Proposal No. 830929
Call H2020-SU-ICT-03-2018

Project start: 1 February 2019
Project duration: 42 months

Cyber Security for Europe

D2.2

Internal Validation of Governance Structure

Document Identification	
Due date	31 January 2021
Submission date	29 January 2021
Revision	1.01 (3 Feb 2021)

Related WP	WP2	Dissemination Level	PU
Lead Participant	Atos	Lead Author	Aljosa Pasic (ATOS)
Contributing Beneficiaries	All WP partners	Related Deliverables	D2.1, D2.3, D2.4

Abstract: Deliverable D2.2 is a report on the validation of the governance model of the Cybersecurity Competence Community. This model which was presented in deliverable D2.1. and Iin D2.2 the model and its assumptions are validated in the real-life scenario, namely with cybersecurity stakeholders in Toulouse in an entity named Community Hubs of Expertise in Cybersecurity Knowledge (CHECK Toulouse). Validation follows a bottom-up approach, based on interviews with all types of stakeholders in CHECK-T, and posterior analysis of findings. Besides deliverable D2.1, validation also considers other inputs, both internal and external, that were delivered during 2020 and that impacted in some way the initial model. Other cybersecurity community organisation and governance modelling experiences in Europe, some of them like CHECK, are also presented and considered in the analysis. Final conclusions and a set of recommendations are summarising the analysis of this validation exercise. The next deliverables offered by the project will test and improve the suggested governance structure, ensuring that it remains up-to-date, flexible and capable of accommodating the ever-adjusting list of challenges and demands.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929.

Executive Summary

The European Commission proposed to set up a Network of National Coordination Centres (NNCC), a Cybersecurity Competence Community and a European Cybersecurity Industrial, Technology and Research Competence Centre, but many options, especially related to the community part, have been left open to answer to this challenge. While the "cybersecurity community" should be composed of all the cybersecurity stakeholders, the design of its governance model is a subject to suggestions and validations coming from pilot projects, such as Cybersec4Europe.

The cybersecurity community should be feasible and sustainable, but many other considerations come into picture when designing and validating governance model, for example incentives for participation and different motivations or objectives of different external stakeholders both public and private, belonging to national and regional levels. During the first year of Cybersec4Europe project we have gathered views from more than 80 stakeholders via surveys, interviews, workshops and through the activities related to the dissemination and standardisation activities and we have also studied best practices in research, data sharing, or other communities that already exist in cybersecurity domain. Various implications for how the governance model should look like have been extracted, for example combination between R&D stimulation and execution with capability-building, policy interventions and funding activities (national and regional). In terms of governance structures, there was support for different combinations that target challenges such as insufficient collaboration between academia and industry or the lack of focused investment from the public and private sectors.

Deliverable D2.2 is describing validation of draft governance model for the community portion of NNCC, which has been described in D2.1. This model relies on the model of a network of Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs), and validation actions took place during 2020 with the ongoing implementation of a prototype "CHECK" delivered in Toulouse, which is called CHECK-T in the further text. Basic postulates and assumptions are validated through a methodology consisting of several steps, such as performing series of interviews, clustering and analysis of responses and comparison between different approaches.

Based on these findings, conclusions are targeting policy makers, but also those that want to set up new CHECKs at different level of governance (national, regional and local). They are based on practical experience with establishing CHECK-T, but also additional inputs from other countries, like CHECK, as well as external inputs, for example from the other pilot projects (ECHO, CONCORDIA and SPARTA).

Some of the initial governance model elements, that refer to a set of decision processes and policies, for a specific case or area of governance, are expected to be implemented in CHECK-T soon. Other rules and procedures that have been extracted from D2.1 are validated with the stakeholders, mainly in the areas related to "Structure", "Objectives" and "Stakeholders". Two types of CHECK emerged after the analysis, namely one that is an economic actor in the cybersecurity landscape and must be sustained by a sound business model, and another that is part of the public administration and financed as a public good. The case of the CHECK-T pilot, that is used to validate governance model from D2.1 in CyberSec4Europe, through its partner UPS-IRIT, is an example of the former type, which brings to the fore notable insights based on day-to-day implementation experiences.

Most participants in CHECK-T found division into four stakeholder groups to be adequate, but there is also feeling that category for other stakeholders could be included, while the further segmentation of demand

side (users) might also be desirable to achieve better insight. There was, for example, discussion on how to engage the civil society. The importance of use cases of importance for the region appears as a relevant issue in strategic decision making, while some partners are missing a procedure to identify sectorial needs and lifelong learning aspects, as well as the links to professional accreditation. Regions can play a relevant role here in particular when rephasing the new regional strategic agenda for the 2021 – 2027, related to the RIS3 and Smart Specialisation Strategy [1].

The interview campaign carried out by UPS-IRIT elicited the additional needs and issues from cybersecurity and regional stakeholders and highlighted more services expected from CHECK-T. Such needs and potential services were meant to constitute the basis upon which to build the organisation's business models and the next version of governance model in CyberSec4Europe.

The points that have been validated in all sets of interviews are the strong emphasis on the issues of training and awareness, as well as cooperation and communication. Knowledge sharing was a particularly popular matter, to be realised in a trustful environment to ensure a coordinated response to cybersecurity menaces – together with the share of good practices across the industry. Training, specifically concerning end users of cybersecurity products, was another strongly felt necessity, even though there was some disagreement over which institution would be responsible for it in between industry actors, academia and public authorities. In both cases, economic actors' participation was highlighted as a necessity, as well as the inclusion of academic actors (e.g. universities and research centres).

Moving on to discrepancies, D2.1 appeared to show a stronger focus towards regulation, particularly regarding the creation of certifications and standards both at the European and international level. In addition, there is some uncertainty over the best modality for participant selection.

In parallel to validation through CHECK-T, we also did validation exercise with participants of a cross-pilot task group [2], as well as with the stakeholders of cybersecurity communities in other countries. The attempt to map it to different options and contexts was done in the other countries, for example in Spain, with the involvement of partners participating in the other pilot projects, ECHO, SPARTA and CONCORDIA, as well as representatives of national cybersecurity body. Another issue is the need to have a coherent cybersecurity ecosystem approach in Europe, with many interconnected CHECKs or other similar structures, as well as organisations such as ECSO. These structures should not only "co-exist" but should rather acknowledge the existence of different CHECK types, that can be coordinated at the national level, as well as EU level, and should form a network of decentralized networks.

Several rules for membership and representation were suggested including different statuses, such as full member, associated member and observers. Membership at CHECK (regional or sectorial/functional) could be decided upon assessment of the commitment and according to the voting process. Representation in legislative bodies on central level – e.g. General Assembly– should be ensured for the full members and for representative elected from the regional and functional/sectorial entities (hubs, nodes, chambers, chapters or whatever type of networked organisation is represented). Other conclusions and recommendations are targeting feasibility and relevance of the approach chosen for a specific territory, phase of formal "pre-configuring", structuring set-up project that would demonstrate the robustness and sustainability of its economic model, the partnership logic and building an environment of trust.

Document information

Contributors

Name	Partner
Aljosa Pasic	Atos
Abdelmakri Benzelek	IRIT
Afonso Fereira	IRIT
Pierre-Henri Cros	IRIT
Mark Miller	CONCEPTIVITY
Natalia Kadenko	TUD
Tobias Fiebig	TUD
Dirk Müllmann	GUF
Christina von Wintzingerode	GUF
Prof. Dr. Indra Spiecker	GUF
Silvia Vidor	UNITN
Antonio Skarmeta	UMU

Reviewers

Name	Partner
Marco Crabu	ABI Lab
Silvia Vidor	UNITN
Antonio Skarmeta	UMU

History

Version	Date	Authors	Comment
0.01	2020-03-28	Aljosa Pasic	1st Draft with ToR
0.02	2020-04-22	Aljosa Pasic	Change of formal, alignment of methodology
0.03	2020-05-18	A. Pasic, A. Benzelek, A. Fereira, P-H. Cros	Integration of first inputs
0.04	2020-09-16	A. Pasic	Minor changes according to conf call minutes from 22/7/2020
0.05	2020-09-16	M. Miller, V. Menezes Miller	Additions throughout the document, (especially 4 and conclusions/recommendations)
0.06	2020-09-24	N. I. Kadenko	Enhanced chapter 3.2.4
0.07	2020-10-02	Various contributions integrated by A. Pasic	chapter 1.1, 4 and updates of the chapter 3.2.1 and 3.2.3, two new figures in chapter 3
0.08	2020-10-05	A. Skarmeta, A. Fereira	Revision and contributions
0.09	2020-10-18	A. Fereira, P-H. Cros	Update of methodology (chapter 1.2), and chapter 3
0.10	2020-10-20	A. Pasic	Reformatting
0.11	2020-10-21	C. Douligeris	Chapter 4.6
0.12	2020-10-26	S. Vidor	First review
0.13	2020-10-30	A.Pasic	Comments from v0.12 addressed
0.14	2020-11-05	C. von Witzingenrode, A. Fereira	Legal chapter added, peer review comment addressed
0.15	2020-11-30	A.Skarmeta, A.Pasic, A.Fereira	Conclusions

0.16	2020-12-10	All partners	Recommendations and final draft
0.17	2020-12-18	T.Fiebig	WPL review
0.18	2020- 12-28	S. Vidor	Review
0.19	2021 – 01 – 07	Marco Crabu	Review
0.20	2021-01-14	A.Pasic	Final integrated version
0.21	2021-01-18	D. Mullmann, A.Pasic	Change in reference style and correction of broken links
0.22	2021-01-18	T.Fiebig, A.Pasic	Changes in table formatting
1.0	2021-01-26	Ahad Niknia	Final Check and Preparation for submission
1.01	2021-02-01	N.Kadenko	Update of status of Dutch platform

Table of Contents

List of Figures

List of Tables

List of Acronyms

A	**ANSSI**	Agence Nationale de la Sécurité des Systèmes d'Information
	AI	Artificial Intelligence
B	**BEST**	Basic Environment for Simulation and Training
C	**C3T**	Regional Centre for Cybersecurity
	CCN	Centro Criptologico Nacional
	CCN	Cybersecurity Centre and Network
	CERT	Computer Emergency Response Team
	CCC	Cybersecurity Competence Community
	CHECK	Community Hubs of Expertise in Cybersecurity Knowledge
	CMMI	Capability Maturity Model Integration
	CNI	Centro Nacional de Inteligencia (National Intelligence Centre)
	CNPIC	Centro Nacional de Proteccion de Infrastructuras Criticas (the National Centre for the Protection of Critical Infrastructure)
	COM	Current Operating Model
	COBIT	Control Objectives for Information and Related Technology
	COVID	Corona Virus Disease
	cPPP	Contractual Public-Private Partnership
	CS4E	CyberSec4Europe
	CSIRT	Computer Security Incident Response Team
D	**DoW**	Description of Work
	DEI	Digitising European Industry
	DIH	Digital Innovation Hub
E	**EC**	European Commission
	ECSO	European Cyber Security Organisation
	ECSCON	European Cyber Security Collaborative Network
	EDA	European defence Agency
	EDIH	European Digital Innovation Hub
	ENISA	European Union Agency for Cybersecurity
	ENISE	Encuentro Nacional de Industria de Seguridad en España
	EOS	European Organisation for Security
	EOSC	European Open Science Cloud
	EP	European Parliament
	EU	European Union
	EUROPOL	European Union Agency for Law Enforcement Cooperation
G	**GDPR**	General Data Protection Regulation
	GEANT	Gigabit European Academic Network
	GUF	Johann Wolfgang Goethe-Universität Frankfurt am Main

I	**ICT**	Information and Communication Technology
	IEEE	Institute of Electrical and Electronics Engineers
	IMEC	Interuniversity Microelectronics Centre
	INCIBE	Instituto Nacional de Ciberseguridad (Spanish National Cybersecurity Institute)
	IPR	Intellectual Property Rights
	IRIT	Institut de Recherche en Informatique de Toulouse
	IT	Information Technology
J	**JTI**	Joint Technology Initiatives
	JRC	Joint Research Centre
K	**KIC**	Knowledge and Innovation Communities
	KRITIS	Critical infrastructures
M	**MOOC**	Massive Open Online Course
	MoU	Memorandum of Understanding
N	**NATO**	North Atlantic Treaty Organisation
	NCCC	Network of Cybersecurity Competence Centres
	NCSA	National Cyber Security Authority
	NCSI	National Cyber Security Index
	NGO	Non-Government Organization
	NIS	Network and Information Systems
	NWO	Nederlandse Organisatie voor Wetenschappelijk Onderzoek
P	**PPP**	Public-Public Partnership
R	**R&D**	Research and Development
	RVO	Rijksdienst voor Ondernemend Nederland
S	**SMEs**	Small and Medium Enterprises
	SRIA	Strategic Research and Innovation Agenda
T	**TNO**	Toegepast Natuurwetenschappelijk Onderzoek
	TUD	Technische Universiteit Delft
U	**UMU**	Universidad de Murcia
	UNITN	Università Degli Studi de Trento
	UP KRITIS	Critical Infrastructures implementation plan
W	**WG**	Working Group
	WP	Work Package

This page has been intentionally left blank.

Glossary

A **Academia**
The group of stakeholders formed by those employed by public and private research institutions, with a primary focus on research.

B **Best Practices**
A widely accepted set of rules and procedures for operating given a concrete situation or application case.
Bottom-Up
Actions and activities originating emergently from stakeholders without being initiated by a higher authority.

C **Commission Proposal**
EU Regulation Proposal 2018/0328 (COD) on a Network of Competence Centres, a suggestion for a binding regulation, i.e., applicable law, which does not have any legal binding apart from signalling future intent of regulation.
Community
The interacting set of all stakeholders.
Competence Centres
Entities that host several stakeholders from academia or industry to develop cybersecurity competencies in one or more verticals.
Competencies
Ability to address technical and societal challenges.
Cooperation
Interaction between multiple stakeholders for their mutual benefit.
Cybersecurity Hubs
See: Competence Centres

D **Digital Single Market**
A joint framework of rules, regulations, and applicable law among all member states to ensure that stakeholders from the digital economy find comparable conditions in all member states.

G **Governance**
The rules, regulations, and operational entities that shape the interaction of public and private actors.
Governance Model
The codified set of rules describing the governance of a social system with public and private actors.
Governance Structure
See: Governance Model

H **Hacktivists**
A person that is politically active in the context of topics concerning digitalization and the Internet, without necessarily belonging to any larger organization or NGO.

I **Industry**
All actors that participate in the market driven digital single market without being a member of government, or NGO entities.

L **Law**
The set of applicable law and regulations of all member states and the EU combined.
Lower Governance Layers
Governance for entities acting below the member state level in the European Union.

M **Massive Open Online Courses**
Educational offerings on the Internet participants can join without the necessity to visit a certain location or institution.
Member State
A nation state that is part of the European Union.
Network Model
A governance model where participants interact on the basis of equal rights and responsibilities while pertaining autonomy in their internal operation.

P **Pilot**
A small-scale (in comparison to the final result) test of a proposal or artefact.
Policy
Codified rules and procedures for a specific case.
Policy Makers
Elected and non-elected officials that prepare, define, and decide generally applicable policies.

R **Region**
An area in the European Union which does not necessarily correspond to a single member state; It might overlap parts of several member states or be a sub-set of a single nation state.
Regional Hub (see: CHECK)
A competence centre associated with a region.
Regulation Proposal
See: Commission Proposal

S **Scientific**
Results obtained and communicated according to academia's best-practices
Sovereignty
The ability to independently act and prevent external intervention in an institution's operations.
Stakeholder
A party that has an interest, concern, or influence in certain area.
Strategic Objectives
A set of long-term objectives that have to be completed to reach an overarching goal, relevant for all member states.
Substructures
Structures of an organisation that are not visible to other organisations interacting with the organization in a network model.

