas: Technical, Operational, Setting up a CSIRT and Legal and Cooperation. The offer for training courses for Cybersecurity specialists is, on the contrary, very limited. The trainings are available upon request by, for example, the National or Governmental CERT of the Member State, and must follow the EU regulation 526/2013.

ENISA and the Network and Information Security (NIS) education partners put together a [NIS universities map](#)⁵ under which there are grouped together courses and

¹ [file://cyberwiser.eu](https://cyberwiser.eu)

² <https://www.cyberwiser.eu/news/behind-scenes-depth-look-technology-behind-cyberwisereu-platform>

³ <https://www.enisa.europa.eu/>

⁴ <https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material>

⁵ <https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/universities>

certification programmes linked to Network and Information Security, most of them for undergraduates, postgraduates or at master level. Out of the 551 courses spread around the EU28, 538 are offline courses (data valid in May 2019). Most of the courses are requiring registration in a full curriculum thus they are not specifically addressing the Cybersecurity professionals and their needs as defined in this paper. Nevertheless, the map provides valuable content mainly to technical people interested in developing a career in Cybersecurity industry, not necessarily engaged in a business activity and with no time restrictions.

Different international consulting companies and organizations include in their offers courses covering Cybersecurity topics:

[Deloitte EMEA Cyber Academy](https://www2.deloitte.com/bd/en/pages/risk/solutions/deloitte-emea-cyber-academy.html)¹ – offers online trainings, awareness programs, onsite trainings and a Hackazone Zone, an online learning platform containing over 125 challenges for performing hands-on exercises related to various Cybersecurity topics. They are targeting highly-qualified technical people but also executives and directive boards, technical and non-technical managers and executives and other employee grades. The Deloitte Academy area of expertise covers Ethical Hacking, Secure Software Development, Reverse Engineering, Monitoring and correlation, DDoS, Advanced persistent threats, Forensic Analysis, Cyber Intelligence, Cybersecurity and Mobile Device Security.

[PwC's Academy](https://www.pwc.com/sg/en/academy.html)² is offering specialized courses to professionals, companies, industries and government bodies in trending domains, between them the face-to-face course “Cybersecurity for Non-Cybersecurity Professionals during which the participants will be getting involved in a proprietary virtual game – [Game of Threats](https://www.pwc.co.uk/issues/cyber-security-data-privacy/services/game-of-threats.html)³. [EY Certify point](https://www.ey.com/gl/en/services/specialty-services/certifypoint/certifypoint--training-courses)⁴ – is offering courses for certifying auditors on different standards such as ISO/IEC 27001:2013 - Information Security Management System, or SS 584: 2015 - Specification for multi-tiered cloud computing security, commonly known as MTCS

[KPMG Cyber Academy](https://home.kpmg/md/en/home/services/advisory/consulting/cyber-security/cyber-academy.html)⁵ offers a blended framework of e-learning, virtual classrooms and workshop-based face to face training. Their offer ranges from penetration testing and security architecture to identity access management and cyber maturity assessment.

What are the companies looking for?

Despite the large offer for free courses, companies are facing difficulties for filling up their Cybersecurity related positions. According to the job openings published on LinkedIn and monitored for 6 months between April-September 2019, the total number at the level of EU28 remains pretty much stable from one month to another

¹ <https://www2.deloitte.com/bd/en/pages/risk/solutions/deloitte-emea-cyber-academy.html>

² <https://www.pwc.com/sg/en/academy.html>

³ <https://www.pwc.co.uk/issues/cyber-security-data-privacy/services/game-of-threats.html>

⁴ <https://www.ey.com/gl/en/services/specialty-services/certifypoint/certifypoint--training-courses>

⁵ <https://home.kpmg/md/en/home/services/advisory/consulting/cyber-security/cyber-academy.html>

and it is around $3500 \pm 5\%$. In general, the average period for a position opened on LinkedIn is one month. The fact that the total number remains almost the same it's a proof of the continuous need for professionals in the area. UK counts for one third of the positions opened followed in top 10 by The Netherlands, Germany, Portugal, France, Poland, Spain, Italy, Ireland and Belgium. (See Figure A2)

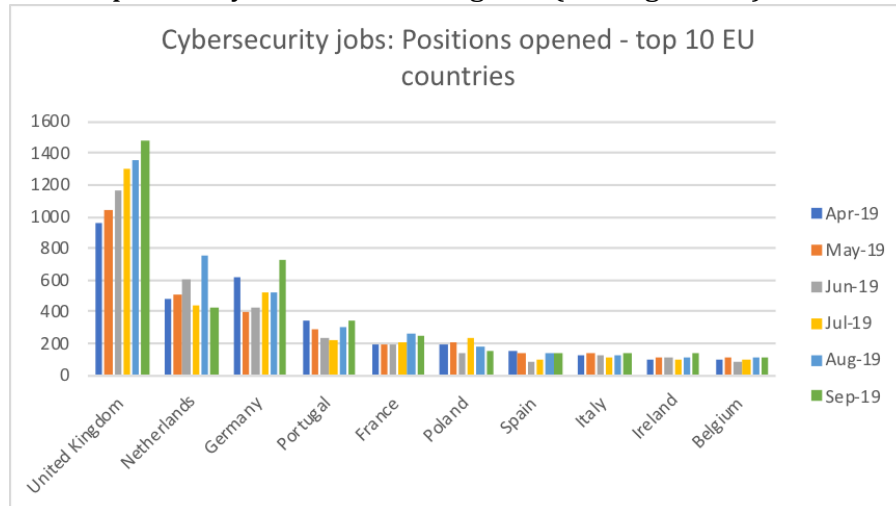


Figure A2: Cybersecurity jobs: positions opened – top 10 EU countries

When it comes to the experience required by the employer, the “Associate” level is most in demand, closely followed by the “entry level” positions. The most in demand job category in the cyber-domain is the IT, followed by far by the engineers. (Figure A3)

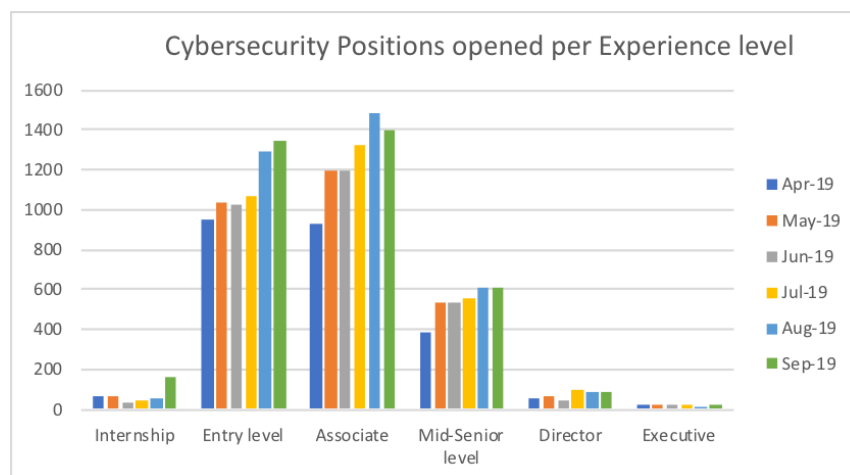


Figure A3: Cybersecurity positions opened per Experience level

If we contrast these data with the offer of courses displayed on the ENISA map with no pretention of an exhaustive analysis and aware about the limitations given by the subjectivity of the data, it can be observed that, countries with a big offer of courses, thus with presumably more entry level Cybersecurity skilled people, are not necessarily the ones also looking for hiring them and the other way around. For instance, Poland has 145 jobs opened in the Cybersecurity industry, but no course was reported on the NIS map. On the other hand, Slovenia encoded information about

12 courses on the NIS map, but the Slovenian companies have no positions open for entry and associate levels. (**Annex A.5.5.**)

How to match the companies needs with the skills offers?

Companies are usually looking for hiring already skilled IT technical people. Yet, in their absence, the companies try to re-skill and/or up-skill existing employees. This trend is confirmed also by the CONCORDIA industry partners questioned on the matter and described in the next chapter.

But the process of developing, displaying, searching for specific skills should be based on a generally agreed structure as to ensure a common language on the skills market.

In support of this endeavor one can get inspired from the US National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework which depicts for different Cybersecurity workforce categories the necessary associated knowledge & skills and the list of tasks to be performed: [NIST Special Publication 800-181¹](#). This framework document is of use for different workforce development, education, or training purposes. At the European level, as already mentioned, ECSO is calling for a specific framework for professional development in Cybersecurity, to be jointly developed with the relevant actors in the field.

The [Cybersecurity Career Pathway²](#) proposes an interactive structure by listing the core Cybersecurity roles at entry- mid- and advanced-level and details the top skills and the top certifications requested for each position. As there is no clear and generally agreed taxonomy on the job titles in the industry, a useful information is also provided on the common job titles employers list in job openings for each role while also positioning the individual roles in the most common NICE Cybersecurity workforce framework categories. An example for an entry level role is depicted in **Annex A.5.1.**

The tool is mainly designed for the use of those interested to start and develop a career in Cybersecurity. Nevertheless, the structure could be used also by the companies when deciding to open a new position on the job market, not only by benchmarking the salary expectations with respect to the competition and the demand but also using similar keywords when describing the tasks as to ease the match between their needs and the skills and qualifications listed by the applicants in their CVs.

