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

Project start: February 1, 2019
Project duration: 47 months

Cyber Security for Europe

D2.4
Roadmap of the Set-Up of the NCC

Document Identification	
Due date	31 July 2022 Extended to 30 November 2022 (Amend No. 830929-46)
Submission date	30 November 2022
Revision	1.0

Related WP	WP2	Dissemination Level	CO
Lead Participant	CONCEPT	Lead Author	Mark Miller (CONCEPT)
Contributing Beneficiaries	TUD, UMU, UNITN, CONCEPT, ATOS, GUF, TLEX, UPRC, UPS-IRIT	Related Deliverables	D2.1, D2.2, D2.3, D10.1, D10.2, D10.3

Abstract

The work of Work Package 2 of CyberSec4Europe has been focused on designing the governance structure that will answer the main challenges faced by the field of European cybersecurity. This Deliverable D2.4 – Roadmap of the Setup of the NCC (National Cybersecurity Competence Centres) Network is a continuation of the deliverables D2.1, D2.2 and D2.3, which have researched, designed, tested and validated diverse aspects of the governance structure that would answer the existing needs of the EU cybersecurity landscape. This deliverable has been following the latest developments of the setup of NCCs, and as such it is focused upon both monitoring the current status of the network environment and further developing the community elements from the previous deliverables. Specifically, this deliverable follows up on the concept of CHECKs that has been developed as a grassroot approach by CyberSec4Europe in the course of this project as a way to build cybersecurity community based on the bottom-up stakeholder engagement. This deliverable offers the toolbox to assess the maturity of the different cybersecurity community dimensions, analyses the current status of NCC and community setup in the diverse Member States, and looks into the institutional aspects of the community as outlined in the Regulation. In summary, recommendations are given to support the NCC and community development with the view of achieving more engagement and involvement from the grassroot level of cybersecurity in Europe. This deliverable D2.4 develops and concludes the recommendations from the previous WP2 deliverables D2.1, D2.2, D2.3.

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.

This page has been intentionally left blank

Executive Summary

This Deliverable D2.4 – Roadmap of the Setup of the NCC (Network of National Cybersecurity Competence Centre) has undergone dynamic evolution during the lifetime of the project. At the time of project setup, the Network existed conceptually as a part of Proposal 2018/0328. Subsequently it has materialized in the final version of the Regulation, and thus the Governance work of WP2 (Work Package 2) has been following the setup that has already occurred. As such, this deliverable expands upon its initial planning and is focused on both the current status and the additional concepts of the Network and the cybersecurity community environment. In course of the project, WP2 has assessed the best governance practices for the Community. The deliverables D2.1, D2.2 and D2.3 analysed governance proposals for the various levels of and diverse approaches to cybersecurity governance, tested them against the input required by the relevant stakeholders, and drew conclusions about the desired characteristics of a governance model that would be able to answer the identified challenges.

In continuation of the first draft of the governance structure presented in deliverable D2.1, this document reports on the further development of the proposed governance structure developed by WP2 of CyberSec4Europe, one of the four pilots initiated by European Commission to test and develop potential network governance designs. Based on stakeholder input in D2.1, D2.2 and D2.3 the concept of CHECKs as a grassroots bottom-up approach was developed by CyberSec4Europe in the course of this project as a way to complement the network setup and provide additional involvement channels. This deliverable further elaborated on these additional options in achieving more engagement and involvement from the grassroots level of cybersecurity in Europe, while at the same time ensuring broader participation from those who may not have the time, the resources or the opportunities to contribute as stakeholders, users, solutions providers and even regulators and public sector agencies.

The novel contribution of this deliverable is the maturity framework for Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs) in Chapter 2. This framework is an attempt to develop a typology and enable better understanding of different EU cybersecurity innovation ecosystems, whether these are organized in a Digital Innovation Hubs (DIH), CHECK or any other “hub”-like format. We base our framework on a set of flexible criteria appropriate to the different cybersecurity dimensions, which can be used to develop the maturation strategies and further develop cybersecurity innovation ecosystems.. Maturity criteria are not exhaustive, and other criteria could also have an impact on the functioning and management of the innovation ecosystem, for example external context. These are often predefined and do not depend on the development or maturity stage. Additionally, there is a strong interdependence of the criteria, which needs to be reviewed. The findings should not be used as a kind of benchmarking, but rather as a tool set to supports overall cybersecurity ecosystem in Europe

In Chapter 3 this deliverable provides detailed overview of the NCC and community development in the partners’ Member States. This chapter provides a comprehensive, up-to-date (at the moment of writing) overview of the best practices in NCC and Community establishment, development, and perspectives and serves as a catalogue of best practices and challenges for the NCC and community development.

The analysis of the Regulation in Chapter 4 examines the conceptual institutional development of European Competence Centre, NCC network and Community. The Regulation Proposal had been subject to an analysis in D2.1 and the further development of the concept of CHECKs in D2.3. With the Regulation entering into force in 2021, WP2 have conducted an assessment of the final wording and comparison with the Proposal with a continued focus on the Community governance. The conclusion has been that, despite the EU’s intention to overcome fragmentation, the Regulation does not provide any organizational structure for the public-private and the inter-institutional collaboration between the Community members. In particular, the Regulation remains silent on the question, how possible members, that are not already well networked and informed should learn about the possibility of application and registration. Additionally, there is no evident benefit or added-value for possible members to increase their interest in going through the application and registration procedure. The Regulation does not specify how or by what means the Community should accomplish the task of promoting, sharing and disseminating cybersecurity expertise throughout the Union.

Chapter 5 reflects on the community-building lessons from the previous deliverables and revisits ECHO, SPARTA and CONCORDIA pilots governance model evolution. This chapter has looked into the current forms of the cybersecurity community organization. It outlines the community setup recommendations based on the previous work of WP2 of CyberSec4Europe, explores the governance evolution by the H2020 pilots that reflects finding the ways of (formal) community involvement, and focuses on the role of ECSO in the community development.

With evidence for clear support for bottom-up approach and openness to a diverse set of actors, initiatives and collaborations, the need to have both top-down and bottom-up approaches became clear in the process of research and validation. The conclusion was that the governance model needs to be flexible, oscillating between formal and informal, when it comes to stakeholder engagement, processes, and actions. From our initial model, we concluded in one of the previous deliverables D2.2 that at least two types of CHECK could exist, depending on its financing and business model, for the similar types of services. The main added value of a CHECK-like structure is the capacity to coordinate and orchestrate exogenous and diverse skill resources.

A number of conclusions and recommendations have resulted from the work in this deliverable D2.4 and the related discussions:

- Institutionalize the Cybersecurity Competence Community

It is key that the National Coordination Centres have a systematic approach to registering communities and hubs. With the Regulation providing no guidelines on how possible members, that are not already well networked and informed, should learn about the possibility of application and registration, it is important to develop mechanisms to do so. The benefits and added value for possible members to get acknowledged as members of the Community through the application and registration procedure should be made clear.

- Use CHECKs to organise the Community, in order to address the existing challenges, while providing flexibility

We offer the concept of a collaborative network of local cybersecurity hubs, 'Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs)', which are envisioned as environments for community-level research, innovation, and capacity building in cybersecurity. CHECKs are a bottom-up approach which will not only complement the "top-down" focus from the EU Member States and the ECCC, but can actively contribute to addressing cybersecurity in Europe. Many similar "hub" like structures of communities already exist and we should acknowledge different types and sorts of CHECKs, including those that are created in top-down manner, with the funding from a government. This concept answers concrete stakeholder demands and is based on requirements, empirical best practices, and stakeholder feedback. The existing diversity in the Member States and their connection to the NCCs and to the Community can be integrated through CHECKs (thus resulting in complementary approaches for addressing the same mission).

- No "one size fits all" approach.

There is an important diversity in the national Member States and the connection between authorities / the NCCs / and the communities (thus resulting in differing approaches to addressing the same mission).

- Explore practical implications of community decision-making.

There is a need to improve the process of research transfer to industry. New mechanisms could offer solution, such as collaborative ranking of the assets that are exploitable for the market and thus can receive funding. In combating fragmentation in the cybersecurity domain the existence and promotion

of “communicating vessels” is of paramount importance. Knowledge should flow where it is needed – i.e., it should be transported between the countries and/or sectors to overcome “the cybersecurity divide” of maturity and funding.

- Insensivitize collaboration

Stimulating CHECKs could act as a path towards overcoming organizational divide. Putting new partners in projects is one of the best ways to incentivize collaboration. Controlling mechanisms to accompany the intentions and measuring the results is another important component of collaborative decision-making.
In the NCC and community approach there should be a balance between top-down, bottom-up, peer-to-peer development, methodology and sharing.

- Dedicate funds to capitalize on the existing community connections and networks.

The H2020 pilot projects (CyberSec4Europe, ECHO, Sparta and Concordia) and their focus groups, as well as the European Cyber Security Organisation (ECSO) and its working groups also represent a rich connected community. The majority of relevant stakeholders are involved in the cybersecurity ecosystem through the four pilots and ECSO, forming an ecosystem with different focusses, maturity stages, and objectives. Thus, deep cooperation, coordination and execution must continue with all of the partners and stakeholders involved. Dedicated funds should be provided, e.g. under the Horizon/Digital Europe Programmes, to deepen the cooperation and coordination of such stakeholders, alongside dedicated funds to set up CHECKs in all Member States.

Europe’s cybersecurity potential is not being fully realized due to the existing fragmentation of the cybersecurity landscape and inefficient cooperation and collaboration. One of the ways to overcome the existing fragmentation is by promoting the already existing and functioning structures, especially at the national level, while actively pursuing the aim of a pan-European community through networking. The concept of CHECKs (‘Community Hubs of Expertise in Cybersecurity Knowledge’) as a grassroots bottom-up approach was developed by CyberSec4Europe in the course of the past years as a way to provide additional involvement channels and complement the bodies and organisations set up by EU legislation, namely the European Cybersecurity Industrial, Technology and Research Competence Centre, the National Coordination Centres and their network, and the Cybersecurity Competence Community. These community-level cybersecurity hubs should enable collaboration between industry and academia, bring market security innovations, and help build capabilities in the area by shortening the chain between decision-making and existing needs on the ground. The governance model would benefit from targeted European cybersecurity funding mechanisms in the next decade to build and maintain a pan-European cybersecurity community.

Document information

Contributors

Name	Partner
Mark Miller, Victoria Menezes Miller	CONCEPT
Natalia Kadenko, Michel van Eeten	TUD
Silvia Vidor	UNITN
Antonio Skarmeta	UMU
Afonso Ferreira	IRIT
Aljosa Pasic	ATOS
Jozef Vyskoc	VAF
Christina von Wintzingerode	GUF
Dirk Müllmann	GUF
Siyanna Lilova	TLEX
Marco Crabu	ABI Lab
Christos Douligeris, Christos Grigoriadis	UPRC

Reviewers

Name	Partner
Alessandro Sforzin	NEC
Marko Hölbl	UM
Marko Kompara	UM

History

Version	Date	Authors	Comment
0.01	2022-02-17	Mark Miller, Victoria Menezes Miller (CONCEPT)	ToC
0.02	2022-06-08	Silvia Vidor (UNITN)	Section 3.5
0.03	2022-06-13	Silvia Vidor (UNITN)	Further modifications to Section 3.5
0.04	2022-07-29	Mark Miller, Victoria Menezes Miller (CONCEPT)	Revisions to ToC – distributed draft for contributions
0.05	2022-08-01	Afonso Ferreira (IRIT)	Input to Section 3.2 – France-Toulouse
0.06	2022-08-05	Antonio Skarmeta (UMU)	Input to Sections 2.2.1 and Section 3.8 – Spain and Murcia section
	2022-08-05	Aljosa Pasic (ATOS)	Chapter 2, Section 2.2
	2022-08-05	Jozef Vyskoc (VAF)	Chapter 2, Section 3.7 – Slovakia
0.07	2022-08-11	Christina von Wintzingerode (GUF) Dirk Müllmann (GUF) Siyanna Lilova (TLEX)	Section 2.8, Chapter 4
0.08	2022-08-19	Aljosa Pasic (ATOS)	Update to Section 2.4
0.09	2022-08-22	Christina von Wintzingerode (GUF) Dirk Müllmann (GUF)	Section 3.3 – Germany

Version	Date	Authors	Comment
0.10	2022-08-24	Mark Miller (CONCEPT)	Chapter 5
0.11	2022-09-09	Silvia Vidor (UNITN)	Section 2.7
0.12	2022-09-09	Mark Miller (CONCEPT)	Abstract, Executive Summary
	2022-09-09	Natalia Kadenko, Michel van Eeten (TUD)	Section 3.6
0.13	2022-09-10	Dirk Müllmann (GUF)	Minor edits – Doc History
0.14	2022-09-12	Marco Crabu (ABI Lab)	Section 3.5
0.15	2022-09-27	Aljosa Pasic (ATOS)	Section 5.2 and 6
		Jozef Vsykoc (VAF)	Section 3.7
0.16	2022-10-03	Christos Grigoriadis, Christos Douligeris (UPRC)	Update of Section 2.5
0.17	2022-10-05	Mark Miller/Victoria Menezes Miller (CONCEPT)	Executive Summary, Chapter 5
0.18		Mark Miller/Victoria Menezes Miller (CONCEPT) / Aljosa Pasic (ATOS) Antonio Skarmeta (UMU)	Executive Summary, Chapter 5 Section 5.1 Section 5.3, Section 5.4
0.19	2022-10-11	Christina von Wintzingerode (GUF)	Chapter 4 Section 4.3
0.20	2022-10-18	Mark Miller (CONCEPT)/ Victoria Menezes Miller (CONCEPT)	Full review, full edit, Executive Summary, Abstract, Recommendations / Conclusions, ECSO Section
0.21	2022-10-19	Christos Douligeris (UPRC)	Section 3.4
0.22	2022-10-19	Mark Miller (CONCEPT)/ Victoria Menezes Miller (CONCEPT)	Early Final Draft Review
0.23	2022-10-27	Natalia Kadenko (TUD)	Introduction, Executive Summary, Chapter Conclusions, WP review
0.24	2022-10-28	Christos Grigoriadis, Christos Douligeris (UPRC)	Update of Section 2.5
		Antonio Skarmeta (UMU)	Section 3.8.2
		Victoria Menezes Miller (CONCEPT)	Overall updates, added images to Section 5.2
0.25	2022-11-02	Alessandro Sforzin (NEC)	Review 1
0.26	2022-11-07	Christina von Wintzingerode (GUF)	Update to Chapter 4
0.27	2022-11-07	Christos Douligeris (UPRC) Antonio Skarmeta (UMU)	Edits to Section 2.3 Edit to Section 3.8.2.2. Edit to Section 5.3
0.28	2022	Natalia Kadenko (TUD)	Integrating reviewer 1 comments, resolving formatting issues
0.29	2022-11-23	Marko Hölbl, Marko Kompara (UM)	Review 2
0.30	2022-11-28	Natalia Kadenko (TUD)	Integrating review 2 comments, Chapter 5 restructuring, WPL final review, submission to PC
1.0	2022-11-30	Ahad Niknia (GUF)	Final check, preparation and submission process