T **Top-Down**
Actions and activities that are mandated from a higher authority, e.g., by applicable law or decisions of the European Commission.
Transparency
Ability to trace and understand all decisions of an organization by its members, or, constituents in case of government organizations.

V **Vertical**
A set of applications of cybersecurity questions united by an overarching industrial context, e.g., the aviation vertical, which contains all cybersecurity actors involved with aviation safety and security.
Voting
A procedure to democratically reach a decision.

W **Workshop**
An activity where stakeholders gather to jointly work on an issue or topic.

1 Introduction

The EU 2018/0328 Regulation Proposal aims to establish a European Cybersecurity Industrial, Technology and Research Competence Centre (the "Competence Centre"), a Network of National Coordination Centres (the "Network" of "Coordination Centres") and a Cybersecurity Competence Community (the "Community"), but the governance model and the role of this Cybersecurity community is not described in this document. Work package 2 (WP2) of CyberSec4Europe is proposing a governance structure on the level of community, suggesting, for example, how relationships could be governed and how tasks are to be divided. CyberSec4Europe developed a draft governance model, described in D2.1, and presented in the first year of the project. The objective of this deliverable is to validate this theoretic model in the real environment, namely with the stakeholders that will be part of this community and that is to be established in Toulouse.

The main idea behind the governance model for the community was a network of Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs). This deliverable is describing validation of model with the ongoing implementation activities related to the so-called CHECK-T, which is basically a prototype CHECK to be established in Toulouse. Basic postulates and assumptions derived from theoretic governance model are validated through a series of interviews, clustering and analysis of responses. This overall methodology is described in chapter 1.2, with general planning depicted in figure 1. The focus is clearly on bottom-up approach, so validation methodology also followed this approach, with specific interview methodology, that is described in chapter 1.3. Overview of different inputs is given in chapter 2, while comparison between theoretical assumptions and real-world situation and opinions from community stakeholders in Toulouse is described in chapter 3. Other experiences in Europe are summarised in chapter 4. Whenever possible, these experiences and their governance models are compared to CHECKs and governance model proposed in D2.1.

Based on these findings, conclusions in chapter 5 are targeting future community building and possible governance model evolution, but is also giving feedback to policy makers, as well as CyberSec4Europe participants that are involved in the next phase of the CHECK, including the next version of governance model. In summary, we present here practical experience with establishing CHECK-T, but also additional inputs from other countries, and the other pilot projects (ECHO, CONCORDIA and SPARTA), all of which are validating different aspects of governance for European cybersecurity community.

1.1 Context of this deliverable

The European Union has articulated the ambition to maintain its sovereignty and become a global leader in the digital economy, guided by both democratic values and the capabilities to be resilient when facing global cybersecurity threats. The ultimate goal of the CyberSec4Europe pilot project is to design the governance structure that will answer the main challenges faced by the field of cybersecurity today and the project deliverable D2.1 has outlined the first approach to be implemented when designing a governance model.

The European Commission has identified four main challenges in the area of cybersecurity that need to be overcome to realise this ambition:

1. Lack of cooperation between Member States, industries and academia, leading to fragmented efforts in research and development (R&D);
2. Insufficient investments in cybersecurity.
3. Increased demand for skills, know-how and facilities, while access thereto is limited;
4. Inconsistency of new policies and governance with the existing and continuous updating legal frameworks.

In order to meet these challenges, the European Commission proposed to set up a Network of National Coordination Centres (NNCC), a Cybersecurity Competence Community and a European Cybersecurity Industrial, Technology and Research Competence Centre. The current EU 2018/0328 Regulation Proposal of the Commission, sent to the EU Parliament, still leaves many options open and does not fully address the underlying challenges, particularly regarding the "community" composed of all the cybersecurity actors.

To design the governance model capable of addressing all the identified challenges, it is essential to take into account the stakeholder views and the current best practices. These inputs are necessary in order to build a resilient cybersecurity community, which will provide a sustainable environment for the long-term solutions to the challenges outlined above. To collect these inputs, the WP2 gathered views from more than 80 stakeholders via surveys, interviews and workshops. We have also studied best practices in research collaboration, data sharing and the most relevant initiatives to create cybersecurity competence hubs, which are presented in the chapter 4.

After analysing these inputs, we have extracted various implications for how the governance model should address the four core problems:

- Stakeholders express widespread support for the objectives of cyber sovereignty, independence, and control at the EU level, combining this with a view that the focus of the network of national competence centres should be broader than only stimulating R&D, and also include capability-building and policy interventions;
- In terms of governance structures, there was support for a combination of the hierarchical and network models, as well as for a governance structure that is open to a diverse set of actors, initiatives and collaborations;
- The insufficient collaboration between academia and industry in the EU is a systemic problem that is visible in the leading cybersecurity research venues where innovative work is published. The new governance structure, therefore, cannot just be a platform but must also address the lack of focused investment if Europe wants to better capitalise on the synergies from joint R&D by academia and industry;
- From examining different types of governance structures, including cybersecurity communities or partnerships such as ECSO, or more generic purpose structures such as DIH; we have identified several elements that could provide valuable lessons for the governance design for the community part of NNCC. The synergy between formal and informal, top-down and bottom-up structures can be achieved by integrating informal structures, thus leading to a more efficient stakeholder engagement throughout all societal levels. Transparency is another key element for facilitating trust in an organization.

Based on these findings, CyberSec4Europe developed a draft governance model for the community portion of NNCC, described in D2.1. The overall approach of CyberSec4Europe is to explore a community-driven

approach for the governance model, to complement – and marginally adjust – the Commission's EU Regulation Proposal 2018/0328 within the legal requirements. At the core of our model are community-level cybersecurity hubs which should enable collaboration between industry and academia, bring market security innovations and help build capabilities in the area. Other issues that have been considered are streamlining of funding and investments, as well as support for SMEs. Notably, they should be able to shorten the chain between decision making and existing needs on the ground. Accordingly, their governance model needs accompanying mechanisms to increase funding and investment, including at the EU level.

In short, what was proposed was a network of Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs), which will provide an auspicious environment for community-level research, innovation, and capacity building in cybersecurity. In this deliverable, we will evaluate the initial proposal with the ongoing implementation of a prototype CHECK in Toulouse. By connecting to the community part of NNCC, while staying close to the operational environment and the cybersecurity professionals, the CHECKs will be well positioned to leverage upon regional and industry-related practices and expertise.

CHECKs can be considered as a possible approach to form focus service groups (regional or sectorial/functional) leading to the Cybersecurity Competence Community. They should be based on a bottom-up work and community-level research, innovation, and capacity building in cybersecurity. This deliverable is validating some of these basic postulates and assumptions through a series of interviews, clustering and analysis of responses and comparison between different approaches.

It is also important to mention the overlap between this deliverable and D2.3, especially its chapter 2, which is also output of the same tasks T2.3 and T2.4. Deliverable D2.3 is looking with more details into the status of the legislative process, as well as other governance models of institutions in the field of cybersecurity, beyond model that is proposed in D2.1. The main goal of D2.3 is to propose changes and further developments of the organizational and responsibility structure of the planned European cybersecurity network and community. In this context, the present deliverable D2.2 had double function:

- to validate governance model assumptions from D2.1 "in the field" and immediately provide this feedback to D2.3, which is included in chapter 5 of this deliverable
- to receive inputs from D2.3 especially in relation to the analysis of external sources

1.2 Methodology and planning

Methodology for validation of the governance structure was discussed and agreed among WP2 participants in the first quarter of 2020. Partners agreed on a comprehensive understanding of the elicitation, description, reflection, and evaluation of issues related to validation. This includes the consideration of the objectives of all relevant stakeholders, including public authorities, private enterprises or academic institutions, the consideration of tangible as well as intangible criteria measuring expected benefits of CHECK model the incorporation of stakeholder preferences expressing the relative importance of the various services and objectives of the future community.

The first step was the decision about relevant inputs for D2.2, both from the previous work in the project and the current external sources, in order to reach agreement on main areas of validation, that we will call "pillars", as well as specific questions and issues to be validated within each pillar. This approach of separation of issues into pillars or clusters is also selected for risk management purposes, as there was an uncertainty regarding the schedule of legal establishment of Toulouse CHECK.

Three main types of sources of validation questions and issues were considered, namely description of work (DoW) with changes submitted and approved in 2019, then deliverable D2.1, and finally external sources and inputs, such as ongoing governance-related work in pilot projects, conclusions of joint meetings and discussions about regulation at EU level. Validation questions and issues have been mapped into pillars or clusters, an exercise that was done separately by different partners, and posteriorly a convergence has been done in order to define "strategic areas".

Concerning the DoW, it has been stated that the governance model described in D2.1 will be validated by applying it to the regional cybersecurity expertise hub, being established by partners in Toulouse. The Toulouse hub will be responsible for implementing the decision processes and policies proposed by the governance model, and the results of the analysis will be laid down in D2.2. By policies, in this context, we refer to codified rules and procedures for a specific case. This is limiting the scope of this deliverable and it is also describing a very specific context of validation.

When it comes to the second input – deliverable D2.1 – the challenge was to agree on issues or topics of importance and to extract specific questions that can be validated. At the general assembly meeting in February 2020 the following areas, issues and questions have been discussed and agreed:

- Governance and structure:
  - How to propose and approve "substructures" (e.g. WG)?
  - What are the procedures of an "executive organ"?
  - What is the mechanism or link to the national body?
  - What are the financing mechanisms?
- Objectives and KPIs:
  - How to define a general orientation/mission/strategy?
  - What is the procedure of identification of "regional interests"?
  - What is the procedure for "problem identification"?
  - What types of funding are available and for whom (e.g. public procurement, incubators)?
  - What are mechanisms (e.g. cascading grants) and KPIs for funding allocation?
- Stakeholders and rules:
  - Which are the rules for "bottom-up approach to cooperation"?
  - Which are the rules for "non-accredited stakeholders"?
  - What are the procedures for "scientific Exchange"?
  - How to motivate practitioners?
  - What is the mechanism for the participation of other disciplines (e.g. legal)?

This initial list of areas and questions is only a starting point to be enhanced and enlarged in the first phase of the validation process set-up.

Finally, when it comes to the third input – which is a collection of external information ranging from conclusions of related and relevant EC meetings, policy and legislative drafting, or ongoing work in other

pilots – the clustering of issues and mapping to the above mentioned key areas of validation is more difficult, as (temporary) recommendations at EU and MS level might change during 2020. In the first approach, however, we took procedures used by EC in inter-pilot collaborations and input gathering such as the preparation of a workshop with national contact points in January 2020 as an example. We detected the following inputs:

- "Common projects", topic aligned with D2.1 "bottom-up approach to cooperation";
- "Common or shared infrastructure", topic aligned with several areas e.g. testbeds, threat intelligence;
- "Capacity building" aligned with D2.1 "MOOC quality criteria decision making";
- "Technology transfer" and "incubation", to be included in the governance model.

One of the key concepts introduced in D2.1 is the CHECK, Community Hub of Expertise in Cybersecurity Knowledge. A CHECK-T is a CHECK covering a geographical territory, and for the D2.2 validation it is focused on the Occitanie region with the centre in Toulouse. However, although the main part of this validation exercise is focused on CHECK-T, it has been agreed among partners to try as well to validate governance model in their own communities. Partners that work in WP2 of CyberSec4Europe are coming from 5 different countries, in which different cybersecurity communities, either existent or future have been described and, in some cases, compared or validated to the CHECK model. In addition, ECSO, which is European Cybersecurity Organisation, and its governance model, has also been briefly compared to it, in order to extract additional conclusions about universal applicability of the governance model or common issues that should be considered in the future model, also developed in D2.3.

From the 13th to the 15th of November 2019, CyberSec4Europe's annual event[1] took place in Toulouse and the whole consortium was invited to visit OcSSImore[2], which could provide an example of governance model to be followed by the CHECKs. OcSSImore is an association bringing together four major companies from the Occitanie region (i-BP, IT-CE, Meteo France and Pierre Fabre), having pooled their digital paths to identify cross-sector and cross-trade security needs. It thus constitutes a pole of research and cooperation in digital security well established in the Occitanie Region, whose objective is the development and the production of innovative and efficient solutions to protect their member industries from cybercrime and thus guarantee the integrity of their work.

We were able to analyse OcSSImore's objectives and procedures, in order to pre-validate the model designed in D2.1. Several relevant areas were identified in their objectives:

- Cooperation between R&D labs;
- Economic development (start-up and SME support, fostering user adoption, etc.);
- Sourcing and prototyping innovative tech;
- Access to and promotion of EU expertise and capabilities;
- Building and implementing a roadmap;

[1] https://cybersec4europe.sciencesconf.org/
[2] https://www.ocssimore.net/

- Monitoring R&I development;
- Alignment with industry long-term goals;
- Turning innovations into solutions.

When it comes to procedures of relevance for governance and stakeholders, we have also identified the following principles, which were mentioned as open for discussion and possible mapping into CHECK-T:

- Innovation separated from funding;
- Unanimous voting rule;
- Solution-oriented research restricted to partners; non-partners can join later;
- Fixed yearly fee for partners;
- IPR issues left to be agreed by partners.

Based on these inputs, the first planning for refinement and validation was made.

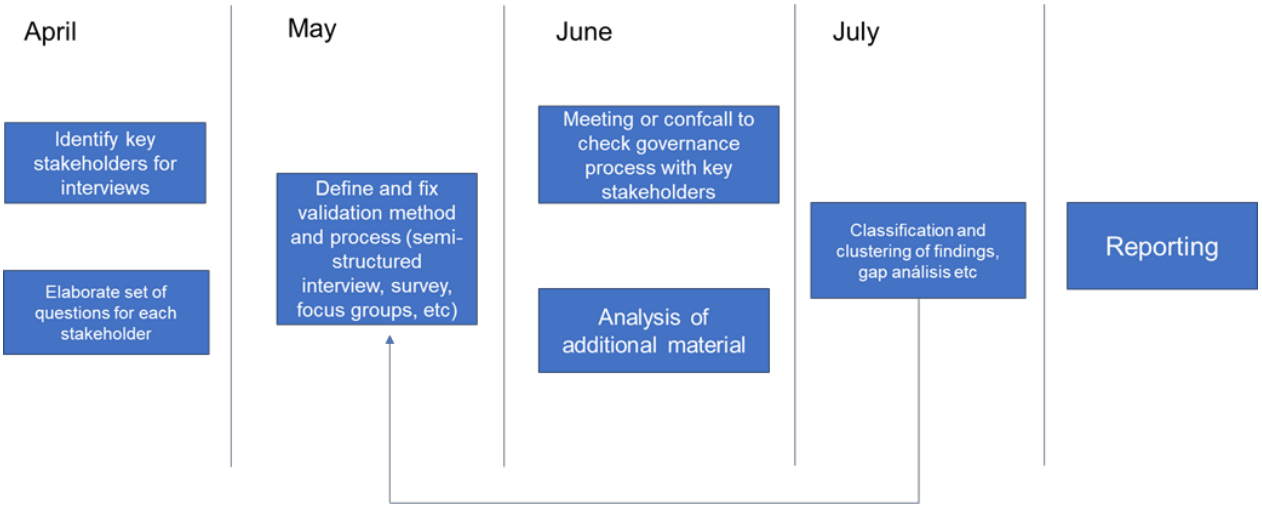

Figure 1: Initial planning of activities

A rough placement of distinct activities in "phases" was done in the second step, which was dedicated to the validation of "pillars" of the model. It was proposed to culminate in a physical workshop bringing together interested stakeholders in Toulouse, as well as a drafting phase that includes structuring (Is there a sub-committee? Which topics? How do they make decisions?), validation of objectives and KPI (How do they measure success? How often?), and stakeholder analysis.

