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

Project start: 1 February 2019
Project duration: 42 months

Cyber Security for Europe

D2.3

Governance Structure v2.0

Document Identification	
Due date	31 January 2021
Submission date	27 January 2021
Revision	1.0

Related WP	WP2	Dissemination Level	CO
Lead Participant	GUF	Lead Authors	Christina von Wintzingerode, Dirk Müllmann (GUF)
Contributing Beneficiaries	GUF, TLEX, TUD, UMU, UPS-IRIT	Related Deliverables	D2.1, D2.2, D2.4

Abstract:

The existing and emerging cybersecurity threats require new models of organisation in order to tackle them efficiently. The EU 2018/0328 (COD) Regulation Proposal of the European Commission contains ideas for the governance design, yet it still leaves a lot of options open. Thus, the ultimate goal of CyberSec4Europe as a project is to design the governance structure for a European network that will answer the main challenges faced by the field of cybersecurity today. The role and the structure of the Cybersecurity Competence Community, which has been left open for interpretation in the Regulation Proposal, will be crucial for mastering the cybersecurity challenges due to its potential in research, development and dissemination activities.

CyberSec4Europe has elicited stakeholder and legal requirements and best practices to design the governance model. Based on these inputs the deliverable D2.1 presented the Governance Structure v1.0 one year ago, exploring a bottom-up approach to answer the stakeholders' demands and to further the cybersecurity research and development in Europe. Since then, additonal governance structures have been analysed and the implementation process of CHECK-T and the Region of Murcia CHECK have delivered some first insights on the challenges, stakeholders' requirements and possible approaches on the hub governance design. Based on these additional findings the governance structure, with a focus on the concept of CHECKs, has been further developed. This deliverable D2.3 now presents the results in Governance Structure v2.0.

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 Union has articulated the ambition to maintain its digital sovereignty and become a global leader in the digital economy. This ambition is guided by European democratic values and, amongst others, requires the capability to be resilient when it comes to cybersecurity threats. The European Commission has identified four main challenges in the area of cybersecurity that need to be overcome in order to realize this ambition:

- 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.

In order to meet these challenges, the European Commission has proposed to establish the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. The current EU 2018/0328 Regulation Proposal of the Commission still leaves a lot of options open, however. Moreover, the proposal does not fully address the underlying challenges, and thus additional governance mechanisms are needed.

In continuation of the first draft of a wider governance structure presented in deliverable D2.1, this document reports on the further development of the proposed governance structure developed by Work Package 2 (WP2) of CyberSec4Europe, one of the four pilots initated by European Commission to test and develop potential network governance designs. The overall approach of CyberSec4Europe is to explore a community-driven approach for the governance model to complement – and marginally adjust – the EU Regulation Proposal 2018/0328, within the legal requirements. In short, we propose a combined top-down and bottom-up approach and addition of a network of Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs) to the European network as outlined in the Regulation Proposal. Furthermore, we propose the introduction of a sub-structure for the Competence Centre, the introduction of a Stakeholder Council as an additional bottom-up element, and a modification of the existing governance structure for network as proposed in the Regulation Proposal.

This deliverable D2.3 offers a continuation of the analysis of existing governance structures started in D2.1 and the first results from the prototyping activities for CHECKs, involving CHECK-T and the Region of Murcia CHECK. The team involved with the implementation of CHECK-T also conducted interviews with stakeholders in order to learn about their needs and requirements regarding CHECKs, e.g., which details make the concept of CHECKs attractive for them to participate and contribute to the cybersecurity Community. These results together with findings from the observation of possible changes in the governance structures of organisations already addressed in D2.1 and the observation of the progress made in the legislative process are the basis for the improvement of the governance structure as proposed in D2.1 with the main focus on the development of a detailed governance approach for CHECKs.

Document information

Contributors

Name	Partner
Indra Spiecker gen. Döhmann	GUF
Dirk Müllmann	GUF
Christina von Wintzingerode	GUF
Dorien Surinx	TLEX
Natalia Kadenko	TUD
Antonio Skarmeta	UMU
Abdelmalek Benzekri	UPS-IRIT
Pierre-Henri Cros	UPS-IRIT
Afonso Ferreira	UPS-IRIT

Reviewers

Name	Partner
Tobias Fiebig	TUD
Christos Douligeris	UPRC
Jozef Vyskoc	VaF

History

Version	Date	Authors	Comment
0.1	27-11-2020	GUF, TUD, UPS-IRIT	1st Draft
0.2	16-12-2020	GUF, TLEX, UMU	2nd Draft; including additional subchapters by UMU and WP2 comments; Chapter 1 extended by description on intentional overlap between D2.2 and D2.3

0.3	18-12-2020	UMU, TUD	3rd Draft incorporating clarifications on subchapters by UMU and TUD contribution on other pilots' governance structure
0.4	11-01-2021	GUF	4th Draft incorporating feedback from WPL review, improvement of document structure and addition of additional conclusions
0.5	14-01-2021	UPRC	5th Draft with suggestions and comments from second review
0.6	18-01-2021	GUF, TLEX	6th Draft incorporating review feedback and addition of chapter on CHECKs & competition law
0.7	22-01-2021	GUF	7th Draft with minor layout improvements sent to WPL
0.7	22-01-2021	TUD	7th Draft forwarded to PC for PLR
0.8	27-01-2021	GUF	Incorporation of comments from PLR
1.0	27-01-2021	GUF	Final version sent to PC and WPL

Table of Contents

1 Introduction 1
1.1 Challenges 1
1.2 Approach and Methods 2
1.3 Document Structure 2
2 Existing Governance Models 4
2.1 Re-evaluation of governance models addressed in D2.1 6
2.1.1 ENISA 6
2.1.2 ECSO 7
2.1.3 CERN 8
2.2 Additional Governance Structures 9
2.2.1 CEN/CENELEC 9
2.2.2 ETSI 11
2.2.3 EIT International 14
2.2.4 IMEC 17
2.2.5 GEANT/NRENs 20
2.2.6 IT Planning Council 22
2.3 Governance models of other pilots 26
2.3.1 ECHO 26
2.3.2 CONCORDIA 26
2.3.3 SPARTA 27
2.4 Comparative overview of analyzed governance approaches 29
2.5 Conclusion 32
3 Stakeholder Viewpoints on CHECKs 33
3.1 Needs and expectations 33
3.2 Strategic application areas and activities 36
3.3 Governance 37
3.4 Funding 37
3.5 Conclusion 37
4 Report on the implementation status of prototype CHECKs 39
4.1 CHECK-T 39
4.1.1 Membership 40
4.1.2 Governance Structure 40
4.2 Region of Murcia CHECK: Regional Cybersecurity Innovation Unit in Murcia (Spain) 41
4.2.1 Membership 41
4.2.2 Governance Structure 41
4.3 Conclusion 43
5 Proposal for the further development of the Cybersecurity Network Governance 44

5.1 Summary of core insights in Chapters 2-4 and consideration of current status of legislative process for Regulation Proposal 2018/0328 (COD) 44
5.2 Further development of CHECKs 45
5.2.1 Number and Structure 46
5.2.2 Relationship 50
5.2.3 Membership 52
5.2.4 Activities 55
5.2.5 Interdisciplinarity 56
5.2.6 Funding 56
5.2.7 Listing in the European Cybersecurity Atlas 57
5.2.8 CHECKs & Competition Law 58
5.2.9 Conclusion 62
5.3 Stakeholder Council 63
5.4 Competence Centre 64
5.5 Network of National Coordination Centres 65
5.6 Cybersecurity Community Establishment 65
5.7 Conclusion 65
6 Conclusion 68

List of Figures

Figure 1: Governance structure of ENISA 6
Figure 2: Governance structure of ECSO 7
Figure 3: Governance structure of CERN 8
Figure 4: CEN-CENELEC Management Centre organisational chart 11
Figure 5: EIT organisational chart 17
Figure 6: Organisation and structure of the IT Planning Council 25
Figure 7: Governance Topic in ECHO 26
Figure 8: Contextual, impact-based symbiosis of four intertwined main domains (as mentioned in the proposed Regulation) 27
Figure 9: Community groups and mission classes for a CHECK-T 34
Figure 10: Synthesis of the needs and expectations 35
Figure 11: The four strategic application areas emerging from the interview campaign 36
Figure 12: List of activities selected to establish the first CHECK-T 37
Figure 13: Vision for CHECK-T 40

List of Tables

Table 1: Overview of positive and negative aspects in the analysed governance examples 31

List of Acronyms

C	**CEN**	Comité Européen de Normalisation
	CENELEC	Comité Européen de Normalisation Électrotechnique
	CERN	Conseil Européen pour la Recherche Nucléaire
	CHECK	Community Hub of Expertise in Cybersecurity Knowledge
	CHECK-T	Community Hub of Expertises in Cybersecurity Knowledge in its Territory
	CNO	Collaborative Network Organization
	CONCORDIA	Cybersecurity Competence for Research and Innovation
E	**ECHO**	European network of Cybersecurity centres and competence Hub for innovation and Operations
	ECSO	European Cyber Security Organisation
	EIT	European Institute of Innovation and Technology
	ENISA	European Union Agency for Cybersecurity
	ETSI	European Telecommunications Standards Institute
	EU	European Union
	EC	European Commission
F	**FITKO**	Föderale IT-Kooperation (the IT Planning Council's office for federal IT cooperation)
G	**GÉANT**	Pan-European research and education network that interconnects Europe's National Research and Education Networks (see NRENs)
	GUF	Goethe-Universität Frankfurt
I	**IMEC**	Interuniversity Microelectronics Centre
	IRIT	Institut de Recherche en Informatique de Toulouse
	IT	Information Technology

J	**JRC**	Joint Research Centre
K	**KIC**	Knowledge and Innovation Communities
N	**NCC**	National Coordination Centre
	NCCC	Network of Cybersecurity Competence Centres
	NGO	Non-Governmental Organisation
	NRENs	National research and education network organisations
R	**ROI**	Return on Investment
S	**SMEs**	Small and Medium Enterprises
	SPARTA	Strategic programs for advanced research and technology in Europe
T	**TEU**	Treaty on the European Union
	TFEU	Treaty on the Functioning of the European Union
	TLEX	Timelex
	TUD	Technische Universiteit Delft
U	**UMU**	Universidad de Murcia
W	**WG**	Working Group
	WP	Work Package

Glossary of Terms

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 **CHECKs**

Community Hubs of Expertise in Cybersecurity Knowledge.

CHECK-T

Community Hub of Expertise in Cybersecurity Knowledge in its Territory.

Community

The interacting set of all stakeholders.

Competences

Ability to address technical and societal challenges.

Cooperation

Interaction between multiple stakeholders for their mutual benefit.

Coopetition

Cooperation of circumstance or opportunity between different economic actors, who, moreover, are competitors.

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.

I **Industry**

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

L **Law**

The set of applicable law and regulations of all member states and the EU combined.

M **Member State**

A nation that is a member of the European Union.

N **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.

Regional Hub

A competence centre associated with a region.

Regulation 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.

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.

1 Introduction

The present deliverable is a continuation of the work of WP2 of the European pilot project CyberSec4Europe. Its subject is the investigation of the governance structure of the European cybersecurity network planned by the European legislator. This Network aims to strengthen cybersecurity within the Union by combining national efforts and better involving European actors in the field of cybersecurity and to strengthen the Union's economic position in this area by improving the translation of research results into marketable products. On the one hand, the report presents the results of the work carried out since January 2020 in the work package on the further development of the cybersecurity network. On the other hand, it makes proposals for their further optimization.

The starting point of the present consideration is identical to that of Deliverable 2.2 “Internal Validation of Governance Structure”. Both deliverables emanate from the legally provided governance structure and its transposition in the pilots. However, the two documents differ in their objectives. The analysis in 2.2 aims at verifying the structure of the cybersecurity network on the basis of the project pilots and the statements of its members and at optimizing it on the basis of their wishes. The analysis presented in this D2.3 focuses on the existing governance structures of other organizations in the field of cybersecurity and as the analysis of the legal requirements on the European level and tries to derive a proposal for an optimized governance structure of the European cybersecurity network. Despite the different directions of both deliverables, there are inevitably overlaps in content within the considerations against the background described. However, these overlaps are intentional and unavoidable.

1.1 Challenges

As mentioned in Deliverable 2.1, to improve cybersecurity in Europe it is necessary to address four key challenges[1]:

1. Lack of cooperation between member states, the industry, and other actors, which currently leads to a segmented research and innovation landscape within Europe.
2. Insufficient investment into security capabilities and research within the European Union, including government and private funding prospects.
3. Limited availability of cybersecurity professionals trained in the European Union, combined with limited ability to retain those professionals, given an increased global demand.
4. Creation of policy and governance models facilitating these goals that would be compatible with existing regulations and the requirements of all involved actors.

As one way to address these challenges, the Commission has announced to set up a Network of Cybersecurity Centres, the continued study of which is the subject of the present work package and this deliverable.

[1] D2.1, p. 1.

1.2 Approach and Methods

The deliverable at hand uses a variety of methods to verify the optimal governance design for the European Cybersecurity Network, and, hence, analyzes:

- existing governance models,
- proposals for European legislation,
- interviews with stakeholders.

On the one hand, governance models of existing projects and initiatives in the field of cybersecurity are examined. From their organizational structure, suggestions for and conclusions about the internal and external organization and task distribution between the institutions, which are planned for the network, are derived. Three groups of organizations will be considered: first, institutions in the European Union that are active in the field of cybersecurity. Furthermore, the other three European cybersecurity pilot projects, and, at last, the two existing efforts to organize CHECKSs, the CHECK-T and the Region of Murcia CHECK.

A further essential methodological aspect is the analysis of the existing European legal basis and of the European legislative proposals. This analysis is conducted by means of the legally recognized interpretation methods at European level. On the basis of the decisions on the structure and organization and their justification in these legal documents, guidelines for decisions to be taken within the framework of the Cybersecurity Network can be derived.

In addition, interviews were conducted by IRIT to determine cybersecurity stakeholder views on CHECKs. Methodical, for this purpose a presentation guideline for interviews was created and the stakeholder expectations were recorded with the Platform Canvas by Simone Cicero. Based on this groups and missions were identified and the interviews were evaluated and the statements summarized in an interaction matrix before presenting the results to the partners in a plenary.[2]

1.3 Document Structure

After this introduction, Chapter 2 examines the governance structures of other projects and organizations. Initially, "new" structures, which have not been considered in D2.1, will be analyzed. Subsequently, a re-evaluation of the models already examined in D2.1 is provided in order to find out whether any changes have occurred since the publication of D2.1. Furthermore, the governance models of the other three European pilot projects on cybersecurity are described.

Chapter 3 investigates the views and opinions of various stakeholders regarding CHECKs, which will serve as institutionalization of the cybersecurity Community.

Chapter 4 reports on the implementation process of CHECK-T and the Region of Murcia CHECK prototypes.

Chapter 5 presents the current status of the legislative process for Regulation Proposal 2018/0328 (COD) and discusses proposals for changes and further developments of the organizational and responsibility structure of the planned European cybersecurity network. In this context, both a possible integration of the European Cybersecurity Atlas into the network is addressed and the task assignments, organization and operation of the network institutions envisaged in the Regulation Proposal are examined.

[2] Cf. *A. Benzekri/P.H. Cros/A. Ferreira*, Progress report (I) on the implementation of the 1st CHECK-T, May 2020.

Furthermore, changes in the task and organizational structure of the Stakeholder Council, the Competence Centre and the Cybersecurity Community Establishment are also examined. The deliverable closes with final conclusions in Chapter 6.

2 Existing Governance Models

In the previous Deliverable D2.1 we have analysed the stakeholders' views on governance, collaboration and data sharing. Subsequently we have proceeded with looking into the existing governance models and their possible relevance as best practices for the future CCN. In order to understand the underlying processes and frameworks, we preceded the analysing of the existing governance structures with the overview of the theoretical background of various governance models.

In the current deliverable in the chapter below we shall recall the main provisions of the theoretical analysis. Further on we'll take another look at the governance structures that had been previously examined. Through this we hope to gain insight into any changes that might have occurred since the publication of the Deliverable 2.1. We'll then proceed to extend the analysis by looking into the new subset of the governance structures, which have been identified and selected by the project partners as those that may provide valuable insights into the best practices. The chapter will be concluded with the table presenting the short comparative overview of the best practices.

The classic literature on governance distinguished three canonical governance models: market, hierarchy and network. When it comes to cybersecurity governance, the invisible hand of the *market governance* is showing itself openly, if at times in a ham-fisted manner. Within this model, the economic exchange largely preserves the autonomy of the actors whose costs and benefits are self-assessed (for example, software patching cost versus cost of possible data loss). Price signals guide firms to develop and deliver security products and services where their utility is the highest. Long-term trust and a sense of obligation play only marginal roles here. Market mechanisms are the default form of governance, against which the overarching governing approach of national and EU bodies is articulated, pushing market dynamics towards public values that the market has not internalized.

The *hierarchical model*, with its vertical chain of command, clear task distribution and specialization, and the underlying skeleton of bureaucratic rules, is according to Powell[3] suited for high-speed mass production. It compensates with stability and predictability for the uncertainty of market mechanisms. The backside of stability is lack of flexibility that is necessary to react to the changes, let alone to anticipate them. Desire of predictability also generates tendencies toward compliance and 'box ticking' instead of proper risk analysis and secure products and services. Unfortunately, for reacting to rapidly shifting cybersecurity environment, high-speed flexibility is crucial. Hierarchical organizations also require a back-up of joint resource pool to safeguard for inevitable insufficient responses. Yet, the request to pool additional resources by organizations in charge of security is always vulnerable to threat inflations. The hardest challenge is that this model requires the commitment of a large group of actors, not just industries, consumers and civil society groups, but also representatives of various national and supranational political bodies, to align within a singular comprehensive hierarchical structure.

One of the ways to realize an ambition for "cyber moon shot" is to act within the framework of what started out as an institutional moon shot of sorts – and namely, within the structures of the EU. A unifying goal of international cybersecurity cooperation answers the modern challenges of policymaking, similarly to the way that the EU predecessors were the answer to the challenges of peacebuilding in post-war Europe. A common European goal is best realized in the *network governance model* as

[3] *Powell,* "Neither market nor hierarchy: Network Forms of organisation", 295-336.

described by Powell – "indebtedness and reliance over the long haul"[4]. A key feature of a successful network model is reciprocity, which fits well with the facilitated exchange of data and knowledge. An environment of trust and the feeling of being interdependent is essential. Pupillo also mentions that "trust-based relationships are essential to cybersecurity and resilience policy"[5], elaborating on the inherent contradictory market incentives (private costs versus shared benefits). In other words, leaving cybersecurity to the domain of market-based relationships will likely fail to create the conditions necessary for realizing the Commission's objectives, while hierarchical structures with their rigid division of authority, tasks and responsibilities lack the adaptivity and innovation that is needed from the cybersecurity research community, both in academia and industry. The network model has its own challenges, such as perceived loss of independence, unclear responsibilities, encapsulation. It is important to not disregard these challenges in designing the governance model that involves various European stakeholders. Like many domains that require intense and timely cooperation, network governance should avoid falling into the trap of enhancing its state of disequilibrium by producing short-term solutions and sacrificing the long-term stability for immediate political gains.[6] Collaborative governance, i.e., "attempts to bring all the relevant stakeholders together for face-to-face discussions during which policies are developed"[7] will help tackle the additional challenges, such as attracting talent and drafting the governance structure that would incorporate input from multiple stakeholders. The latter will ensure sustainable development of the governance model.

Below we shall proceed with analysing the existing governance structures that may be relevant for the goals and ambitions of realizing an NCCC. We have chosen to examine examples of the governance structures on different levels and scopes, from the regional to the European ones; while some of them are conducting their activities in the cybersecurity domain, the others, like CERN, are focusing on the different scientific field, or providing the platform for cooperation in diverse fields (IMEC). Nevertheless, we maintain that their manner of structuring their activities can be relevant for the purposes of our analysis, considering both the global relevance and the European orientation of the goals of this project. With the better understanding of the way these organizations operate, we can develop a viable model for the network uniting several organizations.

[4] Ibid.

[5] *L. Pupillo*, "EU Cybersecurity and the Paradox of Progress,", *CEPS Policy Insight* 6 (2018): 1-6.

[6] *D. Hodson / U. Puetter*, "The European Union in disequilibrium", 1-19.

[7] *M. Bevir, Governance: A very short introduction* (OUP Oxford, 2012).

2.1 Re-evaluation of governance models addressed in D2.1

It is safe to say that there is not a single organization that remained unaffected by the main challenges brought about by 2020, e.g., arising from the Covid19 pandemic situation or preparations for the Brexit finally coming into force in 2021. This is definitely true for the organizations in the field of cybersecurity. While no major readjustments in the governance structures have been observed, the work of the organizations below has acquired new urgency. With so many activities moving online, the amount of security threats has grown accordingly, thus accelerating the existing tendencies and highlighting the existing problems, while underlying the urgency to solve them. From the fraudulent online merchants to cyberbullying and disinformation, many of such incidents are still not dealt with timely. If anything can be ascertained with clarity, it is the fact that close cooperation between the EU countries in the area of cybersecurity is absolutely vital.