This page has been intentionally left blank

Table of Contents

List of Tables

List of Figures

List of Acronyms

A	**ACN**	Agenzia per la Cybersicurezza Nazionale
	AIOTI	Alliance for Internet of Things Innovation
B	**BSI**	Federal Office for Information Security
	BMI	Federal Ministry of the Interior, Building and Home Affairs
C	**CC**	Competence Centers
	CHECK	Community Hub of Expertise and Cybersecurity Knowledge
	CNRS	Centre National de la Recherche Scientifique
	CoMM	Community Maturity Model
	CVCN	National Assessment and Certification Centre
D	**DIH**	Digital Innovation Hub
E	**ECCC**	the European Cybersecurity Industrial, Technology and Research Competence Centre
	ECSO	European Cyber Security Organisation
	EDIH	European Digital Innovation Hub
F	**FITKO**	Föderale IT-Kooperation
I	**ICO**	Institute for Cybersecurity of Occitanie
	IE	Innovation Experiments
	INS21	Institute of Information Sciences and their Interactions
	ISMM	Innovation Services Maturity Model
	ITSMIG	IT Security made in Germany
G	**GDR**	Groupement de Recherche
N	**NCC**	National Coordination Center
	NPCS	Nationale Pakt Cybersicherheit
P	**PEPR**	Programme et équipement prioritaire de recherche
R	**RC**	Regional Clusters
	Regulation	Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres
V	**VCV**	Verwaltungs-CERT-Verbund
W	**WG**	Working Groups
	WP	Work Package

1. Introduction

The European Union has articulated the ambition to maintain its sovereignty and become a global leader in the digital economy, guided by both democratic values and the capabilities to be resilient when 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

The European Commission has set up a Network of National Coordination Centres (NCCs), a Cybersecurity Competence Community and a European Cybersecurity Industrial, Technology and Research Competence Centre. However, many of their options for supporting and developing cybersecurity in the EU, especially related to the community part, have not acquired a specific shape. While the "cybersecurity community" should be composed of all the cybersecurity stakeholders, the design of its governance model is a subject to suggestions and validations coming from pilot projects, such as CyberSec4Europe.

In continuation of the first draft of the governance structure presented in deliverable D2.1, deliverable D2.2 described validation of draft governance model for the community portion of NCC, which has been described in D2.1. This model relies on the concept of a network of Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs). The validation actions took place during 2020 with the ongoing implementation of a prototype "CHECK" delivered in Toulouse, which is called CHECK-T in the further text. Basic postulates and assumptions were validated through a methodology consisting of several steps, such as performing a series of interviews, clustering and analysis of responses and comparison between different approaches. Based on these findings, conclusions were developed targeting policy makers, but also those actors that want to set up new CHECKs at the different level of governance (national, regional and local). Those recommendations were based on practical experience with establishing CHECK-T, but also on additional inputs from other countries, like region of Murcia CHECK, as well as external inputs, for example from the other pilot projects (ECHO, CONCORDIA and SPARTA). The simultaneously developed deliverable D2.3 offered 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 that had been proposed in D2.1, with the main focus being on the development of a detailed governance approach for CHECKs.

This deliverable has further developed the proposed governance structure introduced by Work Package 2 (WP2) of CyberSec4Europe, one of the four pilots initiated by European Commission to test and develop potential network governance designs. Chapter 2 provides the maturity framework for Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs). This framework is an attempt to develop a typology and enable better understanding of different EU cybersecurity innovation ecosystems, whether these are organized in a Digital Innovation Hubs (DIH), CHECK or any other "hub"-like format. In Chapter 3 this deliverable provides detailed overview of the NCC and community development in the partners' Member

States. The selection includes very diverse country-specific situations and serves as a catalogue of best practices and challenges for the NCC and community development. The analysis of the Regulation in Chapter 4 examines the conceptual institutional development of European Competence Centre, NCC network and Community, containing Analysis of Regulation (EU) 2021/887. The Regulation Proposal had been subject to an analysis in D2.1 and the basis for further development of the concept of CHECKs in D2.3. Finally, Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres entered into force on 28 June 2021. This allows for an assessment of the final wording and comparison with the Proposal with a continued focus on the Community governance. Finally, Chapter 5 outlines the different community organization forms, which include updates on the four pilots governance approaches evolution and the Cross-Pilot Governance Focus Group work, as well as ECSO and its role in community organization. Chapter 6 offers conclusions and policy recommendations.

2. Maturity evaluation framework for the Community

2.1. Digital Innovation Hub (DIH) – A comparative analysis, different maturity frameworks

2.1.1. Introduction

The goal of the maturity framework for Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs) is to develop a typology and enable a better understanding of the different EU cybersecurity innovation ecosystems, whether these are organized in a Digital Innovation Hubs (DIH), CHECK or any other "hub"-like structure. We base our framework on a set of flexible criteria, which can be used to develop the maturation strategies and further develop cybersecurity innovation ecosystems. The findings should not be used as a kind of benchmarking, but rather as a tool set to supports the overall cybersecurity ecosystem in Europe.

Different criteria could be identified to create innovation ecosystem types in general, including size, number and type of members, industry sector or specialization in technology (e.g. cybersecurity in industry 4.0 or cloud security), level of centralization and/or involvement of public administration (see D2.2 for conclusions related to CHECK-T and the role of leading actor or initiator).

Many different roles of stakeholders in cybersecurity ecosystems exist, but the leadership roles and description of a central actor can give more insight into the typology. Hub or ecosystem governance is also important, as well as collaboration and partnerships, platform management, outcomes and other issues already reported in D2.1, D2.2 and D2.3.

Maturity criteria are not exhaustive, and others could also have an impact on the functioning and management of the innovation ecosystem, for example external context. These are often predefined and do not depend on the development or maturity stage. Additionally, there is a strong interdependence of the criteria, which needs to be reviewed.

2.1.2. Related Work

The study is based on the literature assessment. The framework reuses some ideas and elements of 7P framework (based on [1] and [2]), for example analysis of the most important parameters for cluster and ecosystem analysis. Several Digital Maturity assessment methods and tools have been recently developed for hubs or ecosystems (note: definitions of these terms have variation), mainly to enable closer insight and eventual benchmarking of National and Regional initiatives. They frequently rely on self-assessment, questionnaires, interviews, success stories and existing reports.

The MIDIH project[3], for example, proposed a 6Ps migration framework for EU industry Digital Transformation (Product, Process, Platform, People, Partnership, Performance (in a socio-economic terms)), which presents some similarities with previously mentioned 7P framework. For each of the area of 6Ps, there is a maturity scale, so in total 6 areas with 5 levels matrices are compiled and evaluated. An interesting result from this project is that two main approaches emerged:

[1] Komorowski, M. (2016). The seven parameters of media clusters: An integrated approach for local cluster analysis. International Journal of Media & Cultural Politics, 12(2), pages 171-191.
[2] Komorowski, M. (2017). A novel typology of media clusters. European Planning Studies, 25(8), page 1-22
[3] MIDIH project website: https://midih.eu/

- Strategy-driven approach, from assessment to implementation, where the first step is a high-level structured method with a set of strategic guidelines along which to conduct the process. This is similar to CyberSec4Europe top-down approach or "government-sponsored CHECKs" where the list of desirable issues comes first.
- Project-driven approach, where the stakeholder joins a hub, such as CHECK, and aims at exploiting the maximum value from its participation and its provided assets (technology, methods, tools, services). It resembles bottom-up approach followed in CyberSec4Europe WP2 that starts with a consultation of stakeholders, stocktaking of available resources and actual context, and an empirical validation of objectives, functions, and other issues.

Another relevant model is coming from 2012 book "The Collaborative Organization" from Jacob Morgan with the emergent collaboration maturity model[4]. However, it is a very basic and generic model, with strict focus on collaboration. The Community Cyber Security Maturity Model[5] is cybersecurity oriented and targets communities to determine their level of preparedness. The model proposes threats to be addressed, as well as metrics, technology, training, and evaluation mechanisms for each of the five levels identified in the model. It targets mainly the public sector in the USA and their operational preparedness, without some aspects that are relevant for the ECCC context, such as R&D. In the same group of models, we can find Community Maturity Model (CoMM)[6] with a focus on communities as a mechanism for organizations to manage knowledge. The model assesses maturity of participation, collaboration, and decision-making, but evaluation and validation are even more limited, within a context of an Alumni association of a French university.

In SmartAgriHubs project, a maturity model for DIHs has been developed[7] with 5 distinct levels of maturity for each service that hub provides. Their Innovation Services Maturity Model (ISMM) helps to identify areas of attention, which is similar to our objective, and helps to structure and share knowledge more efficiently. Another good point is that this model considers the synergies between different tools and organizations for regional innovation and competitiveness, such as competence centers (CC) that can evolve towards a DIH or become part of one, or regional clusters (RC). Research and innovations in agri-food are achieved in the form of Innovation Experiments (IEs), where ideas, concepts and prototypes are developed and introduced into the market, and whose lessons and results can be shared or transferred across DIH or CC in the ecosystem. Finally, there is also a link between increasing DIH maturity and improving the related service offering in community through capacity building, like CyberSec4Europe CHECK objectives.

DIHNET.EU project aimed to create a European network of Digital Innovation Hubs (DIHs). In deliverable[8] it provides a Maturity assessment tool based on a questionnaire for the DIHNET.EU Community. Together with the common approach[9], it serves as a good basis to compare services offered by the DIH (in their context of digitalisation of SMEs and activities related to ecosystem building, financing, testing or digital skills development). It also includes an approach for cross-border technology transfer opportunities or joint cross-border investments due to structured and sustainable collaboration.

Moving to more specific types of DIH, the Alliance for Internet of Things Innovation (AIOTI), issued classification that should serve as a guide to applicants to identify technical and professional requirements

[4] Morgan J, 2013, The Five-Step Maturity Model for Building a Collaborative Organization, https://www.cloudave.com/27679/the-five-step-maturity-model-for-building-a-collaborative-organization/
[5] White, G. (2007). The Community Cyber Security Maturity Model. 99. 10.1109/HICSS.2007.522.
[6] Boughzala I. (2014) A Community Maturity Model: a field application for supporting new strategy building, Journal of Decision Systems, 23:1, 82-98, DOI: 10.1080/12460125.2014.857203
[7] Smart AgriHubs project deliverable D4.1 "Needs assessment report"
[8] DIHNET project Deliverable 2.3 "Maturity assessment Tool"
[9] DIHNET project Deliverable 3.4 "Common Approach for Maturity Assessment"

as an IoT eDIH[10]. They also described specific information on which criteria an IoT eDIH must meet to be a Basic, 1 Star, 2 Stars or 3 Stars IoT eDIH. In the AI field, support to find investments is considered one of the services offering by an AI DIH for strategic and business development and AI maturity technological assessment is considered among the key aspects a Digital Innovation Hub should consider when partnering up with another DIH[11].

Looking at European DIH (EDIH) network, Joint Research Centre (JRC) report[12] is bringing a range of good practices, such as good practices of DIHs offering "test before invest" services, which is very relevant for European DIHs promoted in Digital Europe Programme on and Cybersecurity.

The JRC has also developed a Digital Maturity Assessment [13] which should be used by all EDIHs to measure the progress of the organisations they supported.

2.1.3. Basic Definitions Used in this Framework

Word "network" is mentioned 53 times in ECCC regulation (plus few mentions of related terms). Word "community" is mentioned 70 times, while the word "ecosystem" is mentioned only twice. In Article 4, for example, it is mentioned that "Objectives of the Competence Centre should be contributing to a strong European cybersecurity ecosystem which brings together all relevant stakeholders".

Yet, in discussion among stakeholders in pilot projects of ECCC, as well as among other participants from different projects, the word "ecosystem" seems to be preferred term, when addressing the new multi-level, multi-stakeholder structure created by the ECCC regulation, that spans three different levels: EU, Member States and regional or sectorial layer.

Word "net" and its extension "network", in our context, could refer to both the subject and the object of governance model; we define "network" as "a closely connected group of people, companies, etc. that exchange information". In the context of ECCC regulation, "network" is primarily used for the Network of National Coordination Centres (NCCs), constituted of 27 Centres, one from each Member State (the current list can be found in the National Coordination Centers website[14]).

The term "community" is used for the third layer, where our Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs) are. While a network is characterized by nodes, relationships and topology, community is simply "a stakeholder group that has something in common". We should therefore consider and acknowledge co-existence of different cybersecurity communities and different categorizations of those communities (e.g., by research topic, industry sector, geographic limits, etc.).

In previous deliverables of WP2 we introduced concept of network of communities (e.g., network of CHECKs), that evolves together with the "community of NCCs" in striving to achieve joint value. The existence of many communities and sub-communities, with various degrees of overlapping and interconnections, as well as the existence of related resources (e.g., testbeds, datasets), practices (e.g., awareness building, certification of skills) or technologies, makes an overarching maturity framework rather challenging task.

[10] Alliance for Internet of Things Innovation (AIOTI), White Paper IoT eDIH Network activities, 2020
[11] AI Digital Innovation Hubs Network, Blueprint for cross border collaboration among DIHs, 2020
[12] JRC report, DIH as policy tools to boost EU innovation, 2020
[13] JRC Practical guidelines on the use of the Digital Maturity Assessment (DMA) tool, https://digital-strategy.ec.europa.eu/en/events/webinar-digital-maturity-assessment-tool
[14] National Coordination Centres web site, https://cybersecurity-centre.europa.eu/nccs_en

2.2. Critical Infrastructures and digital supply chains

The goal of this subsection is to enable a better understanding of the criteria that need to be met, in order to further mature cybersecurity strategies for critical infrastructures and digital supply chains. The assessment of maturity for these strategic dimensions is implemented through the 6P framework (Table 1. Critical Infrastructures and digital supply chains
). This methodology is deemed appropriate because it provides the required steps to ensure the proper evolution and scaling of cybersecurity policies and practices within those domains. The applicable maturity levels identified in this framework are: 1) Initial, 2) Managed, 3) Defined, 4) Integrated and finally 5) Exploited.

The model provided in **Error! Reference source not found.** and explained below can be read both horizontally and vertically.