The third, final step was dedicated to analysis, with an introductory discussion and agreement on analytical parameters related to maturity, acceptance/desirability, feasibility and sustainability, where also comparison with the other existing cybersecurity communities, or ongoing community set-ups, has been done.

The original plan had to be revised after the appearance of COVID-19 pandemic and the consequent impossibility to hold physical events, such as the workshop envisaged for the first half of 2020.

In April it was agreed that interviews with stakeholders will take place in Toulouse, while the subset of questions for D2.2 will be extracted from CHECK-T interviews. For this adaptation in the methodology, a

procedure had to be determined. The importance of expanding to include other European experiences has been noted as well.

The following sequence of events has been discussed and agreed upon:

1. UPC-IRIT prepare a report aggregating their findings from the interviews;
2. The report is edited to ensure readability;
3. The WP2 partners execute extraction of possible promising activities from the report and relay them to UPS-IRIT;
4. Based on the pre-selection by the partners, UPS-IRIT selects relevant activities that could be considered for the validation of the implementation of the CHECK in Toulouse;
5. The WP2 partners analyse the governance models explored thus far in the perspective of the selected relevant activities.

After this, in order to execute the third step of the validation of the governance model, a decision was to be made about final analysis and conclusions.

1.3 Evaluation methodology for the interviews

The methodology chosen by IRIT to carry out its mission of creating the first CHECK-T (Community Hub of Expertise in Cybersecurity Knowledge in its Territory) was composed of two stages.

The first stage started with the drafting of a high-level description of what could be a CHECK-T through the expectations of four communities with complementary interests: End-Users, Cybersecurity Solution Providers, Technology Centres, and Economic Development Accelerators.

Around fifty representatives of these communities, located in the French regions of New Aquitaine, Occitanie, and Provence-Alpes-Côte d'Azur, were interviewed based on such a description, along with a questionnaire that ensured that exchanges concentrated on the same issues with all stakeholders and in the same manner.

The outcome of the interviews campaign highlighted that four strategic axes must be implemented for those stakeholders to take an interest in the creation of a CHECK-T, as depicted below.

Area	*Description*	*Evolving activities examples*
R&D	Funding	Concept validation

	Contracts	Specific R&D
Services	Infrastructure	Mutualization of tech platform
	Ecosystem	Seminars to share info
	Support	Legal and tech watch
Market	Lobbying	Influence EU roadmap
	New products and services	Co-innovation
	Facilitation	Connection to new partners
Skills	Alliances	Joint development
	Networking	Event organisation
	Talents	Training

Table 1: The four strategic application areas

As it can be observed, governance issues are transversal. The next step was to discuss these with careful consideration of the specifics of each activity to agree on a governance model that ensures a harmonious and balanced implementation and development of the four activities concurrently. Analysis of interview outcomes and discussions were also done among partners involved in work package WP2; these conclusions are described in chapter 3. Governance must be co-created by all actors, so that they see it as a prolongation of their own, individual activities, which will incentivise them to invest their resources in the CHECK-T in terms of time, funds, membership, staff, visibility, and so forth. Possible strategies to achieve such objectives are discussed further below.

The second stage began by highlighting, based on the application areas, the activities that needed to be carried out to establish this first CHECK-T (see table 1).

These priority activities would give CHECK-T clear roadblocks that could lead to the start of its existence and building activities. One thing that became apparent was that answering calls for proposals is a common feature underpinning these different activities. Because of its potential for immediate returns, this trait was therefore chosen as a first working basis for defining the financial value that CHECK-T should have, in order to bring its potential members to join and work towards effectively implementing and developing the four activities highlighted above.

1.4 Limitations and Constraints

The current circumstances – especially due to the irruption of COVID 19 pandemic - conditioned the activities of these two tasks and despite the best efforts, the legal establishment of CHECK-T had to be postponed. Legal issues, for example, of consistency of different policies with the existing legal frameworks,

was not validated, although we have identified new approaches to manage this in the later phase of the project.

2 Data Sources

While governance model and the main postulates around CHECK were described in D2.1, there are still many open issues when it comes to data sources that could be considered useful, yet feasible and realistic, for the validation with stakeholders in the Toulouse scenario. This includes agreement about the main assumptions from this model and the presentation in a form that could be validated e.g. transforming them into direct questions. Furthermore, additional information is needed from external sources, in order to adapt questions to specific context. During the execution of activities in WP2 many external developments impacted project, and this provoked adjustments or changes in inputs, such as data extracted from the revision of EU regulation that directly changes some of assumptions or proposed policies drafted in D2.1. While chapter 2.1 describes initial internal inputs, based on technical annex and D2.1 deliverable, chapter 2.2 is describing these dynamic external sources and how they impacted overall perception of stakeholders.

2.1 Internal inputs

2.1.1 Inputs from the technical annexes of the project

CyberSec4Europe is a project selected in the H2020 call “Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap”. It has a consortium of 44 participants covering 21 EU Member States and Associated Countries as well as extensive cooperation from public administrations, international organisations and sectorial associations. In the project contract technical annex, CyberSec4Europe describes actions to support the implementation of the EU Cybersecurity Act – including the governance of the related community, which is the target of WP2, and validation of the governance model as proposed in D2.1.

2.1.2 Key aspects and terms extracted from governance model described in D2.1

Given that a governance model refers to a set of decision processes and policies, it is also necessary to clearly describe the meaning and the scope of policies themselves. We understand “policy” as a set of codified rules and procedures for a specific case or area of governance. Besides the decision process and procedures, other rules and procedures that have been extracted from D2.1 are related to the areas of "Structure”, “Objectives” and “Stakeholders”, which are identified as the initial three pillars of the CHECKs’ governance model.

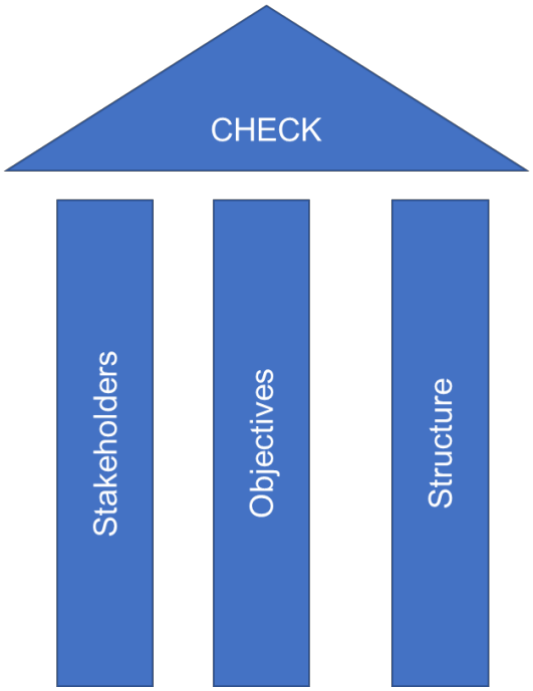

Figure 2: Three pillars of CHECKs' governance model

This simplification of a governance model structure is aligned with the methodology chosen and described in chapter 1.2. However, during the discussion among WP2 participants additional open issues, doubts or questions were mentioned as possible targets of validation for the governance model presented in D2.1. Notably:

- How to propose and approve "substructures" (e.g. working groups)?
- What are the procedures of an "executive body"?
- What is the mechanism or link to other national and regional nodes of the Cybersecurity Competence Network and other CHECKs communities?

Similarly, during the discussion the partners had in February 2020, several possible questions have been identified for the "Objectives" pillar, including decision-making rules about strategic services that CHECK should have:

- How to define general orientation/overall objectives/mission/strategy?
- What is the procedure for identification of problems and challenges specific for the CHECK context?

Similarly, it was discussed about what types of funding are envisaged and for whom (e.g. public or private) and what are the mechanisms (e.g. cascading grants) and indicators for funding allocation within community.

Finally, in the pillar related to stakeholders' issues such as membership rules or cooperation are mentioned questions such as:

- Which are the rules for "bottom-up approach to cooperation" e.g. when research roadmap prioritization must take place?
- Which are the procedures to involve "non-accredited stakeholders" (civil society e.g. non-experts, categorize NGOs depending on the interests they defend, citizens...)?
- What are procedures for "scientific exchange" (with other CHECKs)?
- How to motivate demand-side (critical infrastructure etc.) practitioners to participate in community and cooperate?
- What is the mechanism to incentivize participation of other disciplines (e.g. legal organisations)?

2.1.3 Other internal inputs

During the input collection period, other suggestions were given by project partners, for example as an evolution of initial thoughts or reaction on discussions between the four pilots working on establishing and operating a pilot for a Cybersecurity Competence Network.

2.2 External inputs

Parallel ongoing work and (temporary) recommendations at EU and MS level were also taken as an input, directed towards the prioritization of initial issues. An example was the workshop with national contact points held in January 2020, where some open issues such as common projects between community members and shared infrastructures are mentioned as important parts of the governance model. These open issues, already described in chapter 1.2, were also considered in the validation of the governance model, for example validation of "bottom-up approach to cooperation".

2.2.1 Revision of EU Regulation Proposal

The most important revision of this proposal was done on March 9th, 2020 and more details about changes are also available in D2.3, which is written in parallel to this report. It was clarified, for example, that the Cybersecurity Competence Community should provide inputs to the activities and multiannual work programme and should benefit from the community-building activities of the Competence Centre, but otherwise should not be privileged with regard to calls for proposals or calls for tender.

The Community and its members, which in our model are exemplified by CHECK, might act as observers in several functions of the EU centre. Accreditation has been replaced by registration, and all registrations are vetted for national security. In terms of objectives, supporting everything from capacity building to incubator for start-ups and SMEs has been mentioned.

As a starting point, the EC proposed a cybersecurity competence survey, done in 2018 by the Joint Research Centre (JRC) in collaboration with DG CONNECT. Besides the proposed taxonomy and classification scheme, aligning existing cybersecurity terminologies, definitions, and domains, the project made an online survey addressed to the European cyber-security research community [4], aiming to identify the cybersecurity competence centres. Around 700 centres participated in this survey and between May and June 2020 four pilot projects for establishing and operating a pilot for a Cybersecurity Competence Network were invited to revise and include new members in this register.

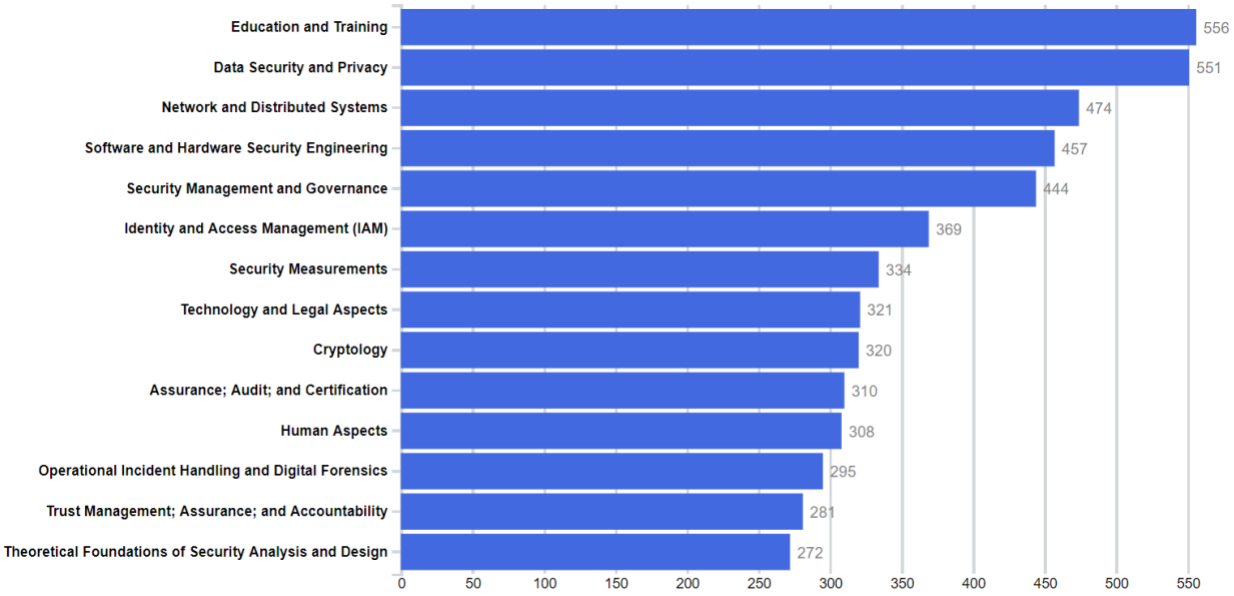

Figure 3: Distribution of participants according to their expertise (©European Union, 2018, reproduced from [4], page 15).

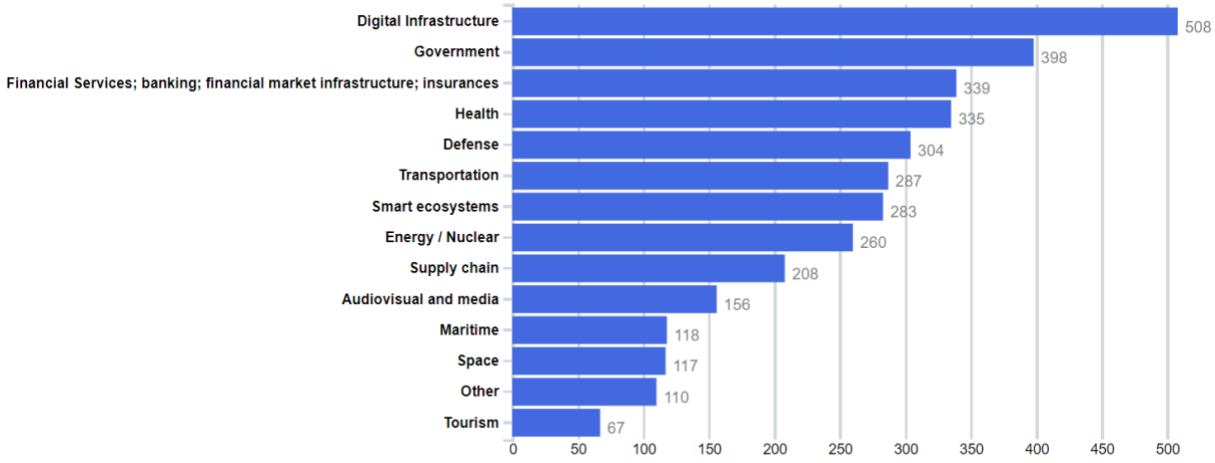

Figure 4: Distribution of participants according to the sectors (©European Union, 2018, reproduced from [4], page 26).