No major changes in the governance models of ENISA, ECSO and CERN could be observed. Their detailed description in D2.1[8] is thus still up to date. For an overview of their governance structures please see the figures below or the comparative overview of positive and negative aspects of evaluated governance structures in subchapter 2.4.

2.1.1 ENISA

Figure 1: Governance structure of ENISA[9]

[8] See D2.1 subchapters 3.1 – 3.3.

[9] Drawn by TUD, based on https://www.enisa.europa.eu/about-enisa/structure-organization (last accessed 16 December 2020).

2.1.2 ECSO

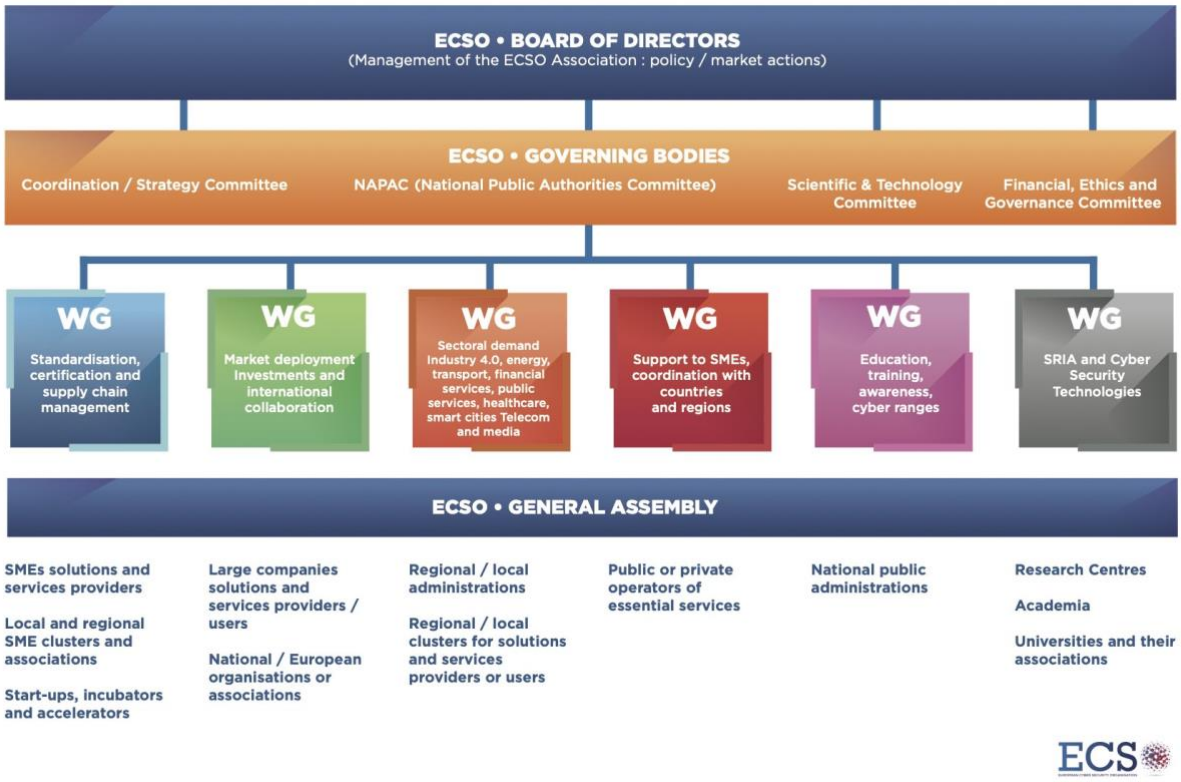

Figure 2: Governance structure of ECSO[10]

[10] ECSO webpage, https://ecs-org.eu/about (last accessed 16 December 2020).

2.1.3 CERN

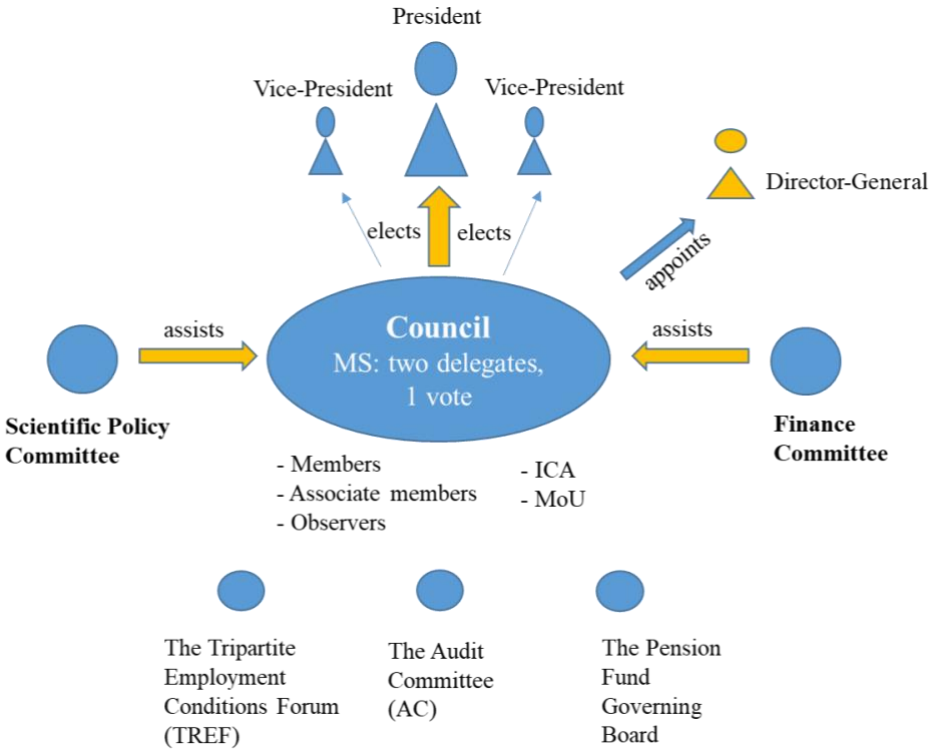

Figure 3: Governance structure of CERN

2.2 Additional Governance Structures

2.2.1 CEN/CENELEC

The European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC) are two private international non-profit organizations providing and promoting voluntary European standards for a wide range of stakeholders, such as businesses, consumers, public authorities and regulators, academia and research centres and other standard users in Europe[11]. They aim to exercise global influence, provide regional relevance, gain wider recognition, operate as a network of excellence, and foster innovation and growth[12].

Their mission is to develop, through transparent procedure, the high-quality standards for products and services. Such standards are to incorporate quality, safety, interoperability and accessibility requirements. They also aim to support European competitiveness and promote sustainable growth, as well as to promote the international harmonization of standards. To that end, the organizations have entered into a number of cooperation agreements with ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission).

2.2.1.1 Membership

The CEN-CENELEC Network includes more than 200.000 technical experts from industry, associations, public administrations, academia and societal organizations. The main stakeholders belong to business, industry and commerce; service providers; consumer, environmental and societal organisations; public authorities and regulators; and other public and private institutions.

There are a number of ways for the stakeholders to get involved[13]:

1. National membership. CEN and CENELEC have adopted a voluntary assessment system (self-assessment combined with peer assessment), based on a set of criteria for membership that have to be continuously fulfilled[14]. This ensures continuous sharing and adoption of good practices among the members.
2. European organizations, associations and federations representing diverse stakeholders, such as business, industry, consumers, environmental and societal organizations, etc.
3. Governmental bodies and other authorities, including the European Commission (EC) and the European Free Trade Association (EFTA).
4. The affiliates who are the national standards bodies/committees in countries that are cooperating with the European Union (either as potential candidates or in the framework of the European

[11] https://www.cencenelec.eu/aboutus/Mission/Pages/default.aspx (last accessed 16 December 2020).

[12] CEN and CENELEC's ambitions to 2020, Available at: ftp://ftp.cencenelec.eu/EN/AboutUs/Mission/CEN_CENELEC_Ambitions2020.pdf (last accessed 16 December 2020).

[13] https://www.cencenelec.eu/aboutus/Communities/Pages/default.aspx (last accessed 16 December 2020).

[14] Guide on the organizational structure and processes for the assessment of the membership criteria of CEN and CENELEC, Edition 4, 2018-01. Available at ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Guides/22_CENCLCGuide22-2018.pdf (last accessed 16 December 2020).

Neighbourhood Policy); special partnership status of standards bodies in other countries (and regions) outside Europe.

5. Relations and Memoranda of Understanding (MoU) with regions and countries outside the European Union and EFTA.
6. International cooperation with ISO (CEN) and IEC (CENELEC).

2.2.1.2 Governance Structure

CEN and CENELEC each have their own respective governance bodies: General Assembly, Administrative Board, Technical Board, Advisory Bodies and Technical Bodies. Next to their internal governance structures, they have created a joint structure to facilitate strategic cooperation: the CEN-CENELEC Presidential Committee. It consists of the two Presidents of CEN and CENELEC, the Presidents-Elect, the six Vice-Presidents and the Director General of CEN and CENELEC. The Presidential committee handles the membership issues, CEN-CENELEC-ETSI Joint Presidents' Group issues, as well as issues linked to European standardization strategy; conducts the selection process for the common CEN-CENELEC Director General and proposes a candidate for appointment by the CEN and CENELEC Administrative Boards; sets up CEN-CENELEC Joint Technical Committees; conducts Common Communications & Visibility Policy; identifies common elements in search of further synergies/optimization of resources; handles CEN-CENELEC contractual relations – services contracts[15]. The Presidential Committee may set up additional advisory bodies if necessary.

Another important structure is the CEN-CENELEC Management Centre (CCMC), tasked with executing the daily operations, exercising coordination and promotion of all CEN and CENELEC activities. Both CEN and CENELEC General Assemblies, the Administrative Boards and the Technical Boards provide tasks for CCMC. CCMC is also responsible for maintaining contact with the European Commission and the EFTA Secretariat. Its tasks are outlined in detail in "Roles and responsibilities of the National Standard Bodies (NSBs), the National Electrotechnical Committees (NECs) and the CEN-CENELEC Management Centre (CCMC)"[16]. They include a wide range of management and coordination activities for the CEN and CENELEC Focus, Coordination and Strategic Groups, support for NSBs and NCs during the full cycle of standardization work, support for the governing bodies, project management, and promoting the European standards model globally by acting as the focal point for a wide range of actors, including "transforming the information derived from those activities and partnerships into market access requirements (market intelligence), and establishing strategic alliances"[17].

The organizational chart for CCMC is presented below.

[15] CEN-CENELEC Internal Regulation part 1. Available at: https://boss.cen.eu/ref/IR1_E.pdf (last accessed 16 December 2020).

[16] ftp://ftp.cencenelec.eu/EN/AboutUs/Governance/RolesResponsibilities.pdf (last accessed 16 December 2020).

[17] Ibid, p.3.

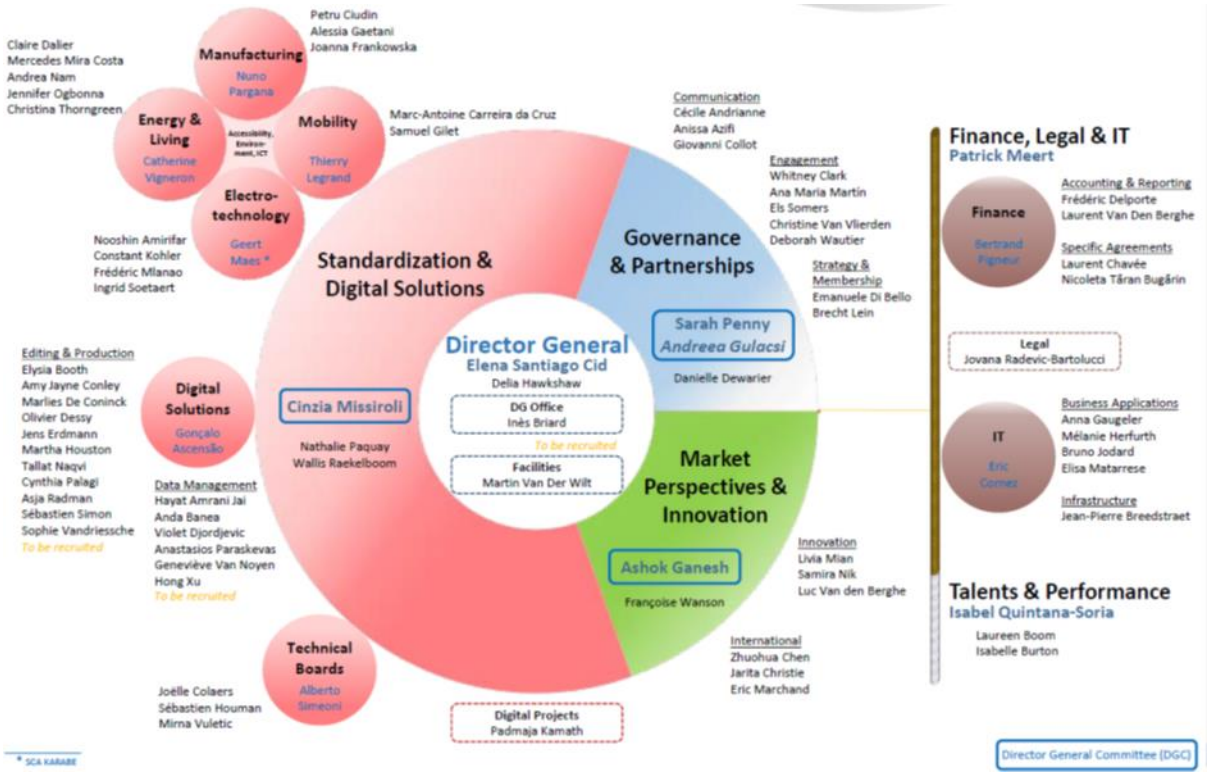

Figure 4: CEN-CENELEC Management Centre organisational chart[18]

2.2.2 ETSI

ETSI (European Telecommunications Standards Institute) is a leading standardization organization for Information and Communication Technology (ICT) standards. Their mission is "to provide platforms for interested parties to work together to produce standards for ICT systems and services that are used globally"[19]. The objective of "is to produce and perform the maintenance of the technical standards and other deliverables which are required by its members. As a recognized European Standards Organization, an important task shall be to produce and perform the maintenance of the technical standards which are necessary to achieve a large unified European market for telecommunications, ICT, other electronic communications networks and services and related areas. At the international level, the Institute shall aim to contribute to world-wide standardization in the fields described above"[20].

2.2.2.1 Membership

According to the ETSI Directives, there are several categories of members:

- **Administration:** An Administration is defined as the part of the public administration responsible for electronics communications and related areas in a country.

[18] https://www.cencenelec.eu/aboutus/MgtCentre/OrgChart/Documents/Org_Chart.pdf (last accessed 16 December 2020).

[19] https://www.etsi.org/about (last accessed 16 December 2020).

[20] ETSI Directives, version 41. February 2, 2020, Article 2. Available at: https://portal.etsi.org/directives/41_directives_feb_2020.pdf (last accessed 16 December 2020).

- **Other Governmental Body:** Another Governmental Body is defined as any other governmental organization or agency not covered by the Administration category above.
- **National Standards Organization:** A National Standards Organization is a standards organization whose function is to carry out at national level the activities related to standstill, public enquiry, establishment of the national position for the vote on draft European Standards as well as the transposition and withdrawal of national standards; and which is normally recognized by its Government as being authorized to make them available to the public at the national level.
- **Consultancy Company/Partnership:** A Consultancy Company/Partnership is defined as any legally established consultancy company/partnership concerned with telecommunications and related areas.
- **Manufacturer:** A Manufacturer is defined as a company having a substantial capacity to develop and/or produce and/or install and/or maintain products to be used in, or directly or indirectly connected to, an electronics communications network.
- An association or organization of such Manufacturers also falls within this category.
- **Network Operator:** A Network Operator is defined as an operator of an electronics communications network or part thereof.
- An association or organization of such Network Operators also falls within this category.
- **Research Body:** A Research Body is defined as any legally established research body concerned with electronics communications and related areas. A Public Research Body is a not-for-profit research organization whose main stakeholders are in the Public sector.
- **Service Provider:** A Service Provider is defined as a company or organization, making use of an electronics communications network or part thereof to provide a service or services on a commercial basis to third parties. An association or organization of such Service Providers also falls within this category.
- **University:** Any not-for-profit institution for higher education or postgraduate training having the legal power to award first and/or higher degrees.
- **User:** A User is an organization making use of services in the field of electronics communications and related areas, whose main interest in electronics communications standards is in that capacity.

The members can have a status of a full member (in a country within the geographical area of the European Conference of Postal and Telecommunications Administrations (CEPT), associate member (applicants not fully meeting the conditions for Full membership), or an observer (for those fulfilling the conditions for Full or Associate membership but choosing not to participate fully in the proceedings of the Institute. All members may participate in the meetings of the General Assembly, which established the condition for obtaining membership. Application for membership may be approved by consensus among the members via online poll, which is organized four times per year, or at the next ordinary General Assembly meeting if the consensus cannot be reached. Membership may be ended by dissolution, abolition, resignation, or expulsion.

2.2.2.2 Governance Structure

The Institute shall comprise a General Assembly, a Board, a Technical Organization, Special Committees, Industry Specification Groups, Coordination Groups and a Secretariat headed by a Director-General.[21] General Assembly, which includes all members, is the highest authority. It meets twice a year, with the representatives of the European Commission (EC) and the European Free Trade Association (EFTA) attending in advisory role with no right to vote. The Board is responsible for the following decisions[22]:

- Determining overall policy and strategy
- Agreeing budgets
- Dealing with membership issues
- Appointing the members of the ETSI Board
- Appointing the Director-General
- Appointing the Finance Committee members
- Endorsing external agreements
- Approving changes to our Statutes and Rules of Procedure

The General Assembly delegates daily functioning and specific activities to the Board. Full and Associate members nominate the candidates for the Board, with representatives of Full members exclusively being capable of becoming Board members. The General Assembly also appoints the Director-General to hold chief executive authority and to perform a number of tasks, such as[23] financial accounting to General Assembly, communicating regularly to the Chairmen of the General Assembly and the Board important information within their areas of responsibility, submitting progress reports to the General Assembly, the practical organization of the meetings and work of the General Assembly, the Board, and the Special Committees, as well as establishing relationships with external bodies and the promotion of the work of ETSI.

The Technical Organization is responsible for the preparation of standards and other relevant deliverables of ETSI. An Industry Specification Group is an activity organized around a set of ETSI Work Items addressing a specific technology area. Special Committees are established by the General Assembly for carrying out certain tasks. A Coordination Group is a structure established in case of need to coordinate with external bodies, where such coordination cannot be accommodated within one of the above-mentioned structures, or within the existing types of partnership engagements.

[21] ETSI Directives, version 41. February 2, 2020. Available at: https://portal.etsi.org/directives/41_directives_feb_2020.pdf (last accessed 16 December 2020).

[22] https://www.etsi.org/about/our-structure (last accessed 16 December 2020).

[23] ETSI Directives, version 41. February 2, 2020. Available at: https://portal.etsi.org/directives/41_directives_feb_2020.pdf (last accessed 16 December 2020).

2.2.3 EIT International

The European Institute of Innovation and Technology (EIT) is an independent EU body. Its goal is to strengthen the EU as innovation environment by increasing Europe's innovation capacities through creating favourable conditions for the entrepreneurial talent and new ideas. It operates by "integrating business, education and research to find solutions to pressing global challenges".[24] One of such challenges that has been specifically outlined is the European fragmented research landscape. According to its website, "The EIT brings together leading organisations from business, education and research, the so-called "knowledge triangle", to form dynamic cross-border partnerships - EIT Innovation Communities".[25]

The EIT was established[26] in 2008, and subsequently amended[27]. The amendments introduced a number of changes, such as adding the following point (k): "establish a Stakeholder Forum to inform about the activities of the EIT, its experiences, best practices and contribution to Union innovation, research and education policies and objectives and to allow stakeholders to express their views".

2.2.3.1 Membership

The EIT creates the KICs (Knowledge and Innovation Communities), which become its operating organs and bring together the members of the above-mentioned "knowledge triangles". Each KIC is a separate legal entity run by a CEO, with their own governance and business plan.

Their activities cover the full innovation chain: training and education programmes, reinforcing the journey from research to the market, innovation projects, as well as business incubators and accelerators. The EIT plays guiding and strategic role, with KICs enjoying operational autonomy.

There are currently eight Innovation Communities[28]:

- EIT Climate-KIC: Drivers of climate innovation in Europe and beyond;
- EIT Digital: For a strong, digital Europe;
- EIT Food: EIT Food connects businesses, research centres, universities and consumers;
- EIT Health: Together for healthy lives in Europe;
- EIT InnoEnergy: Pioneering change in sustainable energy;
- EIT Manufacturing: Strengthening and increasing the competiveness of Europe's manufacturing;
- EIT Raw Materials: Developing raw materials into a major strength for Europe;
- EIT Urban Mobility: Smart, green and integrated transport.

[24] https://eit.europa.eu/who-we-are/eit-glance (last accessed 16 December 2020).

[25] https://eit.europa.eu/who-we-are/eit-glance/mission (last accessed 16 December 2020).

[26] REGULATION (EC) No 294/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:097:0001:0012:EN:PDF (last accessed 16 December 2020).