To properly enable the cybersecurity innovation ecosystems of Critical Infrastructures and Digital Supply Chains a specific methodology for each achieved maturity level is assigned to each of the 6P's of the 6P framework:

- **Product**: The maturity phases for products in the critical infrastructure and digital supply chain domains build upon resources such as cybersecurity methodologies, frameworks and technologies that enhance and automate the current security states of the corresponding sectors. It is vital to collect and categorize existing solutions, and then proceed to test them with sample data and distinct use cases that apply in different business sectors. By completing these steps, products can be integrated into the actual infrastructure and monitored to ensure proper functionality.
- **Process**: The maturity phases implemented for processes aim to identify the cybersecurity needs of existing critical infrastructures and supply chains derived from the corresponding threat surface that initiates those risks. As the process matures, generic threats can be identified, categorized, applied in specific sectors, and finally tested on a real infrastructure.
- **Platforms**: Platforms to ensure the security of critical infrastructures and digital supply chains may include technologies such as Automated Risk Assessment tools, Intrusion Detection Systems and Monitoring Software. The maturity phases required for the proper development of those technologies include the design of initial concepts and architectures that address the specific issues for the referenced sectors, the construction of prototypes and sample data testing, real data testing and finally implementation and maintenance on actual infrastructures.
- **People**: People, in this case ,may include Security Officers, Risk Analysts, Vulnerability Analysts and other business sector-specific analysts. As the people vector matures, individual Security Experts working in different environments applying or inventing security solutions may start forming proper questions and groups to resolve them. As a next step those groups can be further integrated into consortiums that will identify open problems, research them, explain them and build solutions that address them. Having a solid network of people, background research and solutions the consortiums can grow and tap into further issues and business domains.
- **Partnerships**: Partnerships play a vital role in securing critical infrastructures and supply chains. A vast cooperation scheme is required, between research (Universities) and market perspectives (companies). The maturity of this vector grows as individuals or small companies form small partnerships that can be extended to cover multiple topics and ultimately reach a state where wide networks of partnerships including a balanced representation of differentiated stakeholders involved in education and training processes exists.
- **Performance**: Performance in the case of critical infrastructures and digital supply chains refers to the level of security achieved by cybersecurity methodologies frameworks and technologies. This vector may mature as quality and performance metrics are researched, implemented and continuously collected from a variety of sources.

The end-goal is to reach the exploited state in each of the vertical layers to properly evolve the cybersecurity innovation ecosystems of Critical Infrastructures and Supply Chains.

2.3. Research

The analysis of the maturity level in research (Table 2. Research) shows clearly that Europe's initiatives, such as the four H2020 pilot projects and the ATLAS platform, are clearly a way forward to facilitate the convergence of the security domain in Europe and increase its digital sovereignty. For this to become a reality, new steps need to be taken in order to identify roadmaps and future challenges but also, by building on the efforts of the four H2020 pilot projects, the ECSO radar, national efforts within the Member States, as well as the ATLAS platform, which brings together resources, knowledge and where relevant interconnecting tools and platforms, are contained in a Cybersecurity Observatory.

2.4. Education

The assessment of maturity in the area of cybersecurity education (Table 3. Education
) is essential to clarify which elements need improvement to achieve the highest possible level of cybersecurity education in Europe. The aim is that of providing graduates and workers with the necessary instruments to implement cybersecurity measures, as well as creating dedicated professional figures. As seen in Table 3, the analysis of maturity focuses on the actors that are specific to the education field (students and educators) but also covers the contribution of additional elements to the overall quality level, such as the use of tools and platforms, or the presence of partnerships between different education- and training-related institutions. While typically the different parameters will be at different levels of maturity in practice, it is important to underline that the model provided in Table 3 can be read both horizontally (as a progression between different levels of maturity) and vertically (as a "maturity scenario").

2.5. Legal

The maturity of the cybersecurity community can also be assessed from a legal perspective (Table 4. Legal
). The sophistication level of aspects like the existence of collaborative networks, institutional cooperation, legal form, governance and exchange of information are different in the development stages of a community and thus give information about the maturity. However, the borders between the different levels from "no community" to "mature community" are fluid. Especially during the development process or before reaching the next maturity level, it is thus possible that single aspects may have already reached the next maturity level while others are still lagging behind.

2.6. Human and Social Dimensions

The assessment of maturity in the area of human and social dimension (Table 5) is aimed at assessing the EU readiness in well-developed networks of diverse, balanced partnership structures prioritizing human and social dimension by design. Currently, despite the availability of a broad range of talent, cybersecurity cooperation in the EU suffers from the lack of dedicated institutions and structures that would facilitate collaboration, as well as from the underrepresentation of certain stakeholders that are important for a sustainable approach to R&D, such as privacy and ethics activists. While there are limitations to applying the 6P framework to human and social dimension, there are benefits of doing so. The goal of this exercise is to include the human and social component not only in the form of diverse human cybersecurity actors' involvement, but also with the view of values and sustainable development of cybersecurity talent.

2.7. Conclusions

In this chapter a theoretical background for the different forms of collaboration was provided, with special attention paid to the “network”, “ecosystem”, and “community”, with the review of existing initiatives, practices, and assessment methods. Understanding the meaning behind and practical use of these terms is an important component of maturity evaluation and, ultimately, in understanding the necessary steps in setting up sustainable cybersecurity community. In order to ensure the proper evolution and scaling of cybersecurity policies and practices within the outlined domains of different maturity frameworks have been considered and applied for diverse aspects of the community maturity evaluation. While this is not a comprehensive guide, the chapter means to offer a toolbox and an inspiration for the structured cybersecurity community setup and development initiatives.

	Parameters	Initial	Managed	Defined	Integrated	Exploited
"Product"	Cybersecurity methodologies, frameworks and technologies that enhance and automate the current security states of Businesses, Organizations, and Supply Chains	Identify needs and develop initial concepts for methodologies, frameworks and technologies from background work.	Initial methodologies frameworks and technologies applied on sample data to test out their functionalities.	Sector-specific use-cases are built and the efficacy of previously tested solutions is evaluated in a detail-oriented manner.	Implementation of the solution on actual infrastructures to ensure their security.	Monitoring the performance of provided solutions to actively identify shortcomings and propose extensions.
Process	Identify the cybersecurity needs of existing critical infra- structures and supply chains and propose solutions that will mitigate current threats.	Identifying generic threats against critical infrastructures and supply chains and the current state of solutions.	Define a framework to categorize threats and to enumerate possible mitigations.	Identifying sector specific threats against critical infrastructures and supply chains.	Implement the framework on real infrastructures.	Continuous extensions of the framework based on the results of the implementation.
Platforms-Technologies	Automated Risk Assessment tools, IDSs, Monitoring Software, vulnerability enumeration tools, policy enforcement tools	Design of Initial Concepts, this can include high-level architecture diagrams. Also inspired by the needs identified in Products on this maturity level.	Prototypes have been built to support the initial threat mitigation approach and tested on dummy data	Prototypes are tested on actual data pulled from pilot infrastructures.	The prototypes become a product that can be integrated as a security solution in critical infrastructures and supply chains.	Wide use of differentiated platforms for the develop-ment of different competences (both theoretical and practical). Development of analytics platforms for performance analysis
People	Security Officers, Risk Analysts, Vulnerability Analysts, Sector Specific analysts	Individual Security Experts working in different environments studying, applying or inventing security solutions.	Security experts form questions and group up in online communities or small partnerships and small research projects to provide security solutions	Businesses, Organizations, Universities and Research Centers observe the security issues and build a stronger framework to work together towards security solutions.	Consortia are built from people coming from various academic and business backgrounds. The consortia then deal with open problems.	The consortia grow by expanding to further people and security threats
Partnerships	To build concrete steps towards securing critical infrastructures and supply chains, a vast cooperation scheme is required, including both research (Universities/Research Centers) and market (companies).	No presence of partnerships	Single- or limited-topic partnerships between few stakeholders already in contact with each other	Multi-topic partnerships between selected stakeholders, online communities, research communities.	Adaptive, ad hoc partnerships between stakeholders from different environments	Presence of wide networks of partnerships including a balanced representation of differentiated stakeholders involved in education and training processes
Performance	The level of security achieved by cybersecurity methodologies frameworks and technologies.	No data/ measurement of quality available	Output of existing solutions when dealing with sample data. A lot of fine tuning is required to deal with real datasets.	Output of existing security solutions are tested with real, sector specific datasets. A further calibration is required	The solutions are integrated and prevent existing threats.	Continuous data feed from integrated security solutions. New threats are recognized and based on anomalies presented in the datasets. Essentially the software autocorrects itself

Table 1. Critical Infrastructures and digital supply chains

	Parameters	Initial	Managed	Defined	Integrated	Exploited
"Product"	Cybersecurity SRIA, Digital Market on cybersecurity solutions	HE and DE program as initial identification of the challenges	Being able to coordinate several national roadmaps	Coordination of different programs	Being able to coordinate national roadmaps and integrated with the European one	Monitoring the results and the impact on the European industry and society
Process	Creation of roadmap, increasing European competitiveness	Identification of challenges and needs	Define a common vision between the community and ENISA	Identification of the different communities needs	ECCC adopt the roadmap as part of the SRIA	Definition of KPIs and target objective at mid term
Platforms-Technologies	European Cybersecurity Framework, ATLAS	ATLAS as starting points	NCC procedures to include member of the community	Extension of the ATLAS ontology to facilitate the brokering	Procedures in place to manage the community and their information	Possibility to use the platform to create new projects, collaboration and synergies
People	Researchers, policy makers, EU officers, ECCC, NCC, ENISA	ATLAS as focus of the community	Inclusion of other industrial areas affected and where security need to be part of the security by design vision	Build a stronger framework to work together towards security solutions	Inclusion of other agents in the society like NGO, entrepreneurs	The whole security ecosystem is involved
Partnerships	Creation of a community, including different stakeholders, interacting with EDIH for bringing to innovation	4 pilots and ECSO	Extension of the community with national partners	Integration of sectorial community	Multiple level communities and a common communication platform	Common platform for the creation of different WG
Performance	The level of security achieved by cybersecurity methodologies frameworks and technologies.	No indicators available	Identification of indicators of the impact of the SRIA in the community and its acceptance	Intermediate evaluation and analysis	The performance is defined through a collection of KPIs	Regular procedures to update the SRIA and provide new challenges based on the performance measures.

Table 2. Research

	Parameters	Initial	Managed	Defined	Integrated	Exploited
"Product"	Students (interest and enrolment)	Self-initiative; students enrol in generic courses available to the wide public (no CFUs)	Seminar; students choose to attend mini-courses on basic topics (few CFUs)	Course(s); students attend full courses on fundamentals (some CFUs)	Degree; students choose to enrol in an educative path fully or mostly dedicated to cybersecurity	Career; students follow a comprehensive and coherent educative path (with practical experiences) in cybersecurity
Process	Coverage of different knowledge units depending on what is considered as a priority by CHECKs in each country	Cybersecurity only as extra topic/no fundamentals	A few fundamentals are covered	Fundamentals mostly covered	Fundamentals and some optional topics are covered	Knowledge units (fundamental and optional) required by CHECKs are covered by the existing career on the topic

	Parameters	Initial	Managed	Defined	Integrated	Exploited
Platforms-Technologies	Use of platforms for cybersecurity education (e.g. cyber arenas)	No use of platforms	A few tools used and taught by educators are available	One platform that students can use to train on basic skills is available	Some platforms for basic skills and technology-oriented needs (not only theory but also practice) are available	Wide use of differentiated platforms for the development of different competences (both theoretical and practical)
People	Educators	Educators are not experienced and do not have in-depth knowledge of the topic at hand	Educators are competent and have had some years of training/experience	Educators have received formal education in cybersecurity, teach courses on specific subtopics	Educators have limited experience in the cybersecurity field, can cover teaching on multiple cybersecurity-related issues	Educators are experienced in cybersecurity and implement both theoretical and practical teaching
Partnerships	Partnerships for education between academia, industry and public institutions (quality + quantity) supported by CHECKs	No presence of partnerships	Single- or limited-topic partnerships between few stakeholders already in contact with each other	Multi-topic partnerships between selected stakeholders	Adaptive, ad hoc partnerships between stakeholders from different environments	Presence of wide networks of partnerships including a balanced representation of differentiated stakeholders involved in education and training processes
Performance	Outgoing student quality (either taking up a job coherent with the education received or continue with their academic career), impact on society of education	No data/measurement of quality available	Outgoing students know the basics and general concepts (e.g. phishing) for office jobs	Selective, specific competences (for existing courses) are covered and acquired by outgoing students	Internships; outgoing students are useful for companies without guaranteed expertise (general knowledge)	Immediate availability of careers on the topic after education/certified curricula guarantees competence for certain needs and impact on society

Table 3. Education

	No community	Evolving community	Advanced community	Mature community
Collaborative Networks	No collaboration despite awareness of existing stakeholders.	Cooperation / collaboration: Single or case by case cooperation or collaboration on punctual topics, involvement of very few stakeholders, regional or national level.	Coordinated cooperation / collaboration: Adaptive and *ad hoc* partnerships driven from supply side in search of business opportunity, engaged in joint projects and initiatives within simple sub-structures. Occasional partnerships or collaborations with broader range of stakeholders and the other hubs/CHECKS within EU regional level.	Dynamic cooperation / collaboration: Collaborative, multi-dimensional and multi-disciplinary partnerships with stakeholders from different groups. Partnerships or collaborations with other hubs and/or CHECKs, EU-wide level and beyond.
Institutional cooperation	No cooperation with the NCC or the Cybersecurity Center.	In the process of formation as a CHECK but no official recognition as a Cybersecurity Community member. Occasional cooperation with Network of NCCs institutions.	Registered member of the Cybersecurity Community. Contractual agreements in place for establishing the relationship with the Competence Centre and the local NCC(s). Mostly case-by-case and *ad hoc* meetings with Network of NCCs institutions.	The process of admitting additional members is transferred from the Competence Center to accredited founding members. Regular meetings by appointed members with representatives of the local NCC(s) and the Cybersecurity Center. Strategies in place for long-term collaboration with Network of NCCs institutions.
Legal form	No legal form.	Informal relationships with no contractual basis.	Contractual relationships (MoU, single contract or framework agreement).	Separate legal entity, possibly with its own staff.
Governance	No regular meetings or procedures in place.	Informal meetings of designated organizational representatives. Activities and responsibilities are determined *ad hoc* without formal procedures.	Basic rules of procedure and policies are in place. Responsibilities, activities and roles of the members are contractually agreed upon in each case.	Inner governance structure determined by the type of legal entity, supplemented by detailed policies and rules of procedure. Types of membership, roles, rights and obligations of members are determined and formalized.
Exchange of Information	No sharing of information.	Limited sharing in closed community, i.e. within the same group of stakeholders. Exchange of information is still informal and mostly upon (single) request.	Readiness to reach out to other stakeholders / next-level stakeholders / existing platforms. Meetings and sharing of information either upon request or under a contractual obligation. Formal or informal procedures in place to address competition issues.	Open data / sharing by default procedures in place (unless data is confidential, personal, or commercially sensitive). Designated portal for information exchange / joint searchable database. Formal procedures in place to address competition issues.