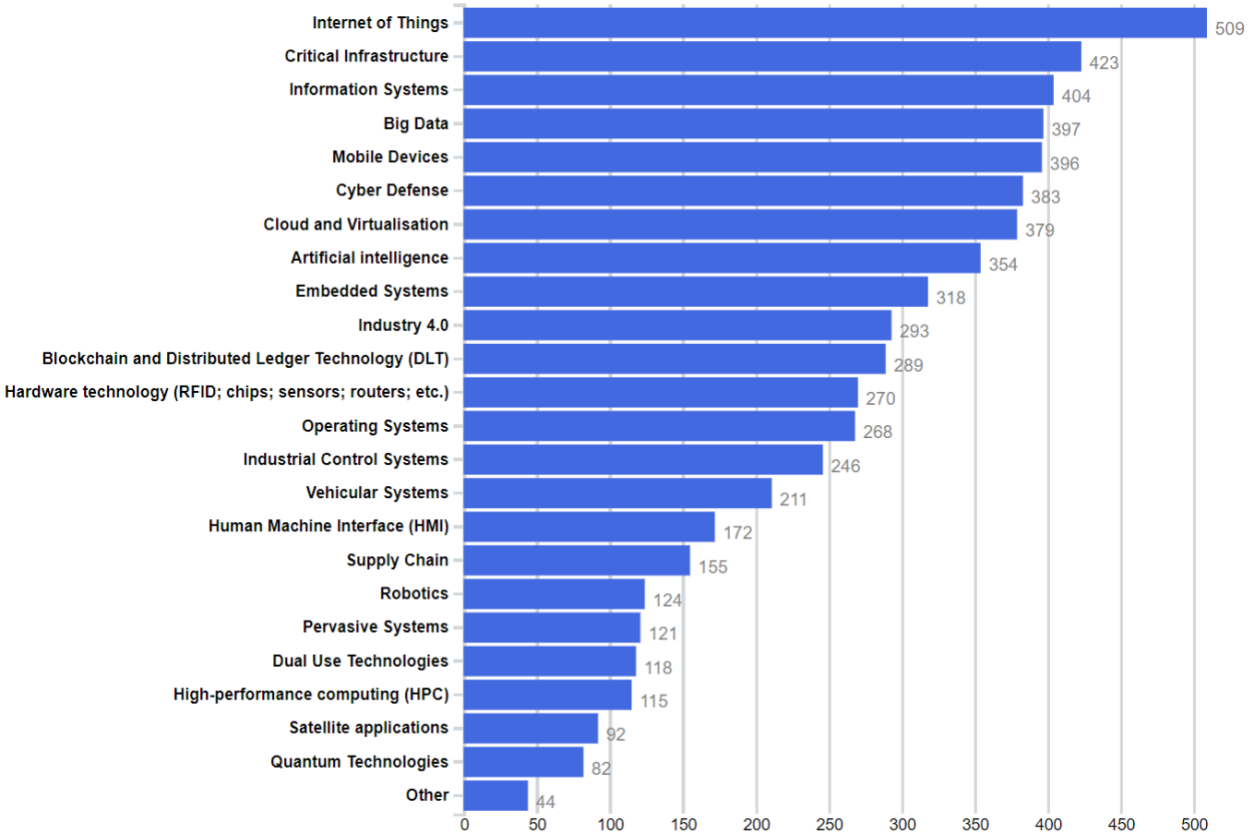

Figure 5: Distribution of target applications and technologies (©European Union, 2018, reproduced from [4], page 27).

JRC shared the topics discussed during the ATLAS governance workshop, for which each pilot is invited to provide their feedback. The idea was to use this document as a template where each pilot should combine their feedback for each of the topics and return one single document consolidating all comments.

JRC also shared a spreadsheet containing the list of institutions that participated in the cybersecurity survey in 2018. The data of these institutions was already imported in the ATLAS database and each pilot identified the members of their consortium, including the name and e-mail of the representatives.

2.2.2 Inputs from pilot projects

CONCORDIA, ECHO, SPARTA and CyberSec4Europe are the four pilot projects chosen to address the Horizon 2020 Cybersecurity call “Establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap”. Regular meetings between the four pilots targeting, establishing and operating a pilot for a Cybersecurity Competence Network took place during 2020 with the representatives of the EC. During

these meetings, the governance of the future Cybersecurity Competence Community was frequently discussed. During the January meeting the discussion, with interventions from Member States' national contact points, focused on the main objectives, where national benefits and types of services were proposed to be mapped into tasks and functions of the community (table 2).

	Support	***Network***	***Share***	***Inform***	***Consult***	***Coordinate***	***Trigger***	***Incubate***
Common projects	X			X	X	X	X	X
Testbeds	X		X	X				
Repositories			X	X	X			
Threat intelligence		X	X	X	X			
Training		X		X				
Education		X		X				
Development of tools	X							
Tech transfer		X						
Research planning	X				X	X		

Table 2: Example of mapping priorities into community tasks and functions

After the cross-pilot specific task force was formed for governance issues, the focus of these meetings was on the ATLAS JRC pilot described earlier.

In another pilot project (ECHO), a conference paper was published about a possible governance model. This work [5] is focused on the selection of activities, processes and structures needed for the network governance and management and considers links between the Enterprise Architecture approach, the COBIT framework and network analysis with examples of NATO and EU initiatives for network organization.

The proposed methodology is using initial analysis and case study on existing networks, followed using the Analytic Hierarchy Process method, to identify alternatives, and then move to the modelling phase with detailed process identification trough COBIT components design and analysis.

The most relevant part of this study is describing the so-called "enablers" according to COBIT 2019, which are components necessary to build the organization's governance model and system: processes, organizational structures and responsibilities, policies and procedures, information flows, culture and behaviour, skills, and infrastructure. ECHO also suggests the CMMI model for evaluation and improvement of an organization's processes against good practices.

ECHO identified the key process areas at management level that are related to decision-making: partnership development; research and technology development; planning for education and training; contract management and control; quality and customer satisfaction management.

While this is a rather theoretical approach based on COBIT, in the case of CCCN the following attributes have been identified: (1) Information sharing for early warning about key security-related events; (2) Arranged partnership – the horizontal connections between network participant is the main focus; (3) Joint projects and joint services with different level of participation of partners – scalable and flexible connections within the network participants (network nodes).

Finally, as the "seed" for the governance model ECHO mentions the BEST-Cyber federation (Basic Environment for Simulation and Training in Cyber Domain), which can be considered as the pilot used in the ECHO team definition of the Current Operating Model (CoM) for federated networking steering of cyber research.

After the first-year findings of the four pilot projects, a cross-project coordination group on governance was established and several meetings have been held. The result is the white paper report on the Governance of European Cyber Security Collaborative Network (ECSCON), presenting the joint efforts between the three pilot projects ECHO, SPARTA and CyberSec4Europe. The aim was to identify the "umbrella" model for effective and efficient coordination of the development of the European Cybersecurity Competence Community in the institutional framework and in relation to organisations such as EC, JRC, ENISA, EDA, EUROPOL and NATO Cyber Organization.

The white paper combines findings from bottom-up research in CS4E/SPARTA with the top-down approach implemented by ECHO. It introduces the term Cybersecurity Competence Community (CCC) which considers different networks – one around ECSO, another one under the Cyber ATLAS initiative of JRC, as well as the four pilot networks and others outside these ones.

In this paper, CHECKs are referred to as "service groups" and "sub-entities" to be brought together under the ECSCON organization with an opportunity to support the creation of new service groups (CHECKs) in the future.

2.2.3 Governance model validation examples

We have also investigated other governance models and the means to validate these. Model validation could be defined as the set of activities intended to verify that the model elements are performing as expected, in line with their design objectives, and business uses. It also identifies potential limitations and assumptions, as well as assessing their possible impact.

Since it is difficult to find similar governance models, we observed the digital innovation hub model validation [6].

Figure 6: Walloon region DIH governance model

While digital innovation hubs (DIHs) were launched by European Commission in the scope of the Digitising European Industry (DEI) initiative in 2016, they also coordinated with Member States and regions towards common goals, so there are some similarities to the CS4E context.

DIHs act as one-stop-shops with a mix of services from training, financing advice, market intelligence and networking opportunities. They are deeply rooted in their regional ecosystem, and the JRC report focuses on their main issues, namely leadership and governance, contribution to regional development, organisation, funding, and collaboration.

During Cybersecurity4Europe conference[3] in Toulouse, CS4E invited several existing communities (e.g. cybersecurity labs in Basque Digital Innovation Hub, GEANT) to present their work on governance; feedback from the audience was also appreciated. Nicole Harris from GEANT, for example, presented a way to collaborate between CSIRTs through several mechanisms such as listing, self-accreditation, and certification programs for CSIRT teams. Anders Pall Skött, from the audience, talked about the establishment of the Danish Competence Centre.

[3] https://cybersec4europe.sciencesconf.org/

In terms of stakeholders and governance, the DIHs are a heterogeneous group and can focus more on horizontal digitalisation support or have a very specific specialisation or priority. What is clear is their objective to contribute to regional development and cohesion policy, and to make available support easier to find by making the system more transparent, communicating it more clearly to its potential beneficiaries.

Compared to objectives proposed in deliverable D2.1 of CS4E, this governance model looks narrower, especially since there are no well-defined links to the network of national nodes or EC centre. Some DIHs assist start-ups, a fact which is also noted as an interesting input for CHECKs. We should also add that towards the end of 2020, new actions were promoted by the EC to fund the network of digital innovation hub at national and EU level [3].

At the CS4E workshop, participants stressed that this concept should help in the communication between national and regional strategies, but also different communities (e.g. Occitanie region with Danish CHECK). Therefore, the capacity to support multilevel governance initiatives as well as a fruitful collaboration between CHECKs are needed.

2.2.4 Other inputs

During the execution, other initiatives and models are mentioned, as well as validation actions. One example is the European Open Science Cloud (EOSC), which is governed by three constituent bodies, and whose governance structure includes representatives from across the user and provider community as well as representatives from the EU Member States and the European Commission.

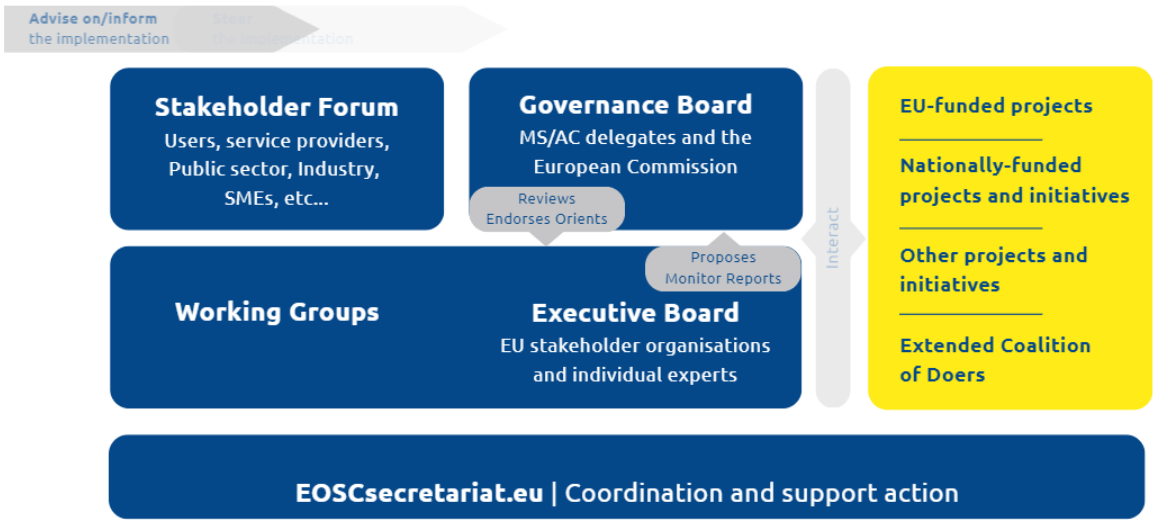

Figure 7: Governance model of EOSC

The EOSC Working Groups[4] form an official part of the EOSC governance structure; they ensure a community-sourced approach to the current challenges faced by the EOSC. The EOSC Secretariat advises on the processes, assists on the operations and supports the coordination of the Working Groups, pooling the best expertise available in the community and delivering synthetical reports on all relevant issues requiring a decision, as requested by the Executive Board.

Five Working Groups have been set up with support from the EOSC Secretariat in order to validate the governance model and provide feedback. The "Landscape" Group is mapping the existing research infrastructures which are candidates to be part of the EOSC federation, which is similar to what the four pilots are already doing, in addition to the 2018 JRC survey. A Working Group exist for designing the "Rules of Participation" that shall define the rights and obligations governing EOSC transactions between EOSC users, providers and operators, while the Working Group "Skills and Training" provides feedback on sustainable training infrastructure. Finally, there is also a "Sustainability" Working Group that provides and validates recommendations concerning the implementation of an operational, scalable and sustainable federation model.

[4] https://www.eoscsecretariat.eu/eosc-working-groups

3 Interviews and analysis

As already described in chapter 1.3, governance issues have been identified as transversal to the listed strategic application areas, depending on the specific activities to be implemented. Thoughts about the appropriate governance model are motivated first and foremost by the census activity described above, as it is the capital on which a CHECK-T must be based. In order to carry out preliminary analysis as efficiently and comprehensively as possible, as it is necessary to quickly determine the group that will participate in the foundation of the CHECK-T, i.e. whether or not it will be composed of representatives from the End Users, Cyber Security Solution Providers, Technology Centres, and Economic Development Accelerators or other stakeholders that have been consulted to choose the strategic axes and its priority activities.

The first analysis was related to the subject matter of CHECK-T as well as its role. Both issues will delimit the appropriate status that is required for a CHECK-T to become a legal entity. The choice of legal status will afterwards help to determine the contractual nature of the inventory, which may be a simple directory of territorial competences in the field or a database of competent persons, staff or not, from the communities contributing to CHECK-T. It is worth noticing that one of the main added values of a CHECK-T is exactly this capacity to coordinate and orchestrate exogenous and diverse skill resources.

Accordingly, the governance model should be discussed by the founders of CHECK-T to establish an internal organisation that is conducive of the role to be implemented, but, crucially, does not constitute a new competitor to CHECK-T's own members. This last point is particularly important because it impacts fundamentally the economic model of a CHECK-T.

In parallel to this analysis, the discussion of the interview feedback was done by project partners to compare it to the envisaged governance model from D2.1

3.1 Discussion and clustering of initial feedback

Discussion and consolidation of validation aspect areas took place among WP2 partners through online meetings in May and June 2020:

1) Clustering of stakeholders. Most participants found four groups to be adequate, but there is also feeling that category for other stakeholders could be included. There was, for example, discussion on how to engage the civil society.
2) The research/innovation capacity of the companies seems an important factor to validate, but also the importance of use cases appears as a relevant issue in strategic decision making. Additional information might be needed to find out how CHECKs would work on local/regional roadmaps.
3) Training appears as one of the pillars of the CHECK governance model, but some partners are missing a procedure to identify sectorial needs and lifelong learning aspects, as well as the links to professional accreditation.
4) Mentoring aspects and seed capital investment strategies were not mentioned. In general, an important pillar could relate to the modality to pursuit innovation in the sector.
5) Finally, testbeds and other resources, such as space for experimentation, are not prominently mentioned in the interviews.