A [Cybersecurity Competency Model Clearinghouse³](#) was developed few years ago in the US in view of promoting skill sets and competencies essential to educate and train the workforce. The model is structured on 5 tiers: Personal Effectiveness Competencies, Academic competencies, Workplace Competencies, Industry-Wide Technical Competencies, Industry-Sector Functional Areas.

¹ <https://www.nist.gov/file/372581>

² <https://www.cyberseek.org/pathway.html>

³ <https://www.slideshare.net/colleenlarose7/competency-model-clearinghouse>

Annex A.5.2. includes more details linked to the different areas from Tiers 4 and 5 depicted in Figure A4: Cybersecurity Competency Model.

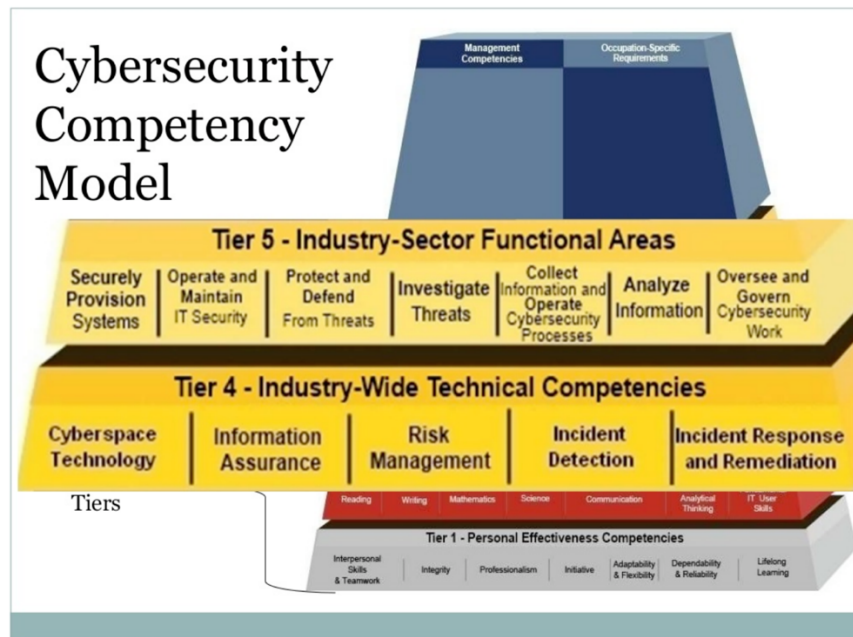


Figure A4: Cybersecurity Competency Model

At the European level, a concerted work on defining what are the competences needed to be owned/developed by different European actors playing a role in the Cybersecurity market or impacted by it, is currently pursued by ECSO in collaboration with their members, and the 4 Cybersecurity pilot projects. It will be based on existing competences frameworks such as [European e-Competence Framework](#) (e-CF)¹, NICE. The work will build, between others, on the [ECSO Information and Cybersecurity Professional Certification](#)² paper which looked into the professional security certification schemes and frameworks in Europe as well as internationally. The main findings are around the fact that the industry is still very dependent on US-centric certificates which are not based on formal training. And, even if in some European countries first steps have been taken to set up a certification scheme, the uptake of these schemes is very limited. The authors of the paper recommend the establishment of an EU-wide certification and accreditation scheme as well as a European framework for professional development in Cybersecurity.

Also, the ECHO pilot project is looking for developing a Cyber-skills framework (E-CSF) as to address the needs and skills gap of cybersecurity professionals based on a mapping of the cybersecurity multi-sector assessment framework. It is intended that the E-CSF will be made up of learning outcomes, competence model and generic curriculum in order to establish a mechanism to improve the human capacity of cybersecurity across Europe. In view of achieving this goal, the ECHO pilot will leverage a common cyber-skills reference, derived and refined from ongoing and

¹ <https://www.ecompetences.eu/>

² <https://ecs-org.eu/documents/publications/5bf7e0d81b347.pdf>

related work in the field (e.g, ECSO, e-Competence Framework, European Qualification Framework).

A.3 CONCORDIA ecosystem

We asked our CONCORDIA industry about their needs in terms of skills and technical people

In view of capturing the data, we invited the CONCORDIA industry partners to fill in a survey organized around two topics: Topic A - their practice in hiring cybersecurity related professionals, and Topic B - their needs in terms of developing cybersecurity skills within their organization.

The CONCORDIA industry partners are mainly representatives of the national and international corporate segment, and to a lesser extent the SMEs one. Less than 30% of the respondents are covering through their activities one or two of the Cybersecurity domains (see list and descriptions in **Annex A.5.3.**), while most of them develop activities touching 3-5 domains, with the Network-, Data/Application-Centric Security domains profiling on the top. When it comes to the industries they are active on, apart of the five CONCORDIA focus areas (telecom, finance, transportation, e-health and defence) some of the industry partners are also covering areas like semiconductor industry, energy, automation, IT, law, services.

The outcome of the survey can be summarized as follows:

Topic A. What are the organization's needs in terms of NEW employee categories & the associated skills?

- When looking for hiring new employees, the level of cybersecurity level requested with respect to the open position is depicted in the figure below. As expected, the IT related jobs require medium and high level of cybersecurity skills. Nevertheless, it can be observed that there is not yet a priority in asking non-technical people and executives to have basic skills in the area.

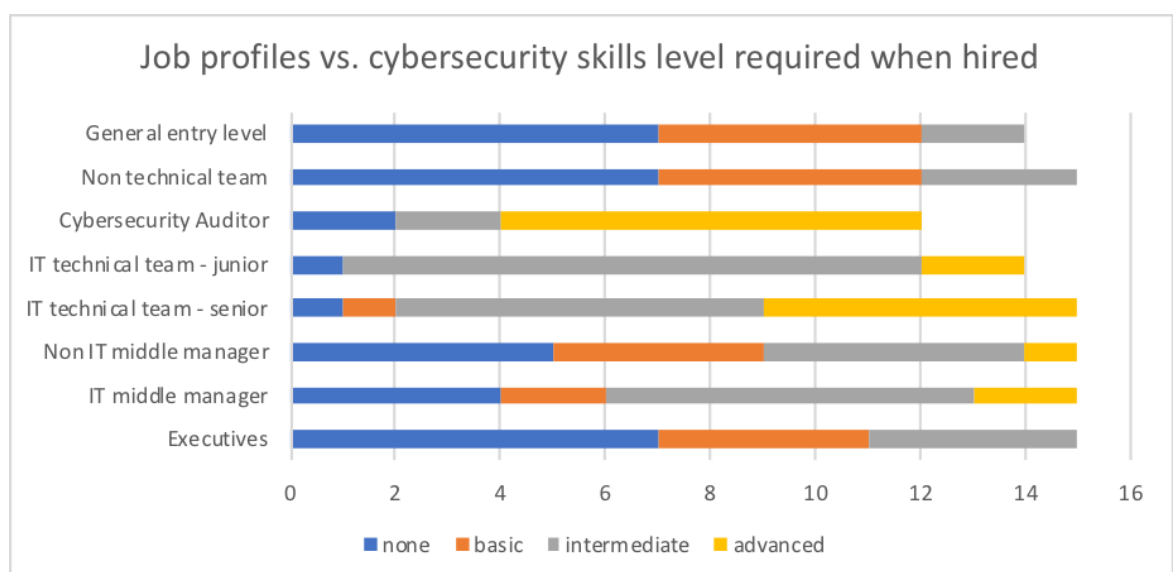


Figure A5. Job profiles vs. Cybersecurity skills level required when hired

- When asked about the relevance of the possession of a CERTIFICATE related to the cybersecurity skills in the process of recruitment, the answers are almost equally spread between Very relevant for IT positions - Relevant for IT positions - Relevant for all the positions - Not necessarily relevant - Not relevant. It worth mentioning that the Not necessarily relevant - Not relevant options were selected mainly by the SME partners.
- 80% of the companies agree that an EU harmonized taxonomy related to the cybersecurity skills linked to different job positions would be useful in the process of recruitment
- In view of addressing cybersecurity needs within their organization, more than half of the organizations would rather prefer to hire an already skilled person than to re-skill or up-skill an existing employee. Nevertheless, in case they decide to invest in personal development of the employees, the in-house courses are preferred to external courses; yet, sometimes both options are approached in parallel: train and grow internally as well as hire from the outside.
- Additional practices in recruiting new employees were reported such as: hiring young people from academics as part time, and up-skill them via training-on-the-job; hiring from outside EU due to the lack of skilled personnel.

Topic B. What are your company needs in terms of cybersecurity skills development for EXISTING employees?

- When asked about what type of content for the courses the organizations are looking for for their employees the vast majority of them pointed towards a mix of technical, hands-on and cyber-business-oriented topics. The weight of the type of knowledge within a course vary though depending on the role the employee is playing in the organization.