Table 4. Legal

	Parameters	Initial	Managed	Defined	Integrated	Exploited
"Product"	Integration of human and social perspective in cybersecurity	No acknowledgement of the importance of integration	Acknowledgement in individual research output	Acknowledgement at the EU level, institutional initiatives	Diverse inputs from the Pilots and other EU Entities	Systemic institutional EU support of the relevant projects
Process	Identifying the needs and existing gaps	Initial awareness	Providing basic framework through Digital Services Act, Digital Market Act	Providing support to the relevant projects on human and social dimension in cybersecurity	Providing both general integration guidelines and support to specific projects on PET, raising awareness, and other relevant initiatives	Structural framework for integrating human and social dimension into cybersecurity initiatives and projects at various levels
Platforms-Technologies	Use of platforms for collaboration to ensure cohesion	Fragmented efforts	Activities of H2020 Pilots and ECSO	Cross-Pilot collaboration	ECCC in collaboration with ENISA and other relevant actors, NCCs and Competence Community, relevant EU bodies and agencies	Systemic collaboration of CCCN structures and relevant EU bodies, new initiatives to address identified challenges
People	Researchers, policy-makers, civil society activists, other stakeholders	limited involvement (volunteering, fragmented projects and initiatives)	Semi-structured involvement and contacts through various semi-formal channels and ad hoc platforms	Involvement in a platform organization with limited mandate	Coordinated involvement in several (sectorial) platforms	Work together as a part of cybersecurity community through diverse inter-connected platforms. tools easily available to ensure cooperation
Partnerships	Partnerships between academia, industry, civil society activists, and public institutions	No partnerships	Limited partnerships based on pre-existing contacts	Project-based partnership	New partnership formed with awareness of social and human dimension, involvement of underrepresented stakeholders	Well-developed networks of diverse, balanced partnership structures prioritizing human and social dimension by design
Performance	Research output on privacy and ethics, establishment of relevant initiatives	Fragmented research output	EU efforts to establish expertise in human and social sciences for cybersecurity	Relevant program documents	Identified research priorities and support to the relevant projects	Established Ethics Focus Groups, EU support for research cycle

Table 5. Human and Social Dimensions

3. NCCs and CHECKs: Monitoring the situation as it develops

3.1. Current situation

CHECKs were developed from the "grassroots" level within the context of the CyberSec4Europe project, with the intention to build the community from the ground up, based on stakeholder demands and initiatives. The NCCs clearly present the opportunity to capitalize upon the existing CHECKs structures representing communities that already exist. In this chapter we describe both the existing CHECKs as well as the NCCs in detail, looking at how these have developed and what is possible within the current construct and concept.

3.2. France -Toulouse

The creation process of the first CHECK-T as described in D2.3 could not be finalised in time for inclusion in this deliverable. Several factors were at play that precluded its establishment, the most important being the lack of interest from the NCC to spearhead such local hubs so far while uncertainty existed about the NCC's own setup and functioning.

However, we feel that our clear vision for CHECKs inclusion in the cybersecurity ecosystem, namely, to connect the stakeholders and the Community on the one hand and the NCC on the other in order to avoid gaps in the network, is still valid and may come to fruition eventually, originating from one of the several undertakings that exist in France, as described in the following.

- A new programme stemming from the EU Recovery funds. In France it gave rise to the Programme et équipement prioritaire de recherche (PEPR), which disbursed 65 Million Euros for seven French research projects in Cybersecurity. The Research Ministry has the intention to ask these projects to animate their French cybersecurity community.
- The Institute for Cybersecurity of Occitanie (ICO). This is a four-year project funded by the Région Occitanie under its Key-Challenges Call for Projects. It's hosted by the CNRS and includes all public-research actors in Occitanie. Because of this, it could represent a seed for a future CHECK, in particular, because UPS-IRIT members are co-leading such an initiative.
- The Groupement de Recherche (GDR) Sécurité Informatique of the CNRS. This is an instrument facilitating French research, created by the Institute of Information Sciences and their Interactions (INS2I) of the CNRS, and open to the entire community. The topics covered by the GDR include coding and cryptography, formal methods for security, protection of privacy, security of systems, software and networks, security of hardware systems, security and multimedia data. This GDR is a long-running community structure that has animated the national community for more than a decade.

The tables below summarise such initiatives.

Title: PEPR	Launched: June 2022
Location: Nationwide	Website: https://www.cnrs.fr/fr/presentation-de-la-strategie-nationale-cyber-7-projets-retenus-dans-le-cadre-du-programme-et
Structure: Several projects	
Strengths: Large funds	
Challenges: Project-based; six years	

Table 6. Summary of PEPR

Title: ICO	Launched: September 2021
Location: Occitanie Region	Website: https://www.ico-occitanie.fr/
Structure: Several projects	
Strengths: All public-research actors in the Region	
Challenges: Project-based; four years. Only public-research actors	

Table 7. Summary of ICO

Title: GDR Sécurité Informatique of the CNRS	Launched: Many years ago,
Location: Nationwide	Website: https://gdr-securite.irisa.fr/gdr/
Structure: Distributed community of researchers with activities coordinated by a Bureau	
Strengths: Very large research base in France. Address list.	
Challenges: Fully distributed. Funded by the CNRS. Not meant to function as a CHECK	

Table 8. Summary of GDR

3.3. Germany

Currently, there are no efforts in Germany to cooperate according to the CHECK model. The communities are organized on a decentralized basis in various associations. The "European Cyber Security Competence Center" (ECCC) is currently consulting with the co-chairs of the relevant working groups on possible forms of community participation in accordance with Article 8 (1) of Regulation 2021/887.

Since 2021, in Germany only the "National Coordination Center for Cybersecurity in Industry, Technology and Research" (NKCS) exists as a part of the competence network according to Art. 8 (1) 2021/887 Regulation. At present, the NKCS is still in the process of being established. It is busy gaining an overview of the situation regarding cybersecurity projects to put itself in the position to recognize and exploit synergy effects. Later, among other things, funding programs are to be awarded.

Apart from this, there are many other IT security projects for the community that are geared towards information exchange and networking. The following list is intended to provide an overview of the most important players without claiming to be exhaustive.

3.3.1. Actors at federal level

"UP KRITIS" is one of the first projects of the German cybersecurity community and aims at information exchange and networking between operators in the field of critical infrastructure.[15] The public participant is the Federal Office for Information Security (BSI), where the NKCS is also located.

The *"Nationale Pakt Cybersicherheit"* (NPCS) has been in existence since 2019 and aims to find and bundle various stakeholders who are committed to cyber security in Germany.[16] The groupings can include all organizational forms, such as associations, initiatives from business and science, or government agencies. The NPCS was launched on the initiative of the Federal Ministry of the Interior, Building and Home Affairs (BMI) and can be understood as Germany's contribution to the "Paris Call for trust and security in

[15]https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/UP-KRITIS/up-kritis_node.html (last 21.08.2022).

[16] https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/nationaler-pakt-cybersicherheit/nationaler-pakt-cybersicherheit-node.html (last 21.08.2022).

cyberspace" published in 2018, through which Germany, together with 73 other countries, has committed itself to cooperation in favour of responsible behaviour in digital issues.

The NPCS exchanges information with the “Bündnis für Cybersicherheit” (“Alliance for Cyber Security”), which was also founded by the Federal Ministry of the Interior in 2018 and acts as an information exchange and cooperation platform between the ministry and the Federation of German Industries[17]. The focus here is on strengthening German industry and protecting Germany as a business location against digital attacks. In addition, cybersecurity projects are to be identified and reviewed via this channel to obtain a comprehensive overview of existing initiatives and alliances.

Since 2018, a similar task has been performed by the *"Cyber Security Cluster Bonn"*, an association with representatives from business, politics and research that aims to bundle competencies in the IT security sector. Its declared goals include the deepening of knowledge and the exchange between members[18].

The *"IT Security made in Germany"* (ITSMIG) working group also awards a seal of trust for IT security products that meet a certain standard (this includes, for example, a headquarters in Germany, no hidden "backdoors" and compatibility with German data protection law) and presents such products to participating companies and stakeholders from politics, business, and science.[19] This working group was founded in 2005 by the BMI and the Federal Ministry of Economics and in 2011 was incorporated into the international competence network Bundesverband IT-Sicherheit e.V. (*"TeleTrusT"*)[20].

The Federal Ministry of Economics and Climate Protection also supports and raises awareness of IT security issues among small and medium-sized enterprises in particular through the *"IT-Sicherheit in der Wirtschaft"* initiative[21]. This is done through funding and the support of projects, website CHECKs, action guides or by providing training and teaching materials. The aim of the initiative is to promote new technologies, such as the use of AI, more quickly through better security concepts in companies[22].

A similar but broader approach is taken by the *"Initiative Wirtschaftsschutz"* of the four security agencies BfV, BKA, BND and BSI, which provide information and expertise for German commercial enterprises[23]. To this end, the government agencies cooperate with various business associations[24]. Combating cybercrime and providing information on cybercrime is an important part of this.

3.3.2. Actors at the state level

Due to the federal state structure, there are also numerous actors at the state level, some of whom act alone and some of whom act on a cross-state basis.

In the *"Sicherheitskooperation Cybercrime"*, the state criminal investigation departments of Baden-Württemberg, Hesse, Lower Saxony, North Rhine-Westphalia, Rhineland-Palatinate, and Saxony have

[17] https://bdi.eu/artikel/news/industrie-und-innenministerium-etablieren-buendnis-fuer-cybersicherheit/ (last 21.08.2022).
[18] https://cyber-security-cluster.eu/ (last 21.08.2022).
[19] https://www.teletrust.de/itsmig/ (last 21.08.2022).
[20] https://www.teletrust.de/ueber-teletrust/ziele-und-nutzen/ (last 21.08.2022).
[21] https://www.it-sicherheit-in-der-wirtschaft.de/ITS/Navigation/DE/Ueber-uns/Initiative/initiative.html (last 21.08.2022).
[22] https://www.it-sicherheit-in-der-wirtschaft.de/ITS/Navigation/DE/Ueber-uns/Initiative/initiative.html (last 21.08.2022).
[23] https://www.wirtschaftsschutz.info/DE/Home/home_node.html (last 21.08.2022).
[24]https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Wirtschaftskriminalitaet/InitiativeWirtschaftsschutz/initiativeWirtschaftsschutz_node.html (last 21.08.2022).

joined forces with the digital industry association "Bitkom" to put a stop to cybercrime by combating and preventing it.[25] To this end, the cooperation offers, among other things, training courses and a central cybercrime contact point.[26]

More than 40 different IT security teams from various federal and state authorities, as well as some companies, have joined forces to form the *"Nationalen CERT-Verbund"* to exchange information on improving operational security.[27] Only German teams are included[28]. In addition, the CERTs (Computer Emergency Response Teams) of the public state administration have joined forces with the *"CERT-Bund"* to form the *"Verwaltungs-CERT-Verbund"* (VCV).[29]

The *"Föderale IT-Kooperation"* (FITKO)[30] does not focus specifically on security but serves to improve the networking of the various digitization projects of public administration in Germany. It is an independent institution under public law based in Frankfurt am Main and was founded in 2020.

3.4. Greece

The General Directorate for Cyber Security (also known as the National Cyber Security Authority - NCSA) of the Ministry of Digital Governance was nominated on July 2022, by Law 4961/2022, as the Hellenic National Coordination Centre, thus acquiring all relevant responsibilities ensuing from the 887/2021 EU Regulation. Indicatively, those responsibilities include: The promotion, encouragement and facilitation of the participation of national stakeholders in international projects and in activities arising from the Competence Centre, the Network and the Community.

- The establishment of synergies with actors at the national level in order to implement activities in the area of cybersecurity, such as promoting and disseminating cybersecurity educational programmes.
- The contribution to the implementation of specific actions for which grants have been awarded by the Competence Centre.

The General Directorate for Cyber Security was already engaged with relevant ad-hoc activities, so being nominated as the National Coordination Centre was the next level of maturity. To enforce its capacity in managing European funds, additional units of the Ministry of Digital Governance (i.e. the Special Managing Authority of the Digital Transformation Programs) are called forth to manage, program, and support the implementation of activities that are funded by the ECCC.

After the incorporation of the NIS Directive into the Greek legislation by the end of 2018 (Law 4577), the General Directorate for Cyber Security has also been the designated National Authority for Cyber Security. As such, the Directorate has identified Greece's Operators of Essential Services (OESes) and has set up a national CISO network through which communication is facilitated between the Operators and the Authority (Ministerial Decree 1027). The CISO network has proven to be an essential tool for disseminating and gathering useful information to the mutual benefit of the OESes and the Authority. Indicatively, through the network, the Authority successfully disseminated funding opportunities and supported the formation of joint proposals that aimed to enhance the cybersecurity capabilities of the participants. The CISO network also

[25] https://www.bitkom.org/Sicherheitskooperation-Cybercrime/Ueber (last 21.08.2022).
[26] https://www.bitkom.org/Sicherheitskooperation-Cybercrime/Schuetzen (last 21.08.2022).
[27] https://www.cert-verbund.de/index.html (last 21.08.2022).
[28] https://www.cert-verbund.de/Gruende_CV.html (last 21.08.2022).
[29] https://www.cert.sachsen.de/kooperationen-4067.html (last 21.08.2022).
[30] https://www.fitko.de/ueber-uns/wer-wir-sind (last 21.08.2022).

made it possible to gather information on the cybersecurity needs of the OESes assisting the authority to better focus its supporting and community building activities.

Apart from the CISO Network the Authority, since the latest definition of its structure in 2020, established dedicated internal units to further support coordination and capacity building activities and promote the development of a network that includes national, European and international authorities relevant to cybersecurity. As such, connections are already in place with main cybersecurity national bodies (i.e. the National CERT, the Cyber Defence Directorate of the Ministry of Defence and the Cybercrime division of the Hellenic Police, etc) and other relevant stakeholders (i.e. universities, research centers, agencies, etc). Additional focus is being given to the planning and implementation of awareness raising activities and training programmes that target not only the general public but also professionals in the cybersecurity field. Thus, the Authority is already in collaboration with national academic institutions and authorities responsible for raising awareness at the national level.

Furthermore, the Authority already participates as a partner in international actions for which grants have been awarded by the European Union. Indicatively, it is one of the three public bodies participating in the CONCORDIA research project that is funded with 16m€ by the HORIZON 2020 program. The purpose of this project is to prepare the linkage between the European cybersecurity competences in order to facilitate the activities of the ECCC. The consortium consists of more than 51 partners, mostly from academia and industry, originated from more than 20 Member States. Some of the contribution of the Authority to CONCORDIA project was in assisting the formation of the relevant stakeholder community and in disseminating the project results.