	ATOS	*TUD*	*GUF*	*UMU*	*UNITN*
1	Collaboration and cooperation	Collaboration, cooperation and trust	Promote scientific exchange	Mentoring start-ups and innovation[5]	Sharing of indicators and knowledge
2	Training and education	Training and education	Accumulate territorial interests	Involvement of civil society	Territorial issues
3	Role and responsibilities	Engagement, networking and liaison	Links and networking	Research & innovation capacity	Transparency
4	KPI and audit		Interdisciplinary possibilities	Territorial interests	Standardized solutions
5	Observatory		Legal	Testbeds and shared resources	Longterm education
6	Engagement, networking and liaison		Funding	Identification of training gaps	Multidisciplinary issues
7	Transparency mechanisms[6]				Bring results to market (research to practice)
8					Include other stakeholders (CERT, civil etc)

Table 3 Analysis of interviews with CHECK-T stakeholders

Stakeholders that were interviewed intended to elicit, and then report, those among their needs that could be fulfilled by an organisation as a CHECK. Therefore, it is also not reasonable to expect all issues to be covered. If in the report there is no mention of something, this is because said something was not declared as a need by a significant number of interviewees. However, participants agreed that the training aspect can indeed be expanded further, in case it makes into the selected activities. The suggestion to involve civil society was also considered. CHECK-T is currently trying to reach out to some citizens collectives and associations and may be able to conduct interviews with them in future.

WP2 participants also highlighted opportunities to deepen the analysis on the various topics listed in the synthesis such as creating competences and skills in cybersecurity – for example on the topic of life-long learning. The D2.1 term "substructures" has been identified with Working Groups (WG) and has been presented by IRIT. The substructure of CHECK-T will be validated via Working Groups. Their setup was

[5] Addition from UMU
[6] Addition from Atos and UNITN

originally intended to take place by the end of 2020, but there is currently some uncertainty on whether this will happen considering the COVID-19 pandemic.

In the final round of analysis, the four selected activity areas are Funding/R&D, Services, Market access and Upgrade skills. Participants of WP2 discussed similarities with the ECHO approach and need to define the bottom-up approach more clearly. Synthesis and conclusions about mapping of initial governance model into "strategic areas" was further enhanced with external contributions in the second part of 2020. Some of these external inputs, such as that of ATLAS, were not influencing decision-making related to "strategic areas". However, others – such as changes in the communication of EC (there remains uncertainty over which stakeholders can be members) – might influence and impact the process.

Another issue being discussed is the link to the national body that represents Member States in the EU Cybersecurity Competence Centre and network. In the case of CHECK-T, they already had contact with the national body ANSSI, which gathered all the French partners from all four pilots in order to coordinate the French position in the different pilots. CHECK-T also has contact with Cyber Campus, an incubator for cybersecurity companies. Once established, CHECK-T will thus become the representative of the region and become the member in place of the individual companies.

Funding mechanisms represent another challenge regarding validation. WG funding will be likely relying on European projects; therefore, it might be possible to explore opportunities there, for example through specific calls for DIHs (Digital Innovation Hubs). However, there is no guaranteed funding or source of revenue. Mechanisms for funding allocation are considered out of scope for the validation of governance model.

While the general orientation is towards a bottom-up approach, CHECK-T is also performing identification of regional interests. Here WP2 participants were challenging some decisions presented by CHECK-T strategic areas, for example the choice of the "banking fraud" topic, that seems related to the scope of WP5 and were suggesting more generic description. A clear procedure should thus be documented for this "regional interest" identification.

Besides, rules for voting rights, decision making, and similar issues need to be drafted in association with more concrete procedures. This is especially relevant for non-registered members (not registered in ATLAS as "members of EU cybersecurity community"). Since it is still not clear whether ATLAS will be relevant, there is no need to validate this.

A further issue concerned the way to motivate practitioners. This was not a subject of CHECK-T interviews, although some incentives have been mentioned. Mechanisms for participation of other disciplines, e.g. legal are not covered, although stakeholders relevant for regional economic development are contacted and included in the model.

As a conclusion, there are still several open issues that have been discussed, but are not possible to validate (known unknowns) such as financing mechanisms, a procedure for identification of "regional interests", a procedure for "problem identification", rules for a "bottom-up approach to cooperation", rules for "stakeholders not registered in ATLAS", or procedures for "scientific exchange".

3.2 Review of main "pillars" for validation of governance model

As we already mentioned in chapter 1.2, one of the steps in the methodology was revision of initial validation "pillars" which are basically clusters of different issues or questions to be validated. These initial pillars were based on sources and information from the first year of the project, including the initial EU regulation proposal. However, it was obvious that a major revision would be needed not only because of changes that were introduced in the second year, but also due to the adaptation to the specific Toulouse context, as well as feasibility. In the rest of this chapter we give an overview of these revised pillars, as well as analysis of answers that we have received for each of them.

3.2.1 Analysis of stakeholders' needs

Apart from the earlier mentioned four community groups (End Users, Cyber Security Solution Providers, Technology Centres and Economic Development Accelerators) identified to allow the interviewees to imagine the expectations from CHECK-T, other actors are not excluded from future participation. Full CHECK-T partners are essentially professional entities that seek to create additional professional value and collaborate with platform owners on a more solid level, having a stronger relationship. For example, creators of professional value who tend to specialize in a niche product or service and improve it over time might be interested to join. In the interviews, it was also commented that partners could be facilitators, aiming to facilitate, process and improve the production of value by acting as brokers, aggregators or connectors. Another type of stakeholder was peer producers: entities interested in providing value on the supply side of the ecosystem/market, looking for opportunities to improve their professional quality and to hone their capabilities towards better performance. Finally, peer consumers are entities interested in consuming, using, accessing the value created by and on the platform.

Transparency mechanisms have not been mentioned during interviews, while the engagement of new partners is considered as one of the crucial issues. Incentives should not be taken for granted, including possible services of activities of CHECK-T such as collaboration (e.g. threat intelligence communities were mentioned five times in the answers). Cooperation has been mentioned six times as a mean to gain in performance; coopetition – meaning alliances between competing solution providers – was in the focus as well. Education and co-construction of dedicated cybersecurity training were also considered very important activities by all stakeholders, but issues were raised in relation to mentoring – especially for start-ups.

Stakeholders from other disciplines would be welcome to join as partners. Discussions on cross-functional issues include some interdisciplinary aspects, together with cost and benefit assessments or legal support services. Regarding ownership (roles and responsibilities of stakeholders), the interviewed participants felt the need for alignment mechanisms, but also for a common charter of trust. Discussions on cybersecurity internal issues (staff of a pole/cluster/agency etc.) were mentioned three times, and some participants also highlighted collective actions with SMEs, as well as support to set up a new business. Finally, services for market and technology watch with the aim to increase partnership were mentioned twice in the interviews.

What is less clear are specific rules for:

1. Responsibility for selecting CHECKs;
2. Selection criteria;
3. Selection procedure.

The results of the interviews performed within the CHECK-T framework is consistent with D2.1, even though there are some differences in how some issues are presented by interviewees.

To begin with the points in common, both sets of interviews put a strong emphasis on the issues of training and awareness, as well as cooperation and communication. Knowledge sharing was a particularly popular matter, to be realised in a trustful environment to ensure a coordinated response to cybersecurity menaces – together with the share of good practices across the industry. Training, specifically concerning end users of cybersecurity products, was another strongly felt necessity, even though there was some disagreement over which institution would be responsible for it in between industry actors, academia and public authorities. In both cases, economic actors' participation was highlighted as a necessity, as well as the inclusion of academic actors (e.g. universities and research centres).

Moving on to discrepancies, D2.1 appeared to show a stronger focus towards regulation, particularly regarding the creation of certifications and standards both at the European and international level. D2.1 result underlined as well as certain attention towards economic development accelerators (such as public authorities, economic development agencies etc.) as sources not only of funding, but also of funding control, and required means to ensure transparency in cybersecurity within the EU. The participation of a variety of stakeholders was encouraged, with a strong emphasis on institutional actors (e.g. EU institutions/agencies and national states) and minor requests for inclusion of customer representation as well as SMEs. There remains, still, wide uncertainty over the best modality for participant selection.

These discrepancies can be explained by the different focus of the two sets of interviews, which addressed two slightly different audiences. If in both cases the interviewees were selected within the economic fields connected with cybersecurity in Europe, D2.1 spaced across a variety of European countries including – among others – EU institutions, Italy, the UK and Switzerland. Also, in both cases the interviewees were mostly selected among participants in the business world. It would be thus interesting to widen contributions to the academic world in order to observe variations and similarities both among different countries and different sectors. Such inclusion may also highlight the possibility for other roles for academia other than education and training.

3.2.2 Objectives and functions

There are several missions, principles and objectives that are valid for all stakeholders.

Guarantee the sharing of data, sensitive information and technological research with other partners on all types of incidents and on the responses provided and sharing expertise and general know-how, infrastructure and investment is clearly within the scope of community objectives.

Transfer of technology, pooling of R&D costs and implementing methodological processes are also mentioned as important objectives, with performance indicators such as transfer of technology from one sector to another, at a lower cost.

Confidence-building and building a local and European base of trust promoting cooperation and coopetition between members is also at the top of objectives for CHECK. In addition to education and training, which was always considered as one of the pillars of CHECKs, scientific exchange has been mentioned explicitly.

Sharing of knowledge and threat intelligence information in a trustful environment was clearly the most important function of CHECK with nine answers, next to five mentioning sharing of knowledge, expertise of threat intelligence information. There are also five answers stating the importance of sharing of expertise for the construction of the trust base, while knowledge and methods dissemination, as well as business-oriented training, were mentioned four times.

3.2.3 Legal provisions

In chapter 4 of D2.1 the initial proposal of the European Commission as well as the amendments of the European Parliament and the position of the Council of the European Union have been described and, under consideration of the other findings in D2.1 regarding general European legal requirements, stakeholder requirements and insights from the analysis of other governance structures, legally assessed. Since then, the Regulation Proposal has remained unchanged. Currently, the legislative procedure is still ongoing [7], with the European Parliament awaiting the Council's first reading position [8].

3.2.4 Territorial dimension and economic development

Discussions on cross-functional and cross-sectorial issues (air/space/land/sea transport, finance, health, energy, agriculture) and transfer of cybersecurity technology between sectors are among the highest priorities. New partnerships and new business relationships in the region were also seen as important issues within territorial economic development, together with the involvement of facilitators/connectors with users via CHECK-T. Synergy and complementarity on themes that have an impact on the region should increase the number of jobs (talent attraction, business creation, start-ups, spin-offs in cybersecurity).

Other territorial issues considered include communication relay on expert seminars, hackathons and challenges, co-innovation, and visibility.

One of the challenges of economic development is in relation to cross-border sales and issues of national tendencies to use the products and services of those within their national borders. True defragmentation of the market will only occur once solutions and services can be verified and eventually certified, such that the consumer can compare them to products, solutions and services which may already exist in their own national environment.

Regional initiatives, such as the Cyber Valleys project, represent some first steps in looking at the market and Europe and the European Union as a whole, but these are still "early days" currently. ECSO is also addressing this within the work of the Working Group 4 (SMEs, countries and regions) and is still open for discussions[7].

Later developments could and should include supporting a marketplace for trusted European products and services ensuring that what the consumer is buying can be trusted. Furthermore, there is also a requirement

[7] https://ecs-org.eu/working-groups/wg4-support-to-smes-coordination-with-countries-and-regions

for the support of political leaders in order to overcome the nationalistic tendency which pervades the thought process of some of the European consumers.

Thus, the goal is not easily achieved as it does require efforts from all of the stakeholders, public and private, while at the same time a number of elements (mentioned above) are already in place.

3.2.5 Networking aspects

This part been observed and deduced from partners analysis. In short, CHECKs should serve as a network within the NCCC and connect both the Network of National Coordination Centres and the Stakeholder Environment as well as the Community. This raises questions on the relationship of CHECKs with other CHECKs or national nodes of the network.

In the analysis phase, mapping of related answers to these issues has been done. Awareness, acculturation, sharing of knowledge, sharing of expertise, an observatory on European call for projects, support for participation in EU projects, lobbying, expression of needs on European funding tools, coordination on complementary actions with local economic agencies, new funding resources, benchmarking, and complementarity were all mentioned in the context of possible network-building.

An important and practical issue that has been raised as a part of this discussion was whether CHECKs may take on the role of a National Coordination Centre in Member States which, due to their size, have no or only limited possibilities for establishing an own Coordination Centre. At the time of writing this deliverable, this was still only speculation, so the discussion is postponed until more information is available.

With regards to inter-CHECK activities, the contribution of use cases for the development of research projects related to cyber threat, as well as cross-CHECK partnerships/new business relationships were mentioned, among others.

Another valuable source of input on the networking aspects is governance best practices (for the detailed analysis and overview, see D2.1 and D2.3). A number of existing organizations of diverse status, goals and reach have been dealing with the networking aspects of their activity according to their task, producing some valuable lessons for the validation process. Overall, two types of input can be distinguished: **positive** (to be considered) and **negative** (to be aware of).

Positive:

- The synergy between formal and informal, top-down and bottom-up structures can be beneficial to the overall success of an institution and interactions. By integrating lower-level, decentralized informal structures participation borders are reduced, leading to a more efficient stakeholder engagement throughout all societal levels;
- Providing membership opportunities for the stakeholders of different levels and foci enables bottom-up approach and diversity of engagement while creating space for small-scale initiatives to solve the concrete tasks (e.g., connecting start-ups with funding);
- Transparency is a key element for facilitating trust in an organization;

- A rigorous system to ensure the prevention of (financial) free-riding and the maximal involvement of the members in the projects relevant to them facilitates trust;
- A clear joint goal has to be defined, such as the development of a vibrant scientific community in Europe and ensuring its prominence on the world stage;
- The flexibility of the governance structure, including the mechanisms to distribute the positions, delegate powers, and create additional structures, would make it adaptable to the latest needs of the organization and state of the world;
- Balanced representation of different stakeholders is key to creating a sustainable network;
- Having a clear document, such as a Governance Charter, facilitates understanding of the goals and processes that will be guiding the network;
- The availability of various models of collaboration, suitable to the needs of different stakeholders with different goals and ambitions, as well as different financing options, would make the threshold lower to join;
- Within EIT, flexible structure of KICs (which can be compared to hubs) combines the guiding and harmonizing role of the EIT with the freedom of lower-level decision-making that is in tune with the market needs. Innovation Hubs are an interesting example of setting up a region-based cooperation network, tailored to certain needs and capitalizing on the available resources;
- When appropriate to the goals of a certain (national) community, a possibility should be explored for the collaboration between the two large structures operating within the same field, combining joint high-level strategic decision-making with the lower-level autonomy;
- The self-assessment and peer-assessment as membership criteria ensure good faith and continuous implementation of best practices when the more stringent official procedure hasn't been implemented;
- Agile structure, suitable for diverse types of cooperation, is a positive factor;
- Tangible scope and impact of each organization's mission and tasks is important;
- Pros and cons should be considered of the decisions of limiting the influence of certain stakeholders, such as commercial providers, in order to ensure that particular group is not dominating the organization's (and network) functioning.
- The network needs to be structured and presented clearly so that the new potential partners could easily determine "who they're going to call" with their specific need. An example of GEANT demonstrates the service portfolio matrix that offers a handy overview of NRENs, their services and membership status, thus facilitating collaboration.

Negative:

- Despite the formalization of the lower-level structures, there is always a danger that an organization will remain a top-down-institution; in the field of cybersecurity, it creates challenges for reaching out to the stakeholders and in reacting to stakeholders' demands;
- Governance best practices that are specific to the goals of fostering research and cooperation have to be applied with caution for the goals of fostering multi-stakeholder and multi-sectoral approach across the network of CHECKs;
- The focus on regional interests in the governance approach needs to be taken into account while transferring this best practice into "lessons learned" for the network. While it is necessary to make

sure that the local interests keep being safeguarded, for an international structure targeted towards the broadest cooperation possible, like a network of CHECKs, it might create development obstacles unless carefully kept in mind;

- The market-oriented approach to building networks is necessary to increase European competitiveness, but it might prove unsuitable for the creation of a sustainable network with diverse stakeholders;
- An often observed side-effect of the diversification of tasks at the different levels, combined with the ambition and magnitude of the goals, is the complexity and inefficiency of the overall governance structure;
- Explicitly excluding certain types of stakeholders from certain activities, such as general meetings is not productive for creating an atmosphere of trust and making out most of the potential long-term collaboration.