[27] by the Regulation (EU) No 1292/2013 in 2013. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:347:0174:0184:EN:PDF (last accessed 16 December 2020).

[28] https://eit.europa.eu/our-communities/eit-innovation-communities (last accessed 16 December 2020).

The relationship between EIT and KICs are regulated by the individual Framework Partnership Agreements and Specific Grant Agreements. The Framework Partnership Agreements are entered into for the purpose of the long-term cooperation and contains the general and specific terms and conditions, rights and obligations applicable to the specific grants that may be awarded by the EIT for actions under the Framework Partnership Agreement. The Governing Board has got the power to extend the duration of partnership with a KIC, as well as reduce of withdraw its financial support for the KIC in case of inadequate results[29].

Each Innovation Community is expected to conform to the following principles[30]:

- long-term strategy
- a diverse and excellent partnership
- a focus on people and talent
- top quality governance and management
- a legal entity suited to its needs
- an integrated network of EIT Innovation Hubs
- a sustainable business model and financial plan
- a policy for intellectual property
- adopted the EIT Community brand
- a communications plan supporting the EIT brand
- a plan for dissemination
- a plan to unlock the untapped innovation potential across Europe through the EIT RIS
- an eye for synergies.

In order to take targeted action to accomplish its goals, EIT makes use of the concept of **Innovation Hubs**, which form the skeleton of the Innovation Community. Each Innovation Community enjoys autonomous management, legal structure and business plan, designed with the EIT's, as well as measurable objectives. According to the EIT website, "*Each Innovation Community has regional Innovation Hubs with partners in close proximity, which is essential to facilitate interaction among members of the regional community. Innovation Hubs are the focal point for the Innovation Communities' activity within these areas of focus. Innovation Hubs build on the existing labs, offices or campuses of some of the Innovation Community's core partners, which serve as clusters for a particular*

[29] Article 7b, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:347:0174:0184:EN:PDF (last accessed 16 December 2020).

[30] https://eit.europa.eu/our-communities/eit-innovation-communities/success (last accessed 16 December 2020).

region, discipline or task. There they bring together people and teams from across the knowledge triangle for ideation, projects and other initiatives".[31]

Several models of Innovation Hubs have been designed, and Innovation Communities can select a certain model in accordance with its strategic needs, be those specialized or more general. Each hub is supposed to implement the principles of the good governance, including the balance of representation within the knowledge triangle (research, education and innovation), transparent decision-making process and separation of powers.

The Innovation Hubs perform the following key functions[32]:

- Connectivity: a physical space for interaction within the local ecosystem. These spaces should attract a wide range of actors from within each Innovation Community and beyond;
- Knowledge management: points for knowledge exchange (within, between and across Innovation Hubs);
- Activity management.

2.2.3.2 Governance Structure

The EIT Governing Board is the main governing body, entrusted with the strategic leadership of the Institute and the overall direction of the operational activities implemented by the EIT Headquarters. It is independent and autonomous in its decision-making and is responsible for the selection, evaluation and support of the EIT Innovation Communities (Knowledge and Innovation Communities).

The Governing Board is tasked with making strategic decisions: adopting the EIT draft Strategic Innovation Agenda (SIA), triennial rolling work programme, budget and other financial decisions, as well as selecting, monitoring and evaluating the activities of the KICs, selecting the Executive Committee and the Director, and promote EIT.

The Governing Board consists of twelve members with prominent expertise from higher education, research, business and innovation that are appointed by the European Commission; these members have a four-year non-renewable term of office. The Governing Board members are expected to act in the interests of the EIT, keeping in mind its goals and mission with the eye for identity, autonomy and coherence, in an independent and transparent way. The Governing Board appoints the Director, who is tasked with the administrative and financial management, for a term of office of four years, which can be extended once. The Executive Committee consists of the EIT Governing Board Chairperson and three members of the EIT Governing Board. Its task is supporting the activities of the Governing Board by overseeing the implementation of its strategic decisions or acting when being delegated to perform specific tasks. Additionally, in accordance with the EIT Regulation, the European Commission appoints an Observer who participates in the meetings of the Governing Board and of the Executive Committee.

[31] https://eit.europa.eu/our-communities/eit-innovation-communities (last accessed 16 December 2020).

[32] https://eit.europa.eu/our-communities/eit-innovation-communities/innovation-hubs (last accessed 16 December 2020).

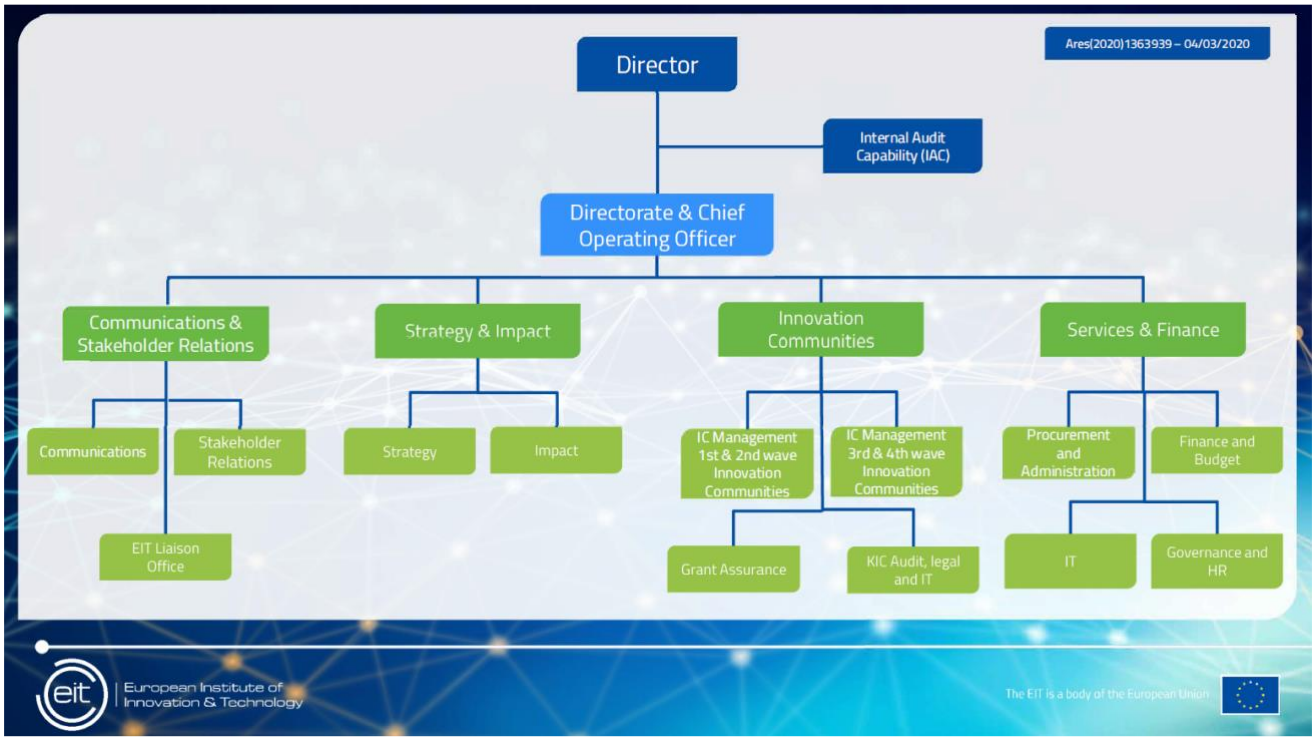

Figure 5: EIT organisational chart[33]

2.2.4 IMEC

IMEC is an R&D and innovation hub that demonstrates the ambition to become one of the world-leading research centres in nano-electronics and digital technologies. IMEC as a non-profit organization was founded in Flanders, Belgium, and subsequently extended its functioning and reach internationally. The focus of IMEC is to conduct research and facilitate collaboration between companies, start-ups and academia on the international level, while safeguarding the regional interests of Flanders and paying attention to the "triple P" bottom line: people, planet, profit. In order to ensure that the above-mentioned goals and principles can be realized, IMEC has come up with the Good Governance Charter, available in English on the international website of IMEC. The Charter outlines the mission, the governance principles, and the organizational structure. It contains references to and summary of certain provisions of the Articles of Association, as well as hyperlinks to the latest composition of diverse boards, remuneration documents, and other similar documents. In addition, it states the commitment of the management team to be "honourable and dedicated"[34].

The main mission of IMEC as organization is "the conducting of cross-border strategic research in the fields of nanotechnology and digital technology, in order to develop the building blocks that contribute towards a better quality of life within a sustainable society"[35]. The chapter also mentions dissemination

[33] https://eit.europa.eu/sites/default/files/eit_organisational_chart_february_2020.pdf (last accessed 16 December 2020).

[34] The Good Governance Charter, Chapter 2: Basic Principles of Good Governance, p.5.

[35] The Good Governance Charter, Chapter 1: Mission and Vision on IMEC, p.4.

of scientific knowledge through training and support, as well as expansion of an IMEC group internationally.

The Charter sets to outline the governance foundation of IMEC as an internationally oriented organization that, nonetheless, clearly has got regional (Flanders) interests at its core. This double mission is integrated into the governance structure and explicitly stated multiple times throughout the whole text of the Charter, starting with Chapter 1: "While keeping in mind the fulfilment of its mission, IMEC is driven by its ambition to be and to remain an international centre of excellence in general, and to contribute towards the enrichment of the industrial fabric of Flanders, in particular".[36] Additionally, the Charter states the commitment to the clear and transparent governance structure, with respect of the rights of the members, and the "honourable and dedicated" directors and management team in charge of the process. Ethical Code of Conduct and Ethics committee assist the team in this task.

2.2.4.1 Membership

The maximum number of members is unlimited, with the minimum number being set at fifteen; the number of members may be increased according to the three-quarters majority decision of the General Assembly, with the additional members nominated by two members of the corresponding sector (see below). The membership period of six years may be renewed for the unlimited number of times. The membership can be terminated at any time by the members themselves - for example, members are expected to step down if they are unable to adequately represent the body that had delegated them - or by the majority decision of the general assembly in case of violating of the Statute[37].

The membership structure is intended to represent a balance between the different sectors:

- member-representatives of the Flemish universities;
- member-representatives of Flemish industry;
- member-representatives of the Flemish trade unions;
- member-representatives of the Flemish universities of (industrial) applied sciences;
- member-representatives of the Flemish Government.

IMEC is an organization that explicitly aims to facilitate collaboration for different stakeholders with diverse needs. One of the examples is the "imec.icon" research program, where "over a period of typically two years, multi-disciplinary research teams of scientists, industry partners and/or social profit organizations work together to develop digital solutions that find their way into the market offer of the participating partners"[38].

Generally, IMEC offers three forms of collaboration: *collaborative, bilateral, government-funded*[39].

[36] The Good Governance Charter, Chapter 1: Mission and Vision on IMEC, p.

[37] https://drupal.imec-int.com/sites/default/files/inline-files/1-Gecoordineerde-statuten-IMEC-vzw-na-BAV-21092016.pdf (last accessed 16 December 2020).

[38] https://www.imec-int.com/en/icon (last accessed 16 December 2020).

[39] https://www.imec-int.com/en/what-we-offer/research (last accessed 16 December 2020).

- **Collaborative form**: pre-competitive collaboration for the joint early development needs, which includes sharing expertise and research among partners across the value chain in order to lower costs and reduce risks.
- **Bilateral:** a cooperation form involving specific expertise or infrastructure;
- **Government-funded:** contributing to the EU research and innovation programs and providing research funding for Flemish companies.

2.2.4.2 Governance Structure

The IMEC Group is controlled by the non-profit foundation IMEC international, which acts as a corporate centre for the entities that are part of the Group. It provides guidelines on business development and human resources, while respecting the autonomy and governance of each of the above-mentioned entities. The two main organs are the General Assembly and the Board of Directors, the latter being the highest-ranking management body that makes decisions on the general policy.

According to the Chapter 1, "[…] the Board of Directors of IMEC International has taken cognizance of the Charter and agreed to comply with the principles. It is also provided for that the directors of IMEC International will be appointed by the Board of Directors of IMEC with a view to ensuring transparency and embedding in Flanders". Thus, the above-mentioned principle of safeguarding regional interests has found integration in the governance structure.

The General Assembly of the members is held annually. According to the Chapter 3, it possesses the following powers:[40]

1. Amendment of the Articles of Association upon the request of the Board of Directors, in accordance with the quorum and majority requirements relating to decisions of the Board of Directors set out in these Articles of Association

2. Appointment and dismissal of members of the Board of Directors and, if necessary, determining their remuneration

3. Appointment and dismissal of the supervisory director and, if necessary, determining his/her remuneration

4. Discharging the directors and the supervisory director of liability

5. Approval of budgets and accounts

6. Exclusion and acceptance of members

7. Pronouncing the voluntary dissolution of the Association

8. Converting the Association into a social enterprise under Belgian law [vennootschap met een sociaal oogmerk]

9. Exercising all other powers and resolutions that are reserved for it by virtue of the V&S Act or by the Articles of Association.

[40] The Good Governance Charter, Chapter 3: Application Of Good Governance In IMEC, p.7.

The Board of Directors is composed of at least twelve directors, who may or may not be members of the Association. Four of them must be nominated by the representatives of the Flemish universities and include at least one representative of the academic staff; at least seven directors must be independent and "elected from among candidates with special expertise that supports the Association's objectives" (The Good Governance Charter, Chapter 3: Application Of Good Governance In IMEC, p.8). "A Director shall be elected from among the candidates nominated by the Flemish Minister responsible for scientific research and technological innovation policy" (p.9), with the General Assembly initiating the appropriate process if the Minister fails to do so within a certain time period.

The Board of Directors may delegate the powers for specific decision-making to an authorized representative. For the more specific tasks, there is also a number of additional sub- structures, such as Audit Committee and Nomination and Remuneration Committee; dedicated ad hoc committees can be set up according to the needs that may arise, designated by the Board of Directors. Such committees may involve external experts; they perform advisory and assistant role.

The governance structure foresees the function of a CEO, who may be delegated the day-to-day management by The Board of Directors, along with several additional powers. The function of CEO can be performed by one of the directors, or by a third party; the CEO is appointed by the Board of Directors upon the recommendation of the Nomination and Remuneration Committee. The CEO "shall arrange to be assisted" by and will become the Chair of the Executive Board (The Good Governance Charter, Chapter 5: Executive management, p. 14), comprised of the individuals with the management roles in IMEC that are, upon being nominated by the CEO, appointed by the Board of Directors. As long as IMEC remains a part of IMEC Group, the Executive Board of IMEC International will be composed of the same individuals as the Executive Board of IMEC (while the directors of IMEC International will be appointed by the Board of Directors of IMEC).

A number of Advisory Boards are required by law perform an active role in the functioning of IMEC. Next to those, the organisation has created the following bodies to aid its functioning:

- The Scientific Advisory Board (composed of at least three experts in the field of nanotechnology and at least three experts in the field of digital technology);
- The Universities Coordination Committee (composed of the CEO of the Association who acts as its Chair, two representatives of KU Leuven, two representatives of Ghent University, two representatives of VU Brussels, one representative of Hasselt University, and one representative of the University of Antwerp);
- The Flemish Industry Advisory Board (composed of ten members who are not representatives of the Executive Board, appointed by the Board of Directors upon nomination (citing reasons) by the Flemish Industry Advisory Board itself and the Association's Executive Board. Six of the members of the Flemish Industry Advisory Board shall be required to have particular expertise in the field of digital technology. The remaining four members must represent Flemish companies or foreign companies that have a branch with an R&D department in Flanders).

2.2.5 GEANT/NRENs

GÉANT is the organization leading collaboration on network infrastructure and services for the purposes of research and education. Its mission is contributing to Europe's economic growth and competitiveness by supporting educators, researchers and other partners in collaboration, liaising with the other stakeholders including the EU, knowledge-sharing and policy debates. GÉANT sets up and operates large-scale, advanced high-speed networks, organises training and networking events (such as

TNC, Europe's largest networking conference for research and education) and providing expertise in project-management and related fields.

2.2.5.1 Membership

The Articles of association distinguish between the national members (one national member per sovereign state) and representative members (a legal entity representing two or more sovereign states, which is not focused on industrial and commercial activities). GÉANT consists of 36 National Members, which are European national research and education network (NREN) organisations, and one Representative Member - NORDUnet - which participates on behalf of five Nordic NRENs. Potential members complete a pro-forma letter that includes the names of appointed representatives or observers and are admitted by the GA.[41] Additionally, entities active in the field of research and education can be admitted, if it is in the special interest of GÉANT to do so. Members may choose to contribute to the TaskForces and Special Interest Groups that are active in spreading knowledge and best practice throughout the community.

2.2.5.2 Cooperation with NREN

National research and education network (NREN) organisations are specialised internet service providers dedicated to supporting the needs of the research and education communities within their own country[42]. The primary focus of NRENs is to provide universities and research institutes with high-quality network connectivity and related services by connecting campuses and institutions to each other, and to the rest of the internet. NRENs in the GÉANT region provide services to more than 80% of all university-level students, as well as to researchers, educators and other campus staff and visitors. Many NRENs go beyond this by also connecting schools, institutes of further education, libraries, museums, hospitals and other public service institutions.

GÉANT has worked with the organisations that are part of this network to build an overview of the services and facilities available in each country.[43] Each NREN offers a range of services tailored to the needs of its national customers in research and education, which might be confusing to the international customers. In order to reduce that confusion and facilitate cross-country research and education collaboration, GÉANT has created an easy-to-use tool providing information about NREN service portfolios. This NREN service portfolio is an extension of the online GÉANT Compendium and presents an overview of different services and membership status of NRENs[44]

2.2.5.3 Governance Structure

The highest governing body is the General Assembly. Representatives of member organisations meet at least twice per year. The GA adopts strategic plans, appoints the board members, makes financial decisions, and amends the articles of associations. The GA is assisted by the Advisory Council, and, if necessary, by the committees and working groups. The GA elects members to the Board of Directors,

[41] https://www.geant.org/About/Joining_GEANT/Pages/Become_a_member.aspx (last accessed 16 December 2020).

[42] https://www.geant.org/About/NRENs/Pages/The_case_for_NRENs.aspx (last accessed 16 December 2020).

[43] https://www.geant.org/About/NRENs/Pages/NREN_service_portfolio.aspx (last accessed 16 December 2020).

[44] https://compendiumdatabase.geant.org/reports/nrens_services (last accessed 16 December 2020).

which carries out representative, managerial and administrative duties; the Board may consist of seven to nine persons, of which at least six shall be nominated by the national or representative members, and the chair is appointed by the GA.

While the representatives of all members are invited to attend the general meeting, the representatives of the entities that are considered to be different from non-profit entities can be excluded from attending, if the chair considers such attendance to be disadvantageous to the business of GÉANT.[45] The number of votes for any national or representative member is determined in accordance with the economic weight/financial commitment.

The Executive Team is a coordinated effort between the two GÉANT offices in Cambridge and Amsterdam. This team exercises collective leadership of all GÉANT activities, with each member having specific areas of lead responsibility.[46] Day-to-day operations are carried under the direction of the CEO and managers.

2.2.6 IT Planning Council

In the course of the Federal Reform II in 2009, the German Basic Law was amended and, thereby, information technology and the ongoing digitization of the government and public administration have become issues with constitutional relevance. This goes back to the insight, that there is a need for a high-quality digital infrastructure in the public sector in order to avoid functional as well as financial disadvantages due to a lacking interactive connectivity. Given the federal form of government in Germany it takes a firm legal and fact-based cooperation structure to ensure the sustainability of decisions and the successful digitization of the public sector.

The IT Planning Council is the central body for the Federal and State IT coordination and cooperation in Germany.[47] The Council is legally based on the State Treaty on IT, which implements constitutional rules. With the State Treaty on IT coming into force on 1 April 2010 the IT Planning Council replaced two former bodies, the working committee of state secretaries responsible for federal and state e-government (St-Runde Deutschland Online) and the federal and state Cooperation Committee for Automatic Data Processing (KoopA ADV), and became their legal successor.[48]

The legally defined tasks of the IT Planning Council are

- Coordination of the cooperation between the Federal and State Governments on IT issues;
- Adoption of IT interoperability and IT security standards;
- Management of e-government projects;

[45] Article 14, “Deed of Amendment of the Articles of Association”, available at https://www.geant.org/About/Our_organisation/PublishingImages/Pages/Formalities/Certified%20copy%20of%20Deed%20of%20Amendment%20of%20the%20Articles%20of%20Association.pdf (last accessed 16 December 2020).

[46] https://www.geant.org/About/Our_organisation/Pages/Executive-Team.aspx (last accessed 16 December 2020).

[47] A survey on the functions of the IT Planning Council has been conducted by *E.Richter/A.Schmehl/I.Spiecker gen. Döhmann*, Die Funktionen des IT-Planungsrats bei normgebenden Verfahren auf dem Gebiet von IT und E-Government, 2013 (available at https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/11_Sitzung/OptIK.pdf?__blob=publicationFile&v=2, last accessed 27. November 2020).

[48] § 7 III State Treaty on IT.