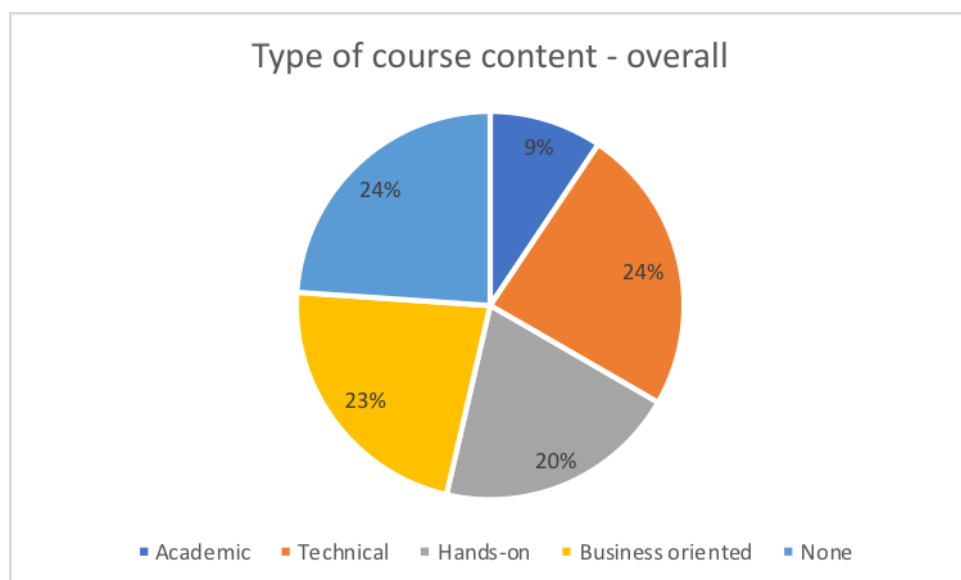


Figure A6. Type of course content - overall

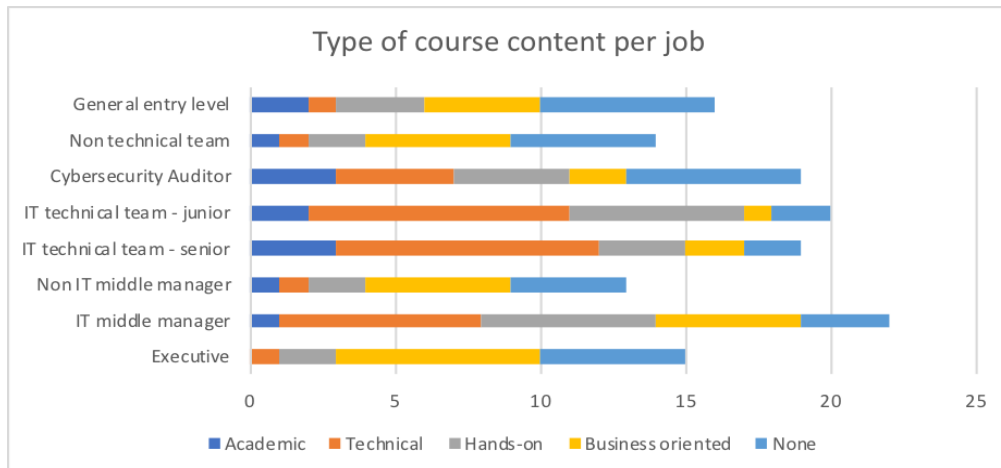


Figure A7. Type of course content per job

- Most of the companies surveyed are offering or would like to offer cybersecurity related courses to the different categories of their employees. Not surprisingly, the most targeted ones are the IT technical team seniors and juniors, but also the IT middle managers. The online format for courses is preferred by far while the blended format has the least traction.
- When it comes to the company normal practice with respect to the courses offered to their employees, apart of two companies declaring that they are offering the employees only courses developed inhouse, all the others are offering a mix of the following options: Develop and run in-house; Contract a course provider to tailor the content for the specific needs; Allow employees to find an online course that fits their needs; Buy off-the-shelf courses.
- The employees are offered the possibility to attend a course for updating their cyber related knowledge with different frequencies which vary from “as frequent as needed” listed by most of the companies to “once every 2 years”, with a preferred length of 2-3 days in case of a Face-to-Face format.
- How important is the Certification option when buying a course for your employees? The in-house courses or baseline security courses offered to the employees are not necessarily selected because of the certification options. Yet the employer is interested in more than a certificate of attendance but of a Certificate issued by the training provider following a test/exam passed and/or Certificate offered by MOOC platforms as proof of the knowledge acquired. When it comes to the certifications based on standards, the following have been listed: CSX, CSX(P), OSCP, CEH, Cyber Essentials.

The CONCORDIA industry partners were also asked to list their top 3 immediate needs in terms of skills, considering the cybersecurity threats their organization is facing. The answers pointed mainly to traditional courses and varied from Security awareness and Security fundamentals to Solid understanding of mobile network security or Use of AI/Machine Learning; from Threat Intelligence analysis, Penetration testing and intrusion detection and Malware analysis, to Secure chip-design, Secure software-design and secure hardware-software co-design. Specific mentions were included on the importance of a hands-on, exercise-based approach

including for the online format of delivery which should be as interactive and real life as possible.

Finally, the partners were asked to add any other comments linked to developing skills for cybersecurity professionals and which were not addressed by the previous questions. The most relevant of them are listed below and will be used in the development of the cybersecurity specific methodology for the creation of new courses and teaching materials.

“Need to easy to access and register courses, that are online, that are mobile device friendly, that cover concepts intuitively, and can provide links to more hands-on courses, if follow-ups are needed”

“We have a number of internal online courses which are obligatory for each employee and others that are obligatory for certain roles.”

“Coaching is an important part during the learning process. Could be on-line. “

"Cybersecurity professionals would benefit from the development of soft skills that could further support them works in a collaborative manner."

"Academic degrees, although interesting, appear to lack basic skills for the cybersecurity practitioners. When hiring a person with a degree in the subject, usually that only means that she/he have the potential to understand the subject provided specific theoretical and on the job training is provided. But even so, in some countries it is difficult to find even that. (e.g. Germany, Austria,...)"

"the semiconductor industry take a special place in the cyber security market; semiconductor companies stay at the beginning of the value chain for the security industry, which are focus on prevention of cyber attacks; secure microcontroller, means develop, qualify and certify products along ISO 15408, EAL4+, 5+ or 6+"

CONCORDIA professional education landscape

CONCORDIA aims at establishing a European Education Ecosystem for Cybersecurity. The first step in this endeavor is to start collecting information on what CONCORDIA consortium offer in terms of skills development (university and industry partners). This data will be contrasted with the needs in terms of skills of different CONCORDIA partners (mainly the industry partners) and of the market as to identify the potential unmet needs in terms of skills development.

To this end we invited all the CONCORDIA partners to provide structured information on the courses/trainings they are organizing for Cybersecurity professionals.

Apart of a general description of the course, its location and the language taught, the following information aligned to the CONCORDIA scope and objectives were also collected:

- **Cybersecurity pillars** addressed – Device-centric // Network-centric // System/Software-centric // Application/Data-centric // User-centric security – see description of the pillars in **Annex A.5.3**.
- **Industry field** addressed - with a focus on CONCORDIA sector-specific pilots: Telecommunication // Finance // Transportation/e-Mobility // eHealth // Defence
- Main **target audience** – different categories of industry professionals
- **Type of course** (face-to-face, online, blended)
- **Entry requirements**
- **Type of Certification** offered

By end of year 2019, the CONCORDIA partners both from industry and academia, provided information on a total of 33 courses (**Annex A.5.4**). The data is displayed on a [dynamic map](#)¹ on the CONCORDIA website for the use of the community at large. The map provides different filters as to help match easier the specific need for skills development with the offer.

Over the course of the CONCORDIA project, the map will be periodically updated with the new courses/trainings developed by the different university and industry partners. Besides, in our effort for establishing a European Education Ecosystem for Cybersecurity, the map is open for submission of courses/trainings for Cybersecurity professionals organized by other European organizations. To date the map displays already 27 courses organized in Europe by different organizations outside the Concordia consortium. The map will thus have the potential to become a marketplace for Cybersecurity skills for professionals.

General considerations

Most of the CONCORDIA courses were launched in 2018 or 2019. They are usually running once or twice a year with few exceptions such as the Cyber Incident Game planned for 4 sessions over a year, and SINA basic scheduled twice a month, with 15 sessions in total over a year. The short courses are between one day and one weeklong and are addressing groups of 10 to 20 people. The longer courses of the equivalent of one university semester (12-14 weeks) are bringing together larger groups of participants, namely between 80-120. Most of the courses are offered against a fee.

Cybersecurity pillars

A close look into the data collected with respect of the five CONCORDIA Cybersecurity pillars (**Annex A.5.3**) addressed reveals the fact that almost 40% of the courses are specifically targeting one cybersecurity pillar, while another 40% are offering content valid for two or three pillars. Nevertheless, some courses are tailored to develop more general skills relevant for all the five pillars.

The most addressed pillars are the Network-centric, followed closely by the Data/Application-centric security and the Software/System-centric pillars.