3.2.6 Funding issues

The abstract concept of a CHECK-T is very appealing, and all stakeholders are very positive about its priorities, membership, activities, and so forth. However, problems start immediately once questions related to the funding of such activities come to the fore, as very few stakeholders are eager to embark in such a journey if they are not first shown how their financial investment will enable these activities to generate their own income in the near future. This is why the orchestration of skill resources emerged as a good subject for a CHECK-T, as it makes CHECK-T primarily a source of revenue for its members, which may be complemented with a tool for lobbying, sharing good practices and information, and capacity building.

In this sense, if a CHECK-T is established as a means for its members to target regional, national, and European calls for proposals, and to coordinate the corresponding responses, then funding problems should normally be overcome through a mix of (i) membership fees paid by its constituting members, (ii) access fees for consultation of its directory, (iii) consultancy fees related to the facilitation of participation in calls for proposals, as well as through (iv) bonus schemes on the results.

On the other hand, if CHECK-T is established as the legal entity that is to be contracted in successful responses to calls of proposals, on behalf of its members, then the question of funding becomes something to which considerable attention must be paid, especially in what concerns IPR issues. One very successful example of this kind of organisation that comes to mind is IMEC[8].

One important point of attention is the fact that calls for proposals usually come with stringent rules on the financial capacity of the bidders. Therefore, CHECK-T bidding in calls for proposals should be able to demonstrate that the amounts for which it bids represent not more than around 20% of its financial capacity, which is given by its capital and turnover. The same must hold for each of its members that want to be part of bidding consortia.

[8] https://www.imec-int.com/en

Eventually, the amount of equity will be the result of the discussions with the founders as it will reflect the level of their ambition. The turnover could be based on the combination of the membership, access, and consultancy fees and bonuses alluded above.

3.3 Summary

Based on the results of the first stage of validation of the governance model, the next step should be the creation of the first centre of the future European network of competence centres for cybersecurity. Analysis of stakeholders' feedback enabled discussion and identification of what a Hub such as CHECK-T would have to do to match their interest and motivation. The next phase is based on the lessons learned from the previous work, which also enables drawing up the roadmap for the coming period.

The CHECK-T model can propose itself as a tool for its members to target regional, national, and European calls for proposals, for instance by setting up and coordinating its competent members that are interested in participating in selected calls. In this case, its role would be either to build and coordinate appropriate skills consortia to respond to calls for projects or to identify and orchestrate the available skills necessary to join, as a partner, larger consortia preparing to respond to calls for projects. This could also be done by considering that CHECK-T, as the representative of the community of competence of its territory, is the one submitting or contributing as a partner to the response submitted to the call.

Both cases described above – coordination of proposals or participation in consortia – imply that a CHECK-T must be in possession of a complete and up-to-date inventory of the skills and the knowledge available in the field of cybersecurity on its territory, and be aware of their availability and intention to participate in the implementation of such collaborative projects.

4 Other experiences in Europe

As it was already mentioned in the introduction and the chapter on methodology, different communities might already exist or, as it proved to be more likely case, are starting to emerge in different EU countries. Some of these communities, their formation, or their governance model, were influenced by DIH model (see for example Figure 6 from chapter 2), while others had rather different objectives and were looking for reorientation. The last phase of validation, therefore, focused on data gathering about the other communities from 5 countries where WP2 partners were coming from, as well as short analysis of compatibility of CHECK model and ECSO. While some of conclusions and outputs might be used for the second version of governance model (see also deliverable D2.3), this data gathering process was also used to make an additional validation with stakeholders outside of CHECK-T.

4.1 ECSO – the European Cyber Security Organisation

ECSO is the result of a need recognised by the European Commission and at the same time Industry/Research/Academic Stakeholders (within the European Organisation for Security (EOS)) that a neutral organisation representing both the public and private stakeholders and their communities was a necessity to effectively address the issues of cybersecurity within Europe. ECSO is one of the few stakeholder organisations that combines both the public sector and the private sector into one body and as such represents the needs and requirements from the differing communities. In many ways, ECSO is both a "bottom-up" and a "top-down" organisation in that the ECSO working groups are truly starting with the "grassroots", while the board of directors and the key chair and vice-chair representatives are engaging directly at the upper policy levels.

ECSO has a significant number of SMEs, large companies, research and academic organisations as members in addition to an important representation of European public administrations, and as such can truly represent the widest selection of stakeholder communities.

In essence, ECSO is a comprehensive representation of the full cybersecurity ecosystem. The "birth" and development of ECSO has not been a simple or easy process and often there are challenges of significant differences of objectives and agendas for the public and private sectors members, however, enough similar requirements exist so that cooperative efforts are genuinely possible within this context.

As ECSO is directly linked with the Horizon 2020 programme, it has been necessary to look at what an ECSO 2.0 or even an ECSO 3.0 might look like. While at the same time there are links to the Network of Cybersecurity Competence Centre(s) as well as the Digital Europe Programme and Horizon Europe as the follow-ons to Horizon 2020.

There is a need to have a coherent cybersecurity ecosystem approach in Europe and ECSO can fulfil this role with its "community" of members. ECSO can also "co-exist" with the CHECKS that might be defined in the future and would be envisaged to do so in a complementary and cooperative process.

4.2 Dutch national platform for cybersecurity research and innovation

In 2016, several ministries of the Dutch central government together with NWO, the Dutch Research Council, founded and funded a platform called "dcypher": the Dutch cybersecurity platform for higher education and research. This platform was meant to bring together the fragmented research landscape and connect researchers with industry. Its first round of funding was for 4 years. Between 2016-2020, dcypher has built a network of academic researchers and helped to forge collaborations with industry and government.

Then, in early 2020, the central government decided not to renew funding for dcypher and instead launched a new platform in the fall of 2020. The underlying reasoning appeared to be that dcypher had done good work in bringing the research community together, but it had not been effective in valorisation: bringing scientific innovation to market or to other contexts where it can generate societal impact. Rather than build on dcypher and extend its mission to include a stronger focus on valorisation, some of the funding ministries decided they needed to rebuild the platform more or less from scratch. After a failed attempt to design the platform by themselves, a design which encountered fierce opposition from various stakeholders, the government then asked a team of five representatives of key stakeholders to design it: one person from central government, one from universities, one from polytechnical schools, one from the cybersecurity industry and one from TNO, the Netherlands Organisation for Applied Scientific Research. The plan developed by this team was delivered to the central government in August 2020. The new platform is currently being realised, mostly in line with the developed plan. As of January 2021, the process of setting up the new platform is still ongoing.

Below we will analyse certain features of dcypher and the new platform, which is still nameless.

4.2.1 Stakeholders

The dcypher platform was not a separate legal entity, but a project organization based on a four-year subsidy from NWO and three ministries (Economic Affairs, Justice & Security, and Education, Culture & Science). It was set up at NWO and consisted mostly of NWO employees who were seconded to the project organization.

The subsidy only covered the costs of the platform itself. Actual research and innovation funding remained separate from the platform. That funding was meant to take place via existing instruments, like those for scientific research at NWO and for business innovation at the Netherlands Enterprise Agency RVO, which is a government agency that helps firms to gain access to government financing, support and networks for innovation and expansion.

The dcypher organization, more specifically its director, was accountable to a committee of officials from the funding ministries and NWO. In addition to this line of accountability, the platform set up a stakeholder board to advise its director. The stakeholder board consisted of around 20 people and included representatives from academic research groups, polytechnical school, government entities, large businesses, SMEs and security providers. It had no formal power other than advising the director, who would put items on the agenda regarding the activities and direction of dcypher. Not all the funding ministries were represented in the stakeholder board, as they felt this would have created a complicated role conflict (they

would end up advising themselves). While this is reasonable, it also created a strange governance structure, where the stakeholder board was providing direction to the platform and being positive about its results, while the committee of the platform's funders was separate from this conversation. Some of the funders, in the end, decided that they did not want to extend dcypher, because it lacked a strong connection with businesses, even though the businesses in the stakeholder board were very positive and petitioned the funders to continue dcypher.

The plan for the new platform has tried to learn from this strange governance model. It proposes an independent multi-stakeholder board for the new platform that is the main line of accountability for the platform director. This decouples the platform funding from the platform oversight and strategy. Funding will come from the Ministry of Economic Affairs for at least the first few years, while the course of the platform would be set by the board. The board would contain representatives from government (both in its role as an investor as well as its role of launching customer), security industry, large industrial users of security solutions, universities and polytechnical schools.

4.2.2 Objectives and functions

The dcypher platform had as its key objective to "improve the knowledge infrastructure" to protect Dutch society, develop expertise and innovation. It organized matchmaking events between academics and industry, presented three National Cyber Security Research Agendas, organized a yearly Summer School to help attract students to the field and played a modest role in coordinating four NWO research calls, including two in collaboration with U.S. Department of Homeland Security and two subsidy schemes to help SMEs bring research innovations to market.

The research funding schemes were administered by NWO, not the platform. The research proposals required industry co-funding (in-kind and in-cash). This was meant to ensure that academic research would be focused on realizing innovation with impact in the market and society. The amount of funding going into these instruments in those four years was modest, especially in comparison to the surrounding countries.

In 2020, when the subsidizing ministries decided they did not want to continue dcypher, their main critique was that the platform had been too focused on scientific research and not enough on valorisation. They seemed to associate this with dcypher's institutional location within NWO.

The new platform might be hosted at RVO, which is a government agency that administers business grant and subsidy programs. Irrespective of the hosting, the idea is to fund programs that better cover the whole "knowledge chain" from fundamental research to new products to actual adoption.

The new platform's mission is to contribute to a more secure, digitally autonomous and economically stronger Netherlands. Its vision is to better connect demand, supply and funding for cybersecurity education, research, innovation and application. A core objective is to better leverage the existing but fragmented funding for cybersecurity research and innovation. The platform meant to reduce the fragmentation across different funding mechanisms by bringing together different actors from across the knowledge chain around specific themes, such as automated vulnerability research. The themes would emerge basically from the actors that have funding to invest. Their funding would not go into the platform as such, but the incentive

to work with the platform is that the platform would then try to attract additional investments from other actors that are also interested in that theme, thus achieving a multiplier effect that benefits everyone by having more critical mass than each actor can achieve by itself.

4.2.3 Territorial dimension and economic development

The platform has a national focus. It also has a stronger focus on economic development than dcypher had. It will connect with regional initiatives in cybersecurity, often part of broader ICT-focused development agendas of regional economic boards, cutting across themes like AI, big data, and security. On the educational side, there are human capital agendas for various regions, which aim to better connect schools, especially the polytechnical schools, with demand for labour with IT skills, including security.

4.2.4 Networking aspects

The new platform builds on a strong existing network that was built by dcypher. It contains governmental agencies involved in cybersecurity, academic researchers, educational institutions, and a variety of companies – though with a focus on the supply side of cybersecurity products and services. The new platform is meant to better connect the demand side of the market, to create impact but also because those actors have funding to invest as they need new solutions. This can be private actors, like banks, and public actors, like the Ministry of Defence, which is launching a cybersecurity innovation hub.

4.2.5 Legal provisions

Both dcypher as well as the new platform are not set up as separate legal entities. Given that government funding is involved, setting up foundations or a similar independent legal person is seen as highly problematic by the governmental funders. For this reason, the funding agencies are aiming to host the new platform at RVO, which is legally positioned to administer subsidies and other transfers to private entities for operating costs. For the ministries themselves, such transfers are more complicated also in light of state aid regulations of the EU.

4.3 German Cybersecurity Community

The beginnings of the institutionalized cybersecurity community in Germany date back to 2005 and the *"National Plan for the Protection of IT Infrastructures"*. [10] Even then, the topic of critical infrastructures played a central role, and actors were the first to join forces in the UP KRITIS initiative, which is still active today. [11] Since then, a community has emerged in Germany, which consists of a multitude of very diverse initiatives and associations. They differ in their goals, topics and participating actors. In general, a distinction can be made between internationally, nationally, regionally and locally oriented associations. Similarly, a distinction can be made between public, private and public-private initiatives, depending on the type of participants. Further differentiation is possible, particularly based on the size of the companies involved. Finally, a thematic categorization of the objectives of the mergers can be made, with a distinction between divisional, operational, preventive and consumer-related initiatives.

Current government-initiated collaborations between different actors of the cybersecurity community in Germany are the *"Alliance for Cyber Security"* and the *"National Pact for Cyber Security"*. The first mentioned initiative was founded in September 2018 by the Federal Ministry of the Interior, Building and

Homeland Affairs and the Federation of German Industries in order to improve national and international networking between public and private actors, but also to strengthen Germany's digital sovereignty. [12] The alliance is a key player in the implementation of the German government's cybersecurity goals. One of its first tasks is to improve cooperation between national and international actors. To this end, the work undertaken has produced an initial overview of existing initiatives and alliances in the field of cybersecurity in Germany. [13]

The goal of implementing the Federal Government's cybersecurity strategy is also being pursued by the *"National Pact for Cyber Security"*, which was founded in October 2019 under the leadership of the Federal Ministry of the Interior, Building and Homeland Affairs. [14] At the same time, however, the circle of participants here is broader than the one of the Alliance for Cyber Security. The initiative aims to network all relevant actors in the field of cybersecurity, i.e. state, economy, science and civil society, and to cooperate in a spirit of trust in order to comprehensively promote awareness of and precautions against the dangers of cyberspace. The main objective of the initiative is to take a holistic view of all existing measures and initiatives as well as the steps required to improve cybersecurity in the form of recommendations for action.

However, there are many other institutionalized organizations of the cybersecurity community in Germany, from which the following should serve as examples for different approaches:

First, there is the "*UP KRITIS"* association, one of the oldest institutionalizations of the German cybersecurity community, pursues the goal of information exchange in the field of cybersecurity and prevention in the area of critical infrastructures. In the meantime, more than 540 members from this field are united in it, including the Federal Office for Information Security as coordinator and organizer of the alliance.

In contrast, the *"Alliance for Cyber Security"* is aimed at companies of all sizes and sectors with the aim of working together to improve cybersecurity prevention. [15] Here, too, the Federal Office for Information Security plays a leading role. However, the Federal Association of German Industry and the Federal Association for Information Technology, Telecommunications and New Media are also involved. The focus is on a trusting exchange of information on the cybersecurity situation, protective measures and cybersecurity incidents.

Another example is the *"Aktionsbund Digitale Sicherheit"*, in which forty players with a mainly civil society background have joined forces, pursues the goal of supporting consumers on the Internet by providing assistance and thus enabling them to use new technologies safely. [16]

Given Germany's federal structure, there are also a large number of regional and local initiatives and associations. For example, the "*Bavarian IT Security Cluster Association"* aims to pool IT security expertise in Bavaria and promotes research, development and application, but also the marketing of IT security products in this regional environment. [17] Comparable initiatives exist in almost all German states, e.g. in the form of the *security partnerships* in Berlin [18], North Rhine-Westphalia [19] and Rhineland-Palatinate [20], where even the Office for the Protection of the Constitution is involved as a provider of information on current attack scenarios. In turn, local initiatives are often linked to the local chambers of industry and commerce, such as the *Working Group for Corporate Security of the Osnabrück Chamber of Industry and*

Commerce [21], or are found at the major technology locations, such as in the form of the *Munich Security Network [22]*.