All the above initiatives agree with the National Cybersecurity Strategy, which was issued by the end of 2020. In the strategy, sound cooperation between the Public and Private sectors is recognised as a critical factor in achieving a high level of cybersecurity and thus a strategic goal is set to enhance the cybersecurity investments environment with emphasis in the promotion of research and development. Relevant strategy actions include:

- The promotion of networking for the implementation of innovation in the field of cybersecurity (e.g. technology parks, innovation complexes).
- The development of enhanced cooperation with academic and research institutions in cybersecurity issues.
- The establishment of a program partnership with relevant national authorities, through which private companies will be facilitated to provide secure services to the public sector via Public-Private Partnerships (PPPs).

In addition, the strategy defines as a strategic goal the continuous and effective support of capacity building and awareness raising activities in order to maintain a high level of awareness of all participants in the National Cybersecurity Ecosystem.

It is important to note that the approved Cybersecurity reform fiche of the National Recovery and Resilience Plan, which was signed in 2021, supports the implementation of the cybersecurity strategy. Notably, it incorporates a series of measures for the compliance of national public and private entities with the EU framework and obligations derived, among others, from the participation to the EU Cybersecurity Competence Network and Centre. Another key action is the definition and implementation of Research, Development and Innovation priorities in the field of cybersecurity with a focus to the security of contemporary technologies, where the Digital Innovation Hubs (DIHs) are anticipated to be utilized in the process. Furthermore, additional actions will support the implementation of capacity building initiatives and the communication/awareness strategy.

Since NCSA has been recently assigned as the Greek NCC, and is currently in a recruitment process to cover its additional needs, there is currently no planned action on implementing a structured CHECK framework.

3.5. Italy

3.5.1. The National Coordination Centre

The National Coordination Centre, nominated by the Government of Italy and led by Mario Draghi, is the Agenzia per la Cybersicurezza Nazionale (ACN, translated as "National Cybersecurity Agency"), instituted within Law Decree 82/2021 on the 14th June 2021[31].

The ACN is the Italian national cybersecurity authority, tasked with the protection of Italian cyberspace. Its main functions, as described in L.D. 82/2021, include:

- implementation of the Italian and European cybersecurity strategies;
- promotion of a coherent regulatory framework in the cybersecurity sector;
- inspection and sanction functions (in collaboration with the Italian Data Protection Authority);
- support of public and private entities for the prevention and mitigation of cyber incidents, as well as the restoration of systems after attacks have taken place;
- implementation of public-private initiatives to strengthen Italian and European cybersecurity resilience;
- focus on Italian and European strategic autonomy in the digital sector;
- development of training courses for the workforce and promotion of awareness campaigns to foster cybersecurity culture[32].

The ACN also brings, under a single institutional body, the operation of several other cybersecurity-related structures which were previously dispersed under different Ministries and institutions, such as the Italian Computer Security Incident Response Team (CSIRT) and the Centre for National Evaluation and Certification (previously under the Ministry of Economic Development)[33].

There is, at the moment, no available information concerning the development of the Italian Cybersecurity Competence Community. This is due to the fact that the ACN is still currently in a phase of recruitment (which is planned to continue until 2023) and establishment within the Italian cybersecurity panorama.

As the National Cybersecurity Authority, the Agency has, among its tasks, that of developing the National Cybersecurity Strategy. Furthermore, pursuant to the aforementioned Law Decree, ACN is designated as the exclusive competent national authority and single point of contact (PoC) for the purposes referred to in the legislation on the security of networks and information systems (NIS), national cybersecurity certification authority, National Coordination Centre with reference to the European Cybersecurity Industrial, Technology and Research Competence Centre, and central element of the National Security Perimeter for Cyber (PSNC). These competences were previously attributed to a plurality of institutional actors.

31 https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2021-08-04&atto.codiceRedazionale=21G00122&elenco30giorni=false

32 https://www.acn.gov.it/strategia-nazionale-cybersicurezza

33 https://www.cybersecitalia.it/a-cosa-serve-lagenzia-per-la-cybersicurezza-nazionale/12621/

The creation of ACN aimed at systematizing the experience gained in the previous five years of work, under the framework of the Prime Ministerial Decree of February 17, 2017 "Directive containing guidelines for national cyber protection and IT security", as well as that acquired by other countries, by recognizing cyber security and resilience as autonomous, placing them under the Prime Minister's responsibility and at the basis of the Country's digitization process, also through a broader role of coordination and close synergy with all competent Administrations. It was therefore defined a further pillar assigning it to a single government entity which supplements those already existing on cybercrime prevention and countering (within the duties of National Police), military defence and security of the State in the cyber domain (pertaining to the Ministry of Defence) and intelligence (under the responsibility of the Intelligence community). This in order to ensure the coherence of initiatives, the efficiency of spending, the ability to provide a clear and updated situational awareness to the political Authority, as well as to identify a single interface in charge, in compliance with the competences attributed by the legislation in force to other Administrations, of the coordination between the public entities involved on cyber security and resilience matters, also to guarantee a common national posture consistent with cybersecurity and resilience policies defined by the Prime Minister in international fora.

The National Cybersecurity Strategy is accompanied by an implementation plan which indicates for each goal defined in the National Cybersecurity Strategy – namely protection, response, and development – the measures to be put in place for its achievement, organized into thematic areas. A list of the entities responsible for their implementation, as well as other interested parties – for which reference has been made to the following paragraph on the national governance – is provided for every measure, without considering those who, directly or indirectly, benefit from the resulting effects.

At the moment, the National Cybersecurity Agency (ACN), together with the Dipartimento per la Trasformazione Digitale (DTD), will steer the enforcement of the investment by fostering synergies and interconnection across the Public Administration, the industry and the technology service providers.

The objective of the investment through the "PNRR" is to strengthen the national digital ecosystem by enhancing cyber threat monitoring and management services. Thus, capabilities to monitor, prevent and respond to cyber risks and events will be significantly strengthened through a national cyber services network, appropriately integrated with key public and private partners.

In this regard, the ACN is specifically working in order to build interventions for the Public Administration to protect citizens' data and services, following the set-up of the National Cybersecurity Services and the activation of the network of assessment and certification laboratories under the supervision of the Center for National Assessment and Certification (CVCN). Finally, the ACN is also currently in a phase of recruitment (which is planned to continue until 2023) and establishment within the Italian cybersecurity panorama.

3.5.2. The evolution of the national cybersecurity legislation

To face the increased interconnection and interdependence between IT systems and their related threats, both the EU and Italy adopted some legislation in continuous evolution.

In a nutshell, during the last five years, Italy has adopted the following acts and regulations on cybersecurity:

- Prime Minister's Decree (DPCM) of 17 February 2017, which updated the national cybersecurity architecture established by DPCM of 23 January 2013;
- Legislative Decree of 18 May 2018, no. 65 (thereafter "NIS Decree"), which provides for an obligation upon Opera- tors of Essential Services and Digital Services Provides to both notify cyber

incidents having a relevant impact on service continuity and implement security measures based on risk assessment;

- Law Decree of 21 September 2019, no. 105 (thereafter "Perimeter Decree"), which established the National Security Perimeter for Cyber, with the aim of protecting digital assets from malfunctioning, interruption, also partial, or improper use of which may determine a prejudice for national security. It provides, compared to the NIS Decree, for stricter criteria on incident notification and higher security levels, also for the supply chain, as well as specific procedures for procurement of ICT intended to be used on such digital assets;
- Law Decree of 18 July 2020, no. 76, which moved forward digitalization of the Public Administration, providing that such digitalization shall happen in compliance with network and information security principles, including workforce's professional development and promotion of the awareness on the importance of network and information security;
- Law Decree of 14 June 2021, no. 82, providing for urgent provisions on cybersecurity, definition of the national cybersecurity architecture and establishment of the National Cybersecurity Agency;
- the Italian Cloud Strategy, adopted in the context of the triennial plan for ICT in the Public Administration for 2020-2022 and defined by the Department for digital transformation in collaboration with the National Cybersecurity Agency, with the aim of encouraging the use of solutions based on cloud computing by the Public Administration;
- Legislative Decree of 8 November 2021, no. 207, implementing the Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code. It provides, among others, for cybersecurity requirements for public electronic communication networks or for publicly accessible electronic communication services, the obligation to notify significant cyber incidents, as well as the adoption of cybersecurity measures, attributing the competence on the subject to the National Cybersecurity Agency;
- Law Decree of 21 March 2022, no. 21, which provides, among others, for the redefinition of the exercise of special powers on electronic communication services based on 5G, as well as on other services, goods, relations, activities and technologies which are relevant for cybersecurity, including those related to cloud technology. Specifically, it redefined the obligations and notification procedures by interested companies as well as the procedures for the exercise of the special powers, the monitoring and sanctioning by the Government, establishing the participation of the National Cybersecurity Agency, the possibility of using the National Assessment and Certification Centre (CVCN) and the carrying out of inspection and verification activities.

3.6. The Netherlands

Over the past three years, the community around research and innovation in cybersecurity has been reshaped and is now consolidating into a new structure. About 10 years ago, several government ministries funded a platform organization to bring together cybersecurity researchers from various disciplines, though with an emphasis on computer science, and representatives from businesses and government. This organization ended up being called "dcypher": Dutch cybersecurity platform for higher education and research. It was manned by employees from the National Research Council (in Dutch: NWO), the Dutch funding agency for scientific research. These employees were seconded to dcypher. The organization only had a budget of several hundred thousand euros to support these seconded staff, most notably the director and communication specialist, and some yearly networking events. There was no funding for actual research or innovation.

The platform organization had a mandate for a limited term of several years. When the end of the term approached, a complex process emerged where various ministries disagreed about how to proceed further. Since the area of cybersecurity research and innovation had actually lacked consistent funding, a critical part of the struggle and puzzle was how to achieve more structural funding. The main funding instruments

on the horizon were innovation subsidies, which were allocated by the government for a variety of sectors. These funds, and the associated instrument, were set up under the auspices of the Ministry of Economic Affairs. Given the central role of funding for the platform and the community, this means that the Ministry had a critical vote in the future of the platform.

For a variety of reasons, the Ministry decided that dcypher was not the platform for the future. The main concern was the lack of valorization of research into innovations in the market that dcypher had achieved. This critique was a bit disingenuous, since dcypher had neither the mandate nor the funding to achieve valorization. Rather than trying to reform dcypher, the Ministry decided to terminate the organization, despite protests from academics and business people in the community. The decision seemed partially motivated by the fact that the dcypher was tied to NWO, which made it, in the eyes of the Ministry, too focused on academic research.

The Ministry then set up a new platform organization, partially with input from people in the community. The organization is independent but hosted by RVO, which is an agency of the Ministry that administers subsidy programs for businesses. It is more costly than the old dcypher by virtue of having more personnel, including innovation managers.

The new platform is governed by the board that consists of several representatives from government and industry (both in terms of producers and users of security innovations), one representative for the universities, one for the polytechnical schools and one for TNO. (TNO is an independent research organization set up by law that is neither part of any university, nor of the government, but that does receive large structural funding from the government.) The board decided to adopt the name of the old platform: dcypher.

The idea of dcypher is to bring together and bundle the existing funding instruments that were fragmented across many different ministries with private investments around priority areas in cybersecurity research and innovation. The funding should cover the whole range of Technology Readiness Levels (TRLs). Given that dcypher has only been operating for about two years, it cannot really be evaluated whether it can realize this ambition. That said, in its first two years it only managed to bring into life two small programs, e.g., around automated vulnerability research, that was funded solely by the Ministry of Economic Affairs.

Next to dcypher, the Ministry has set up another different organization that will function as the Netherlands national Center in the NCC network that the European Commission is setting up. This Center is also hosted by RVO. The ministry argued that dcypher could not take on this role, since the center will have to allocate subsidies, which means it has to be a fully public entity.

Given that the academic community has only a very limited presence in the new dcypher organization, and the community did not include many members of the community that was tied to the old dcypher, a large number of academics decided they needed their own network organization, not to compete, but to complement, the new dcypher. They founded the Academic Cyber Security Society (ACCSS). Legally it is an association that is funded, at this point, by institutional and individual academic memberships.

Given that these developments happened over the past two-three years, it is hard to evaluate the current arrangement. It is a strength of the new platform that it is independent and has representatives from across all TRLs. In principle, it could foster organic coordination across the triple helix of government, industry and academia. The platform also has low entry barriers. At least in its current form, participation is not tied to substantial membership fees. The platform has potential to function like a Dutch CHECK.

Yet, there are also weaknesses to the new structure. While the platform itself is well-funded, it has no funding for research and innovation funding. This needs to come from participants in the platform. The idea

that dcypher would bring together existing fragmented funding instruments into larger programs is sound, but it is very unclear whether this ambition will be realized. Even if it is, the new structure is still struggling with very limited current funding for research in those instruments. A report from community members has pointed out that the current funding is nowhere near enough to reach the stated ambitions of the government. The government will have to commit substantial resources or drastically curtails its ambitions. Neither option has been chosen so far. If nothing happens in terms of funding, then at some point, the unspoken de facto decision will end up being that the ambitions are basically abandoned.

3.7. Slovakia

Currently there is no visible CHECK-like activity in the Slovakia. It appears that the only association of legal entities aimed at cybersecurity area in Slovakia is the Cybersecurity cluster[34] co-funded by the European Regional Development Fund 2014-2020. As of now it is focused at awareness raising through organizing conferences, workshops and education activities at secondary schools.

Slovakia has an NCC established. Formally the role of the NCC is assigned (by Act No. 69/2018 Coll on cybersecurity) to the National Security Authority which has delegated this task to the Cyber Security Competence and Certification Center[35] which also administers the NCC web[36] (unfortunately the web site is currently only available in Slovak).

3.8. Spain

Once the decision on defining the NCC around INCIBE's organization was taken, most of the work is still continuing in the formalization setup of the center and the preparation of the different activities to be carried out.

Several meetings were agreed upon between INCIBE and the Spanish partner of the 4 pilots in order to discuss the different models of governance identified by the four pilots. Furthermore, INCIBE representatives were invited to a Panel discussion at the Third CyberSec4Europe Convergence Event which took place, in Brussels, from June 2-4, 2022, and during which INCIBE had the opportunity to express their work and ideas.

For the time being, there is no a formal statement from INCIBE on how the community at the national level will be structured although their point of view is to rely on the actual national initiatives and the collaboration defined in the context of the Foro Nacional de Ciberseguridad (National Cybersecurity Forum)[37]. This Forum is part of the cybersecurity structure within the framework of the National Security System, together with the National Security Council, the National Cybersecurity Council, the Permanent Cybersecurity Commission, as well as the competent Public Authorities and the national reference CSIRTs. In this context, research centers and industries are also represented in the different working groups created.