– Planning and development of the Federation's core network.[49]

2.2.6.1 Membership

The Federal Government Commissioner for Information Technology and one IT responsible representative (usually state secretaries) from each of the 16 Federal States are the members of the IT Planning Council board.[50] Additionally, the Federal Commissioner for Data Protection and Freedom of Information and three representatives of local authorities appointed by the national associations of local authorities[51] may attend the meetings, but with an advisory role only.[52] As far as a Council's decision affects the responsibility of a certain Ministerial Conference its members have to be involved, too.[53]

2.2.6.2 Governance Structure

The organizational structure consists of permanent structures as well as temporary cooperation groups. The board of the IT Planning Council, the FITKO office (Office for Federal IT Cooperation) of the Council and the KoSIT office (Coordination Office for IT Standards) are permanent structures.

The board is the main decision body of the IT Planning Council. It meets three times a year.[54] The chair of the IT Planning Council board is rotating annually between the federal and the state members,[55] with the states being in charge in alphabetical order[56].

On request of the Federation or of three States the board can make decisions in form of resolutions or recommendations, which have to be published in the Electronic Federal Gazette.[57] Resolutions need the approval of the Federation and a majority of 11 States, representing at least 2/3 of the budget.[58] Recommendations can be adopted by simple majority of the attendant board members.[59] In case the IT Planning Council adopts a resolution on IT interoperability or IT security standards, these resolutions are binding for both federal and state governments, who also have to meet the implementation deadline the IT Planning Council has set for that standard.[60] Preferably, market standards are the source for the Council's standard setting.[61] On request of the Federation or three States the need for such resolution as

[49] § 1 I 1 State Treaty on IT.

[50] § 1 II 1 State Treaty on IT.

[51] I.e. the Association of German Counties, the Association of German Cities and the German Association of Towns and Municipalities.

[52] § 1 II 3 State Treaty on IT.

[53] § 1 IV State Treaty on IT.

[54] § 1 IV State Treaty on IT requires at least two meetings per year. § 2 of The Rules of Procedure of the IT Planning Council suggest two to four meetings per year and by request of the Federation or three States additional meetings have to be set up.

[55] § 1 III 1 State Treaty on IT.

[56] § 1 III 2 State Treaty on IT i.c.w. § 1 II 1 Procedural Rules of the IT Planning Council.

[57] § 1 V State Treaty on IT.

[58] § 1 VII 1 State Treaty on IT.

[59] § 1 VII 2 State Treaty on IT.

[60] § 3 II 2 State Treaty on IT.

[61] § 3 I 2 State Treaty on IT.

well as the technical quality and consistency of the standard have to be assessed by an independent institution.[62] The IT Planning Council has to consider the outcome of the assessment, however, is not bound by it their further decisions.[63]

The FITKO office has only recently been added to the governance structure. While initially located in Berlin at the Federal Ministry of Interior, the office of the IT Planning Council was reorganized and moved to Frankfurt in 2020. Background is an amendment to the State Treaty on IT in 2019,[64] which introduced the establishment of a joint public-law institution called FITKO.[65] The new office receives technical instructions from the chair of the board and serves as the main organizational support entity to foster the implementation of the Council's resolutions and recommendations by providing and bundling the necessary resources and competences in one institution. The Federation and the States each provide half of the funding.[66] The FITKO president is appointed by the IT Planning Council for a term not exceeding 5 years, which can be renewed.[67] The president manages and represents the institution and is supervised by a governing board, that consists of the IT Planning Council members.[68]

KoSIT is legally based on a resolution of the IT Planning Council. It consists of an Advisory Board and the Coordination Office itself. KoSIT coordinates the development and operation of IT standards for data sharing within the public administration, assists the adoption of IT interoperability and IT security standards and the management of joint federal and state-level e-government projects.[69]

Due to the variety and technical complexity of the subject-matters the IT Planning Council is dealing with, it is sometimes necessary to set up temporary cooperation groups[70] for the deeper investigation and development of specific issues. The Council members are free to participate in the cooperation groups. Depending on the thematic focus it is also possible to include representatives from industry and academia in the work of a coordination group. Currently there is only one active group, the Strategy Cooperation Group, which assists the IT Planning Council. In the past three coordination groups successfully completed their work: the EU Cooperation Group, the Cooperation Group on EU Interoperability and the Cooperation Group on Information Security Guidelines.

[62] § 3 III 1 State Treaty on IT.

[63] § 3 III 3 State Treaty on IT.

[64] Electronic Federal Gazette, http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl119s1126.pdf (last accessed 15 September 2020.)

[65] § 5 I Amendment to the State Treaty on IT.

[66] § 6 I Amendment to the State Treaty on IT.

[67] § 7 III Amendment to the State Treaty on IT.

[68] §7 I, II 1 Amendment to the State Treaty on IT.

[69] IT Planning Council webpage, https://www.it-planungsrat.de/EN/it-planing-council/Organisation/KoSIT/KoSIT_node.html and KoSIT webpage, https://www.xoev.de (both last accessed 15 September 2020).

[70] IT Planning Council webpage, https://www.it-planungsrat.de/EN/it-planing-council/Organisation/Kooperationsgruppen/Kooperationsgruppen_node.html (last accessed 20 October 2020).

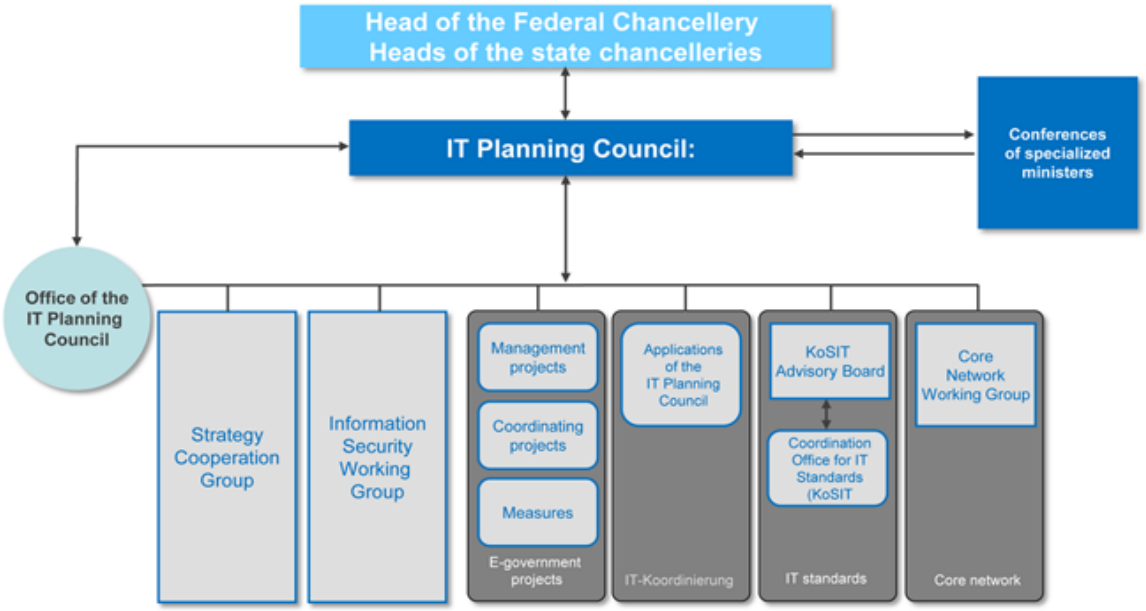

Figure 6: Organisation and structure of the IT Planning Council[71]

[71] IT Planning Council webpage, https://www.it-planungsrat.de/EN/it-planing-council/Organisation/Organization_node.html (last accessed 15 September 2020).

2.3 Governance models of other pilots

Along with CyberSec4Europe, there are three other pilots tackling the issue of governance of cybersecurity Centre, Network and the Community. The diversity of approaches is supposed to ensure that the final shape of the structure will combine the best practices and insights. The Convergence event on December 9-11, 2020 has brought together all the approaches in the Governance Panel.

2.3.1 ECHO

ECHO's approach can be roughly described as top-down, with different levels of membership. ECHO's vision of the network is transformation of the pilot's assets into a network, which consists of several functioning focus groups and regional chapters (at least one per Member State). The Central Hub would be interfacing with the European Cybersecurity Competence Centre. At the moment of writing, ECHO was working on the design of the key processes and organizational structures for ECHO Group and ECHO Network, as well as on the transition from ECHO pilot project to a sustainable Collaborative Network Organization (CNO) in cybersecurity.

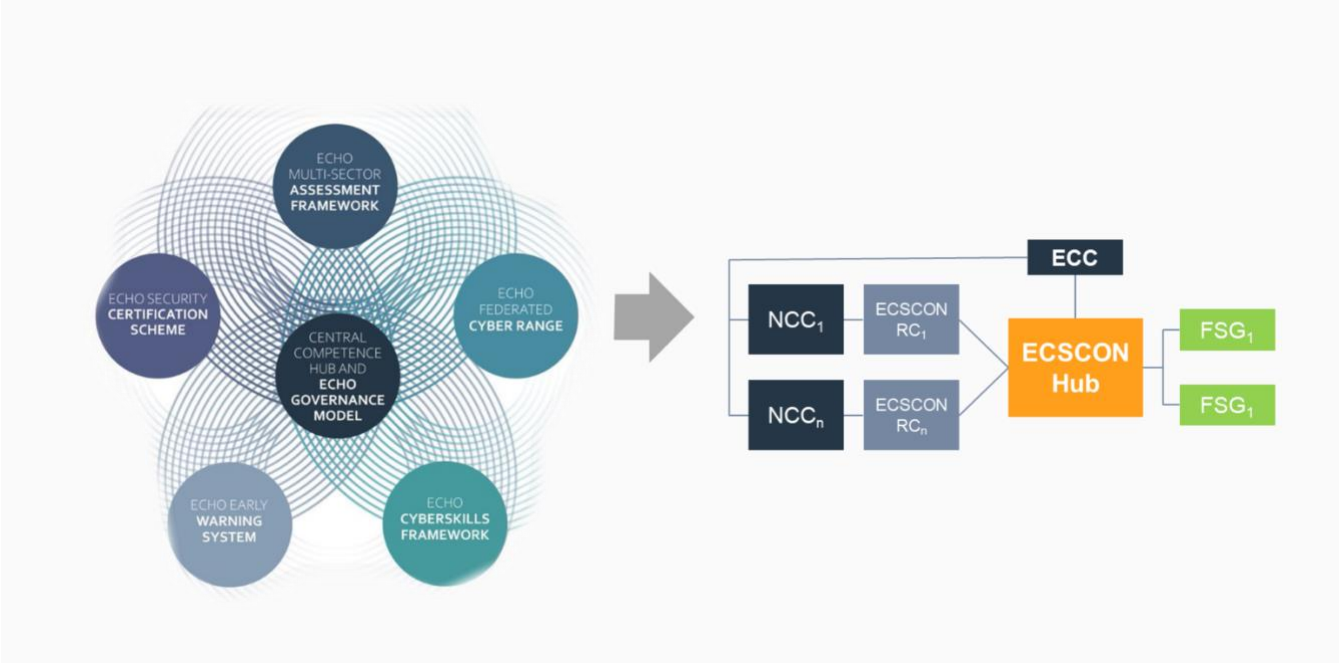

Figure 7: Governance Topic in ECHO[72]

Through the portfolio of the demonstration cases, accompanied by the audit and evaluation process, ECHO is working on identifying the best practices for decision-making, such as decision points and types of decisions to be taken.[73]

2.3.2 CONCORDIA

CONCORDIA is building their approach around the needs of the cybersecurity communities and mediating between them. It is focussed on realizing the existing potential for establishing connections

[72] Velizar Shalamanov, "ECHO Governance Model. Where to be after 31 January 2023? Where to arrive in 2027?", Presentation at the Convergence virtual event, December 11, 2020.

[73] Ibid.

and collaborations, acknowledging challenges, and ensuring sustainable partnership. According to CONCORDIA, it is important to ensure balanced representation of all stakeholders, rather than allow one of them to monopolize the vision on cybersecurity.

Figure 8: Contextual, impact-based symbiosis of four intertwined main domains (as mentioned in the proposed Regulation)[74]

As a part of CONCORDIA's approach to multi-stakeholder governance, it identifies the following groups: The User, Customers Who Are Willing To Pay, Suppliers & Value Ecosystem, Physical, Cyber-Physical & Cyber Ecosystems and Society, Malicious Actors, Technology & Data Titans, Investors & Financers, Policy Makers, Standardisation Development Organisations & Markets, Authorities, and Law Enforcement.[75]

2.3.3 SPARTA

SPARTA is focussed on research and "radical innovation with targeted objectives" as the cornerstones of the European strategic autonomy. These goals are realized through the following instruments[76]:

- Roadmap
- Partnership
- Technical Programs
- Governance

[74] Arthur van der Wees, "From Communities to Hybrid Interconnected Ecosystem of Ecosystems", Presentation at the Convergence virtual event, December 11, 2020.

[75] Ibid.

[76] Thibaud Antignac, "Governance perspectives for strengthening European cybersecurity capacities", Presentation at the Convergence virtual event, December 11, 2020.

As a part of the governance-related activities, SPARTA have conducted an assessment of their governance structure in the initial stage of the project. The have concluded that, while there was "strong utilization" of the Roadmap committee, the other governance bodies (notably the Certification Task Force, the Ethics Board, and the Advisory Committee) were less prominent, which can be explained by the early stage of the research programs. Instead of micro-managing, sufficient place was given to the initiative of the leaders for the technical programs, the work packages and tasks, which was evaluated as a successful strategy. However, the centralized way of governing these activities will likely play a prominent role in the future. The efforts to establish the organizational framework for governance have been evaluated as successful.[77]

[77] Dirk Kuhlmann (ed), "D1.2. Lessons learned from internally assessing a CCN pilot", https://www.sparta.eu/assets/deliverables/SPARTA-D1.2-Lessons-learned-from-internally-assessing-a-CCN-pilot-PU-M12.pdf (last accessed 16 December 2020).

2.4 Comparative overview of analyzed governance approaches

The table below gives a concise overview of all existing governance structures that have been evaluated for D2.1 and D2.3,[78] showing the positive aspects and aspects to be aware of:

Governance Example	Positive aspects to be considered	Aspects to be aware of
CEN-CENELEC	CEN-CENELEC demonstrates a good example of collaboration between the two structures, which combined 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.	As a side effect of the diversification of tasks at the different levels, combined with the ambition and magnitude of the goals, the overall governance structure is rather complex.
ETSI	Agile structure, suitable for diverse types of the tasks.	The organization is geared towards the technical kind of cooperation, which differs from the strategic cooperation on all levels in accordance with the tasks of CyberSec4Europe.
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.	While the Governing Board includes representatives of the diverse sectors, and the governance of the Innovation Hubs is supposed to provide for the balance of diverse stakeholders, the overall approach is market oriented. This approach is necessary to increasing the European competitiveness, but it might prove unsuitable for the creation of the sustainable network with diverse stakeholders
IMEC	The flexibility of the governance structure, including the mechanisms to distribute the positions, delegate powers, and create additional	The focus on regional interests in the governance approach needs to be taken into account while transferring this best practice into "lessons learned": the

[78] The order of governance examples is not ment to be a ranking of the organisations, but reflects the order in which they have been dealt with in this document.

	structures, makes it adaptable to the latest needs of the organization and state of the world. Balanced representation of different stakeholders is ensured in the Good Governance Charter IMEC has worked out various models of collaboration, suitable to the needs of different stakeholders with different goals and ambitions, as well as different financing options.	governance of the international part of IMEC remains firmly embedded in the local structures. 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 it mind.
GÉANT-NREN	Tangible scope and impact of the organizational mission and tasks. A number of conditions ensure that the influence of commercial providers is not dominating the organization's functioning The service portfolio matrix offers a handy overview of NRENs, their services and membership status, thus facilitating collaboration	Explicitly excluding certain types of stakeholders from the general meetings is not productive for creating the atmosphere of trust and making out the most of collaboration.
IT PLANNING COUNCIL	Permanent structure with a legal task definition and the power to adopt binding resolutions to ensure compliance with standards in public administration digitisation.	The addition of FITKO is resulting from the insight, that even a clear task allocation and the power to make decisions remain ineffective as long as there are no formal substructures to provide the necessary organisational and competence resources.
ENISA	The synergy between formal and informal, top-down and bottom-up structures as found in ENISA 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.	Despite the formalization of the lower-level structures, ENISA remains a top-down-institution; in the field of cybersecurity, it creates challenges for reaching out to the stakeholders and in reacting to stakeholders' demands.

ECSO	ECSO is based on a model of membership opportunities for societal stakeholders of different levels and foci, which enables bottom-up approach and diversity of engagement. ECSO has come up with a number of low-level initiatives, such as ECSO Cybersecurity Business Matchmaking events, aimed at bringing European start-ups and SMEs closer to funding opportunities.	ECSO is currently in progress regarding the issues of governance transparency.
CERN	Transparency is a key element for facilitating trust in an organization. The effects of a transparent organizational construct can be seen well in CERN. There is a rigorous system in place to ensure the prevention of (financial) free-riding and the maximal involvement of the member states in the projects relevant to them. The development of vibrant scientific community in Europe and ensuring its prominence on the world stage is given clear priority.	The CERN governance is specific to its goals of fostering research and cooperation and is insufficient for the goals of fostering multi-stakeholder and multi-sectorial approach.

Table 1: Overview of positive and negative aspects in the analysed governance examples

2.5 Conclusion

Having examined different types of governance structures, and keeping the stakeholder requirements in mind, we have identified a number of elements that could provide valuable lessons for the governance design for the NCCC. An overview of the identified strengths and weaknesses can be found in Table 1: Overview of positive and negative aspects in the analysed governance examples

1.

We find that the synergy between formal and informal, top-down and bottom-up structures as found in ENISA can be beneficial to the overall success of an institution. By integrating informal structures participation borders are reduced, leading to a more efficient stakeholder engagement throughout all societal levels. This ties in with the model of membership opportunities for societal stakeholders of different levels and foci, which we found in ECSO. Furthermore, we find that transparency is a key element for facilitating trust in an organization. The effects of a transparent organisational construct can be seen well in CERN. The commitment to the balanced stakeholder representation, as evident in the structure of IMEC, as well as the flexible collaboration structure offers valuable lessons for the purposes of our project. The flexible, task/project-oriented approach as exhibited by EIT, CEN-CENELEC and ETSI offers the necessary agility and capitalization on the existing resources, but lacks the overarching strategic vision that takes into account long-term sustainable development beyond the market-dictated goals.

The examination of the IT Planning Council shows the advantages of a permanent structure with a legal task definition and the power to adopt binding resolutions to ensure compliance with standards in public administration digitisation. However, even a clear task allocation and the power to make decisions remain ineffective as long as there are no formal substructures to provide the necessary organisational and competence resources. The latest addition of FITKO can be seen as a reaction to this insight.

3 Stakeholder Viewpoints on CHECKs

The IRIT team launched an interview campaign in order to identify the main needs and expectations, types of financially sustainable activities and a multidisciplinary pool of actors that would be willing to participate in the creation and development of a Community Hub of Expertise in Cybersecurity Knowledge in its Territory (CHECK-T) with the objectives to:

- Mobilise communities of actors with different but complementary challenges
- Project a common vision
- Identify a consensus on the expected missions within the consortium
- Highlight the benefits for each stakeholder by sharing contributing and paying in common

The content of the following subchapters will show overlaps with D2.2. These are intentional. While the focus of D2.2 is on the methodology used by the IRIT team, D2.3 focuses on analyzing the outcome of the interview campaign. The information baseline for both approaches is the same, though.

3.1 Needs and expectations

The campaign included a total of 40 stakeholders from four large community groups (cybersecurity end users, cybersecurity solutions providers, technology centres and economic development accelerators) and six mission classes:

- Expertise Development: Guarantee the sharing of data, sensitive information and technological research with other partners on all types of incidents and on the responses provided.
- Technological leadership: Sharing expertise and general know-how, infrastructure and investment costs by obtaining R&D funding.
- Transfer of uses, pooling of R & D & I costs: implementing methodological processes transferable from one sector to another, at lower cost.
- Design driven by need: Eliminate barriers by studying use cases and demonstrating scientific and technological know-how before large-scale deployment towards industrial products.
- Confidence-building: Building a local and European base of trust promoting cooperation and coopetition between members (ethical framework, protection of freedoms, dissemination of trust).
- ROI of companies: facilitate the obtaining of funding in Cybersecurity Innovation and accelerate the maturation of projects and products to the market and awareness-raising, co-innovation activities.