Besides, there is international cooperation as well as international initiatives. One example is the *German-Chinese Industry 4.0 project [23]*, which is carried out by the Federal Ministry of Economics and Energy together with the Society for International Cooperation.

To conclude, the German cybersecurity community serves as example for a community in a federal, decentralised form of government. An ample plurality in terms of geographical orientation and outreach, thematic approach and different forms of cooperation between private and public actors in initiatives and associations can be observed for this community. However, it can be seen from the governmental initiatives "Alliance for Cybersecurity" and "National Pact for Cybersecurity" that there is still a need to improve the networking and to get an overview of all actors and activities in the German community in order to thrive from the plurality.

4.4 Italian Regional Associations

4.4.1 Distretto Produttivo dell'Informatica (IT Production District) - Puglia Region

The IT Production District is a legally recognized non-profit association made of organizations operating in the fields of research, development and production of technologies as well as IT products and services in the region of Puglia. As part of the region's Production Districts, it is aimed at promoting, sustaining and favouring development programs focused on improving competitivity, innovation and internationalization in the area of Puglia. The IT Production District, more specifically, is tasked with promoting the growth and the improvement of its associates through activities including:

- R&D collaborative projects;
- Information and best practice sharing;
- Creation of shared IT infrastructures; and
- Education and training.

The District currently involves about a hundred parties spanning from industry, to academia, to employers' associations and trade unions. Among these parties are included all the universities situated in the region of Puglia – namely, the Universities of Bari, Foggia and Salento, as well as Bari's Polytechnic University – and more than 90 enterprises operating in the IT sector. Thanks to its wide-reaching membership, the District can claim to be representative of the interests of IT activities in the region.

The IT Production District of Puglia is governed by a District Committee, assisted in its functions by a Scientific Committee. The District Committee is composed of eight industry representatives, one association representative, one trade union representative and four academic representatives. The Scientific Committee, on the other hand, is composed only by three academic representatives and three industry representatives. The two Committees work together to define and realize the projects outlined in the District's three-year-long Development Plans.

Since 2017, the District has launched its own IT Observatory, which is the instrument through which the District realizes researches and analyses of the state of the IT system in Puglia. The Observatory is managed by a dedicated Strategic Steering Committee which defines its research aims; such Committee is composed

by the President of the District, one representative from the District Committee, and one representative for each University and each employers' association.

4.4.2 Regional Centre for Cybersecurity (C3T) - Tuscany Region

The Regional Centre for Cybersecurity (C3T) of Tuscany is an initiative of the Regional Council of Tuscany aimed at promoting research, stimulating knowledge diffusion and favouring innovation in fields contributing to the progress of regional industry and society. It has been established within a series of regional measures aimed at promoting strategies for the development of 'Industry 4.0' through the cooperation of academic and industrial actors, in agreement with the 2016 National Plan for Industry 4.0. The Plan highlighted the relevance of cybersecurity technologies as strategic matters for the development of digitisation processes in Italy, and encouraged the creation of regional competence networks – among others, in relation to cybersecurity technologies. The aim of the Regional Council of Tuscany is thus the creation of a Regional Centre for Cybersecurity for the use of SMEs, as well as for the regional public administration, to improve regional competences in the matter within national and European policies on cybersecurity.

The centre involves all the main university institutes of Tuscany, namely the Universities of Florence, Pisa and Siena, the National Research Council and the School for Advanced Studies (Lucca), as well as the Region of Tuscany itself. Its governance structure is straightforward, if not a little underdeveloped: it includes only a 'Technical Coordination Group' composed by one representative for each academic institution and three representatives for the Region of Tuscany. The main tasks of the group include verification and monitoring of the activities listed within the Memorandum of Understanding established between the different parties.

The activities entrusted to the Centre include a variety of services, including:

- Technical and scientific support for SMEs and Public Administration, specifically for the implementation of the GDPR;
- Certification services;
- Research projects and technological transfer;
- Education and training; and
- Creation of a Regional Monitoring Centre for Cybersecurity.

4.5 Community of CHECKs in Spain

In Spain, the situation related to the cybersecurity community was already well advanced before the European Union articulated the ambition to create a centre of competence. The main authorities, such as the National Cyber Security Council, or the Specialised Situation Committee, are assisting in the coordination of the stakeholders on cybersecurity matters as well as collaboration among the public authorities and between them and the private sector. Among public institutions, there are several important organisations, such as the National Cryptologic Centre (CCN), within the National Intelligence Centre (CNI), the CCN-CERT, which is the Information Security Incident Response Team of the National Cryptologic Centre, the National Centre for the Protection of Infrastructures and Cybersecurity (CNPIC), or Joint Cyber Defence

Command, responsible for the planning and execution of actions related to cyber defence in networks and information systems and telecommunications of the Ministry of Defence.

In 2019 the Spanish National Cybersecurity Institute (INCIBE), emerged as the organisation with the mission to organise and prepare Spanish community of stakeholders, starting with the Spanish project partners participating in four pilots in the context of European Cybersecurity Network and a Competence Centre. This again was not completely new for INCIBE. For many years, this organisation was supporting cybersecurity professionals, entrepreneurs, representatives of the academic and research sector, as well as cybersecurity companies. In 2017, for example, elaborated a catalogue and knowledge map of cybersecurity research in Spain, with characteristics, history, lines of research, and the results obtained from their research activity. INCIBE is also very active in the organisation of events, such as the Cybersecurity Summer BootCamp, an international specialized cybersecurity training programme, or ENISE, an annual event that has objective to generate business opportunities, facilitate the internationalisation, stimulate networking or promote entrepreneurship and innovation in cybersecurity.

It was in the scope of the 13th ENISE 2019 event, held in Leon during October 22 and 23 2019, that Spanish "seed" community of European Cybersecurity Network and a Competence Centre held its first meeting, with the presentations coming from all four pilot projects: CONCORDIA, CS4E, ECHO and SPARTA. Also, INCIBE presented the main objectives behind EU and Spanish challenges in the area of cybersecurity that need to be overcome with the help of the future centre, network and community:

- Lack of cooperation between Member States, industries and academia, leading to fragmented efforts in research and development (R&D);
- Insufficient investment in cybersecurity;
- Increased demand for skills, know-how and facilities, while access thereto is limited;
- Inconsistency of new policies and governance with the existing legal frameworks.

The objective if this initial meeting was also to collect feedback on the 2019 version of EU 2018/0328 Regulation Proposal of the Commission, sent to the EU parliament, that leaves many options open and does not fully address the underlying challenges, in particular regarding the "community" composed of all the economic cybersecurity actors.

One of the open discussions that started in the initial meeting and continued during the next 3 meetings in 2020 was the design of the governance model for Spanish community capable of addressing the identified challenges, having in mind Spanish specific situation.

CyberSec4Europe partners UMU and Atos presented draft governance model developed in this project with a community-driven approach and cybersecurity hubs which should enable collaboration between industry and academia, bring market security innovations, and help build capabilities in the area.

This work, led by ATOS and UMU, has resulted in a series of meeting between INCIBE and the other Spanish partners involved in the different Cybersecurity Pilots, in order to trigger collaboration and share ideas around the possible governance and structure of the Cybersecurity Competence Community (CCC) in Spain.

The main objective was to extend the idea of CHECK governance model developed and described in WP2 of CS4E, in a rather decentralized administrative context and operational scenario as it is Spain, without

losing coherence. The assumption was that different CHECK might exist, in some cases at the regional level or, in the other cases, cybersecurity hubs with focus on specific technology or sectors.

Community Hubs of Expertise in Cybersecurity Knowledge were presented to the Spanish community as a possible approach to form focus service groups (regional or sectorial/functional) at the national level as well, in order to organise Community. They should be based on:

- Bottom-up approach (e.g. WG topics defined by interest from the community);
- Common interest and strategic areas (e.g. research, innovation, and capacity building in cybersecurity);
- Different focus: regional, national, sectorial.

The complexity of having a large number of members under an umbrella organisation could be overcome by delegation to CHECKs, as well as sharing of the funds, tasks or risks. One example is registering and certification, as well as, monitoring of information sharing, etc.

In that sense, there is a similarity to ECHO's definition of CNO (connected networked organisation) as a breeding environment, with CHECKS at the national level and a Matrix of regional entities, as well as functional/sectoral entities.

In summary, initial Spanish approach for the governance model needs to consider the existence of different CHECK types that can be coordinated at the national level, as well as EU level, forming in a network of decentralized CHECKs (CHECKs-networks).

Several rules for membership and representation need to be defined including different statuses, such as full member, associated member and observers. Membership at CHECK (regional or sectorial/functional) could be decided upon assessment of the commitment to the network and according to the voting process. Representation in legislative bodies on central level – General Assembly– should be ensured for the full members and for representative elected from the regional and functional/sectorial entities (hubs, nodes, chambers, chapters or whatever type of networked organisation is represented). Working Groups or Taskforces would be grouping networks of experts from the full members of Spanish community, whether from the CHECKs or key stakeholders directly, working on detailed policies and agenda for concrete topics of cybersecurity and providing advice to the Strategic and Technical Committee. This committee, composed by representatives from the WGs, and an elected representative from stakeholders, could also include representatives of national associations/chapters and from National Public Administrations (note: this was only a proposal presented by UMU in July 2020, and at the time of writing this deliverable no feedback has been received).

Inside of Spanish CHECKs (hubs, nodes, clusters or whatever shape and name they have), the governance might be defined based on their own characteristics and context (e.g. strong focus on cybersecurity for the industry sector which is very important for the region). At the national level there should be a representative of the CHECKs at the working groups level (WGs) and over it a Strategic and Technical Committee that will advise the NCC with representative elected from the WGs and the different stakeholder groups from the different CHECKs. Large companies with a presence in different regions, and that address cybersecurity in many technologies and sectors, namely Telefonica, Indra or Atos, prefer to be involved directly in the work of WGs, as they would not be able to adhere to only one or two CHECKs.

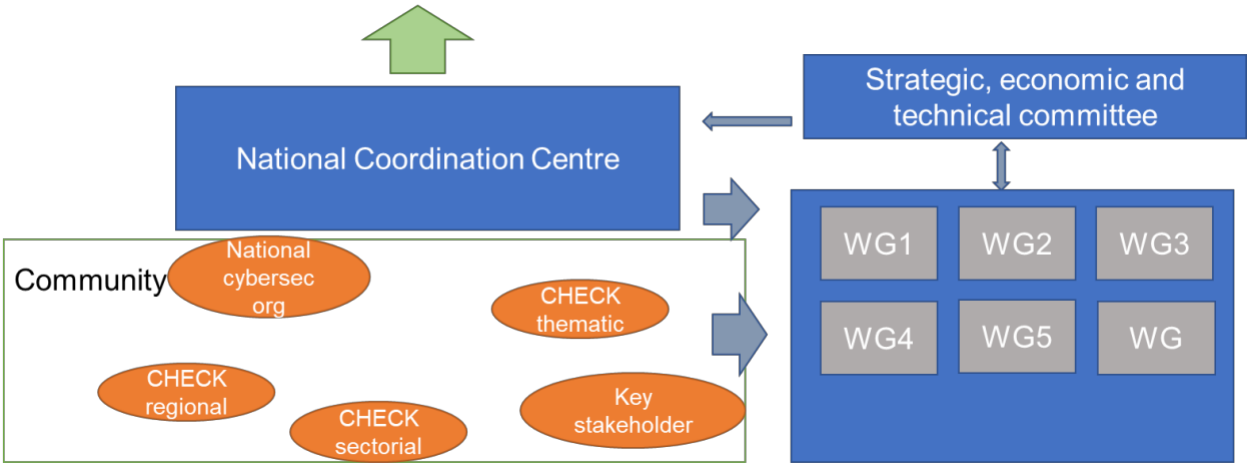

Figure 8: Proposal for Spanish cybersecurity community model

During the 4the meeting of Spanish community (organised by INCIBE and held online on July 13th), UMU has presented also possible priority areas, based on the model being validated by CHECK Toulouse. These are funding and R&D, services for the community and by the community, market and education/training/awareness.

4.5.1 Murcia regional cybersecurity unit

Following the idea of regional CHECK, an initial work at the Region of Murcia in Spain has been launched by the University of Murcia and the regional government with the idea of creation of a Regional Cybersecurity Innovation Unit. The objective is to establish it as a reference centre in cybersecurity within the framework of the Agenda for the Digital Transformation of Administration and Society in the Region of Murcia to promote the role of cybersecurity and its deployment in the field of Society of Knowledge, and the interrelation with similar entities at national and international level.

Based on initial interviews and contacts with the General Director of Strategy and Digital Transformation of the Murcia Government, it has been defined as a first approach of the objective of this Innovation Unit

Objectives:

- Promote collaboration between organizations and entities in the Region of Murcia to raise awareness, disseminate and promote cybersecurity in the administration, in academia and society in general;
- Generate synergies between all the organizations involved in the development of collaborative projects, as well as to promote the development of new initiatives;
- Ensure through training the availability of highly qualified professionals;
- Create a space for discussion and generation of socio-ethical-legal knowledge in the area of cybersecurity;
- Raise public awareness of the importance of cybersecurity through demonstration spaces, workshops and collaborative events;

- Collaborate with other reference centres in cybersecurity both nationally and internationally;
- Extend the use of systems for the prevention, characterization, detection and containment of cyber-attacks in society in general, as well as promoting information exchange mechanisms related to incident management;
- Collaborate in future regulations on cybersecurity at the national and European level and be one of the instruments for its deployment;
- Define and execute pilot projects for safe technologies at the regional level, as well as a space for co-innovation at the regional level.

Initial pilot activities defined:

- Cyber Thread Intelligence pilot for administrations and regional public entities;
- Assessment of ICT infrastructure threats in pandemic situations and possible protection scenarios;
- Analysis of non-invasive technologies and with support to protect the identity and privacy of the user and the organization of demonstrators to improve the trust of the agents;
- Definition and development of training and awareness modules for different regional actors.

4.6 Cybersecurity Community in Greece

Greece has advanced in establishment of a cybersecurity community and with the Presidential Decree of 82/2017, a National Cyber Security Authority (NCSA) was established, along with a Single Point of Contact, both of which currently operate at the Ministry of Digital Governance [9]. This first step was very important because the newly established NCSA was given the overall coordinator role for the cybersecurity policy in Greece. NCSA was responsible for coordinating the public sector and the operators of essential services of Greece, in order to take all necessary steps towards a secure Greek Cyberspace. Its main objective is to shield the nation from external threats and to provide a secure digital environment for all Greek citizens.

Shortly after the Presidential Decree, in March 2018, Greece issued the National Cyber Security Strategy. The establishment of the National Cyber Security Strategy determined the main principles for the creation of a safe online environment in Greece and set the strategic objectives and the action framework through which these could be achieved.

Most of these objectives were put forward immediately from the NCSA with the cooperation of corresponding stakeholders. Using the strategy as a guide, the NCSA issued the Greek National Law 4577/2018 that transposed the NIS directive into the Greek legal framework, determined the main threats and vulnerabilities of the public sector through structured questionnaires, identified the operators of essential services (National Critical Infrastructures), defined a minimum set of security requirements, and developed a novel cybersecurity assessment model among others.