3.8.1. CHECK - Murcia

In the Murcia Region, an evolution of the previous work on CHECK is under evaluation based on the possibility of the Recovery Funds strategy in Spain.

[34] https://clusterkb.sk/en/about-us#s0
[35] https://cybercompetence.sk/en/
[36] https://kyberkomunita.sk/
[37] https://foronacionalciberseguridad.es/

The idea is to agree with other regional government offices on the definition of a Regional Network of Innovation and Competencies in Cybersecurity (RC3).

The importance of cybersecurity at the European, and therefore national level, has been highlighted with the pan-European definition of a structure made up of the ECCC (EU Cybersecurity Competence Center and Network), as well as the network of mirror centers at the national level formed by the network of National Coordination Centers (NCC).

Within this structure, a key component is the community of cybersecurity skills, which are composed of active participation from industrial, academic, administrative agents and society in general which contribute to identifying and advising on strategies.

It is proposed that, following the structure proposed at the European level, a regional Cybersecurity Innovation and Competences network can be set up, made up of regional nodes or hubs that are in charge of integrating the competences and knowledge in the field of cybersecurity to develop a series of innovation policies and strategies in cybersecurity in the field of regional competences among them, in particular:

- Coordinate with the Center National Coordination Centers.
- Contribute to the wide deployment of the latest cybersecurity technology, in particular through pilot projects.
- Support research and innovation based on a comprehensive research and industry agenda, and large-scale demonstration in next-generation cybersecurity capabilities.
- Promote high cybersecurity standards not only in cybersecurity technology and systems, but also in skills development.

These centers must also establish different Working Groups (WG) in order to organize the regional community of competences. Within the framework of these Working Groups, the lines of action are designed for the full use of the technologies and activities that are developed in the node/hub.

Examples of such Working Groups are:

- Training working group.
- Strategic and Technological Working Group
- Demonstrations working group
- Coordination Working Group with the network of centres.

In the concrete case of Murcia, the idea is to create a MURCIA-CHECK Regional Cybersecurity Unit.

The Regional Cybersecurity Unit will be established as a reference center in cybersecurity within the framework of the Agenda for the Digital Transformation of the Administration and Society in the Region of Murcia to promote the role of cybersecurity and its deployment in the field of Society of Knowledge, and the interrelation with analogous entities at a national and international level.

Objectives

- Promote collaboration between organizations and entities of the Region of Murcia to raise awareness, disseminate and promote cybersecurity in the administration, in academia and in society in general.
- Generate synergies between all the organizations involved for the development of collaborative projects, as well as to promote the development of new initiatives.

- Ensure the availability of highly qualified professionals through training.
- Create a space for discussion and generation of socio-ethical-legal knowledge in the area of cybersecurity.
- Raise public awareness of the importance of cybersecurity through demonstration spaces, conferences and collaborative events.
- Collaborate with other centers of reference in cybersecurity both nationally and internationally.
- Extend the use of cyber-attack prevention, characterization, detection and containment systems in society in general, as well as strengthen information exchange mechanisms linked to incident management.
- Collaborate in future regulations on cybersecurity at national and European level and be one of the instruments for its deployment.
- Define and execute pilot projects of secure technologies at the regional level, as well as a space for co-innovation at the regional level.

The initial lines of activities identified are:

- Cyber Thread Intelligence pilot for regional administrations and public entities.
- Assessment of ICT infrastructure threats in pandemic situations and possible protection scenarios.
- Analysis of non-invasive technologies with support to protect the user's identity and privacy and the organization of demonstrators to improve agent confidence.
- Definition and development of training and awareness modules for different regional actors.
- Interaction with the regional DIH Agora[38] in order to integrate the innovation aspects with the productivity regional sectors.

3.8.2. CIBERREG Proposal – Impulse to Cybersecurity from the Territories

Nine Autonomous Communities participate in the project, the actions of which are aligned with strategies and regional policies that try to promote cybersecurity in their territories with consequent economic and social growth derived from these actions.

The CIBERREG project – Boosting cybersecurity from the territories aims to be a unique and collaborative work environment with a high degree of participation of Autonomous Communities so that, based on the actions and experiences of each region, the working groups and forums created to share advances in a collaborative way allow a qualitative advance in the adoption of the principles of cybersecurity in the economic fabric of each territory.

It is necessary both to innovate in cybersecurity and to bring cybersecurity closer to all vectors of attack: i.e., closer to companies, citizens... and on the one hand, due to the rapid evolution of technologies, there is a need by organizations to adopt them in order to be increasingly competitive and efficient. Also, it is essential to maintain the pace of innovation in cybersecurity in order to adopt new technologies without exceeding an acceptable level of risk. For this, the project generates spaces for public-private regional collaboration, involving administrations, companies and academia, to drive innovation, the adoption of cybersecurity solutions and to generate talent.

In this sense, the CIBERREG project – Boosting cybersecurity from the territories includes actions promoted by regional governments and linked to the following lines of action:

[38] https://www.agoradih.es/

- (LA1) Regional cybersecurity centers
- (LA2) Promotion of the business ecosystem in the cybersecurity sector
- (LA3) Demonstration Centers
- (LA4) Talent management
- (LA5) Awareness actions

Strategic Objectives

- Contribute from the public impulse to the digitization process and hyperconnectivity in a cybersecure environment so as to produce a sustainable socio-economic transformation in terms of productivity and employment.
- Promote regional cybersecurity projects, ensuring their efficiency and maximizing their impact through coordination, collaboration and complementarity between regions considering the strengths of each region.
- Promote territorial balance so that no region is left behind in a global objective such as promoting the culture of cybersecurity for companies and citizens.
- Promote the strategic growth of a key sector such as ICT, but also other sectors' strategic economic strategies in regional economies through the transformation and digital specialization.
- Establish the foundations for a stable and sustainable collaboration environment in the medium and long term that ensure coordinated progress in cybersecurity aspects.

Operational Objectives

- Execution of regional tractor projects that pose specific challenges that in turn can be extrapolated to other regions through the exchange of knowledge and experiences so that the opportunities of each region multiply.
- Execution of projects and actions aimed at key economic sectors that may represent a tractor effect on them, but also its subsequent extrapolation to others.
- Execution of projects that incorporate a different degree of technological challenge, from the adoption of existing solutions to the promotion of research through demonstration centers, so that all the territories can advance with respect to their starting situation.
- Carrying out of actions aimed at promoting talent specialized in cybersecurity both for ICT professionals as well as for other students and professionals, as well as the raising awareness in particular for users of digital environments.
- Constitution of public-private collaboration networks with the participation of different agents: representatives of regional governments, companies and business associations, and other actors key as local entities.
- Transversal collaboration between regional governments to solve challenges and obstacles that allow a faster and more sustainable progress of the actions of each territory.

3.9. Conclusions

In this chapter several different case studies of Member States have been analysed. This chapter provides a comprehensive, up-to-date (at the moment of writing) overview of the best practices in NCC and Community establishment, development, and perspectives. The information presented in this chapter supports the other WP2 findings and policy recommendations, and namely, the need of a tailor-made approach in institutionalizing European cybersecurity community. In order to realize the full potential of Europe's vibrant and dynamic cybersecurity community in achieving more engagement and involvement from the grassroots level of cybersecurity in Europe, it is vital to explore, map, and

integrate the existing diversity of the community initiatives. With specific national needs, maturity stages, initiatives, and political context, it is important to maintain strategic vision of the integrated European Cybersecurity Community as end goal.

4. Analysis of Regulation (EU) 2021/887

The Regulation Proposal[39] had been subject to an analysis in D2.1 and the further development of the concept of CHECKs in D2.3. Finally, Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres entered into force on 28 June 2021. This allows for an assessment of the final wording and comparison with the Proposal with a continued focus on the Community governance.

4.1. Competence Network and amendments during the legislative process

The Regulation provides for the interaction of various institutions. At the center is the European Cybersecurity Competence Centre whose tasks, organisation and funding are the main regulatory object of the Regulation. Its mandate is to support the Union in strengthening capacities and capabilities in all areas of cybersecurity and improve the EU's competitiveness in this area (Art. 3 of the Regulation). The Centre shall achieve this by pursuing the objectives set out in Art. 4 of the Regulation, which include in particular the promotion of cybersecurity research, innovation and implementation, the creation of capacities, skills, knowledge and infrastructure in this field and the bringing together of stakeholders in a common European cybersecurity ecosystem. To this end, it can make recommendations, implement measures within the framework of European programmes, acquire infrastructures and services, and promote cooperation between Member States. Its tasks (Art. 5 of the Regulation) are divided into strategic and implementation tasks. The strategic tasks include, for example, the development of a cybersecurity agenda, which defines the priorities of the Competence Centre's activities, the provision of support to SMEs and start-ups in this area, and the coordination of other cybersecurity stakeholders. In addition, the Centre is tasked to promote the exchange of expertise in this area in general. The Centre's implementation tasks include the coordination and management of the European Cybersecurity Network, the establishment of a work programme, but also the provision of educational, advisory and support tasks vis-à-vis both the Commission and Member States.

In addition to the Competence Centre at European level, the Regulation provides for the National Coordination Centres as further institutions within the Network. Their establishment is regulated in detail in Art. 6 of the Regulation. According to Art. 7 of the Regulation, their tasks include the provision of expertise, the functioning as a national contact point, the support of the Competence Centre in its tasks. In particular, that includes the coordination and involvement of stakeholders, the improvement of knowledge about cybersecurity in the Member States and the promotion and dissemination of the results of the Network's work. The individual centres of the Member States work together through the Network.

Finally, the Regulation provides for the Cybersecurity Competence Community. According to Art. 8 para. 1 of the Regulation, the Community supports the Competence Centre and the Network and pursues the goal of promoting, sharing and disseminating cybersecurity expertise. According to Art. 8 para. 2 of the Regulation, it consists of stakeholders related to the field of cybersecurity from industry, research, politics and civil society and is thus intended to bring together these key players with other national and European cybersecurity institutions. In order to become a member of the Community, a registration by the Competence Centre is required both for Union institutions, bodies and agencies according to Art. 8 (6) of the Regulation and for all other stakeholders according to para. 4. As part of the registration process, the Competence Centre CHECKs whether applicants meet the requirements for admission to the Community pursuant to Art. 8 (3) of the Regulation. An entity that wants to become a member must be established in a Member State and be able to prove that it contributes to the mission of the Community and has expertise in the field of cybersecurity in one of the areas mentioned in Art. 8 para. 3 lit. a) - f) of the Regulation. The tasks of the Community are regulated in Art. 9 of the Regulation and include, in addition to supporting the Competence

[39] Regulation Proposal (EU) 2018/0328 (COD).

Centre in fulfilling its mission and objectives, participation in working groups and supporting the Competence Centre and the National Coordination Centres in promoting their projects. In addition, Art. 8 para. 9 of the Regulation mandates that the Community provides strategic advice to the Competence Centre in connection with its agenda and the work programmes.

While the basic structure and distribution of tasks described above was already provided for in the Regulation Proposal, changes to the structure, organisation and decision-making of the Competence Centre have occurred in the course of the legislative process. Thus, the originally envisaged Industrial and Scientific Advisory Board (cf. Art. 11 Para. 2 lit. c), 18 et seq. Regulation Proposal) has been replaced by a Strategic Advisory Group (Art. 11 para. 2 lit. c), 18 ff. Regulation). Apart from minor changes in the number of members, their selection and working methods, the advisory and support tasks of the Advisory Group have remained largely unchanged. The Governing Board, whose tasks according to Art. 13 of the Regulation concern the strategic orientation of the Competence Centre, has also experienced changes in the legislative process only in its composition and the decision-making process, which have led to a shift of influence within the Centre in favour of the Member States. Thus, the Union provides fewer representatives than originally envisaged (cf. Art. 12 para. 1 of the Regulation and Art. 12 para. 1 of the Regulation Proposal) and decisions are to be taken, as far as possible, on the basis of consensus. If this is not possible, they must be taken by 75% of the votes (cf. Art. 15 para. 1, 2 of the Regulation). In the Proposal, the Commission, which now has only one vote similarly to every Member State, was to have 50% of the voting rights, whereby decisions were to be taken with 75% of the votes with simultaneous representation of 75% of the financial contributions made to the Centre (cf. Art. 15 para. 3 Regulation Proposal). As in the Proposal, no voting rights in the Governing Board are envisaged for the Competence Community. Moreover, its members can only participate in its meetings upon invitation (Art. 14 para. 5 of the Regulation Proposal). In contrast to the Proposal, there is no longer any provision for the members of the Advisory Group to attend the meetings, which represents a further weakening of the influence of the actors on the decisions of the Centre. The process of appointing the Executive Director (Art. 16 of the Regulation) and his duties in terms of managing day-to-day operations (Art. 17 of the Regulation) have remained essentially unchanged. The biggest change has been with regard to the financing of the Competence Centre. It is now mainly the responsibility of the Union (cf. Art. 21 (1) of the Regulation), while the Member States can limit themselves to making voluntary contributions (cf. Art. 21 (7) of the Regulation). This was clearly regulated differently in the Proposal, which provided for the payment of total contributions by the Member States (Art. 22 Regulation Proposal).

4.2. Evaluation

The analysis of Proposal (EU) 2018/0328 (COD) revealed weaknesses,[40] which could have been remedied in the course of the legislative process. In this respect, it is to be examined whether the provisions of the final Regulation have indeed remedied the situation and to what extent they achieve the declared regulatory objectives[41]. The focus of this analysis will be on the Competence Community and the integration of its potential into the European Competence Centre and the National Coordination Centres.

[40] On this in detail *von Wintzingerode/Müllmann*, Ein europäisches Netzwerk für Cybersicherheit, in: Taeger (ed.), Den Wandel begleiten - IT-rechtliche Herausforderungen der Digitalisierung, 2020, p. 475 ff; *von Wintzingerode/Müllmann/Spiecker gen. Döhmann*, NVwZ 2021, 690 et seq.

[41] Summarised in recital 58 Regulation (EU) 2021/887, the objectives are to strengthen the competitiveness and capacities of the Union, to maintain and further develop the Union's technical and industrial capacities in the field of cybersecurity research, to increase the competitiveness of the Union's cybersecurity industry and to turn cybersecurity into a competitive advantage for other Union industries. In the context of the specific criticisms, the objectives are revisited in detail.