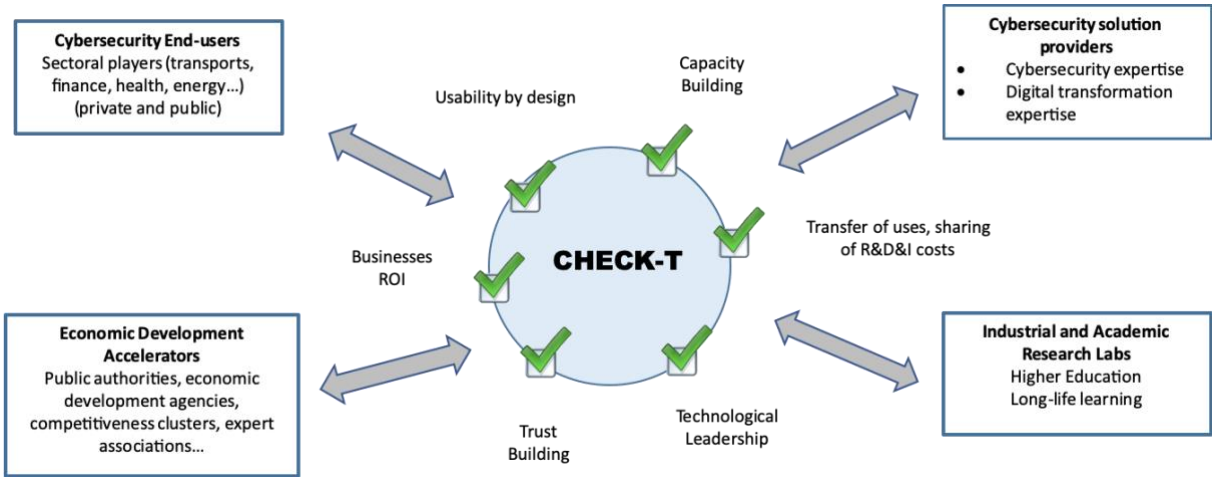

Figure 9: Community groups and mission classes for a CHECK-T[79]

[79] *A. Benzekri/P.H. Cros/A. Ferreira*, Progress report (I) on the implementation of the 1st CHECK-T, May 2020, p. 4.

The possible interactions between the actors (from one community group to another and peer-to-peer by highlighting the concept of coopetition[80]) were synthesised, based on the needs and expectations expressed by them during the interviews:

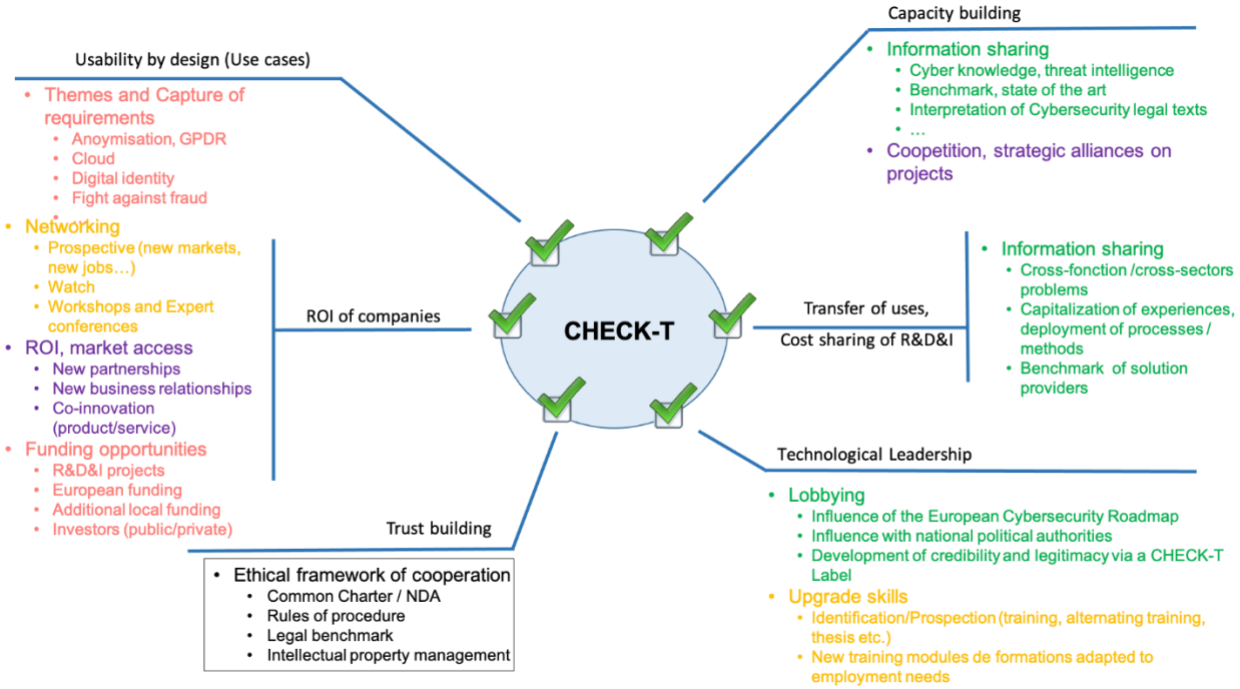

Figure 10: Synthesis of the needs and expectations[81]

[80] Coopetition being understood as cooperation of circumstance or opportunity between different economic actors, who, moreover, are competitors.

[81] *A. Benzekri/P.H. Cros/A. Ferreira*, Progress report (II), July 2020, p. 4.

3.2 Strategic application areas and activities

Subsequently, four strategic application areas, which must be implemented in order for the stakeholders to take an interest in the creation of a CHECK-T, and priority and evolving activities have been identified, from which those, that need to be carried out to establish the first CHECK-T, have been highlighted in a separate chart:

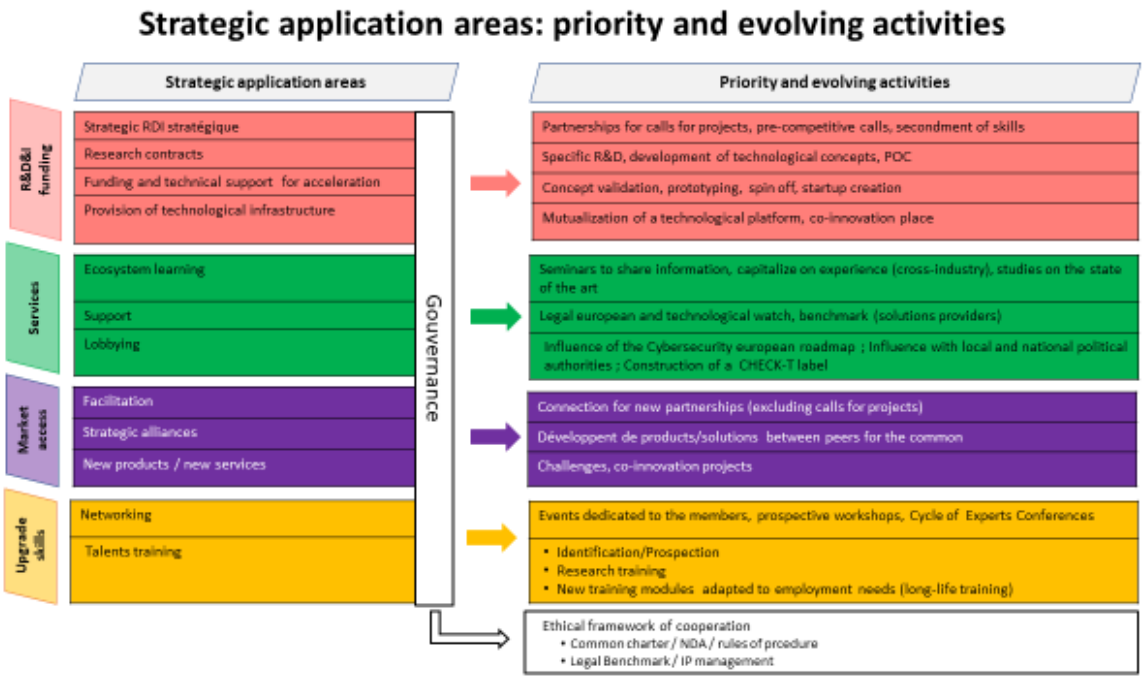

Figure 11: The four strategic application areas emerging from the interview campaign[82]

[82] *A. Benzekri/P.H. Cros/A. Ferreira*, Progress report (II), July 2020, p. 5.

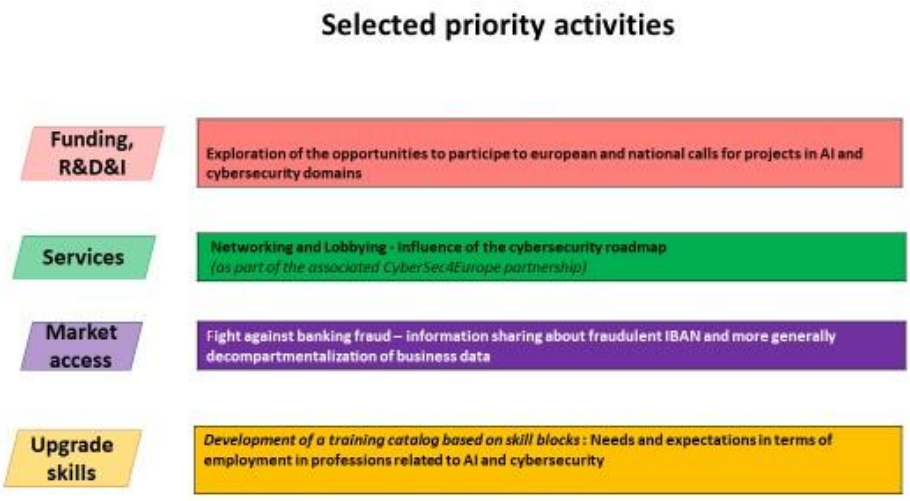

Figure 12: List of activities selected to establish the first CHECK-T[83]

3.3 Governance

The results from the interview campaign indicate that governance issues are transversal. They must be discussed with careful consideration of the specifics of each activity, the objective being to agree a governance model that ensures a harmonious and balanced implementation and development of the four activities concurrently. Moreover, the 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 etc.

3.4 Funding

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.

3.5 Conclusion

Although the interview campaign involved only a part of those European stakeholders that may be Community Members of the future NCCC, the findings of the IRIT team allow at least a *first view* on some of the essential aspects to be considered for the creation phase of a CHECK.

[83] *A. Benzekri/P.H. Cros/A. Ferreira*, The Road to a CHECK-T. A report on methodology, October 2020, p. 2.

As a general observation it can be said that stakeholders are interested and willing to contribute to the Cybersecurity Community. The keys to their commitment, however, are the possibility of active involvement in the shaping of activity programs and governance structures, confidence in collaboration partners and the existence of benefits from their contribution to CHECK activities. Hence, an activity-driven bottom-up approach, based on the needs and expectations of community groups is an approach to be followed. Funding is an additional issue to be aware of as stakeholders might abstain from participating in a CHECK if they see no benefit being generated from their investment.

A broader and more detailed view should be available by closely accompanying the further prototyping phase, i.e., the development and implementation of CHECK-T.

4 Report on the implementation status of prototype CHECKs

The idea to establish a Cybersecurity Network in Europe results (amongst others) from the insight, that the existing wealth of expertise and experience in cybersecurity research, technology and industrial development are not being fully utilized because the efforts in the industrial and research communities are fragmented, lacking alignment and a common mission.[84] Creating a network purely consisting of public European and member state institutions thus cannot enable the power that lies in the broad knowledge that already exists on the private and academic sector. A pure top-down approach will not encourage stakeholders from academia or industry to actively take part in the realization of European cybersecurity.[85] A combined approach consisting of top-down and bottom-up elements is thus favorable.

Integrating CHECKs into the NCCC, as generally outlined in D2.1,[86] adds one bottom-up element to the combined approach, providing structures for the accumulation of special expertise, furthering of scientific exchange and coordination of research and development activities of different stakeholders. CHECKs would serve as sub-network within the NCCC, reflecting the complexity and interdependence of the cybersecurity ecosystem in a multidimensional network and ensuring an efficient flow of information and knowledge management.

During the last months preparations have been made for two test projects implementing the concept of CHECKs. The current implementation status and individual vision on the appropriate governance structure will be introduced in the below subchapters. The fact that both of the candidates are still under construction gives us the opportunity to accompany the implementation process of CHECKs and see their governance structure grow and develop. The focus of observation lies on learning from their experiences in order to add practical insights to the further development of the general concept of CHECKs in Chapter 5.[87] An evaluation of the governance approaches of CHECK-T and the Region of Murcia CHECK is not subject of this deliverable.

4.1 CHECK-T

The creation process of the first CHECK-T covering the territory of the French regions New Aquitaine, Occitanie and Provence-Alpes-Côte d'Azur is still in progress, thus no „final" membership and governance structure could be analyzed in this subchapter. However, even though this early stage of the first CHECK-T, there is yet a clear vision for its inclusion in the cybersecurity ecosystem, namely, to connect the stakeholders and the Community on the one hand and the NCCC on the other in order to avoid gaps in the network.

[84] Recital 6, 2018/0328 (COD).

[85] See D2.1, p. 19.

[86] D2.1, p. 67 et seqq.

[87] For the validation of governance structure see D2.2.

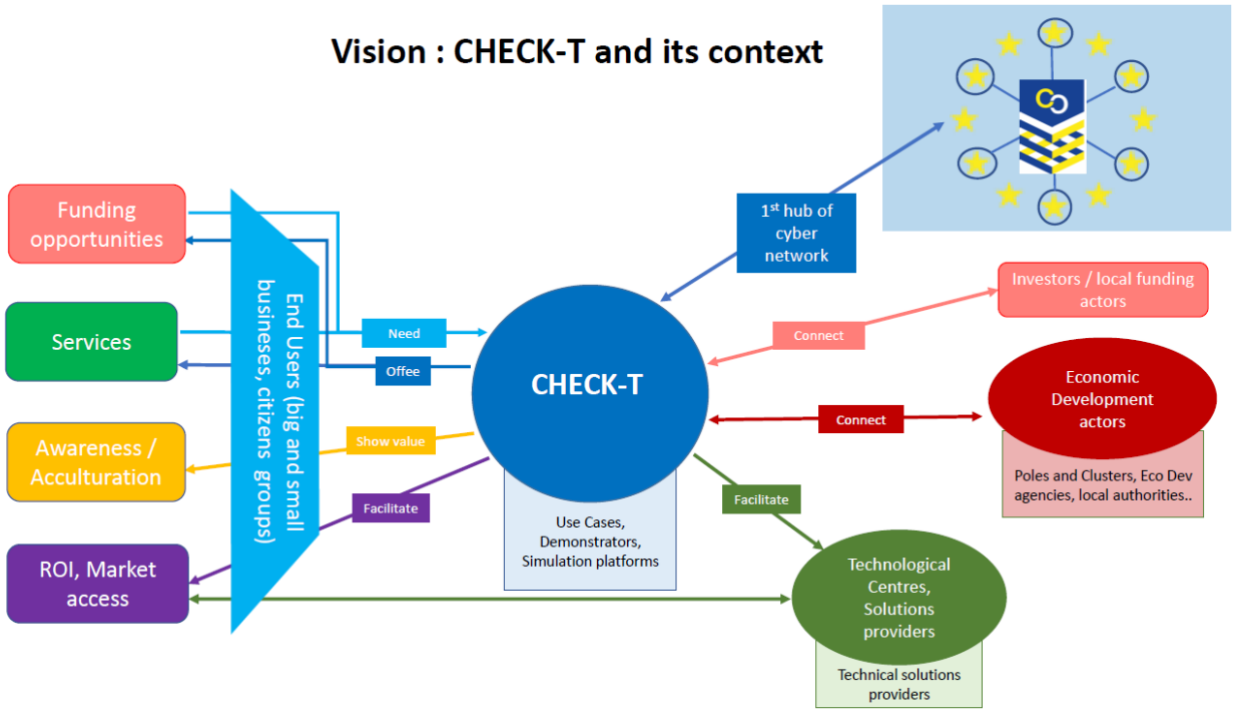

Figure 13: Vision for CHECK-T[88]

4.1.1 Membership

The members of the CHECK-T are to be identified from a multidisciplinary pool of actors from four large community groups in a certain geographical territory: cybersecurity end-users, cybersecurity solutions providers, technology centres and economic development accelerators.

This approach of stakeholder and community-oriented membership reflects the general vision of CHECKs as bottom-up elements within the complementary overall governance approach we propose for the NCCC in D2.1.

4.1.2 Governance Structure

Although there is not yet a final governance structure for the first CHECK-T we can still observe the approach on building such a governance structure.

Led by the results from the interview campaign (see subchapter 2.3), the governance structure will be co-created by all actors, so that they see it as a prolongation of their own individual activities, which will incentivize them to invest their resources in the CHECK-T. Following this approach, CHECK-T will not just be a bottom-up entity itself within the NCCC, but also its creation will be the result of a bottom-up approach. The establishment of a co-creation committee has, thus, been proposed to stakeholders from the four community groups during the interview campaign. This committee aims to define the activities within each Working Group (WG) to best meet the expectations of those who want to be part of the CHECK-T:

- Kick-off of the operational experimentations

[88] *A. Benzekri/P.H. Cros/A. Ferreira*, Progress report (II), July 2020, p. 2.

- Kick-off of the reflection on the governance model
  - ethical framework of cooperation
  - business model
  - legal status

One further aspect of the co-creation approach is to encourage discussions about the governance model in order to establish an internal organization that is conducive of the role to be implemented, but crucially does not constitute a new competitor to the CHECK-T members. In particular, this will have an important impact on the economic model of the CHECK-T.

The further approach on governance issues and development of the governance model for CHECK-T will be presented in due course.

4.2 Region of Murcia CHECK: Regional Cybersecurity Innovation Unit in Murcia (Spain)

As mentioned in D2.2 section 4.5. within Region of Murcia (Spain) an initial work is being defined in order to configure a regional CHECK. The CHECK Region of Murcia is configured around a model of collaboration between its members (without a legal form), with the anticipation of evolving in the medium term towards a legal form of association, which then presents an interesting combination of simplicity and flexibility that is adequate for the development of CHECK activities.

4.2.1 Membership

In the initial stage there is only one membership for all the founding stakeholders. In a following stage, different levels and kinds of membership will be considered.

4.2.2 Governance Structure

The organizational structure of the Region of Murcia CHECK is configured as follows:

4.2.2.1 Joint Monitoring Commission

The Joint Monitoring Commission is the highest body provided for in the agreement. It is responsible for monitoring and controlling the collaboration agreement and is made up of all members institutional representatives and must meet at least once a year, ordinarily, to approve the accounts for the year that ends, the work plan and the budget for the following year.

In addition to the powers in the matter of approval of the annual accounts and the budget for the next fiscal year, it will also have powers to validate the strategic orientation and the lines of work of the CHECK.

Predictably, the agreements of the Joint Monitoring Commission will be adopted by a simple majority of the persons present or represented, when the affirmative votes exceed the negative ones, except for questions related to the dissolution of the association, modification of the statutes, disposition or disposal of assets and remuneration of the members of the representative body. Such decisions have to be taken unanimously.

4.2.2.2 Operational Steering Committee

In order to streamline CHECK operations, once these operations have a remarkable work rate, the creation of an additional collegiate body responsible for the executive management of CHECK is contemplated, which in turn delegates the daily management of CHECK to the Directorate of CHECK.

The Operational Steering Committee will consist of the representatives of the Region of Murcia CHECK members with a scientific-technical profile. These representatives will be selected by the members of the Joint Monitoring Commission.

The Operational Steering Committee will be in charge of adopting ordinary decisions and will be responsible for the strategic decisions of the CHECK, defining its long-term objectives and ensuring that the CHECK has the necessary resources to achieve them. It is also responsible for defining and modifying CHECK services and activities. The Operational Steering Committee will define the strategy and main programmatic lines of CHECK, which will be approved by the Joint Monitoring Commission later. By incorporating members of the regional innovation ecosystem, the Operational Steering Committee will have a balanced vision of what the key players in the regional ecosystem require.

The Operational Steering Committee will work on a basis of consensus and collaboration as a priority. Only in case of different opinions, the Operational Steering Committee will take decisions by majority.

4.2.2.3 Directorate and Technical Secretariat

At the present time, the Region of Murcia CHECK governance approach provides for the initial availability of two different management roles, namely the Directorate and the Technical Secretariat.

The CHECK Directorate (management) will be in charge of the daily management of the Region of Murcia CHECK, will resolve conflicts and will supervise the progress of the work. The Directorate will carry out its functions with the support of the other members, who will meet regularly to agree on the corresponding actions at all times to promote and consolidate the CHECK. In an initial phase, the assignment of Regional Government personnel to the CHECK Management functions is contemplated. Subsequently, the launch of a selection process is contemplated in which a person who meets a technical expert profile and a long career of working promoting business digitization will be incorporated.

The Technical Secretariat will work to provide support to the CHECK Directorate, being responsible for the administrative tasks, communication and coordinating with the rest of the CHECK Murcia Region members.

4.2.2.4 Working Groups

As initial attempt within the framework of these working groups, the lines of action are designed for the full use of the – still to be defined - technologies and activities to be carried out in the CHECK. The working groups consist of CHECK members, i.e., they are not open to external participants, and have been constituted as follows:

- Ecosystem working group.
- Strategic and Technological working group
- Business working group
- Financing working group

4.3 Conclusion

The descriptions of these two test projects reveal that different approaches on the set-up of CHECKs are possible.

The creation process of CHECK-T and the governance issues arising in that context give a good overview of how a bottom-up approach can be appealing to stakeholders in order to motivate their willingness to invest their resources, not only for their own benefit but to contribute to European cybersecurity at the same time. A multidisciplinary pool of actors and their involvement already in the development of activities and governance, instead of just imposing a top-down structure, are very promising in regard of the contributory power of bottom-up structures for the Community integration in the NCCC.