The Greek NCSA in cooperation with all relevant stakeholders inside Greece and worldwide managed to climb 31 places and rank 1st in the NCSI index. The NCSI index measures the preparedness of countries to prevent cyber threats and manage cyber incidents and is a measure of the maturity of a nation in terms of cybersecurity posture. Except for the legal initiatives, NCSA has also participated in several educational, awareness and research activities. Being one of the first National Authorities that participated in the

consortium of CONCORDIA, one of the four pilots which are chosen to address the Horizon 2020 Cybersecurity call "Establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap". The NCSA of Greece participates in the policy-making and dissemination work packages, and the participation in this consortium further improves its cooperation and awareness capabilities.

One of the produced outcomes is the maturity assessment framework, can help organizations achieve progressive improvements in their cybersecurity maturity by first achieving stability at the current level, then continuing to a more advanced level in an organization-wide, continuous process improvement, using both quantitative and qualitative data to make decisions. For instance, at maturity level 2, the organization has been elevated from an "ad hoc" to a "managed" level, by establishing sound security controls, procedures, and processes. Moreover, the developed framework can be used at a European level to prioritise mitigation plans and funding related to cybersecurity. When a full security review or assessment cannot be implemented, undertaking efficient cybersecurity risk assessments and implementing mitigations in large, established critical infrastructures could also be a tentative solution.

Finally, by following the GDPR and the NIS directive, which aim at protecting organisations against cyberattacks, we can observe an overlap in several aspects. Adoption from the organisations is often a challenging task as stakeholders face difficulties to understand their roles and design consistent cybersecurity frameworks inside their organisations, due to the regulations' requirements overlapping. To address this issue the mapping of GDPR and NIS directive requirements is needed. In that way, organisations will be able to adopt these regulations properly and help them to identify current potential security issues and structure new security plans.

5 Conclusions and recommendations

This deliverable objective was to report on CHECK governance model validation activities that took place during 2020 and that focused on specific implementation of this model in Toulouse. This model, built on bottom up inputs, is assumed to address the main challenges of stakeholders in a heterogeneous community, as well as cultural and organisational diversity, that we have in Europe. The project deliverable D2.1 has outlined the first approach with a governance model, while tasks T2.3 and T2.4 were applying this model in practice, and are directly linked to establishing CHECK in Toulouse. While the main partners involved in building CHECK-T, and in these two tasks, were collecting stakeholder outputs in the form of opinions, suggestions, lessons learned etc, the other work package 2 (WP2) partners were analysing these outputs, both individually, as well as jointly, with a convergence of different analysis results. In addition, each partner tried to describe, and in some cases influence, cybersecurity communities in their own countries, based on the previous validation experience from CHECK-T.

The work performed in the past 12 months focused on validation of parts of governance, such as cooperation model between different stakeholders, including institutional partners, industries and academia to evaluate opinions on ways to pool resources and maximise efforts in cybersecurity, as well as to increase investment in cybersecurity, or give support to growing demand for skills, know-how and facilities.

Stakeholders in Toulouse gathered in the validation exercise expressed widespread support for the general idea and objectives of the future centre, network and community, and confirmed many priorities such as capability-building or policy and R&D roadmap inputs. We can conclude that in terms of governance structures that have been proposed in D2.1, there was a claear support for bottom up approach and openness to a diverse set of actors, initiatives and collaborations. Validation exercise also helped to examine different types of alternative governance elements, mainly used for report in D2.3, while analysis of received feedback, as well as incorporation of inputs from external initiatives, revealed also need to be flexible, maintaining balance between formal and informal, top-down and bottom-up approaches, leading to a more efficient stakeholder engagement throughout all levels.

Conclusions are targeting policy makers, but also those that want to set up new CHECKs. They are based on practical experience with establishing CHECK-T

To start with, it’s important to differentiate at least two types of CHECK, namely one that is an economic actor in the cybersecurity landscape and must be sustained by a sound business model, and another that is part of the public administration and financed as a public good.

The case of the CHECK-T pilot, that is used to validate governance model from D2.1 in CyberSec4Europe, through its partner UPS-IRIT, is an example of the former type, which brings to the fore notable insights based on day-to-day implementation experiences. This includes some mistrust from the part of public administrations, because of issues related to their perimeter of action and influence.

The spring 2020 interview campaign carried out by UPS-IRIT elicited the needs from cybersecurity and regional stakeholders and highlighted services expected from CHECK-T. Such needs and potential services

were meant to constitute the basis upon which to build the organisation's business models. For instance, it could allow the creation of a map of a secure industrial ecosystem that would include links to the other stakeholders.

The offered services could contribute to the economic security of the so-called essential sectors of the territory, in this specific case that of the Region Occitanie, and would have as primary vocation to support the rise in the capacities of SMEs and subcontractors of these sectors, in their approach to crisis management, in particular related to cybersecurity. The development and deployment of services related to the establishment of a CHECK-T would be done in close partnership with solution providers and the research and higher education communities in the Occitanie region.

In parallel to validation through CHECK-T, we also did validation exercise with participants of a cross-pilot task group, as well as with the stakeholders of cybersecurity communities in other countries. The attempt to map it to different options and contexts was done in other countries, for example in Spain, with the involvement of partners participating in the other pilot projects, as well as representatives of national cybersecurity body.

There are several conclusions that can be drawn from validation exercise with the lessons learned and recommendations for each of them. Validation methodology, for example, included preliminary analysis to quickly determine the stakeholder groups that would or should participate in the foundation of the CHECK-T. In this part representatives from the End Users, Cyber Security Solution Providers, Technology Centres, and Economic Development Accelerators have been consulted. In order to quickly ensure the feasibility and relevance of the approach chosen for a specific territory, it is recommended to go through a phase of formal "pre-configuring" of the organisation to be established. Its effective implementation implies favouring legal support by an actor in the territory with a certain notoriety in the targeted ecosystem. It enables CHECK to attract funds and to deploy, in its territory, a structuring project that would demonstrate the robustness and sustainability of its economic model, whereby kickstarting the legitimacy of the CHECK in the eyes of its stakeholders. As part of the partnership logic, this model is based on a legal support from a third party and it must favour a structure with mainly public capital, because the production of common deliverables by a multidisciplinary ecosystem requires, as a sine qua non that cannot be overstated, an environment of trust from the outset. Once that types for membership and representation are defined, for example full member, associated member and observers, decision support rules could be decided accordingly to their commitment and with according voting rights. Incentives and motivation of different stakeholders should be considered from the start and proper analysis of these should be done in order to include it in the strategy. Besides those that are already mentioned in this deliverable, reputation of core group, as well as early members, and trust relationships should be considered. The bottom-up approach of the community organization advocated by CyberSec4Europe should be consistently pursued. However, this may be challenging in the countries and communities with the top-down organizational approach to establishing CHECKs. The commitment to building the collaborative governance environment for nurturing the network governance model will be needed in order to come up with creative tailored solutions for each community. Ensuring transparency of the CHECK establishment process and fostering trust-based cooperation between diverse stakeholders will contribute to the successful and sustainable community organization through CHECKs, boost and harmonize the cooperative cybersecurity environment in Europe.

The next step in validation methodology was analysis related to the subject matter of CHECK-T, as well as its role. Both issues also delimit the appropriate status that is required and the contractual nature. While assumption that the main added value of a CHECK-T is capacity to coordinate and orchestrate exogenous and diverse skill resources, cooperation and communication have also been validated as the central focus for entities participating in CHECKs, with the aim of creating a trustful environment to respond to cybersecurity menaces. The development of effective training practices should become an early priority action, specifically concerning end users, in order to improve the general awareness towards cybersecurity issues. The research and innovation capacity seem an important factor, but given the territorial nature of CHECK-T, the importance of sector specific use cases, which are strategic for the region, appeared as a relevant issue in strategic decision making. Additional validation might be needed to find out how CHECKs model would work with different priorities. Mentoring aspects and seed capital investment strategies were not highlighted, while testbeds and other resource sharing, such as space for experimentation, were also not prominently mentioned during the validation with stakeholders.

Finally, when it comes to economic model and networking aspects, validation based on CHECK-T found some difficulties due to the context and delays, both due to the COVID and development of EU regulation. The construction of CHECK economic model should be based on diversified financial resources, the foundation of which would come from major programs in the area, proposed by local authorities in a first step, before being completed by e.g. and inter-alia (i) membership fees paid by its constituting members, (ii) access fees for consultation of its expertise, (iii) consultancy fees related to the facilitation of participation in calls for proposals, as well as through (iv) bonus schemes on the results. CHECKs should be represented at the ATLAS as another actor in the cybersecurity community. One important activity of CHECK, in this role, could be to provide the member assessments, in cooperation with the National Coordination Centres. Assuming existence of different CHECK types, that can be coordinated at national level first and later at EU level forming in network of decentralized CHECKs (CHECKs-networks), which could be basis to constitute the EU Competence Community, the flexible governance model at national level should be also replicated at the EU level. Alignment between EU, national and regional interests or research agendas should find place on a regular basis. Once active, the National Centres should interface with the recently activated European Digital Innovation Hubs (EDIHs), which follow model similar to CHECKs. Considering that, for example, the Italian Regional Associations examined in 4.4 also applied to become EDIHs, it is possible to observe the similarities between the two projects. Interface would thus be necessary to avoid any kind of duplication in structure and limit overlap in tasks performed.

Besides these recommendations, that will be also considered in the future version of governance model, CHECK-T validation highlighted some of the issues that could become the best practice for the future CHECKS or similar structures. They should be, for example, be as plural as possible with a balance between research organizations, universities, companies or business associations and regional public entities. As the main governing or operational bodies within CHECKs, the existence of a management committee, an executive committee, a technical committee or a secretariat, as well as individual figures such as the president or the technical coordinator, are possible options. It is also important to engage actors who can reach out to the wider target groups, such as cluster organisations, industry associations and chambers of commerce, Other important partners are organisations who can provide capacity building, skills upgrading

and training. Incorporating existing structures might be beneficial as there are both formal and informal means of engaging with stakeholders and collecting feedback. The internal organization and interconnection of CHECKs should be as flexible as possible and should be able to pursue a variety of different objectives. This would make it possible to set up CHECKs that are both topic- and sector-specific, as well as area-oriented, as well as to have different regional, national or either cross-border CHECKs. Investment in research is difficult for highly specialised start-ups and SMEs, and they might lack experience of participation in EU programmes. Coordination and support should be given to these kinds of stakeholders. Large organisations have critical role in accelerating research and innovation, as well as support to scaling up innovative results. They should have proper incentives to this in collaboration with smaller organisations and start-ups. Given that situation in France, and in CHECK-T is different from other countries and regions that are mentioned in this report, we also recommend to include analysis of parameters such as maturity, acceptance/desirability, the feasibility of implementation and sustainability of future community "hub", whether they follow CHECK governance or some other model. In relation to setting objectives, actions related to stimulation of R&D, but also others such as capability-building and policy interventions, support and interlinking is needed, not only between research and industry, but also with regional development, investment instruments and funding mechanisms. Establishing the CHECKs-network needs active networking between all European CHECKs, e.g. a constant flow of information and knowledge exchange, to avoid the perpetuation of the current fragmentation of the efforts of the industrial and research communities. The diverse stakeholder setup will ideally enable allocating public investments to research via proposals that have secured co-funding from the private sector. This would avoid misalignment between innovation priorities and market. Consortium-building for European and national-funded projects has high transaction costs, which are often not recuperated by collaborating on just a single project. The CHECKS can enable more efficient consortium-building. Subsequently, it will be possible for competition to emerge among proposals with different consortia across the platform, where participants have access and support at board level in their own organizations. This process could be facilitated by developing standard contracts that can be reused across consortia and projects.

References

[1] Guide on Research and Innovation Strategies for Smart Specialisation, available at https://s3platform.jrc.ec.europa.eu/s3-guide, last access January 2021

[2] Four pilots for Cybersecurity Competence Centre and Network joint website, https://cybercompetencenetwork.eu/, last access January 2021

[3] Digital Innovation Hubs, https://ec.europa.eu/digital-single-market/en/digital-innovation-hubs, last access January 2021

[4] Nai-Fovino I, Neisse R., Lazari A., Ruzzante G., European Cybersecurity Centre of Expertise - Cybersecurity Competence Survey. EUR 29330 EN, Publications Office of the European Union, Luxembourg, 2018, ISBN 978-92-79-92954-0, doi:10.2760/42369, JRC111211.

[5] Georgi Penchev and Velizar Shalamanov, Architecture and Process Oriented Approach to Institution Building of Network Organizations (Case of Cyber Security Competence Network), Information & Security: An International Journal 46, no. 1 (2020): 99-113

[6] JRC report, Digital Innovation Hubs in Smart Specialisation Strategies, Early lessons from European regions, available at https://s3platform.jrc.ec.europa.eu/documents/20182/201464/Digital+Innovation+Hubs+in+Smart+Specialisation+Strategies/, last access January 2021

[7] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, https://eur-lex.europa.eu/procedure/EN/2018_328, last access January 2021

[8] Legislative observatory of European Parliament, European Cybersecurity Industrial, Technology and Research Competence Centre and Network of National Coordination Centres, https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2018/0328(OLP), last access January 2021

[9] Maglaras, Leandros & Drivas, George & Noou, Kleanthis & Rallis, Stylianos. (2018). NIS directive: The case of Greece. EAI Transactions on Security and Safety. 4. 10.4108/eai.15-5-2018.154769.

[10] Federal Ministry for the Interior, Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI), July 2005, pp. 7 et seq., https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/05-12-09/05-12-09-anlage-nr-16.pdf?__blob=publicationFile&v=2 (26.09.2020).

[11] Articles from Federal Office for Information Security/Federal Office for Civil Protection and Disaster Assistance, UP KRITIS, https://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/UPKOrganisation/upk_organisation_node.html, last access January 2021

[12] Bündnis für Cybersicherheit: Industrie und Innenministerium intensivieren Kooperation, https://bdi.eu/artikel/news/industrie-und-innenministerium-etablieren-buendnis-fuer-cybersicherheit/, last access January 2021

[13] Cybersicherheitsinitiativen presentation from Bundesverband der Deutschen Industrie e.V., https://issuu.com/bdi-berlin/docs/201912_publikation_bdi_cybersicherheitsinitiativen, last access January 2021

[14] Nationaler Pakt Cybersicherheit gestartet - bestmögliche Vernetzung im Bereich der Cybersicherheit in Deutschland, https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2019/10/nat-pakt-cybersicherheit.html, last access January 2021

[15] Allianz für Cyber-Sicherheit web page https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/startseite.html, last access January 2021

[16] Deutschland sicher in netz web page, https://www.sicher-im-netz.de/, last access January 2021

[17] IT-Sicherheitscluster e.V. web page, https://www.it-sicherheitscluster.de, last access January 2021

[18] Verband für Sicherheit in der Wirtschaft Berlin - Brandenburg e. V., https://www.vsw-bb.de/sicherheitspartnerschaft.html, last access January 2021

[19] Sicherheid fur Nordrhein-Westphalen web page, https://www.im.nrw.de, last access January 2021

[20] Rheinland-Pfalz web page, https://mdi.rlp.de/de/startseite/, last access January 2021

[21] Industrie- und Handelskammer Osnabrück - Emsland - Grafschaft Bentheim web page, https://www.osnabrueck.ihk24.de/servicemarken/ueber-uns/ihk-netzwerke/unternehmenssicherheit, last access January 2021

[22] Sicherheitsnetzwerk München web page, https://it-security-munich.net/, last access January 2021

[23] Platform industrie 4.0 web page, https://www.plattform-i40.de/PI40/Redaktion/DE/Dossiers/internationale-kooperationen.html, last access January 2021