¹ <https://www.concordia-h2020.eu/map-courses-cyber-professionals/>

Interestingly, the least covered skills are in the area of Device-centric security which deals with data acquisition and the devices producing raw data such as embedded systems, sensors, IoT devices. The User-centric security pillar is also less addressed in the courses curricula although it deals with issues like privacy, social networks, fake news and identity management. This could be explained by the fact that CONCORDIA partners are mainly acting in the areas linked to the transportation and usage of data, and less in those dealing with data acquisition and devices producing raw data.

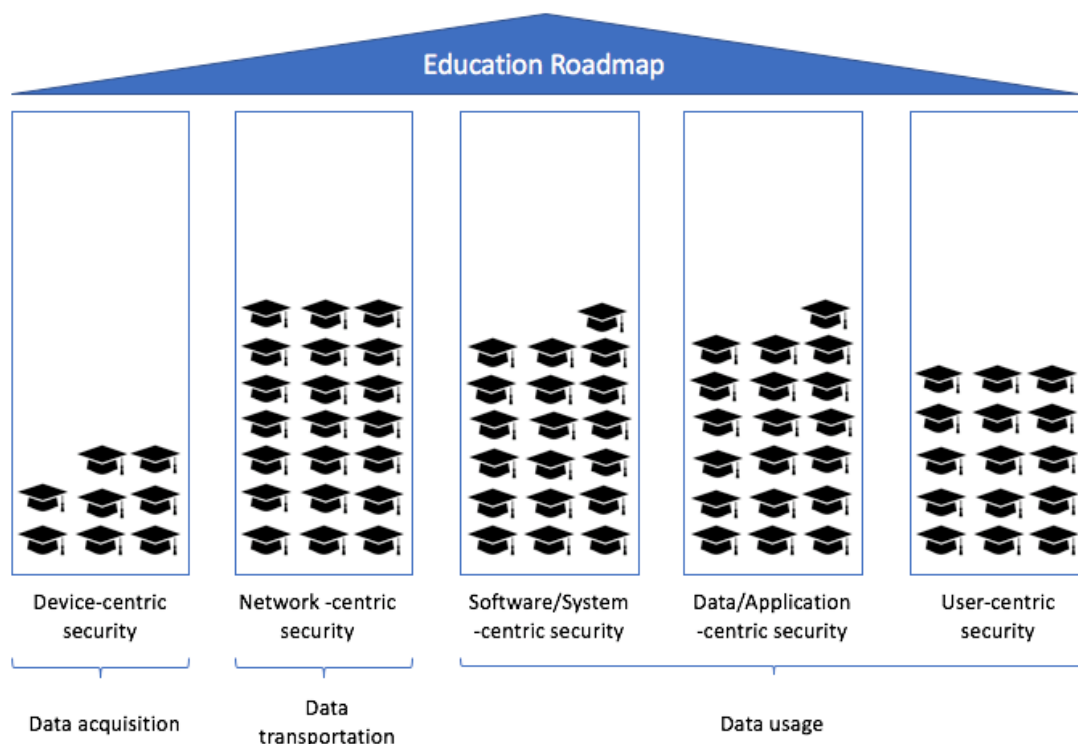


Figure A8: CONCORDIA courses – content vs. the cybersecurity pillars addressed

Industry fields

The five CONCORDIA sectors (Telecom, Finance, eHealth, Defence, Transportation / e-Mobility) are almost equally covered by the to-date CONCORDIA training portfolio with Telecom sector being the most addressed. The majority of the courses help develop skills applicable to at least 4 CONCORDIA industry sectors. Nevertheless, a number of other courses are targeting different other industries such as cloud, IoT, critical information infrastructure or operating systems, while almost a quarter of the courses are not related to any industry in particular.

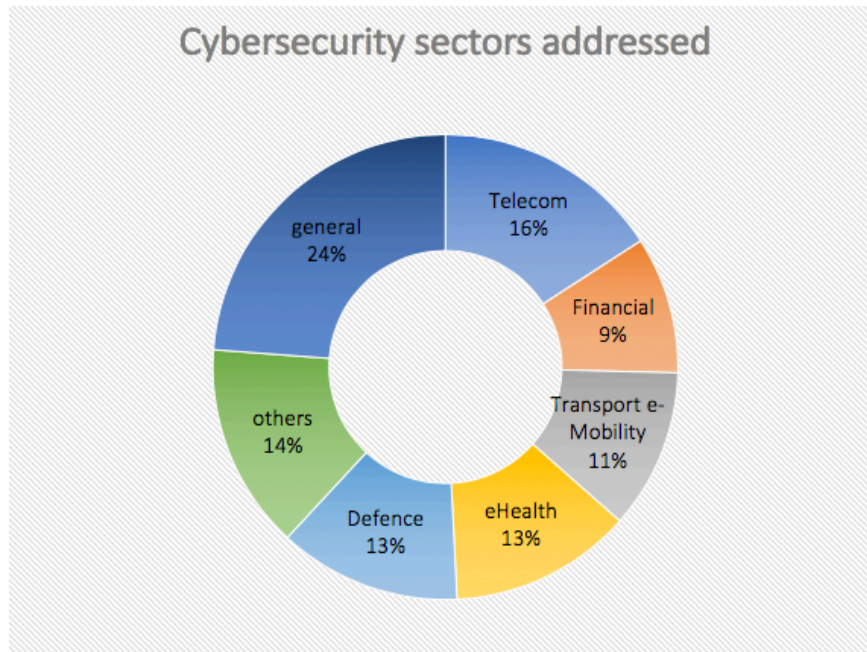


Figure A9: CONCORDIA courses – content vs. industries relevance

Target audience

The existing CONCORDIA courses are mainly addressing the technical people, and to a lesser extent the middle managers of non-IT departments and the executives of big and small companies.

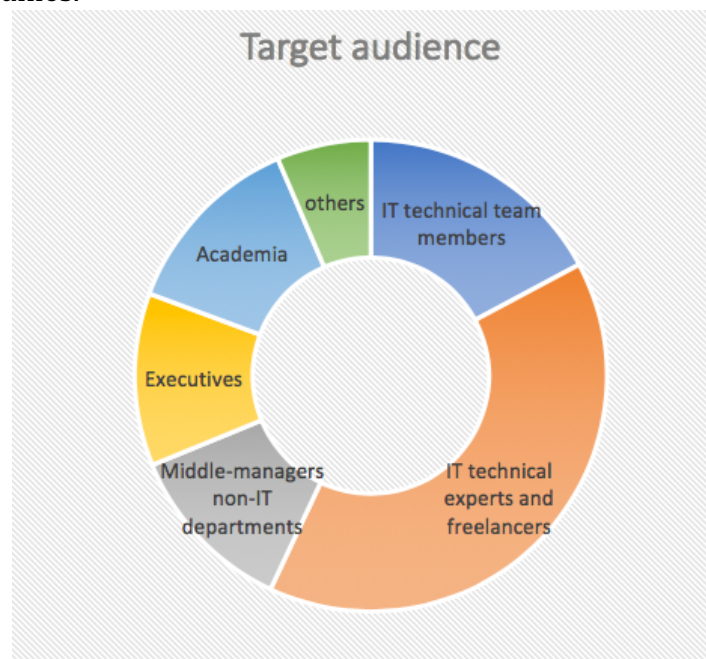


Figure A10: CONCORDIA courses – distribution of the target audience

Delivery method - F2F, online or blended?

According to the (ISC)² Cybersecurity Workforce Study 2018, the employers' main choice in offering skilling opportunities to employers is the online version as this is the most cost effective one from the management perspective. The face-to-face option

ranks 5 in the list of options for professional development in the workplace, after conference attendance, personal study review and on the job with peers' alternatives. On the other hand, the same study reveals that the employees are more prone to attend the face-to-face (F2F) courses as these give them more opportunities to interact and network, to exchange experiences, and it is closely followed by the internet-based training.

When it comes to the CONCORDIA courses, the vast majority of them is offered exclusively in a face-to-face format while only two are fully online and three others are blended. Thus, they are very much aligned to the employees' appetite to consume this type of service.

Language taught

18 out of the 33 CONCORDIA courses are taught in English or offer this option as alternative to German or French. This already proves an openness to the European Cybersecurity skills market as language is not, in this case, a barrier. Nevertheless, 20% of the courses are exclusively taught on less common languages such as Czech, Dutch, Slovene or Italian.

Content

Content wise, the CONCORDIA courses are focusing on developing specific technical skills. This is reflected in the target audience those main group is the technical team, followed by academia and students' group. Nevertheless, some other courses take a broader approach to the topic and have low or no entry requirements thus are more accessible to a larger audience such as senior managers, managers of non-IT departments, startups.

Certification

To date, none of the courses organized by CONCORDIA partners are offering industry recognized certifications. Nevertheless, some of them are preparing the participants in view of applying for ISACA and (ISC)2 certifications. The vast majority of course providers are issuing certificates of participation, sometimes signed by a Cybersecurity expert. Others offer certificates of completion issued by a well-established online training platform such as Coursera.