As can be observed, the approach taken on the creation of the Region of Murcia CHECK is different to that of CHECK-T. Instead of starting from an activity-driven position, the Region of Murcia CHECK is rather focussing on the creation of a collaborative structure as a first step and the establishment of working groups within this structure as a second.

Both of these prototypes follow a territorial / regional approach, i.e., each of them is subject to their national jurisdiction and European law but has not to deal with a combination of Member States laws. It will be interesting to also see additional test projects with a sectoral and even a cross-border approach in the future.

Additionally, both approaches start from a rather loose connection of their members for the initial phase towards the goal of reaching a legal form in a subsequent phase. This does not only allow for flexibility during the implementation phase, but it might also be seen as a necessary process of trust-building between the members of a CHECK and their active involvement before entering into legal bindings.

5 Proposal for the further development of the Cybersecurity Network Governance

The further development of our proposal for a NCCC governance model is based on the conclusion reached in D2.1 that a combined approach with both top-down and bottom-up elements will serve the intentions of the Regulation Proposal best in order to establish a true network structure for cybersecurity in the European Union. In addition, one of the core findings in D2.1 was the importance of a better and active integration of stakeholders from different areas into the governance model. Accordingly, D2.1 introduced two bottom-up elements which could provide for such an integration, CHECKs and the Stakeholder Council.

The holistic governance model development for all elements of the NCCC has been continued under consideration of the insights already gained in D2.1 and those described in chapters 2-4 of this deliverable, which also include the first practical experiences and lessons learned from the implementation process of CHECK-T and the Region of Murcia CHECK.

5.1 Summary of core insights in Chapters 2-4 and consideration of current status of legislative process for Regulation Proposal 2018/0328 (COD)

The variety of the analysed governance structures in Chapter 2 gives a good overview of the possible governance model design approaches. Although none of those governance structures is comparable to the NCCC as envisioned by the Regulation Proposal, the analysis gives valuable insights that can be transferred to the different levels of institutions as such, their relationships towards each other and their collaboration in the future NCCC.

To start with, it is in general most important that the governance structure design is fitted to the strategic goals and tasks of a single institution or a network in order to enable a smooth and successful performance. So, before starting to design any governance structure one has to know the tasks and activities that will have to be fulfilled later on. Hence, the strategic set up and the activity planning should be the first step in creating an institution.[89] Furthermore, the need for a fitted governance structure is also why it cannot be expected that a one-fits-all kind of governance model design works out well for a network with different types and levels of institutions that have different tasks. It is inevitable for the governance model to reflect the complexity of the network, its parts and all functions and tasks involved. The more complex and diverse the goals and the tasks are, the more complex the governance structure has to be, which can be seen from the example of CEN/CENELEC.

A problem that has already been raised in D2.1[90] concerns the lack of substructures in the Competence Centre. The efficient use of decision power substantially depends on the adequate preparation of decisions and on the proper handling of the various administrative activities. Substructures provide for the necessary resources. The latest addition to the IT Planning Council structure, FITKO, serves as a good example both for the need for substructures and their possible set-up.

Another important aspect is the need for transparency in the decision procedures. As regards entities with public actors involved, this is first and foremost a question of their compliance with the principle

[89] See for example the experiences made in relation with the creation process of CHECK-T by the UPS-IRIT team, *A. Benzekri/P.H. Cros/A. Ferreira*, The Road to a CHECK-T. A report on methodology, October 2020, p. 3.

[90] D2.1, p. 65 et seqq.

of democracy[91] and the rule of law[92], which are both foundational constitutional principles[93]. But beyond that, and irrespectively of the actors involved being public or private, transparency is one of the keys to trust and acceptance of decisions as can very well be seen on the example of CERN[94].

The interview campaign for CHECK-T as described in Chapter 3 revealed several important insights. There is a broad spectrum of needs and expectations from different Community groups that could be covered by CHECKs. The concept of CHECKs is appealing to stakeholders, who are very positive about its priorities, membership, activities etc. However, in order to gain their commitment, it is crucial to involve them in the creation of governance, i.e., there is a need for a bottom-up approach by ensuring true participation, and to find a funding scheme to show them how their (financial) investment will enable CHECK activities to generate their own income in the near future.

The observations made on the implementation of the prototypes in Chapter 4 show that different set-up approaches are possible, and the concept of CHECKs is in general adaptable to the circumstances of a certain territory, region or sector. However, once the initial implementation phase is over, both approaches aim at a permanent structure on the long run. Therefore, the further development of CHECKs has to consider how a long-lasting collaboration within as well as between CHECKs can be best designed and how it can provide for the necessary flexibility for meeting the needs and expectations of all the Community members.

The status of the legislative process of the EU Regulation Proposal 2018/0328 (COD) has remained unchanged since the submission of deliverable D2.1, which contains a legal analysis of the Proposal. Currently, the legislative process is still ongoing[95], with the European Parliament awaiting the Council's first reading position[96]. The further development of the governance model design for the NCCC in this deliverable therefore refers to the same legal basis as described in D2.1. However, once a new version of the Regulation Proposal is available, possible changes have to be analyzed and the governance model design subsequently harmonized.

5.2 Further development of CHECKs

The further development of the governance model of the European Cybersecurity Network in the field of CHECKs raises a number of fundamental questions about their organization, composition, tasks, financing and their relationship to other institutions. In the following, the design options in essential areas of the CHECKs will be analyzed and various proposed solutions as well as the advantages and disadvantages associated with them will be discussed.

[91] Article 2, 10(1) TEU.

[92] Article 2, TEU; ECJ Case 294/83 Les Verts v Parliament, 1365 par. 23 (ECLI:EU:C:1986:166).

[93] *H.C.H. Hofmann*, General principles of EU law and EU administrative law, in: C. Barnard / S. Peers (Eds.), European Union Law, 2nd Ed. (2017), p. 208; also see D2.1 p. 72, 74 et seq.

[94] See subchapters 2.1.3 and 2.4 of this deliverable and D2.1 subchapter 3.3, p. 26 et seqq.

[95] https://eur-lex.europa.eu/procedure/EN/2018_328 (last accessed 11 January 2021).

[96] https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2018/0328(OLP) (last accessed 11 January 2021).

5.2.1 Number and Structure

5.2.1.1 Criteria of Organisation

First, it is necessary to think about the fundamental question of how many CHECKs shall exist throughout Europe and how they should be organized. The answer to this question depends to a large extent on the criteria used to establish CHECKs and on their objectives.

On the one hand, it seems possible to organize them according to the territory, so that a CHECK is established in every region of Europe. In this case, the catchment area of a CHECK could be based on different criteria. One possible criterion would be the political structure, so that a CHECK is located in every territorial entity, e.g., a federal state or a national region. However, depending on the size of a local entity, this type of organization may lead to the problem that the facilities of a CHECK are not equally accessible to all companies and stakeholders in its catchment area. This will be a particular problem for territorial states. For smaller regions or states, on the other hand, the area-based establishment of CHECKs could prove to be problematic because their size and number of inhabitants mean that they have too small a cybersecurity community for which the establishment of a CHECK structure is not economically viable. Furthermore, the orientation towards national political structures ensures that the goal of creating a pan-European cybersecurity community[97] is not pushed forward, but rather cements an exchange at national level.

These counterarguments can also be used for setting up a large number of CHECKs at, for example, the municipal level. Organizing at this level would also bring about an undesirable fragmentation of the national community, which would even more counteract the effect of bringing them together in a European cybersecurity community. In many CHECKs, very few people would then be working together, with many of the topics that are important for cybersecurity remaining unresolved due to regional conditions. If there is hardly any cybersecurity industry in an area, they would also be at risk of being left completely idle. This way, there would be the risk that no real added value would arise from their cooperation and work. In addition, there would be higher costs for a large number of inefficient CHECKs, within and between which there would be hardly any synergies. On the other hand, it would still be conceivable to organize municipal CHECKs within established territorial and regional affiliation structures, which would possibly cross regional and national borders. However, if these structures are not based on legally or politically defined territorial structures, there is also a risk of a diffusion of responsibility at the legal, financial and political level, which could endanger the success of the CHECKs.

It would also be conceivable to set up CHECKs within the European regions[98]. This would be in line with the idea of establishing a genuine European cybersecurity community through cross-border contact. At the same time, it would very likely bring together significantly more actors who have not previously been in contact and cooperation with each other due to national borders. For small member states, this form of organization would have the advantage that they would be able to avoid the establishment of a CHECK, which might be unprofitable or not viable given their size. It would allow them to connect their comparatively small community with across their boarder, to gain external input with an international dimension and a revival it. What speaks against this approach, however, is that not all the

[97] Cf. Recital 16, 2018/0328 (COD).

[98] More information about European regions is available under www.euregio.eu.

territory of the Union is assigned to a European region. Moreover, the organizational form of the existing European regions is very different and ranges from the establishment of legal entities under public law, to associations under private law, to loose associations without legal backing.

As an alternative model to the area-dependent organization of the CHECKs, topic- or sector-oriented mergers could be aimed at. For example, players from one industry sector could join forces in an industry-oriented CHECK to work on the topics and cybersecurity issues that are essential for their products. Similarly, CHECKs could act as an association of all those involved in a specific topic and thus become a platform for the exchange of information on research and development in this area.

A major advantage of such an organizational form would be the possibility of establishing CHECKs on a pan-European basis. If there is only one CHECK for a research issue or an industry in the European Union, all relevant actors in the field can come together in this CHECK and form a true European cybersecurity community. It would also achieve a desirable focus on aspects that are important for the respective actors. Against this kind of organization there are again problems of access for a large number of actors - especially small SMEs - to the facilities of a CHECK, if long distances have to be covered for meetings. Furthermore, if CHECKs are organized in a theme- and sector-oriented manner, the discussion of issues that are not directly relevant to the topic but are nevertheless relevant to the participants is in danger of being lost in the face of a certain blindness to the sector or topic. In this case, however, it would be necessary to assign the CHECK to a superior body, i.e., to an NCC. Against this background, in order to avoid competition between the NCC, in the worst case for the lowest level of accreditation to the cybersecurity community, consideration should be given to a declaration of competence by the European Competence Centre for the accreditation of members in the case of topic- or sector-specific, and possibly even all cross-border CHECKs.

The comparison of the various possible forms of organization shows that, in view of European diversity, there can be no European "one-size-fits-all" approach. The conditions in the European member states and the requirements to be met are too different for this. Just as the establishment of several or even one CHECK is not worthwhile for small countries, an excessively small sized CHECK in area states could lead to a fragmentation even of the national cybersecurity research community. The establishment and organization of CHECKs should, therefore, 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. However, the establishment of a CHECK should also require certain basic requirements to be met. For example, topic- and sector-specific CHECKs should have to be organized on a European level, i.e., bring together members from a certain number of member states of the Union. Regional CHECKs should also be issued with this requirement, but the handling of their fulfilment could be more flexible. For example, membership of internationally active players could be sufficient to meet the European requirement, or the reference to geographical location in the middle of a territorial state or on the edge of the Union territory could be sufficient, which can make cooperation across European borders very difficult. In addition, the possibility of a partnership cooperation between different CHECKs should be considered, which could also compensate for the lack of a European reference of a CHECK. A flexible organization will ensure that the needs of the local community can be taken into account and that the CHECKs represent a real added value for the community. Requirements for their establishment, in turn, can ensure that not only already existing and functioning structures are further promoted, especially at national level, but that the aim of a pan-European community is actually pursued.

The freedom to set up CHECKs in the member states fully complies with the principle of subsidiarity[99] at the legal level. This principle states that the European Union will only act where the member states cannot exercise their powers to a satisfactory degree. However, the approach proposed here allows for a tailored response to local circumstances. It ensures a combination of the desired Europeanization of the cybersecurity Community while at the same time respecting regional requirements. Insofar as only basic requirements for CHECKs are regulated at European level, this does not only respect the principle of subsidiarity. It also accommodates the continuing legal uncertainties with regard to the regulatory powers of the European Union, which exist in the area of the establishment of CHECKs by the Union.

The establishment of CHECKs should not be seen solely as a governmental task but can rely to a large extent on the initiative of private actors. Art. 8 (4) of the Draft Regulation 2018/0328/EEC (COD) provides that the responsibility for the concrete admission of members to the cybersecurity community lies with the European Competence Centre. This idea can be applied to the establishment of CHECKs. The act of establishing a CHECK should be done either by the European Competence Centre or by an NCC, depending on its character as a regional or topic-specific Centre. CHECKs should have a prominent role within the European cybersecurity Community, with particular influence in advising policy decisions, a leadership role in cybersecurity community collaboration, and project-oriented interdisciplinary work. Therefore, in order to ensure compliance with high suitability and quality requirements and, in particular, to prevent inflationary establishment of unsuitable CHECKs, verification of compliance with the requirements should be carried out on the part of the state, i.e., by the European Competence Centre or a National Coordination Centre when a CHECK is established. However, the coming together of actors in a CHECK to be founded or even the preparation of a foundation does not have to take place with the participation of a public actor or be based on its initiative. Rather, it seems quite possible that suitable private partners in a region or a topic area could come together to prepare the foundation of a CHECK. However, government funding of such a founding initiative does not seem at all out of the question if the public sector would thus like to provide special support for the work of the cybersecurity Community in its area.

Even after approval as a CHECK, it does not appear necessary to have the admission of further members controlled by a public body. In view of the strictly regulated foundation process, the members themselves have a high interest in only admitting further suitable members. They will, therefore, place high demands on the suitability and quality of applicants.[100]

The creation of a CHECK thus consists of two steps: first, the private or publicly supported formation of a cooperation of actors and second, the official and public recognition of a CHECK through the awarding of the status by the European Competence Centre or by a National Coordination Centre.

The concrete demands that can be made on the establishment of CHECKs must be compared with the wishes and possibilities of the actors in practice in the further course of the work on the project. Since the current pandemic situation has made the work in the model projects more difficult and slowed them down considerably, there is unfortunately no practical experience to date on the question of organization. Against this background, it has also not yet been possible to ask the actors for feedback on these points. The further verification and development of requirements is therefore the subject of the work following this deliverable.

[99] Art. 5 III TEU.

[100] Also cf. Chap. 5.2.3.

5.2.1.2 Necessity of CHECKs besides NCCs

While the relationship of CHECKs to NCCs is dealt with in Chapter 5.2.2, it must be considered in advance as a preliminary question in the present context of the number and structure of CHECKs to determine whether CHECKs are mandatory at all in addition to NCCs. In view of the different functions that NCCs and CHECKs have within the European cybersecurity network, the investigation of the question seems surprising at first. However, it concerns a problem that can arise particularly in small or low-inhabitant member states. On the one hand, the community here may be so small that it does not have enough players ready of its own accord to set up a CHECK that is worthwhile or there may be extensive personal conflicts with the NCC. On the other hand, there could be an undesirable competition for the financial resources available for the area, which could result in insufficient funding for both the CHECK and the NCC. Such a competition must be prevented.

The NCCs shall have the tasks set out in Article 7(1) of Regulation (EEC) No 2018/0328 (COD). These include supporting the Competence Centre in its objectives and the coordination of the Competence Community, examining applications for admission to this community, facilitating participation in cross-border projects for actors from the Member States, acting as a national contact point and creating synergies in activities at national and regional level. Furthermore, the Coordination Centres contribute to the identification and solution of sector-specific cybersecurity problems, carry out projects of the Competence Centre and promote and disseminate the work of the network, the Competence Centre and the Competence Community at national and regional level.

The tasks of the CHECKs as an institutionalization of the Cybersecurity Community result from Art. 8 para. 1 and Art. 9 of the Regulation 2018/0328 (COD). Like the Coordination Centres, they support the European Centre in fulfilling its legal mandate and objectives and promotes and disseminates expertise on cybersecurity in the EU (Art. 8 para. 1, 9 no. 1 of the Regulation 2018/0328/EEC (COD)). Their members shall participate in activities promoted by the Centres, in measures provided for in the work plan of the Centre of Expertise and in the working groups set up by its Management Board (Art. 9 No. 2, 3 of the Regulation 2018/0328/EEC (COD)). They shall also support the Centres in the promotion of projects and promote and disseminate the results of the activities and projects they carry out (Art. 9 No. 4, 5 of the Regulation 2018/0328/EEC (COD)).

Even if parallels can be seen in the tasks of both institutions, a diffusion of the functions of both institutions should be avoided, as the purpose of their work and their task as representatives for different groups within cybersecurity would otherwise suffer or disappear completely. Their organizational separation is accompanied by a division between a community institution, which consists primarily of scientific and economic actors, and an organization that belongs more to the political and administrative level. The goal of this separation is to ensure an organizational bottom-up approach. It serves to ensure the flow of information regarding research topics, requirements and developments in the field of cybersecurity from the practical level to the level of political decision-makers in order to be able to make practical decisions and set the course.[101] This flow of information and its authenticity could suffer if the work of the two institutions were to be too strongly intermingled. This would also impair the support of

[101] D 2.1, p. 65.

the NCCs by the CHECKs in the performance of their tasks (cf. Art. 9 No. 2 of the Regulation 2018/0328 (COD).

Consequently, a certain initiatory and organizational influence of the NCCs on the establishment of CHECKs must nevertheless be allowed in exceptional cases. Otherwise, the establishment of CHECKs would not be possible in some member states. This would then lead to the even more problematic situation that the influence of the Cybersecurity Community in these countries on political and administrative decisions concerning cybersecurity would still be lower.

In cases in which otherwise it would not seem reasonably possible to provide financial or human resources for a CHECK, the NCCs should be allowed to take the necessary steps for the organization and implementation of a CHECK. For example, it could be possible for the NCCs to create a forum in which public and private stakeholders can meet. It must be ensured, however, that an NCC cannot influence the content of a CHECK. Furthermore, it seems to be necessary to make the cases in which a CHECK is to be initiated or continued by an NCC subject to the permission of the European Competence Centre, all the more to guarantee that an exceptional situation described above actually requires the intervention of an NCC.

Consequently, the involvement of an NCC in a topic- or sector-specific CHECK does not seem possible, since in these cases a European initiative from several member states is required for the establishment of a CHECK, which implies the existence of sufficient organizational resources so that an intervention of an NCC is not necessary.

5.2.2 Relationship

In order to achieve the goal of CHECKs to link stakeholders from all areas of cybersecurity and integrate them into the Community and the NCCC, it is necessary to define the relationship of CHECKs towards other members of the NCCC (i.e., the Competence Centre, the National Coordination Centres and the Cybersecurity Community) as well as the relationship of CHECKs towards each other. The question of relationships can be seen either under a more organizational or a more legal perspective.

Considering the nature of CHECKs as community driven bottom-up elements within the NCCC and in contrast to the top-down approach the Regulation Proposal follows, CHECKs should be able to be established and to act independently from the Competence Centre and the National Coordination Centre at their residence. Typically, the participants[102] of a CHECK and, depending on the legal form, the CHECK itself[103] are subject to the freedoms and rights of the Charter of Fundamental Rights of the European Union as well as to comparable basic rights in the Member States. This has to be respected in their relationships. However, there should be regular exchange between CHECKs and the NCCC in order to strengthen the network structure and to ensure a constant and effective flow of information. The initial contact and afterwards regular exchange could e.g., be encouraged by including CHECKs into Atlas (see subchapter 5.2.7). As regards the relationship between the Competence Centre and the CHECKs it could be either based on a contract, on the basis of Art. 187 TFEU, creating a joint

[102] Private actors like e.g. individual persons, research institutes or companies designed under private law.

[103] Unless fulfilling public tasks.

undertaking, or on the basis of a European Partnership.[104] A deeper investigation of questions arising in this context should be subject to the further creation process of CHECK-T.

Another important relationship will be that between the CHECKs themselves as soon as more CHECKs have been established. The general idea that has already been raised in D2.1, that CHECKs could form a sub-network within the overall European network[105] could encourage and accelerate the knowledge exchange between CHECK members and thus also accelerate dissemination activities towards the Community and other stakeholders as well as the National Coordination Centres and the Competence Centre. From the existing governance structures that have been analyzed for the deliverable there is none that comes without at least one superior hierarchy element. They may, therefore, provide best practices for the inner governance structure of a CHECK, but not for the relationships between CHECKs.[106] Considering them coexisting as independent and equal entities, something like a CHECK representatives exchange and representation forum might suit the long-term goal of establishing a CHECK network best. Unfortunately, the creation process of CHECK-T has not yet grown far enough to draw a first set of insights from their experiences. However, this should be kept in mind for a later point in time and should take into account the fact that ddifferent CHECK types can be coordinated at the national level first and later at the EU level forming the CHECKs sub-network to constitute the EU Competence Community. A European CHECK representation for the sub-network could consist of

- Working Groups (WGs) or task forces grouping networks of experts from the full members of the CHECKs, working on detailed policies and agenda for concrete topics of cybersecurity and providing advice to a Strategic and Technical Committee.
- The Strategic and Technical Committee should be composed of representatives from the WGs, and elected representatives from stakeholders, representatives of national associations/chapters and maybe from national public administrations.[107]
- A General Assembly composed by representatives of all public/private stakeholders' categories could review and approve the general strategy of the European CHECK representation.

From a more legal perspective, it has to be added that the legal form of a CHECK will also be one aspect for the kind of relationships the CHECK may have towards other actors in the cybersecurity ecosystem. In general, a CHECK designed under private law can commit to contractual relationships as well as non-binding cooperation models. Based on the strategic set-up and planned activities of a CHECK it should, therefore, be investigated which relationships are crucial for the successful activity performance and to

[104] D2.1, p. 45.