4.2.1. Competence Centre, National Coordination Centres and Network

Governing Board of the European Competence Centre

Voting Rules

The revision of the voting rules of the Governing Board42 has not introduced more clarity. The combination of a fundamentally consensus-oriented approach with voting in case of failure to reach a consensus[43] initially appears to be an improvement over the Regulation Proposal. The latter had given the Union, represented by 5 members of the Commission,[44] a disproportionately high share of the vote for each type of decision,[45] so that without the Commission's vote the required majority could never be reached. Less obvious at first glance, but very similar to the Regulation Proposal in their pro-Commission effect, are the special voting rules in Art. 15 para. 3-5. In no less than 14 of 26 areas of responsibility the Union has not one but 26% of all votes[46] and thus still has a de facto veto right in most areas of responsibility. Neither consensus decisions, nor the required 75% majority in case of dissent can be achieved without the Commission in these cases. The weighting of votes in the Governing Board thus does not consistently correspond to its membership structure.

Design of the decision-making process

One of the main points of criticism of the Regulation Proposal from a rule of law point of view was the lack of rules that shape the process of decision-making in the Governing Board, such as how information is collected and decisions prepared, whether and how detailed reasons must be given for decisions, or how conflicts of interest are to be dealt with.[47] Unfortunately, this deficiency was not remedied in the further course of the legislative process. In the meantime, the Governing Board has fulfilled its obligation to issue rules of procedure[48] and regulate the avoidance and handling of conflicts of interest[49]. However, the rules of procedure do not contain any rules on the decision-making process itself.

A certain degree of transparency[50] is at least achieved by publishing the minutes of the meetings[51]. Indirectly, the knowledge that minutes are to be published can in principle contribute to ensuring e.g. careful preparation and higher traceability of decisions. However, the Governing Board does not have to publish

[42] Art. 15 Regulation (EU) 2021/887.
[43] Art. 15 para. 1 of Regulation (EU) 2021/887.
[44] Art. 12(1) Proposal Regulation (EU) 2018/0328 (COD).
[45] In Art. 15 para. 1-3 Proposal Regulation (EU) 2018/0328 (COD), with a general majority requirement of 75%, a voting share of the European Commission of 50% in each decision was provided for.
[46] Art. 15 para. 4 of Regulation (EU) 2021/887.
[47] *von Wintzingerode/Müllmann*, Ein europäisches Netzwerk für Cybersicherheit, in: Taeger (ed.), Den Wandel begleiten - IT-rechtliche Herausforderungen der Digitalisierung, 2020, p. 482 f.; *von Wintzingerode/Müllmann/Spiecker gen. Döhmann*, NVwZ 2021, 690 (692).
[48] Art. 13 para. 2 of Regulation (EU) 2021/887.
[49] Decision No GB/2021/1 of the Governing Board of the European Cybersecurity Industrial, Technology and Research Competence Centre adopting its Rules of Procedure, 20 October 2021, available at https://cybersecurity-centre.europa.eu/system/files/2021-11/ECCC%20Decision%20No%20GB20211%20RoP_final.pdf (last access 10.03.2022). The regulations on possible conflicts of interest can be found in Art. 17 of the Rules of Procedure.
[50] Article 34 (1) of Regulation (EU) 2021/887 obliges the competence centre to carry out its activities with a high degree of transparency. This does not indicate when a high level of transparency within the meaning of the Regulation has been achieved. Paragraphs 2 and 3 of the same article only provide information to the extent that the transparency of results for the public is in the foreground, while the establishment of procedural transparency is to take place only to a very limited extent.
[51] Art. 13 para. 5 ECCC Decision No GB/2021/1 RoP.

the internal version of the respective minutes of the meeting but only a summary, for which the rules of procedure do not impose any minimum content requirements with regard to completeness or detail.[52]

National Coordination Centres

The Member States had to notify their National Coordination Centres by 29.12.2021. So far, Coordination Centres for 23 out of 27 Member States have been published on the list of the Competence Centre.

Legal nature

The position of the Council, which in the legislative process had advocated an obligation for Member States to designate only public institutions as National Coordination Centres, has prevailed. Coordination Centres must be public bodies or bodies in which the Member State has a majority holding and which carry out public administration tasks. Given their role as a link between the Competence Centre and the Community members in the Member States and their mandate to promote the participation of civil society and various groups of stakeholders, this not only makes functional sense, but also serves the rule of law and the democratic legitimacy of decisions. Not least in view of the fact that the National Coordination Centres can also manage financial resources, this requirement is to be regarded as adequate.

Different categories of National Coordination Centres

Without being clearly designated as such or being obvious at first glance from the structure of Art. 6, the Regulation provides for two categories of National Coordination Centres. In principle, the Governing Board lists all notified Coordination Centres within three months.[53] According to the wording, all National Coordination Centres notified by the Member States automatically belong to the Network,[54] without the need to be included in the list of the Competence Centre.

Beyond mere membership of the Network and public listing with the Competence Centre, National Coordination Centres can apply for recognition "as a body having the necessary capacity to manage funds {...}"[55]. In these cases, recognition by the Commission is a prerequisite for a National Coordination Centre to be able to receive direct EU funding itself and to provide Union financial support to third parties.[56]

Therefore, there are two categories of National Coordination Centres, basic ones and Coordination Centres with fund managing tasks.

It is to be welcomed that the rules on the designation of National Coordination Centres in Art. 6 have been differentiated in the course of the legislative process as this has resulted in a more complete picture of the selection requirements in comparison to the Regulation Proposal[57]. In the interest of clarity, however, the possibility of giving Art. 6 a clearer structure should have been used, too.

Cooperation in the Network

[52] Cf. Art. 13 para. 1 and para. 5 ECCC Decision No GB/2021/1 RoP, which use the term "publishable summary" in the original wording.

[53] Art. 6 para. 3 Regulation (EU) 2021/887.

[54] Art. 6 para. 7 of Regulation (EU) 2021/887. The original English version does not allow for any other conclusion.

[55] Art. 6 para. 6 subpara. 1 sentence 1 of Regulation (EU) 2021/887. Art. 6 para. 2 allows Member States to ask the Commission for an opinion on the capacity to manage funds even before the formal application and even before the designation of a National Coordination Centre.

[56] Art. 7 para. 2, 3 of Regulation (EU) 2021/887 as well as Communication of the Commission on the Guidelines within the meaning of Art. 6 para. 6 subpara. 3 of Regulation (EU) 2021/887, p. 1 f., available at https://ec.europa.eu/newsroom/dae/redirection/document/80257 (last access 26.04.2022).

[57] Cf. Art. 6 Proposal Regulation (EU) 2018/0328(COD).

There is a variety of different networks in other regulatory areas of Union law.[58]Due to the lack of legal requirements, however, no uniform concept or structure behind them can be identified[59] and the content of the 'network' concept remains limited in terms of organisational law[60]. The typology of the Network of National Coordination Centres must therefore be derived from the Regulation itself.

The Coordination Centres become part of the Network by notification to the Governing Board[61] and are supposed to cooperate through the Network, where relevant[62]. The wording *where relevant* suggests that cooperation between the National Coordination Centres is at least not assumed to be the norm and does not seem to be the main aspect of network formation. A mandate for the formation of a proactive network that could offer added value for its members - and via this for European cybersecurity as a whole - through its own initiative and by a constant exchange cannot be derived from this. It is true that the capacity requirements for the National Coordination Centres laid down by the Regulation also have an indirect effect on the Network. If this were a way to (additionally) stimulate the professional exchange and coordination between the Member States and to maintain them at a high level, this would already be a partial success for the improvement of cybersecurity in the Union. However, the tasks of coordinating the National Centres and ensuring the exchange of expertise lie with the European Competence Centre.[63] The term 'Network' in the Regulation therefore has the character of a summary designation for the National Coordination Centres as a whole in relation to the European Competence Centre. On the other hand, it is probably not a description of a specific line of action[64] of national and European administrative units.

It should be noted, however, that the European Commission has already initiated a call for proposals for the establishment and implementation of the tasks of the National Coordination Centres and the Network.[65] It therefore remains to be seen how the work of the Coordination Centres and the Network will look in the near future and whether their full potential for enabling better coordination between Member States will be unlocked.

European Cybersecurity Network?

Bringing together public stakeholders and private actors to address cybersecurity challenges in the Union is a sensible approach. Only if expertise at all levels is involved can its full potential be realised. The formation of a network is, in principle, one way to achieve this due to its ability to gather knowledge through the interaction of public and private actors[66]. However, the Regulation explicitly provides for the concept of a

[58] Examples in Schoch/Schneider/Schoch, VerwR VwVfG, Einl. Rn. 542.

[59] Schoch/Schneider/Schoch, VerwR VwVfG, Einl. Rn. 541.

[60] *S. Augsberg,* in: J.P.Terhechte (ed.), VwREU (2nd ed., 2022), § 6 marginal no. 53 with further references; *R. Schmidt,* in: W. Kahl/M. Ludwigs (eds.), Hdb. VerwR, vol. 1: Grundstrukturen (2021), § 9 marginal no. 20 with reference inter alia to *S. Groß*, in: W. Hoffmann-Riem/E. Schmidt-Aßmann/A. Voßkuhle (eds.), GVwR, vol. I (2nd ed., 2012), § 13 marginal no. 12.

[61] Art. 6 para. 7 of Regulation (EU) 2021/887.

[62] Art. 7 para. 4 of Regulation (EU) 2021/887.

[63] Art. 5 para. 2 lit. d) Regulation (EU) 2021/887.

[64] On the network as a mode of action, see *Hoffmann-Riem* in: Terhechte (ed.), Verwaltungsrecht der Europäischen Union, 2nd ed., 2022, § 3 marginal no. 27 f. with further references.

[65] Communication available on the website of the European Centre of Excellence at https://cybersecurity-centre.europa.eu/news/coming-soon-new-call-deployment-network-national-coordination-centres-2022-02-17_en. Further information and updates are also available on the European Commission's Funding & Tenders Portal at https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2022-cyber-02-nat-coordination (both last access 30.06.2022).

[66] *M.P. Schwind*, Netzwerke im Europäischen Verwaltungsrecht, 2017, p. 131 f. It should be taken into account that the term network is used with different meanings and different compositions are possible depending on the network term.

Network[67] only for the National Coordination Centres. The relationship of the European Competence Centre to the individual National Coordination Centres and to their Network is hierarchical. The Cybersecurity Competence Community is envisaged as another group of actors outside the Network.[68] Whether the designation as a Competence *Community* is a synonym for the *Network* of Coordination Centres, which merely serves to better conceptually distinguish the two groups of actors, or whether there is a different understanding of the group's characteristics or its actions behind the differentiation, cannot be clearly determined. In any case, the establishment and involvement of the Competence Community is also done by way of a top-down approach[69], similarly to the Network of Coordination Centres. Overall, the Competence Centre, the Coordination Centres and the Competence Community are not (equal) actors of *one single* European Cybersecurity Network. The previously mentioned effects of such an overall network are accordingly not to be expected based on the Regulation.

4.2.2. Cooperation with other EU Cybersecurity Institutions and Networks

The Regulation establishes the Competence Centre, Network of National Coordination Centres and Cybersecurity Community with the overarching aim to "bring together resources, overcome fragmentation of efforts across the EU and stimulate the development and deployment of technology in cybersecurity".[70] Despite the EU's intention to overcome fragmentation, however, the new framework introduces a new set of actors in an already complex web of European cybersecurity institutions and networks without clarifying the relationship between them. The European Competence Centre will be at least the fourth EU-level body (together with ENISA, EC3 and CERT-EU) with competences in a specific field related to cybersecurity – in this case with a mandate to improve the Union's policies on innovation, research and technological development.[71]

Nonetheless, the Regulation remains largely silent on the Competence Centre's relationship with the existing EU-level cybersecurity stakeholders, noting only generally that the Center should ensure synergies between and cooperation with relevant Union institutions, bodies, offices and agencies, in particular ENISA, while avoiding any duplication of activities (Article 5(2)(c) of the Regulation). The Centre's relationship with ENISA and the CSIRT Network is only scratched in the Regulation's recitals, with Recital 16 clarifying that the Centre should not carry out the operational cybersecurity tasks associated with CSIRTs but also noting that the Competence Centre and the Competence Community should support stakeholders wishing to report and disclose vulnerabilities. That, of course, would have to happen "while avoiding any duplication with ENISA". How such avoidance would be ensured in practice, however, remains to be seen as the Center and the Community are established.

Additionally, neither the Regulation, nor the NIS2 Directive Proposal[72] elaborate on the relationship between the Competence Centre and the NIS Cooperation Group. The Cooperation group also has an important role in enabling strategic cooperation between EU cybersecurity stakeholders and serves as a

[67] For the restrictions, see the previous section III. 1. b) cc).
[68] Cf. Art. 1 para. 1 p. 2, Art. 8 f. VO (EU) 2021/887.
[69] See below under 2.
[70] European Commission, Impact Assessment accompanying the 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, COM(2018) 630 final.
[71] The legal basis for Regulation (EU) 2021/887 is 173(3) TFEU, which regulates the Union's competence in introducing measures to improve the competitiveness of the Union's industry and foster "better exploitation of the industrial potential of policies of innovation, research and technological development".
[72] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.

platform for the exchange of information and best practices on research and development in the field.[73] It is therefore surprising that neither the Regulation, nor the NIS2 Directive Proposal stipulate how these two entities relate to one another or envision specific means for their collaboration. The NIS2 Directive Proposal also envisions the formal establishment of the EU-CyCLONe Network, which would serve as another national-level cooperation and information exchange forum. Given the growing number of European institutions in the field of cybersecurity, the current lack of overarching framework for cooperation of stakeholders within the Union becomes ever more problematic. According to Article 8(2) of the Regulation, the Competence Community should involve the main EU cybersecurity stakeholders, including national cooperation centres, relevant European Digital Innovation Hubs, as well as Union institutions, bodies, offices and agencies, such as ENISA. This showcases the EU legislator's high ambitions for the Community to unify and pool resources from the multiple layers of cybersecurity stakeholders. As previously pointed out, however, the Regulation does not provide any organisational structure for the public-private and the inter-institutional collaboration between the Community members. It is therefore unlikely that the Community will achieve the aim of overcoming the fragmentation of EU cybersecurity stakeholders.

4.2.3. Focus: Competence Community

A closer look at the Regulation of the Competence Community as a third group of actors will explore the question of how the goal of pooling, networking and utilising the efforts and wealth of expertise and experience in research, technology and industrial development in the field of cybersecurity in an efficient manner is to be achieved[74] in the Union.

Members and Membership

A community is characterised, among other things, by a mutual bond and/or pursuit of common goals.[75] The compound term "Competence Community" in the Regulation thus suggests that potential members must not only have a certain affinity, but above all must also have certain competences in the field of cybersecurity.