Alumni

Although no consistent data was collected with respect to the participants to the courses organized by the CONCORDIA partners, the following information was considered to be a good estimate on the graduates so far:

- Total number of participants over the whole period the courses run: 5900+
- Gender distribution: 91% males and 9% females
- Age distribution: the majority of the attendees are in their early stages of their careers or in the growing stage as 62% of them are between 25-34 years old. 35% of the participants are between 35-54 years old and only 3% are between 55-64 years old
- Country of origin – most of the participants come from the countries in which the course is hosted (in case of the face-to-face courses). In case of longer

duration courses (the equivalent of one university semester) the participants group is multinational like in case of a course organized in Germany which, apart from other EU participants, attracts people from China and India; or the case of the courses in Slovenia attracting also participants from Croatia, Spain, Portugal and Turkey.

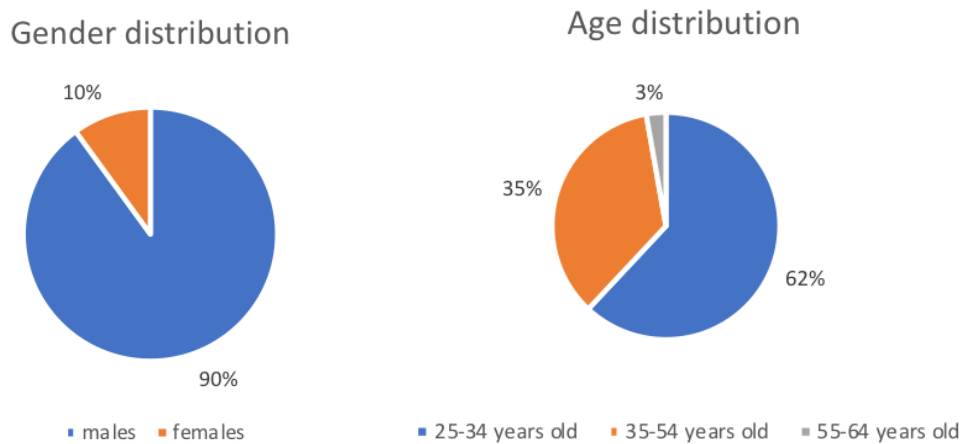


Figure A11: CONCORDIA courses – past participants distribution per gender and age

The external courses plotted on the CONCORDIA map

The CONCORDIA map was open for external submissions starting mid-July 2019. Over a period of 2 months there were submitted 27 courses via the [Register your Course](#)¹ form. This pool of external courses following to a certain extent the characteristics of the CONCORDIA courses and could be described as follows:

- **Pillars:** most of the courses address the Software/System-centric, Network-centric and Application/Data-centric pillars while the less targeted one is the User-centric pillar
- **Industry:** the vast majority of the courses are developing skills fit for the Telecom industry, followed by the Transport industry; some of the course providers reported also other areas of use of the skills acquired via their courses such as Energy.
- **Target audience:** most of the courses are targeting the corporate audience, mainly the technical team members but also the managers of the non-IT departments and the senior management group. Some of them are targeting the users - individuals using 5G technology or those interested to learn the approaches used by hackers, while one is specifically addressing the public administration
- **Delivery method:** face-to-face is the model used by 70% of the courses while only 4 are run online and only 1 is offered in a blended format.
- **Language:** the language used is, generally, country specific. Nevertheless, some of the course providers offer the course (also) in English, or provide the documentation in English

¹ <https://docs.google.com/forms/d/e/1FAIpQLScg5QrSQEOikUAJguXL3OrBhIPh3FzZzSvBk2RhGmh6ZRIMtQ/viewform>

- Content: only 20% of the courses do not require any entry requirements as the content provided is considered introductory or close to introductory to the specific topic. All the other courses require basic to medium skills in the technical domains addressed by the course.
- Certification: 2 of the courses are offering official certificates recognized by the national authorities while the others are offering certificates of attendance.

A.4 Conclusions

The findings so far proofed heterogeneity both of the cybersecurity jobs market and of the cybersecurity courses offer. Besides, the lack of an agreed terminology cross domains and industries related to competencies needed for a specific job makes difficult for the companies to fill in the open positions, but also for course providers to design their curricula as to answer to the market needs, and for the individuals to identify the skills they need to possess or develop as to match the job opened on the market.

Pillars

In an attempt to create a high-level structure of the courses offered in Europe, we used the data driven approach and its five pillars advocated by CONCORDIA. We thus invited the course providers to register their courses on the CONCORDIA map by mentioning, between other elements, the cybersecurity pillars the skills developed under the specific course could be used. The findings gathered from 60 courses (33 from CONCORDIA partners and 27 from external course providers) shows that the least covered pillars in CONCORDIA are the Device-centric security pillar dealing with data acquisition and the devices producing raw data such as embedded systems, sensors, IoT devices, and the User-centric security pillar dealing with issues like privacy, social networks, fake news and identity management. These findings, although not necessarily representative for the whole European market, match the threats identified in the first chapter, especially those linked to the user-centric security pillar.

Target

More general cybersecurity awareness needs to be offered across different industries, not necessarily technical ones, thus targeting non-traditional cyber audience. Although there are quite a few online courses addressing this general need, there is little or none tailored to some specific non-technical audience yet targeted and impacted by cyberattacks. In this respect the following topics could be envisaged: Economics of Cybersecurity within an organization, Cybersecurity for lawyers, Cybersecurity for physicians, Cybersecurity for investors. The Cybersecurity for Investors course for instance, could answer to problems identified in the ENISA analysis on [Challenges and opportunities for EU Cybersecurity startups](https://www.enisa.europa.eu/publications/challenges-and-opportunities-for-eu-cybersecurity-start-ups)¹) and could be co-organized in collaboration with [Invest Europe](https://www.investeurope.eu/)². The knowledge acquired by the investors will help them not only when looking for investing in Cybersecurity

¹ <https://www.enisa.europa.eu/publications/challenges-and-opportunities-for-eu-cybersecurity-start-ups>

² <https://www.investeurope.eu/>

companies but also when assessing the viability of any of the companies as cybersecurity should be treated as a business risk.

The industry survey reveals an increased interest in Cybersecurity awareness courses as untrained staff is the greatest cyber risk to the business.

When it comes to the technical area, in a data-driven environment and data-driven economy, a Cybersecurity professional must have competences in the area of data analysis. Thus, a specific curriculum for data scientist positions would be beneficial to be developed. Some other topics could be further identified based on the analysis to be done in the Deliverables linked to the Threat landscape, legal environment and economic perspectives.

Content

Content wise, the courses would need to be developed in relation with an agreed EU competence framework. They should not stay at a general level as to ensure their relevance for a broad cross industry audience, but should be industry specific and built starting from clear learning objectives defined in direct collaboration with the targeted industry representatives. No matter the target audience, a broad approach to the topic would be advisable, as to cover both technical knowledge and soft skills, but also some managerial skills¹. The weights of the different subjects should be balanced though, according to the profile of the target audience. The hands-on approach and real case scenarios adapted to the specific audience should be favored.

Language

EU is a multi-cultural continent and local language skills are important to communicate. Yet, the free movement of people comes with free movement of skills and the language should not be a barrier. Thus, in an attempt to build an international network of Cybersecurity experts looking into exchanging information in support of better protecting Europe against cyberattacks, the trainings should, at least partially be taught in English, the language of the computer (most programming languages use English language keywords). Choosing English as a main language would increase also the participation in the different MOOCs which are in their vast majority taught in English, still a barrier for non-English speakers². It will also support the mobility of the Cybersecurity professionals from countries with a big offer of courses, thus presumably more Cybersecurity skilled people to countries with big demand on job market.

Certification

Undoubtedly, certifications are important in the process of recruitment of the cyber professionals. And at the international level there are quite a few very specific certifications for the IT professionals. In Europe though, as revealed in the ECSO study, the industry is still very dependent on US-centric certificates which are not based on formal training. And, even if in some European countries first steps have been taken

¹ <https://insights.dice.com/cybersecurity-skills/>

² [https://www.academia.edu/23952938/Planning to Design MOOC Think First ?e_mail_work_card=title](https://www.academia.edu/23952938/Planning_to_Design_MOOC_Think_First_?e_mail_work_card=title)

to set up a certification scheme, the uptake of these schemes is very limited. There is thus room and a need for a European Cybersecurity certification scheme. During the duration of the project we will be looking into developing a framework of a certificate.

The analysis helped identifying some topics and some good-to-have courses' characteristics. These findings will be further considered when developing the cybersecurity specific methodology for the creation of new content and teaching materials. Besides, the course content development and deployment are intended to be designed in such a way as to be aligned to the CONCORDIA certification framework.

The paper will be periodically updated as to capture the new trends, challenges and offers in the cybersecurity education and will contribute to the definition of the education pillar of the Cybersecurity Roadmap for Europe.