[105] D2.1, p. 68

[106] E.g. the KICs within EIT International show similarities with the concept of CHECKs as autonomous hubs with individual legal and governace structures, placed across different countries. A closer look reveals some differences, though. The EIT creates the KICs as its operating organs and plays a guiding and strategic role with a Governing Board that is tasked with making the strategic decisions. So the KICs are not that independent as we would propose necessary for the CHECKs to be and, what is even more important, the EIT governance structure does not seem to provide for a relationship between the KICs.

[107] The inclusion of public actors is to be handled with appropriate care, e.g. by giving them only an observative status. Their involvement in a bottom-up Community organisation like a CHECK could cause conflicts between fundamental rights of private actors and the rule of law bindings of public actors. We have to be aware that this can slow down the complete idea of CHECKs.

include these requirements in the general decision on the legal form and internal governance structure of a CHECK.

Matching with the ECHO governance model described in subchapter 2.3.1, CHECKs can also be considered as a possible approach to a form of focus service groups (regional or sectorial/functional) at the national level to constitute the Cybersecurity Competence Community. The focus service groups are based on:

- bottom-up approach work
- community-level research, innovation, and capacity building in cybersecurity
- different levels: regional, national, sectorial

The complexity of a large number of members of an umbrella organisation, sharing of the association funds and risks can be managed by forming additional regional hubs, focused on members' registering and certification, as well as information sharing, support and coordination with the focus (sectorial/functional) groups (based on group of services or customers globally or regionally).

In that sense, similar to ECHO's definition of a CNO as a breeding environment, CHECKs at the national level are a matrix of regional entities (R, chapters) and functional/sectorial entities (F, service groups) with a central hub, exercising the governance and agreed (delegated) central management role (C, e.g., national CHECK representation).

5.2.3 Membership

Other important questions regarding the CHECKs arise in connection with membership. For example, it must be determined who in principle can become a member of a CHECK. Furthermore, it must be decided who is responsible for the selection of members and according to which procedure and based on which criteria this selection is carried out. Guidance for the decision on these issues can be found in Art. 8 of Regulation Proposal 2018/0328 (COD), which provides for who can become a member of the Cybersecurity Community. Paragraph 2 stipulates in principle that industrial, academic and non-profit research institutions and associations as well as public and other institutions dealing with operational and technical issues may become members. Thus, the circle of potential members is very broad. This decision of the legislator should also be maintained with regard to the CHECKs as an institutionalization of the Community. In this way, a broad participation of a large number of persons and institutions active in the field of cybersecurity is basically guaranteed. However, it is problematic in this context that the Regulation Proposal in Art. 8 para. 4 sentence 1 of Regulation (EC) No 2018/0328 (COD) also assumes that the members of the community are institutions. Individuals are thus excluded.[108] This is likely to make it particularly difficult to involve experts in science and at public research institutions. They could only become part of a CHECK through the institutions that employ them. However, in view of limited financial resources, it is a particular challenge for them to get their institution to become a member of and enter into obligations towards a CHECK. The same will also apply to micro, small and medium-sized enterprises. Against this background, the possibility should be provided for individuals to be members of a CHECK, whereby the requirements for membership must take into account the special financial needs of this group.

[108] A change of this is already considered in the legislative resolution of the European Parliament from April 17th 2019, Art. 8 par. 4 s. 1 P8_TA(2019)0419.

However, a restriction of access from the point of view of eligibility should then be made via the admission criteria in the course of the process of joining a CHECK. Guidance on this issue is also provided in the Regulation Proposal 2018/0328 (COD). Art. 8 para. 3 sentence 2 of the Regulation Proposal 2018/0328 (COD) states that members must have expertise in the field of cybersecurity in the areas of research, industrial development or training and education. On the one hand, these criteria are very narrow, as they disregard the area of consulting, production and design. At least these areas should be included as possible fields of activity for members of the CHECKs. They represent areas in which cybersecurity can be implemented in practice and as an economic product, which can provide important input for the practical work of the CHECKs. On the other hand, the criteria mentioned in the Regulation Proposal are so vague that they hardly offer any room for narrowing down the suitability of candidates. There is therefore an urgent need to concretize the criteria in such a way that it can be determined in what way and to what extent proof of expertise in cybersecurity can be provided. The criteria should be uniform throughout Europe to ensure that the standards used in the CHECKs do not vary too much. Against this background, a basic European standard should be developed by the European Competence Centre to verify the basic suitability of becoming a CHECK member.

According to Art. 8 para. 4 of the Regulation Proposal 2018/0328/EEC (COD), the responsibility for the concrete accreditation of a member lies with the European Competence Centre.[109] Particularly in the phase of setting up a CHECK, the involvement of the European Competence Centre in the process of accrediting the members ensures a high level of requirements. However, it seems questionable, particularly in view of the plea for a large number of different CHECKs, whether the involvement of a central European body is actually necessary when a member is subsequently accredited to a CHECK. The members of a CHECK who have been accredited by the Competence Centre when it was established will themselves have a strong interest in not lowering the professional standard of the CHECK by accepting unsuitable members. Rather, once a CHECK has been established with the participation of the Competence Centre, the process of admitting additional members to it could be transferred to the accredited founding members. This way, particular account would also be taken of the principle of subsidiarity. By designing the criteria defined by the Competence Centre and examining them in the course of an admission process, the members of the CHECK could themselves determine who can become a further part of the CHECK. This would greatly simplify the admission process, as it would no longer require the involvement of a central European body which, with limited financial, time and personnel resources, would have to carry out all accreditations for CHECKs throughout the Union. Since the exclusion or non-inclusion of an actor in a CHECK can be associated with disadvantages and thus may have a negative impact on its position, it must be possible to challenge such a decision. As a first instance, either the National Coordination Centres or the Competence Centre seems suitable. Subsequently, however, a judicial review of the admission decision will also be possible.

However, certain restrictions must be made in this respect. If a broad participation in a CHECK is desired, especially from different disciplines, it must be ensured that the criteria to be fulfilled for acceptance take into account subject-specific characteristics, especially in non-technical disciplines.

[109] The Parliament provides for the Competence Centre to not only do the accreditation but also determine the assessment procedure (amendment 117 and 128, P8_TA-PROV(2019)0189). The Council wants to change to wording of the proposal from “accreditation” by the Competence Centre to “registration” and deletes the power of the Competence Centre to determine the assessment procedure (proposal and remark 199 and 249, Interinstitutional File 2018/0328 (COD)).

Access to a CHECK must also be possible without discrimination, whereby it must be ensured in particular that members who are not dominant in view of their economic importance do not deny small or medium-sized companies access to CHECKs in order to be able to determine the work and content of the CHECKs. The admission process should be standardized throughout Europe in terms of procedure and organization based on the specifications of the Competence Centre so that the same access barriers are encountered in every CHECK.

The application process should be open to anyone who would like to participate in the work in the CHECKs. Only in this way can it be ensured that the community is represented in all its diversity and is involved in the processes. Otherwise, there is a danger that CHECKs will only be used to continue working together in an institutionalized way. In addition, the possibility of an unsolicited application allows actors to be involved who are not yet involved in existing exchange circles and are therefore unknown. Irrespective of the possibility of applying for admission to a CHECK, CHECKs should also be able to invite actors who they consider to be particularly suitable for working in a CHECK to apply and thus draw attention to the possibility of working in a CHECK.

Special attention should be paid to the question of whether non-European actors can also become members of a CHECK. The question arises in view of the motivation of CHECKs to promote a European cybersecurity policy that is shaped by the values of the European Union. This goal could be counteracted by the influence of non-European interest groups. There would also be a danger that the know-how funded from European funds would flow into non-European countries. The solution to this question is addressed in Art. 8 para. 3 sentence 1 of Regulation (EC) No. 2018/0328 (COD), according to which only institutions established in the Union can be members of the Competence Community. This solution is also relevant for membership in a CHECK. On the one hand, it cannot fall short of this approach. The place of establishment is decisive for the legal determination of whether a company is to be regarded as European.[110] It cannot be excluded from the market or a European institution for reasons of equal treatment. This must also apply to access to CHECKs. Non-European players, on the other hand, should continue to be excluded in view of the idea of promoting European cybersecurity in order to prevent influence and the outflow of ideas and products promoted at European level. In the case of non-European companies with representative offices on the European market, this means that they can become part of a CHECK if they have their own branch, e.g., as a subsidiary, in a member state of the European Union. However, a (parent) company based abroad cannot be a member of a CHECK. In analogy to European Private International Law, the place of permanent residence is to be taken into account for the membership of individuals.

The membership status at CHECK (regional or sectorial/functional) could differ according to the commitment of the participants to the network and with according voting rights. Depending on whether the member is a full member, associated member or observer the rights and obligations such as e.g., voting rights or financial contributions could vary. Flexibility in management operations should be presented by some form of procedures describing the interactions of regional-services dimensions of the organisation.

In view of the proposal to handle the establishment of CHECKs in a flexible manner so that regional and sectorial/functional CHECKs with overlaps can be established, institutions and individuals must

[110] Cf. *Jarass*, in: Jarass (Ed.), Charta der Grundrechte der EU, 4th Ed. 2021, Art. 51, par. 59 with refrence to Art. 54 sec. 1 TFEU.

also have the possibility to be a member of more than one CHECK. Any other solution would unnecessarily limit the community and content input in a CHECK.

5.2.4 Activities

The selection and implementation of activities is one of the most important steps in the creation of a CHECK and has to be handled with appropriate care. In D2.1 some general ideas for the function and activities of CHECKs have been mentioned.[111]

With the progress in creating CHECK-T we have gained insights in the crucial role activities play in the creation phase and, later, in the performance of a CHECK, how possible activities can be identified, and which activities actually seem to be attractive for certain stakeholders to participate in a CHECK. The strategic set-up has to bear in mind that stakeholders will only invest their human and financial resources and expertise if they, in turn, benefit from their participation. The activities have, thus, to provide for such benefits. Additionally, the activities should also contribute to the funding of the CHECK (see subchapter 5.2.6).

From the findings in the UPS-IRIT report,[112] it becomes very clear that the decision on the subject matter of a CHECK and derivation of activities have to be the first steps of the creation phase. The governance design for the phase of strategical set-up and activity planning must, therefore, provide for a deep enough investigation and evaluation process.

The legal form should then be chosen in a way to best serve the performance of the CHECK. Hence the legal form depends, amongst others, on the activities. One of the guiding principles of design and architecture is, thus, also true for CHECKs: form follows function.

The same principle can be observed for the general inner governance of a CHECK. Apart from the fact that the outer legal form can also be partly decisive for the internal set-up, e.g., by laying down legal requirements for representation, responsibilities, reporting duties or by limiting decision power, the choice of activities and the governance design are interdependent. There is no one-fits-all governance model for all possible activities. Instead, there is a need for an individual governance design taking into account the specifics of a certain activity while at the same time the overall governance structure has to ensure a balanced implementation of all chosen activities.[113]

For an example of the strategic set-up and activities see the charts provided for CHECK-T in subchapter 3.2.

Activies should also include the ideas already brought up in D2.1. Firstly, CHECKs could be tasked with the accreditation of Community members in cooperation with the National Coordination Centres.[114] Since the Community represents the stakeholder environment, the accreditation process should, thus, not involve the Competence Centre. Being accredited as a Community Member requires proof of superior expertise. Therefore, the accreditation procedure done by CHECKs would assure that this

[111] D2.1, p. 68 et seq.

[112] *A. Benzekri/P.H. Cros/A. Ferreira*, The Road to a CHECK-T. A report on methodology, October 2020.

[113] *A. Benzekri/P.H. Cros/A. Ferreira*, The Road to a CHECK-T. A report on methodology, October 2020, p. 1 et seq.

[114] D2.1, p. 77.

expertise and the willingness to actively participate in the European cybersecurity strategy is actually derived from superior expertise itself. Secondly, CHECKs could take on the role of a National Coordination Centre in case there is no adequate institution in a Member State.[115] These two functions of CHECKs may be unsuitable as initial activities. Nevertheless, should these tasks be considered and developed for the time when a CHECK has reached a more mature status.

5.2.5 Interdisciplinarity

An important aspect of the CHECKs is their interdisciplinary orientation. Not only technical disciplines are important for cybersecurity, but economic, legal or psychological issues also play a decisive role in the field of cybersecurity. Without attention to these issues, cybersecurity remains incomplete. The idea of European cybersecurity is also characterized by the fact that technology is shaped by European values, such as democracy, individual freedoms and the protection of these freedoms. Against this background, a purely technical consideration would therefore fall short.

In view of this premise, the question then arises as to which disciplines should be involved in a CHECK. The answer to this question can only be: Any. The exclusion of one discipline from a CHECK would imply that this discipline cannot contribute anything to cybersecurity. However, this idea is wrong. In view of the increasing digitalization, automation and networking, cybersecurity extends into all areas of life and society. For this reason alone, it would be short-sighted not to involve a subject area. The added value of interdisciplinarity lies in the holistic view of a problem or a technology and the resulting comprehensive understanding. In addition, a genuine European cybersecurity culture can only be said to exist if all areas and perspectives of society are also involved. This requirement makes interdisciplinarity indispensable for the work of the CHECKs.

The possible objection that the involvement of different disciplines is not appropriate for every problem and task of a CHECK is only partially justified. After all, without the involvement of a discipline, one cannot know its view on a problem and on the available solutions. Moreover, without the involvement of a discipline, there is a risk of being deprived of valuable insights and new perspectives.

The integration of non-technical disciplines into the work of CHECKs will depend to a large extent on the specific working methods and tasks of a CHECK. In the context of research questions and projects, for example, it is already quite common practice today to work in an interdisciplinary manner and to have the problems to be investigated assessed by all disciplines. This could also be established in CHECKs.

5.2.6 Funding

One very important question for the successful establishment of CHECKs are the possible funding options.

Considering the presented general approach on the purpose of introducing CHECKs to the NCCC. CHECKs could be funded by the EU for the accreditation of Community members and for territorial or sectoral tasks or projects individually assigned to them. Public procurement rules have to be taken into consideration for such funding.

[115] D2.1, p. 68.

Public funding could also be established by applying for EU, national or regional calls, which, however, requires compliance of a CHECK with the financial rules related to such calls.

Private funding by external stakeholders could be generated by taking on e.g., consultation, education or research assignments. However, such approach could hit a snag due to the nature of participants of a CHECK probably being competitors of such stakeholders. Such obstacles could in general be overcome by a transparent governance structure of the CHECK combined with a careful case-by-case handling, including e.g., non-disclosure agreements, clarification of questions regarding intellectual property or other legal requirements.

Another possibility could be to raise a fee for participants who want to join a CHECK. However, it comes without surprise that the balance between the amount of investment on the one hand and the possible benefit for the participant on the other hand is not that easy to find.

From the findings in relation with CHECK-T it becomes clear that stakeholders are quite cautious about funding issues, especially in the creation phase of a CHECK.[116] It is therefore of high importance to find a funding method with enough potential for immediate returns and the UPS-IRIT team identified that answering calls for proposals would meet that requirement and thus bring potential members to join and work towards effectively implement and develop the activities of CHECK-T.[117] Establishing the CHECK as means for its members to coordinate skills consortia would enable further ways of funding like membership fees paid by the constituting members, access fees for consultation of the directory, consultancy fees related to the facilitation of participation in calls for proposals or bonus schemes on results could then be established to overcome funding problems.[118] Another way to establish funding could be to let the CHECK as a legal entity respond to calls for proposals on behalf of its members. This, however, requires some additional attention e.g., concerning IPR issues.[119]

The further development of the governance model should, therefore, follow up on the experiences of CHECK-T's funding scheme development.

5.2.7 Listing in the European Cybersecurity Atlas

We propose to list CHECKs in the Cybersecurity Atlas.[120] This enhances the visibility of existing CHECKs with their individual scopes of activities and territorial or sectoral approach. Furthermore, this could help to facilitate a relationship between CHECKs, National Coordination Centres and the Competence Centre. The inclusion of CHECKs will at the same time also serve the objectives of Atlas, e.g., mapping competences, raising visibility of participants within the Community, better coordination

[116] *A. Benzekri/P.H. Cros/A. Ferreira*, The Road to a CHECK-T. A report on methodology, October 2020, p. 3.

[117] *A. Benzekri/P.H. Cros/A. Ferreira*, The Road to a CHECK-T. A report on methodology, October 2020, p. 2.

[118] *A. Benzekri/P.H. Cros/A. Ferreira*, The Road to a CHECK-T. A report on methodology, October 2020, p. 3.

[119] *A. Benzekri/P.H. Cros/A. Ferreira*, The Road to a CHECK-T. A report on methodology, October 2020, p. 3.

[120] For more information see the Cybersecurity Atlas webpage oft he European Commission, available under https://cybersecurity-atlas.ec.europa.eu.

of efforts, providing information on networks of institutions researchers, time dynamics, popular topics and territorial specialties or hotspots [121].

Considering that CHECKs are responsible for the accreditation of Community Members[122], the CHECKs could also be assigned with transferring the accreditation outcome to the responsible Atlas maintenance team at the Competence Centre or National Coordination Centre. This would build a direct link between CHECKs as part of the Community to either the National Coordination Centres or the Competence Centre and thus support Atlas as an integral network tool of the NCCC.

5.2.8 CHECKs & Competition Law

Since the CHECKs will bring together several organizations, businesses and institutions, potential competition law concerns appear, as the CHECKs create a forum for businesses where market related information and behaviour can be discussed.

The competition concerns can be divided in three domains: anti-trust, state aid and misuse of dominant market power, which will be touched upon shortly below, to provide a preliminary insight. The competition law concerns depend, however, on how a certain CHECK is set up and which activities it will engage in.

Important to note is that fines for anti-competitive behaviour may be imposed on each of the entities separately or on the CHECK as a whole, in which case the fine will consist of a cumulation of all the individual fines.

5.2.8.1 Anti-trust

The cornerstone to the Union's ant-trust legislation lies in article 101 of the Treaty on the Functioning of the European Union, which reads as follows:

> *"1. The following shall be prohibited as incompatible with the internal market: all agreements between undertakings,* ***decisions by associations of undertakings*** *and* ***concerted practices*** *which* ***may affect trade*** *between Member States and which* ***have as their object or effect the prevention, restriction or distortion of competition within the internal market****, and in particular those which:*
>
> *(a) directly or indirectly fix purchase or selling prices or any other trading conditions;*
>
> *(b) limit or control production, markets, technical development, or investment;*
>
> *(c) share markets or sources of supply;*
>
> *(d) apply dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;*
>
> *(e) make the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts.*
>
> *2. Any agreements or decisions prohibited pursuant to this Article shall be automatically void.*

[121] Examples taken from *I. Nai Fovino*, Cybersecurity Atlas. An introduction, p. 5, 12 et seq. (presentation held at CyberSec4Europe General Meeting on 7 October 2020).

[122] See above, subchapter 5.2.4 (Acitivities) or D2.1, p. 77.

3. The provisions of paragraph 1 may, however, be declared inapplicable in the case of:

- any agreement or category of agreements between undertakings,

- any decision or category of decisions by associations of undertakings,

- any concerted practice or category of concerted practices,

which contributes to improving the production or distribution of goods or to promoting technical or economic progress, while allowing consumers a fair share of the resulting benefit, and which does not:

(a) impose on the undertakings concerned restrictions which are not indispensable to the attainment of these objectives;

(b) afford such undertakings the possibility of eliminating competition in respect of a substantial part of the products in question."

Having regard to the above, an agreement, decision or concerted practice between undertakings is anti-competitive, when:

- It may affect trade between Member-States, meaning it can potentially have a cross-border effect;
- It has as its object or effect the prevention, restriction or distortion of competition within the internal market.

CHECKs unite entities from one domain, albeit from different sectors, backgrounds and different levels in the production- or supply chain. This poses a risk to horizontal restrictions – between competitors – and vertical restrictions – between entities active on a different level of the supply- and/or distribution chain for what concerns the agreement.

Sharing publicly available information between competitors, cooperation between competitors or agreements between entities on a different level in the supply/distribution chain are not necessarily anti-competitive, but could pose an – unintended – risk in specific circumstances. For example, an exchange of information on price (increases), price components, indicative or recommended prices, areas of activity, customers and quantities could become problematic when exchanged between competitors.

The acceptance of members should not be arbitrary as to avoid that competitors would be pushed out of the market, for example because they cannot get the same financial support or because they do not have access to certain infrastructure. The rules must be clear, objective, transparent and made known to potential applicants in advance and the CHECK should provide for an independent selection committee and the possibility of appeal against negative decisions on admittance.

Regarding information exchanges, similarities can be drawn from trade associations which have a long-standing practice of drafting guidelines on conducting activities of the association in a competitive way. Such good practises can also be implemented in every CHECK, to prevent any violations of competition law and to foster transparency. Firstly, every meeting should be preceded by a meeting agenda, for which the topics are preventively checked for compliance with competition law. By setting up an agenda beforehand, misleading wording and certain topics can be avoided. Secondly, the CHECKs should draft a code of conduct which pays special attention to avoiding anti-competitive behaviour. This should include rules on not influencing commercial decisions of the members, rules on benchmarking and information exchanges, rules for meetings, including agenda and meeting minute guidelines, legal advisors at sensitive meetings, only official social events and competition law training for its members.