A.5 Annexes

A.5.1. Cybersecurity Career Pathway - example

Source: <https://www.cyberseek.org/pathway.html> (data collected from September 2017 through August 2018)

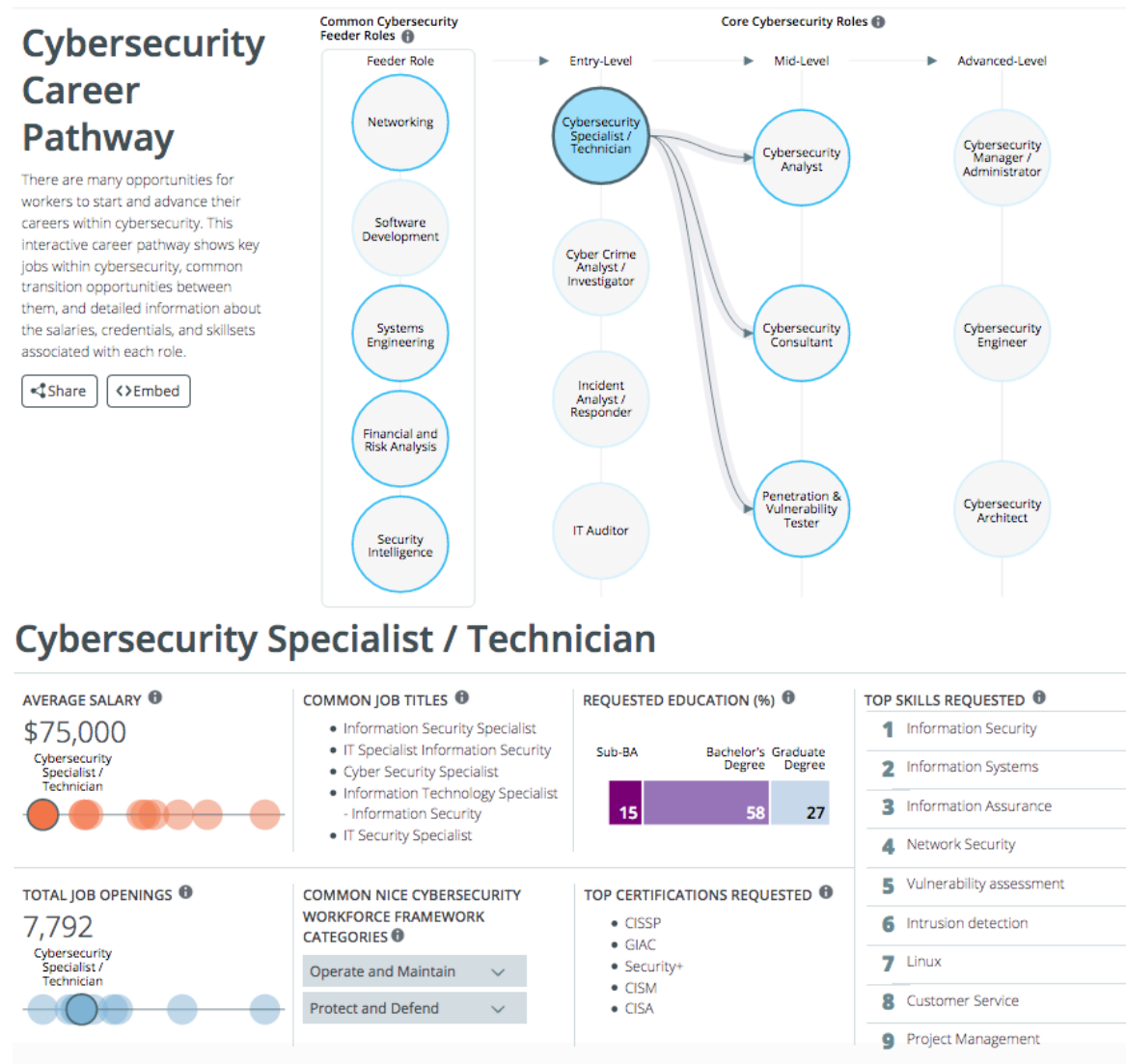


Figure A12. Cybersecurity Career Pathway – example for Cybersecurity Specialist/Technician

A.5.2. Cybersecurity competencies

Source: <https://www.slideshare.net/colleenlarose7/competency-model-clearinghouse>

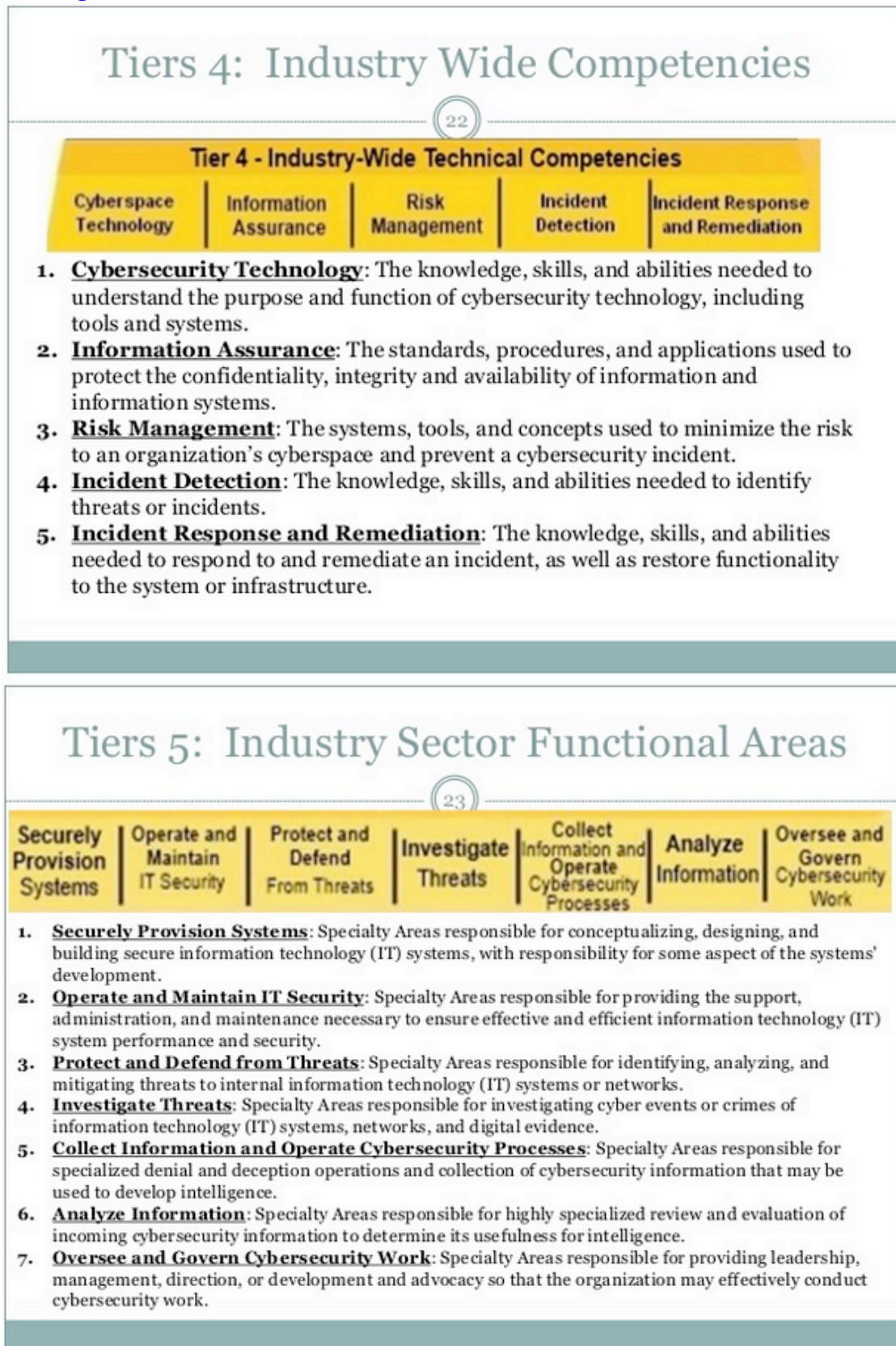


Figure A13: Cybersecurity Competencies – Tiers 4 and 5

A.5.3. The 5 pillars of the research and technology

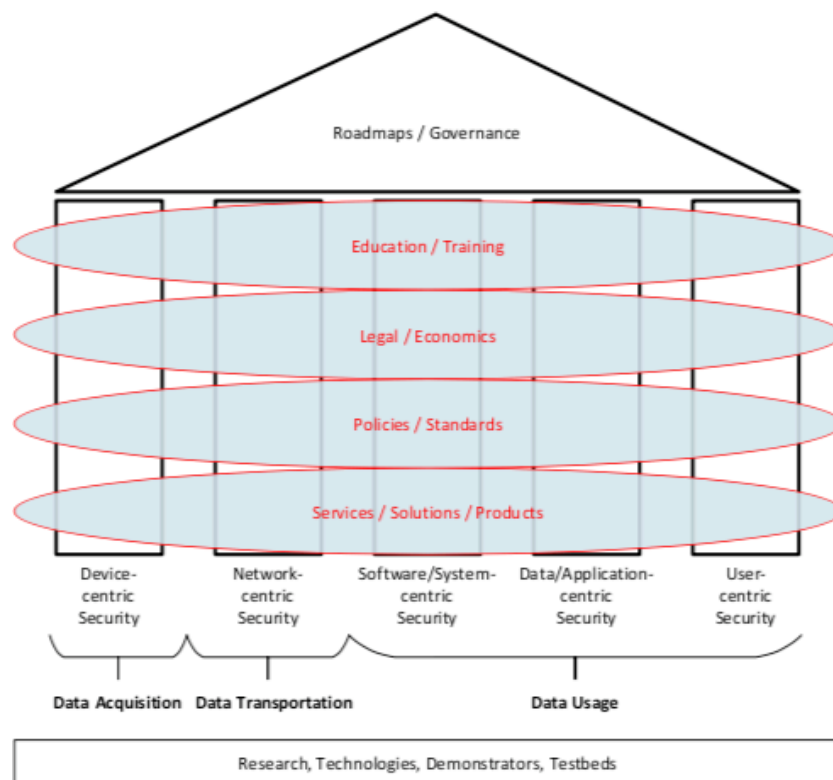


Figure A14: CONCORDIA - The five pillars of the research and technology

CONCORDIA has a data-driven approach to security and addresses it via the five pillars of research and technology as illustrated in the figure above. The individual pillars are described as follows:

- **Device-centric Security:** DCS addresses the *data acquisition* and the devices that produce *raw data*, such as embedded systems, sensors, IoT devices, drones, and the associated security-centric issues, such as IoT security.
- **Network-centric Security:** NCS refers to the *transportation of data* as well as with the networking and the security issues associated with this. Topics range from DDoS protection, Software-Defined Networking (SDN) to encrypted traffic analysis.
- **Software/System-centric Security:** SSCS centers around topics such as middleware, secure OS, and security by design. malware analysis, systems security validation, detection of Zero-days, and recognizing service dependencies are specifically addressed.
- **Data/Application-centric Security:** DACS addresses issues such as data visualization and the security of applications like cloud services.
- **User-centric Security:** UCS addresses issues like privacy, social networks, fake news and identity management.

A.5.4. The CONCORDIA courses

Title	WHO	WHAT
CyberRange: IT Ethical Hacking	Airbus Cybersecurity	Hands-on Labs on different topics and countermeasures in a simulated network.
ICS-Ethical Hacking	Airbus Cybersecurity	Hands-on Labs on different topics of threats scenarios and countermeasures in a simulated industrial environment.
Cyber Incident Handling Workshop	Airbus Cybersecurity	Table-top game to learn how to deal with cyber incidents from different perspectives.
CyberRange: Advanced Persistent Threats and Targeted Attacks	Airbus Cybersecurity	Hands-on labs to learn current techniques of APTs and Targeted Attacks.
Cyber Incident Game	Airbus Cybersecurity	Play the hacker role: plan a cyber-attack on an classical network or an industrial network infrastructure.
Cybersecurity for business	EIT Digital	An innovative training to empower and train in improving and championing Cybersecurity for the future
Security and Privacy for Big Data	EIT Digital	Learn how to identify key security and data protection issues and how to apply privacy preserving methodologies in compliance with the current regulations
ENISA Summer School (assisting the organization)	FORTH	Network and Information security: policy, economic, legal and research matters
CSIRT Cyber Training	Masaryk University	Hands-on tailor-made Cybersecurity training for IT administrators and CSIRT/CERT members. Everything from servers hardening to network monitoring & analysis
Capture the Flag by Team Locals	Research Institute CODE	Learn and evolve your Cybersecurity capabilities. And have fun at our Cybersecurity competition!
IT Competence Education and Training	Research Institute CODE	In our flexible Cyber Range, participants are provided with self-learning modules,

		individual exercises as well as defensive/offensive hands-on scenarios.
SINA Basics	Secunet	Basics and functions of the Secure Inter-Network Architecture (SINA)
TRANSITS I/II	SURFnet	Training for new and experienced computer security incident response team (CSIRT) personnel, and individuals interested in establishing a CSIRT.
Reliable Software and Operating Systems	Technical University Darmstadt	Dependability and Security Issues for SW systems
Security and the Cloud: The Issue of Metrics	Technical University Darmstadt	SW and Distributed Systems Security
ICT Security	University of Maribor	Basics; Physical security and biometrics; Cryptography basics; Secure e-commerce; Protection of communication technologies; Standards, security policies and security planning; Software security; User aspects of security and privacy
Data protection	University of Maribor	Introduction to the topic; Advanced cryptography; Usability and related standards; Practical aspects of data protection
ADVANCED INFORMATION SECURITY	University of Maribor	Provide in-depth knowledge on techniques for securing and protecting information, computer systems and computer networks
Data security and privacy	University of Insubria	Models, tools and languages for managing access control and privacy policies/ preferences in a data management system
DATA SECURITY FUNDAMENTALS	University of Insubria	Basic knowledge for the design and verification of mechanisms for data protection in information systems and networks
Internet Security Protocols	University of Twente	MOOC to discuss the details of Internet security protocols,

		such as HTTPS, SSH, DNSSEC, IPSec and WPA
Internet attacks and defence	University of Twente	MOOC to discuss how to detect and mitigate Internet attacks. Topics include DDoS, IDS and Firewalls
Certified Information Systems Auditor CISA - certification and exam preparation	SBA Research	The course helps in preparing for the exam in view of CISA certification. The Certified Information Systems Auditor (CISA) is a globally recognized certification for professionals in the areas of auditing, control and information security.
Certified Information Security Manager CISM - certification and exam preparation	SBA Research	The course helps in preparing for the exam in view of CISM certification. The Certified Information Security Manager (CISM) is a globally recognized certification for experts in the field of information security management in companies.
Certified Information Systems Security Professional CISSP - certification and exam preparation	SBA Research	The course helps in preparing for the exam in view of CISSP certification. The CISSP examination covers 8 areas of security which are necessary for the essential protection of information systems, companies and national infrastructures.
Certified Secure Software Lifecycle Professional CSSLP - certification and exam preparation	SBA Research	The course helps in preparing for the exam in view of CSSLP certification. The CSSLP certification guarantees that you have comprehensive knowledge in all areas of the secure development lifecycle.
CyberSecurity Essentials	SBA Research	The aim of the course is to provide participants with an introduction to the topics of cyber security as well as IT and information security. The course provides participants with sound basic knowledge and essential threat scenarios as well as modern solutions and methods for coping with cyber risks.

Incident Response	SBA Research	The aim is to learn tools and techniques for clarifying an APT incident. The course participants will also have the practical opportunity to investigate a simulated APT attack using hard disks and memory images.
Windows Hacking	SBA Research	The aim is to convey the most frequent and dangerous gaps in Windows networks and thus provide the necessary knowledge for securing security-relevant networks and servers.
Secure Coding in C/C++	SBA Research	This training is especially designed for C/C++ developers. It covers secure software development practices and attacks.
Web Application Security	SBA Research	The course teaches developers the most common and dangerous bugs in web application development. Testers learn how to test security aspects.
IoT Security Essentials	SBA Research	The course teaches the typical and dangerous security vulnerabilities of Internet-enabled hardware, including the OWASP Internet Of Things Top 10.

A.5.5. Courses offer on NIS map vs. Jobs opened on LinkedIn

EU Country	Academic Courses offer ENISA map	Jobs opened - Entry &Associate levels - Oct'19	Jobs opened - Total - Oct'19
Germany	148	511	762
United Kingdom	97	1,068	1,459
Czech Republic	46	18	30
France	33	150	229
Belgium	31	54	98
Netherlands	22	375	559
Spain	22	63	124
Finland	18	9	18
Portugal	16	313	347
Italy	15	134	192
Cyprus	12	0	1
Slovenia	12	0	0
Sweden	10	24	68
Ireland	7	58	120
Austria	6	15	29
Greece	5	4	7
Romania	4	35	78
Estonia	3	5	11
Latvia	2	3	5
Denmark	1	20	41
Hungary	1	9	21
Luxembourg	1	19	31
Bulgaria	1	15	27
Croatia	1	0	0
Malta	1	0	0
Poland	0	96	145
Lithuania	0	5	8
Slovak Republic	0	5	11

Annex B: Startup scene (T3.5)

Much innovation in the cybersecurity sector has been driven in the start-up world and task T3.5 was also trying to assess trends and to map stakeholders in EU. Buying or investing in cybersecurity start-ups has been more frequent than in other IT areas, creating therefore a strong exit market for cyber-security-focused start-ups.

In this overview we present several initiatives that target cybersecurity start-ups, including corporate-led incubators (Google and Thales Station F), public sector initiatives (Ciberemprende), and pan-European services provided by public-private partnership companies (ECSO Cyberinvestor matchmaking and EIT Digital services for start-ups).

















We spoke, for example, to some start-ups from Google Startups Accelerator¹ that kicked off in October 2019 in Malaga, Spain. With a focus on cybersecurity startups, it includes companies like Koodous (collaborative antivirus, it is spin off from Hispasec), SecureKids (targeting protection of minors, owners of IS4K), TechHeroX (focused on online education for cybersec), Keynetic (with SDN security solution), CyberSmart (digital compliance), Keystroke DNA (authentication), CyberBlue or ironChip. Google for Startups initiative was already present in Spain and in 2018 it made an important impact (see figure below), including startup ecosystem diversity (especially targeting women entrepreneurs).



Figure B1. Impact of Google for Startup initiative in Spain for 2018 (source: Google)

In Concordia consortia we have one start-up Cyber-detect that received support from Station F, cybersecurity startup incubator in France managed by Thales. In 2019 many other start-ups were selected by this incubator to access services such as visibility boost or support for fundraising. The figure below shows start-ups that have been selected with there are of focus or solution description.

¹ <https://www.blog.google/outreach-initiatives/entrepreneurs/google-startups-accelerator-empowers-ai-startups-europe/>

 <p>ITsMine</p> <p>Cybersecurity Data Loss Beyond DLP</p> <p>DATA PROTECTION & PRIVACY</p>	 <p>Crayonic</p> <p>Secure Digital Identity for Things and People</p> <p>IDENTITY & ACCESS MANAGEMENT IOT, ENDPOINT & DEVICES PROTECTION</p>	 <p>SEKOIA.IO</p> <p>Bringing security operations to a new pace</p> <p>ADVANCED THREAT & VULNERABILITY DETECTION</p>	 <p>Cypheme</p> <p>Next-generation anti-counterfeit solutions</p> <p>IOT, ENDPOINT & DEVICES PROTECTION ANTI-COUNTERFEITING</p>
 <p>Weakspot</p> <p>Identification of risks related to the exposure of a company on the Internet</p>	 <p>KETS Quantum Security</p> <p>Communications protection using future-proof, scalable, and easily-deployed hardware.</p>	 <p>Acklio</p> <p>Software solutions for IoT infrastructure networks</p> <p>IOT, ENDPOINT & DEVICES PROTECTION</p>	 <p>CryptoNext Security</p> <p>We protect your data against the quantum computer</p> <p>CRYPTOGRAPHY QUANTUM CRYPTOGRAPHY</p>
 <p>Alsid</p> <p>Real-time Protection for Directory Infrastructures</p> <p>INFRASTRUCTURE SECURITY</p>	 <p>Biowatch</p> <p>Wrist vein pattern recognition embedded into watches and bracelets</p> <p>DATA PROTECTION & PRIVACY</p>	 <p>Inpher</p> <p>Make predictions without revealing the past</p> <p>CRYPTOGRAPHY</p>	 <p>Keeex</p> <p>Invents the Augmented Data</p> <p>DATA PROTECTION & PRIVACY</p>
 <p>Multisense</p> <p>Upgrade your security to protect you and your customer</p> <p>IDENTITY & ACCESS MANAGEMENT</p>	 <p>Nethone</p> <p>Data-driven predictive intelligence and machine learning</p>	 <p>QED-it</p> <p>Bringing privacy to Blockchain using Zero-Knowledge Proof cryptography</p>	 <p>Skeyecode</p> <p>Patent-pending cryptographically individualized applications</p> <p>IDENTITY & ACCESS MANAGEMENT</p>

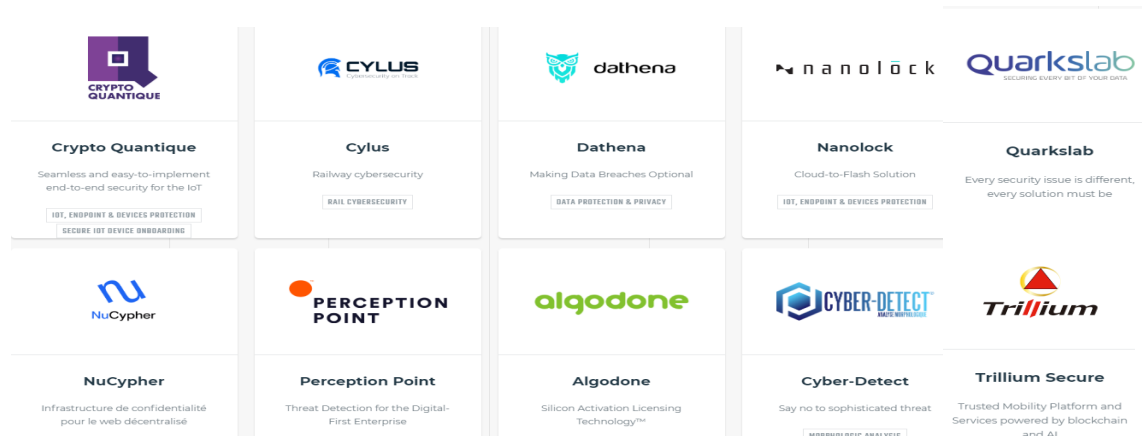


Figure B2: start-ups selected by Station F incubator in 2018 and 2019

Another imitative, this time with public funding that targets cybersecurity start-ups is Ciberemprende in Spain, managed by National Institute for Cybersecurity (INCIBE). In 2019 they awarded 34.000 to DirectDump (DFTools), forensic monitoring software, while the other winners were ClickDefense (24.000€) for their solution for detection of illegitimate clicks in online advertising, AuthUSB (20.000€) for solution related to secure access to USB storage. Other start-up mentioned in their report (and some of them interviewed for Concordia) were Acerodocs, document protection and usage control, CriptoCert, certification software, CyberBlue, decision support and cybercrime detection through emotion analysis, TechHeroX, cybersecurity awareness; Eurocybcar, vehicle cybersecurity; InproTech (Inprosec Auto), cybersecurity in converged IT (Information Technology) and OT (Operation Technology); and finally RKL Integral, that targets risk assessment for converged safety and security.

On pan-EU level we had several meetings with cybersecurity startups during two ECSO Cyberinvestor events, discussing what can we offer from Concordia. These events (14 May 14th in Madrid and Oct 15th in Luxembourg) revealed that ECSO is doing already great work for creating a vibrant cybersecurity ecosystem and all start-ups interviewed were satisfied with the support. ECSO is usually collaborating with local organizers (e.g. INCIBE, EEN and Fundacion Conocimientos Madrid, in the case of Madrid event), and is open for the collaboration with Concordia.

For the event in Luxembourg, Concordia was included as a strategic partner (see figure below) and we plan to continue this collaboration with ECSO in 2020.



Figure B3: strategic partners of ECSO Cyberinvestor days

If we look at start-ups that have been selected for Cyberinvestor days by ECSO, we observed that there is a predominance of local start-ups (Spanish in Madrid event, and Benelux in Luxembourg event) and that some start-ups repeat the experience. The ECSO Cyber Investor Days in Luxembourg received support by the government and were kicked off with a press conference by Étienne Schneider, Minister of the Economy of Luxembourg. Pascal Steichen, CEO of the SECURITYMADEIN.LU, presented the local cybersecurity ecosystem. Final report for these events is still not available, but the report for the previous events can be found at https://www.thehaguesecuritydelta.com/media/com_hsd/report/224/document/Final-ECSO-Report.pdf



Figure B4: Startups selected by ECSO for the Cyberinvestor days in Madrid



Figure B5: Startups selected by ECSO for Cyberinvestor days in Luxembourg

Finally, EIT Digital, which is Concordia partner, was also interviewed in several occasions. More specifically, opportunities for collaboration were mentioned, such as EIT Venture program in RIS countries, support for summer course (not linked to credits of master study), or Cybersecurity 360 program for Professionals. However, EIT digital has no effort in task T3.5 and the collaboration in the area of services for startups in 2019 was not considered. EIT digital regional nodes (e.g. Madrid), however, are organizing events that can also be of interest for Concordia. One of the regions that would be especially interesting for Concordia, as it was expressed by the advisory board feedback received during the Concordia Open Doors event, is the Eastern Europe (in EIT Digital this region is covered by regional innovation scheme – RIS¹).

¹ <https://eit.europa.eu/our-activities/eit-regional-innovation-scheme-ris>

In collaboration with Startup Wise Guys accelerator, cybersecurity focused program CyberNorth was started to receive investment and take part in a 3 month long acceleration in Tallinn, Estonia. In 2019 selected teams are autom8 (Turkey, NLP frameworks to automate the detection of security and other flaws in source code), Odin Vision (Ukraine, biometric identification), Cyber Struggle (Turkey, cyber security certifications), Cyex.io (Hungary, AI-based cybersecurity exercise generator), Fakeskiller (Ukraine, detection of fake identification), Hive.id (Ukraine, digital identity verification), Scoriff (Estonia, identifying high risk companies), Webtotem (Kazakhstan, SaaS for securing and monitoring website). Outside of EIT Digital, we have established contacts with Oxolabs cybersecurity incubator from Hungary that started its work in 2019¹. Again, the follow-up and further collaboration will depend on resources available for startup factory and incubator (tasks T3.5 and T5.1) and related services.

As an additional idea for startup factory concept, technology transfer funding was also considered. Academic research is often considered high-risk by the traditional investors, so more recently TT funds are enabled by InnovFin Equity – managed by EIF. They form part of “InnovFin –EU Finance for Innovators”, an initiative launched by the European Commission and the EIB Group in the framework of Horizon 2020. Some examples of European investors in TT funds include K.U. Leuven/CD3 (Belgium), IP Group (UK), Chalmers Innovation Seed Fund (Göteborg, Sweden), the UMIP Premier Fund (Manchester, UK) and Karolinska Development (Sweden).

¹ <https://cybersecurity.oxolabs.eu/>