Important when using publicly available information, is that the conclusion which is based on it never restrict the freedom to conduct business, for example by restricting business to the members of the CHECK. When decisions or publications are based on analysis or statistical research which uses company data from one of the members, it cannot implicitly show which entity's data is presented.

In the unlikely event the CHECK would engage in drafting sectoral terms and conditions could be problematic in the light of competition law when such terms influence aspects of importance to competition.

Less apparent is standardisation, cooperation and research and development activities – activities which are expected to take place in CHECKs – that can also have anti-competitive results. Should the CHECK engage in standardisation, for example by developing a new standard, it will be important that no entity is excluded from the possibility to use this norm if it falls under the conditions. Hence, the obtainment of the standard cannot be limited to the entities which take part in the CHECK and transparent and objective assessment criteria (fair, reasonable and non-discriminatory – FRAND) must exist. If these conditions are respected, the standardisation activities will fall under the exception of article 101 (3) TFEU. The same goes for the development and use of a quality label.

Specifically, for research and development, a group exemption exists. Regulation (EC) nr. 1217/2010[123] sets out several conditions for this exemption to apply, concerning, inter alia, access to the final result and intellectual property rights, access to pre-existing know-how in certain circumstances, joint exploitation and production.

5.2.8.2 State aid

The relevant articles on state aid are:

Article 107 TFEU:

> *1. Save as otherwise provided in the Treaties, any **aid granted by a Member State or through State resources** in any form whatsoever which **distorts or threatens to distort competition by favouring certain undertakings or the production of certain goods** shall, in so far as it **affects trade between Member States**, be incompatible with the internal market.*
>
> *[…]*
>
> *3. The following may be considered to be compatible with the internal market:*
>
> *[…]*
>
> *(b) aid to promote the execution of an important project of common European interest or to remedy a serious disturbance in the economy of a Member State;*
>
> *[…]*

Article 108 TFEU:

[123] COMMISSION REGULATION (EU) No 1217/2010 of 14 December 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to certain categories of research and development agreements, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:335:0036:0042:EN:PDF.

1. The Commission shall, in cooperation with Member States, keep under constant review all systems of aid existing in those States. It shall propose to the latter any appropriate measures required by the progressive development or by the functioning of the internal market.

2. If, after giving notice to the parties concerned to submit their comments, the Commission finds that aid granted by a State or through State resources is not compatible with the internal market having regard to Article 107, or that such aid is being misused, it shall decide that the State concerned shall abolish or alter such aid within a period of time to be determined by the Commission. If the State concerned does not comply with this decision within the prescribed time, the Commission or any other interested State may, in derogation from the provisions of Articles 258 and 259, refer the matter to the Court of Justice of the European Union direct. On application by a Member State, the Council may, acting unanimously, decide that aid which that State is granting or intends to grant shall be considered to be compatible with the internal market, in derogation from the provisions of Article 107 or from the regulations provided for in Article 109, if such a decision is justified by exceptional circumstances. If, as regards the aid in question, the Commission has already initiated the procedure provided for in the first subparagraph of this paragraph, the fact that the State concerned has made its application to the Council shall have the effect of suspending that procedure until the Council has made its attitude known. If, however, the Council has not made its attitude known within three months of the said application being made, the Commission shall give its decision on the case.

*3. **The Commission shall be informed, in sufficient time to enable it to submit its comments, of any plans to grant or alter aid**. If it considers that any such plan is not compatible with the internal market having regard to Article 107, it shall without delay initiate the procedure provided for in paragraph 2. The Member State concerned shall not put its proposed measures into effect until this procedure has resulted in a final decision.*

[…]

As the CHECK is ought to maintain a relationship to the National Coordination Centre, attention must be given to the rules on state aid, should the CHECK implement national funds (separate from the European funding through Horizon and Digital Europe). According to the Union's law, state aid cannot distort competition by favouring certain companies. Safeguarding this is of course the responsibility of the state, however, due care must be given to the rules on membership as these can have an effect on who can be a member of the CHECK and who consequently has access to funding.

5.2.8.3 Misuse of dominant position

Misuse of a dominant market position is constrained by article 102 TFEU:

Any abuse by one or more undertakings of a dominant position within the internal market or in a substantial part of it shall be prohibited as incompatible with the internal market in so far as it may affect trade between Member States.

Such abuse may, in particular, consist in:

(a) directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions;

(b) limiting production, markets or technical development to the prejudice of consumers;

(c) applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;

(d) making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts.

The risk to misuse of dominant market position is only of minor importance to CHECKs as several conditions need to be met to speak of a collective dominant position, which include there to be tacitly coordinated behaviour.

5.2.9 Conclusion

The concept of CHECKs and the CHECK sub-network is able to provide a significant added value for the NCCC as a true network and hence to European cybersecurity as well as to the individual Community members and the single market.

In summary the main findings for the further development of CHECKs are:

- CHECKs can be organised territorial/regional as well as sectoral/topical. Instead of a "one-size-fits-all" strategy a flexible case-by-case approach should be chosen in order to reflect the individual circumstances and to meet the specific needs and requirements, e.g. in a certain area or of a specific sector/topic. This way CHECKs are adaptable to European diversity.
- The creation of a CHECK consists of two steps: first, of the private or publicly supported formation of a cooperation of actors and second, of the official and public recognition as a CHECK through the awarding of the status by the European Competence Centre or a National Coordination Centre.
- CHECKs are necessary besides the NCCs. Even if parallels can be seen in the tasks of both institutions, a diffusion of the functions of both institutions should be avoided, as the purpose of their work and their task as representatives of different groups within cybersecurity would otherwise suffer or disappear completely.
- Considering the nature of CHECKs as community driven bottom-up elements within the NCCC they should be able to be established and to act independently from the Competence Centre and the National Coordination Centre.
- A regular exchange between CHECKs and the NCCC will strengthen the network structure and ensure a constant and effective flow of information.
- CHECKs forming a sub-network will encourage and accelerate the knowledge exchange between CHECKs, i.e. the Community, and thus also accelerate dissemination activities towards other stakeholders as well as the National Coordination Centres and the Competence Centre.
- CHECKs can be seen as a institutionalised form of the Community. The question of membership in a CHECK finds guidance in Art. 8 Regulation Proposal 2018/0328 (COD), which describes who can in principle be a member of the Community. While it is an advantage to have a very broad circle of possible Community members in the first step, the criteria are nevertheless vague and might not equally serve as membership criteria for CHECKs.
- The accredited founding members of a CHECK will themselves have a strong interest in not lowering the professional standard of the CHECK by accepting unsuitable members. The process of admitting additional members to a CHECK, once it has been established with the participation of the Competence Centre, could be transferred to the accredited founding

members. This will reduce administrative efforts and at the same time ensure the quality of CHECKs.

- The activities of a CHECK play a crucial role for creation phase as well as the later performance. The strategic set-up of a CHECK has to bear in mind, that stakeholders – on the threshold to becoming Community members – will only invest their ressources if they see the chance for a return on investment.
- The legal form of a CHECK should reflect the strategic activity set-up.
- CHECKs should be tasked with the accreditation of Community members.
- The set-up and activity planning of a CHECK should follow an interdisciplinary approach. Rather than only technical disciplines, also economic, legal, educational, social or psychological issues play a decisive role in the field of cybersecurity and have to be taken care of. Furthermore, a holistic approach would also ensure European cybersecurity to be shaped by European values, such as democracy, individual freedoms and the protection of these freedoms.
- Funding options are an important issue for the successful implementation of CHECKs. A combined scheme consisting of public funding (e.g. for CHECKs accrediting Community members or by applying for EU, national or regional calls) and private funding (e.g. membership fee for participating in a CHECK or income generated by taking on consultation, education or research assignments) is a promising approach.
- CHECKs should be listed in Atlas. This will enhance their visibility in the European cybersecurity ecosystem, help to facilitate a relationship between CHECKs, National Coordination Centres and the Competence Centre and will also serve the objectives of Atlas, e.g. mapping competences, raising visibility of participants within the Community, better coordination of efforts, providing information on networks of institutions researchers, time dynamics, popular topics and territorial specialties or hotspots.
- CHECKs create a forum for businesses where market related information and behaviour can be discussed. Competition law rules, especially those regarding anti-trust measures and rules on state aid, have to be considered in the context of CHECKs. However, the individual competition law concerns depend on how a certain CHECK is set up and which activities it will engage in. This has to be kept in mind for the further development and set up of CHECKs.

5.3 Stakeholder Council

The introduction of a Stakeholder Council in D2.1[124] resulted in our findings on the governance structure of the Industrial and Scientific Advisory Board and its limited ability to fullfil the role assigned to it by the Regulation Proposal. It has to ensure a regular dialogue between the private sector, consumer organisations and other relevant stakeholders. It, thus, has to promote a sufficient representation of stakeholders in the work of the Competence Centre[125] and secure the benefit the Competence Centre should gain from this stakeholders' representation[126].

[124] D2.1, p. 70 et seq.

[125] Recital 27, 2018/0328 (COD).

[126] Recital 28, 2018/0328 (COD).

Under due consideration of the Council's latest position[127] to even completely delete the Industrial and Scientific Advisory Board as a Competence Centre Body without any replacement, we would like to express our strong concerns on this possibility as this would completely counteract the above-mentioned intentions of the Regulation Proposal.

We therefore emphasize the importance of including a stakeholder representation body in the structure of the Competence Centre and adhere to our proposal of a Stakeholder Council as described in D2.1.

5.4 Competence Centre

There is also a need for further development of the existing governance model in the area of the Competence Centre. In the course of Deliverable 2.1, the establishment of an Executive Board alongside the Governing Board and the Executive Director was proposed.[128] The reason for this introduction is the need to relieve the Governing Board from the workload.[129] The Governing Board is the only decision-making body envisaged to date that can effectively perform its complex tasks, which require a high level of expertise, only if less weighty individual issues and matters of day-to-day business can be delegated. The natural recipient of these tasks is actually the Executive Director, who is assigned a role comparable to that of a managing director.[130] In view of this comprehensive allocation of tasks to the Executive Director and the character of the tasks, which in some cases go beyond the day-to-day business and require broad legitimation, the establishment of an Executive Council has been provided for. It now seems questionable how the tasks can be distributed between the above-mentioned institutions within the structure of the Competence Centre. The division of tasks between the administrative, executive board and executive director of ENISA can serve as a model for this.

Art. 15 of Regulation (EU) 2019/881[131] provides that the Administrative Board shall determine the general guidelines for the work and direction of the European Union Agency for Cybersecurity. This includes, for example, the direction of ENISA's activities and compliance with the rules and principles laid down for its work. Furthermore, it is responsible for the programme and budget planning as well as working arrangements, the adoption of annual reports, ensuring that the agency's work is free of conflicts of interest and corruption, regulating matters relating to the staff of the agency and appointing the Executive Director and the Accounting Officer.

The task of the Executive Board, on the other hand, is to assist the Administrative Board in accordance with Article 19(1) of Regulation (EU) 2019/881. In concrete terms, this means that it prepares the draft decisions of the Administrative Board and also assists the Executive Director in implementing the decisions of the Administrative Board, irrespective of the latter's duties.[132]

---

[127] Council of the European Union, 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 – Mandate for negotiations with the European Parliament, 5341/3/20, 9 March 2020.

[128] Deliverable 2.1, p. 78.

[129] *von Wintzingerorde/Müllmann*, Ein europäisches Netzwerk für Cybersicherheit, in: Taeger (Ed.), Den Wandel begleiten, Edewecht 2020, 475 (482).

[130] Art. 17, 2018/0328 (COD).

[131] Regulation 2019/881 of 17. April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15 et seqq.

[132] Article 19(2), Regulation (EU) 2019/881.

The Executive Director, on the other hand, directs the agency[133] and thus manages its current business. He implements the decisions taken by the Administrative Board, prepares and implements the programme and budget planning. He/she also prepares the annual reports and action plans, implements measures to combat fraud and corruption and is involved in exchanges with the business community, consumer organisations and the Union's institutions and bodies.

The Executive Board and the location of its responsibilities between those of the Management Board and the Executive Director ensures a better burden sharing between the bodies and thus a discharge of both the Management Board and the Executive Director. They can, therefore, deal more intensively with important aspects of the day-to-day business or the basic orientation of the authority. The Administrative Board of the Competence Centre in particular would then have more time to deal with important questions of norms and standardization or administration. In addition, the freed-up time and personnel resources could significantly improve the collection of information and involvement of stakeholders. The administrative approach established within ENISA should therefore also be adopted for the Competence Centre.

5.5 Network of National Coordination Centres

In accordance with EU competences the Regulation Proposal 2018/0328 (COD) does not contain specific provisions for the governance structure of the individual National Coordination Centres and their Network as this is subject to the Member States‘ sovereignty. Nevertheless, networking and information exchange activities between the National Coordination Centres are desirable in order to gradually establish a common view on a European cybersecurity strategy rather than keep sticking to national, Member State oriented approaches.

5.6 Cybersecurity Community Establishment

We stick to our initial proposal in D2.1[134] to designate the accreditation of Community members to CHECKs in cooperation with the National Coordination Centres instead of involving the Competence Centre in the accreditation process. A notification on newly accredited Community members to the Competence Centre could be included in the contributions of the National Coordination Centres to Atlas.

However, since the CHECK development has not yet reached a mature enough status, a set-up for testing the accreditation process and maybe necessary further elaboration of details will have to follow at a later point in time.

5.7 Conclusion

On the basis of the results found in Deliverable 2.1 and the insights gained in Chapters 2 to 4, there are opportunities for further development in all areas of the governance model for a European cybersecurity network envisaged to date, but also the need to clarify structural and organizational issues.

First of all, it is necessary to further develop the idea of CHECKs. Their optimal design requires answering a variety of questions and making fundamental decisions about the direction of the institution. Both will be based on practical experience gained in the pilot projects, analysis of existing and planned

[133] Article 20(1), Regulation (EU) 2019/881.

[134] D2.1, p. 76 et seqq.

legal frameworks, expediency and teleological considerations, and stakeholder feedback. With regard to the CHECKs, a decision on their number and structure appears to be necessary first. The recommendation developed here opposes a "one-size-fits-all" approach and opens up the possibility for CHECK initiators to establish both topic-specific and sector-specific CHECKs, as well as regional CHECKs, provided that basic requirements for the establishment of a CHECK are met. In this way, the different starting conditions in the member states, but also in the different regions of Europe, can be taken into account and yet, at the same time, a Europe-wide network for the involvement of the cybersecurity community can be created.

However, the process for creating CHECKs should be uniform at the European level. While the initiative to create can come from a coalition of private actors or from governmental or semi-governmental bodies suggesting it to private parties, the act of designating an initiative as a CHECK should be done either by the European Competence Centre or a National Coordination Centre. By verifying the existence of the necessary conditions for the establishment of a CHECK, the quality of the work of the CHECKs and the qualification of the actors gathered in them will be ensured.

The NCCs may have a special role to play in the context of supporting the establishment, operation or work of CHECKs, especially in smaller member states with a not very developed cybersecurity community, but in view of the different actors that will be active in the respective institutions and the different roles that are to be performed, care must be taken to ensure a clear separation of their activities to and tasks.

In light of this consideration and the bottom-up approach expressed in the organization and function of the CHECKs, their relationship with the NCCs, but also with each other, as well as the granting of freedoms in the exercise of the tasks assigned to each should be through regular exchanges. Just like the relationship between the CHECKs themselves, the relationship with the other institutions should therefore be regulated by contract. Representatives of the CHECKs should also be part of the bodies of the other institutions.

In connection with questions of membership in CHECKs, it is recommended that individuals also be allowed to participate in the work of CHECKs. It is important in this context, as well as in general, that they meet the criteria for the membership. However, to maintain the goal of advancing European cybersecurity, non-European actors should be excluded from working in CHECKs.

As examples of the activities that a CHECK and its members can undertake, one can be referred to the implementation in CHECK-T and the discussion in Deliverable 2.1. In addition, the idea of conducting CHECK work in an interdisciplinary manner is essential, with every discipline that can play a role in cybersecurity becoming part of a CHECK.

Given stakeholder awareness of issues related to the financial burdens of membership in a CHECK, it is important to ensure that the activities and benefits from membership in a CHECK must outweigh any funds that may need to be raised for that membership. Support for the work through public funds in addition to monies payable, for example, as membership dues by participants in a CHECK should therefore also be considered.

The establishment and operation of CHECKs, however, must be in accordance with the law. In this context especially the European competition law could be problematic. Possible concerns relate to the domains of anti-trust, state aid and the misuse of dominant market power.

However, there are also many unanswered questions and various redesigns to be made with respect to the bodies and the institutions other than CHECKs.

In view of the Council's consideration to eliminate the Advisory Board of the European Competence Centre, the importance of the community's influence on political decisions, as it could be done by the Stakeholder Council, should be pointed out again. Against this background, its introduction is strongly recommended.

In order to relieve the Governing Board in particular, an Executive Board should be introduced into the structure of the Competence Centre, to which the processing and preparation of time-intensive tasks can be assigned. The governance structure of ENISA can serve as a model for the distribution of tasks and the relationship between the actors.

In the context of the network of National Coordination Centres, it should be noted that the regulation of their cooperation, organization and work is, to a large extent, the task of national legislators. Nevertheless, basic issues of information exchange and cooperation should be addressed and regulated from a European level by the regulation in order for to be able to create a unified structure and a pan-European perspective on the work of NCCs to be performed.

6 Conclusion

One year has passed since D2.1 set the first milestones for a governance model for the NCCC. Amongst others, one important attribute of the desired governance model was the needed flexibility to adapt to the emerging cybersecurity challenges. At that point in time none of the project partners in CyberSec4Europe could have even guessed that only a few weeks later the Covid19 pandemic would showcase the importance of such flexibility. Instead of conducting meetings in person and workshops to discuss and develop further and more detailed ideas for the network governance model in general and especially the concept of CHECKs, we found ourselves stuck in homeoffices, developing contingency plans and workarounds. D2.3 is the result of everybody in WP2 not only being willing, but successfully managing to flexibly adapt to the new circumstances.

Based on the findings in D2.1 and continuing its approach of performing a theoretical and a legal analysis in combination with studying best practices and gathering stakeholder opinions we developed Governance Structure v2.0 in Chapter 5 of this deliverable.

In D2.1 the paradigms generated from the stakeholders' input were summarised as follows[135]:

1. Enabling innovation by facilitating a tight collaboration between industry and academia.
2. Streamlining investment and funding processes to facilitate innovative research.
3. A focus on distributed capacity building leveraging existing centres and competence hubs.
4. An overarching bottom-up approach, which does not suffocate those existing structures, but instead nurtures and integrates them, to generate the NCCC as an emerging property of these Centres.

The stakeholder input on CHECK-T not only confirms the importance of these paradigms but shows that stakeholders consider the concept of CHECKs matching their needs and requirements and that they are willing to contribute to European cybersecurity as members of the Community. The power that lies in this European bottom-up resource cannot be overestimated.

The analysis of already existing governance structures has been amended by 6 additional structures and also a summarising description of the governance approaches of the other 3 pilots. Furthermore, the structures of ENISA, CERN and ECSO, which have already been subject to the analysis in D2.1, have been re-evaluated for changes since the initial analysis. If they had changed during the year, this could have presented valuable insights in possible needs for changes and provide for lessons learned that can be considered for the NCCC governance model. Actually, their governance structures have not changed, which is also an important outcome, indicating a certain stability and maturity of these structures.

Even if limited by the restrictions for travelling and personal meetings the development of CHECK-T and the Region of Murcia CHECK have been continued and possible inner governance structures have been drafted. The further testing and improvement of their approaches in the coming months is eagerly awaited.

Subsequently, we have used the prototype CHECK blueprints in combination with best practices and the Regulation Proposal 2018/0328 (COD) to continue the governance structure design as begun in D2.1. The general concept of CHECKs has been refined and elaborated in more detail. Amongst other aspects the integration of CHECKs into the NCCC was of importance in order to put the above-described

[135] D2.1 p. 93 et seq.

power into effect. In that context we also discovered synergetic potential for CHECKs and the Cybersecurity Atlas. In addition, other essential aspects of the structure and organization of institutions of the European cybersecurity network, e.g., the establishment of a Stakeholder Council or the implementation of an Executive Board into the structure of the European Competence Centre, have been considered in depth and suggestions for their design have been made.

We stick to the detailed proposals made in D2.1 for substructures of the Competence Centre, which will have its seat in Bucharest,[136] and for the introduction of a Stakeholder Council. Cybersecurity challenges will not fall short in the future but increase. The Governing Board of the Competence Centre must have the ressources to take important decisions as outlined in the Regulation Proposal. It is therefore inevitable to relieve decision-makers from daily business issues. As regards the Stakeholder Council, this would prove European diversity and integrative power and thus underline the European values. Especially in times when democratic and rule of law principles are being attacked by different groups within and outside the EU, those values cannot be held high enough.

[136] For detailed information see https://www.consilium.europa.eu/en/policies/seat-selection-cybersecurity-centre/# (last accessed 07 January 2021).