A variety of entities may be considered as members. From industry, including SMEs, academic and research institutions, civil society, European standardisation organisations, and public bodies dealing with operational and technical cybersecurity issues, to stakeholders from sectors with an interest in cybersecurity and facing cybersecurity challenges.[76] The Regulation therefore defines a broad notion of Competence Community in terms of potential members and how they deal with or are affected by cybersecurity challenges.[77] This broadness is not least due to the objective of bringing together the main stakeholders in terms of technological, industrial, research and scientific capacities in the field of cybersecurity in the European Union.[78] [79]

[73] Article 11 of Directive (EU) 2016/1148 f the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive),

[74] Recital 7 Regulation (EU) 2021/887. The dimension of the objective is further clarified by EC 8, 9 and 12.

[75] Translation of definition in Duden online, available at https://www.duden.de/Rechtschreibung/Gemeinschaft (last access 21.06.2022).

[76] Art. 8 para. 2 sentence 1 Regulation (EU) 2021/887.

[77] According to Art. 8 para. 3 sentence 1 of Regulation (EU) 2021/887, the only restriction is that only institutions established in the Member States can be registered as members. This is only consistent if one considers that the Regulation has cybersecurity in the Union in mind. In addition to the competitiveness of the European internal market, it is also about the ability to secure oneself and independence from non-European suppliers of cybersecurity products.

[78] Art. 8 para. 2 sentence 2 of Regulation (EU) 2021/887.

[79] However, by whom and according to which criteria the importance is to be determined remains completely open. Whether the goal of bringing together the "most important" stakeholders is successfully achieved cannot be objectively determined at all due to the lack of normative standards.

With regard to the required competences of the Community members, the Regulation contains a combination of capacity requirements and a catalogue of areas of expertise in the field of cybersecurity. An entity wishing to become a member of the Community must demonstrate that it can contribute to the mission of the Competence Community and has expertise in at least one of the specified areas.[80] This catalogue is also recognisably intended to include as many types of institutions as possible by listing a wide range of areas of cybersecurity expertise. The Regulation thus envisages a multidisciplinary Competence Community. In addition, requirements are also set for the representatives to be appointed by the registered members. They must have expertise related to industry, technology or research in the field of cybersecurity.[81]

Obtaining Community membership follows a staged procedure. First, the National Coordination Centre of the Member State in which the respective institution is established must check whether the criteria for membership are met. If this is the case, the institution can apply for registration as a member of the Community with the European Competence Centre.[82] The registration is valid for an unlimited period of time, but can be revoked by the European Competence Centre under certain conditions.[83] A renewed registration procedure after revocation is not regulated in the Regulation, but there are also no exclusions or blocking periods that permanently or temporarily prevent the re-examination and re-registration of an institution.

However, it is questionable how institutions that are not already well networked and informed should learn about the possibility of application and registration. And even those institutions that have the relevant information will only be interested in membership and go through the two-step procedure if this offers them a recognisable added value. Ensuring that all eligible institutions are reached will therefore be an essential prerequisite for the emergence of the Competence Community and the exploitation of its potential.

Role of the Competence Community

Unlike the European Competence Centre and the Network of National Coordination Centres, the Competence Community is not listed in the title of the Regulation. However, its establishment is immediately specified in Art. 1(1), so that initially the impression of equivalence to the Competence Centre and the National Coordination Centres could arise. In view of the goal of using the existing cybersecurity knowledge and expertise of the members of the Community in the Union, this would also be obvious. How the role of the Competence Community is designed in detail in the Regulation and whether these rules are suitable for exploiting the potential of the Community will be analysed below.

Tasks

In the literal sense, a distinction can be made between its own tasks and support tasks. The Community has the broadly formulated task of promoting, sharing and disseminating cybersecurity expertise throughout the Union. [84] The Regulation does not specify how or by what means this task is to be accomplished. In addition, the Community has a supporting role in fulfilling the missions of the Competence Centre and the Network by involving both in its work[85] and by providing advice through its working groups and the Strategic

[80] Art. 8 para. 3 sentence 2 lit. a) - f) Regulation (EU) 2021/887.
[81] Art. 8 para. 8 sentence 2 of Regulation (EU) 2021/887.
[82] Art. 8 para. 4 p. 1 f. VO (EU) 2021/887.
[83] Art. 8 para. 4 p. 3 f. VO (EU) 2021/887.
[84] Art. 8 para. 1 subpara. 2 of Regulation (EU) 2021/887.
[85] Art. 8 para. 2 sentence 3 of Regulation (EU) 2021/887 refers to the National Coordination Centres, among others.

Advisory Group in the Competence Centre on issues related to the agenda, the annual and multi-annual work programme[86] .

The tasks of the members of the Community are regulated in Art. 9 of the Regulation. These tasks assign the members a supporting role in the fulfilment of the tasks of the Competence Centre and the Coordination Centres and provide for participation in certain activities and the working groups established by the Governing Board.

Independent performance of tasks is only envisaged to a very limited extent. The members' own tasks could only arise indirectly through the Community's own tasks regarding the promotion, sharing and dissemination of expertise. Due to the lack of an internal structure of the Community, however, an organised division and execution of these tasks is just as little possible, at least within the framework of the Regulation, as a subsequent self-monitoring with regard to the success or failure of the performance of tasks and possible need for improvement. Thus, the Regulation does not encourage the formation of a Community through the organised joint performance of tasks.

Integration into the organisational structure of the European Competence Centre

Attendance at meetings of the Governing Board. Members of the Community may attend meetings of the Governing Board as observers only, without voting rights, at the invitation of the Chairperson of the Governing Board.[87] Permanent observer status is not envisaged for the Community. Neither the Regulation nor the Rules of Procedure of the Governing Board contain any rules on the selection criteria for which member(s) of the Community should be invited to a meeting. In this respect, it is important to ensure equal distribution of participation opportunities for representatives of different groups of stakeholders and within these groups. Even if the participating members of the Community do not have voting rights, the position as observer possibly conveys impressions and information that Community members not participating in the respective meeting do not receive at all, only incompletely or only at a much later point in time and which in turn would have an influence on their own strategic or economic decisions, for example. Even the appearance of favouring certain members or interest groups should therefore be avoided.

Strategic Advisory Group. As part of the permanent structure of the Competence Centre, a Strategic Advisory Group is also established, in addition to the Governing Board and the Executive Director.[88] This group consists of a maximum of 20 members selected by the Governing Board from among the representatives of the members of the Competence Community, on the proposal of the Executive Director, taking into account various requirements and restrictions.[89] The Competence Community itself is not involved in this selection process. Thus, the Strategic Advisory Group is explicitly not a representation of the members of the Community to the Competence Centre in the sense of democratic participation. Nevertheless, the rules on the composition of the group are intended to ensure that it reflects the composition of the Community in as balanced a way as possible.[90] Otherwise, the procedural rules for appointing the members of the Advisory Group[91] still show room for improvement. For example, there are no rules in case

[86] Art. 8 para. 9 of Regulation (EU) 2021/887.
[87] Art. 12 para. 6, 14 para. 5 Regulation (EU) 2021/887.
[88] Art. 11 para. 2 lit. c) Regulation (EU) 2021/887. The selection of members for the Strategic Advisory Group is provided for in the Single Programming Document 2022-2024 of the Governing Board in the period up to and including 2023 (p. 14), available at https://cybersecurity-centre.europa.eu/system/files/2022-03/GB%20decision%20No%202022_6_ECCC%20SPD%202022-2024_Budget%202022.pdf (last access 05.07.2022).
[89] Art. 18 para. 1-2 Regulation (EU) 2021/887.
[90] Cf. Art. 18 para. 1 p. 5-6 Regulation (EU) 2021/887.
[91] Art. 18 para. 3 of Regulation (EU) 2021/887 in conjunction with Art. 20 of the Rules of Procedure of the Governing Board. Art. 20 of the Rules of Procedure of the Governing Board (see fn. 17 above).

more than 20 equally suitable member representatives respond to the call of the Executive Director and whether or how extensively the decision for the selection of the listed members would have to be justified and published. It must also be ensured that the call of the Executive Director is made equally accessible to all members of the Competence Community.

The working methods of the Advisory Group are only roughly determined in the Regulation.[92] It is envisaged that it will adopt rules of procedure.[93] As its name suggests, the Strategic Advisory Group has only an advisory-supporting role in the Competence Centre[94]. It may, inter alia, decide on and organise public consultations, but these require the approval of the Governing Board.[95] The Governing Board may, but is not obliged to, invite a representative of the Advisory Group to its meetings.[96] Thus, the Group has neither the right to attend meetings nor to vote on decisions and, unlike ENISA,[97] does not have permanent observer status on the Governing Board. The Governing Board does not have to follow the recommendations of the Strategic Advisory Group, nor does it have to justify or at least give reasons for deviations.[98] The degree of participation of the Advisory Group in the work and decisions of the Board is therefore weak overall.

It is to be welcomed that the Council's position in the legislative process of not integrating a body of the Competence Community into the structure of the Competence Centre was ultimately not able to prevail[99]. The Strategic Advisory Group is at least one permanent point of contact between the Competence Centre and the Community. However, with the decision not to design the Strategic Advisory Group as a representation of the Competence Community and to create very limited opportunities for its participation, an opportunity was missed, as it was in the Regulation Proposal[100], to create a real incentive not only for participation in the Advisory Group, but also for membership in the Competence Community. Both would be needed to make use of the entire potential available in the Union in the area of cybersecurity.

Working Groups. Another field of activity for the members of the Community are working groups, established by the Governing Board, where relevant taking into account the recommendations of the Strategic Advisory Group.[101] The coordination of the working groups is carried out, where necessary, by one or more members of the Strategic Advisory Group.[102]

[92] In deviation from Art. 18 para. 3 of Regulation (EU) 2021/887, the Governing Board has so far only made a provision in Art. 20 of its Rules of Procedure for the appointment procedure, but has not defined and published the working methods of the Strategic Advisory Group. It is quite conceivable that the rules of procedure will be supplemented after the advisory group has been established.

[93] Art. 19 para. 5 of Regulation (EU) 2021/887.

[94] Cf. Art. 20 of Regulation (EU) 2021/887.

[95] Art. 20 lit. c) Regulation (EU) 2021/887.

[96] Art. 12 para. 7 sentence 2 Regulation (EU) 2021/887.

[97] Unlike ENISA, the Strategic Advisory Group is not a permanent observer in the meetings of the Governing Board, Art. 12(7) of Regulation (EU) 2021/887.

[98] Neither does the Regulation provide for a duty to state reasons, nor is there a voluntary commitment by the Governing Board in its rules of procedure.

[99] Council of the European Union, Mandate for negotiations with the European Parliament, 9 March 2020.

[100] The criticism towards the design of the role of the Scientific-Technical Advisory Board in the analysis of the Regulation Proposal is in this respect transferable almost unchanged to the Strategic Advisory Group, cf. *von Wintzingerode/Müllmann*, Ein europäisches Netzwerk für Cybersicherheit, in: Taeger (ed.), Den Wandel begleiten - IT-rechtliche Herausforderungen der Digitalisierung, 2020, p. 483; *von Wintzingerode/Müllmann/Spiecker gen. Döhmann*, NVwZ 2021, 690 (693).

[101] Art. 13 para. 3 lit. n) in connection with Art. 8 para. 9 and Art. 9 lit. b) of Art. 8 (9) and Art. 9 (b) of Regulation (EU) 2021/887.

[102] Art. 19 para. 2 sentence 2 of Regulation (EU) 2021/887.

Unlike the Strategic Advisory Group, the working groups are not permanent structural elements in the Competence Centre with specific tasks of their own. Working groups can be formed as needed to collaborate on issues relevant to the work of the Competence Centre[103] and to provide advice on the agenda, the annual and multi-annual work programme[104] .

This is therefore a thematically more narrowly defined assignment of tasks on a case-by-case basis by the Governing Board to individual members of the Community. Unfortunately, neither the Regulation nor the Rules of Procedure of the Governing Board[105] provide for procedural rules or criteria for the selection of these Community members. Such rules would be desirable not only from a rule of law perspective, but also for community building. Ensuring a certain plurality and diversity of the working groups can indirectly lead to Community members, who are not already networked, to meet and exchange ideas. This, in particular, would promote the dissemination of expertise and could give rise to new impulses for research and development.

Cooperation with the National Coordination Centres and the Network
The Regulation assigns tasks to the National Coordination Centres and the Network, among others, related to the Community and its members.[106] The Network, like the Competence Centre, shall cooperate with the Community as appropriate.[107] The National Coordination Centres shall serve as focal points for the Community at national level and shall assist the Competence Centre in particular in coordinating the Community through coordination of its members.[108] The promotion and dissemination of relevant work results of the Network, the Community and the Competence Centre at national, regional or local level is also one of the tasks of the National Coordination Centres.[109] Another task of the National Coordination Centres is to promote, facilitate and encourage the participation of civil society, industry, in particular start-ups and SMEs, academia and research and other stakeholders in cross-border projects and cybersecurity activities at national level.[110] While this task is not directly related to the Community, it does not explicitly exclude its members. In addition, National Coordination Centres can help stimulate interest and encourage appropriate institutions to join the Competence Community.
Conversely, the Community shall, inter alia, involve the National Coordination Centres in its work[111]. Its members shall work closely with the National Coordination Centres to assist the Competence Centre in fulfilling its mission[112] and shall assist the National Coordination Centres in promoting specific projects[113] .

The Regulation thus identifies possible interfaces between the Coordination Centres as public actors and the Community or its members as predominantly private law actors. The role of the National Coordination Centres "in the middle of the action" offers a suitable starting point for the creation of national, regional or local communities and networking within the Community, if designed actively and purposefully. The

[103] Cf. wording in Art. 19 para. 2 sentence 1 of Regulation (EU) 2021/887.
[104] Cf. wording in Art. 8 para. 9 of Regulation (EU) 2021/887.
[105] Art. 14 of the Rules of Procedure of the Governing Board (see above) deals with "working groups", but the Regulation does not refer to the working groups in the Regulation. In terms of content, it deals with "*ad hoc* working groups", the necessity, formation and composition of which seem to be conceived differently from the working groups mentioned in the Regulation. A clearer description in the Rules of Procedure (and, if necessary, a definition of the terms) would be desirable.
[106] Cf. Art. 7 para. 1 of Regulation (EU) 2021/887.
[107] Art. 3 para. 2 of Regulation (EU) 2021/887.
[108] Art. 7 para. 1 lit. a) Regulation (EU) 2021/887.
[109] Art. 7 para. 1 lit. h) Regulation (EU) 2021/887.
[110] Art. 7 para. 1 lit. c) Regulation (EU) 2021/887.
[111] Art. 8 para. 2 sentence 3 Regulation (EU) 2021/887.
[112] Art. 9 lit. a) Regulation (EU) 2021/887.
[113] Art. 9 lit. c) Regulation (EU) 2021/887.

complementary mandate for the Community to work closely with the Coordination Centres supports this approach. However, the Regulation does not lay down structures for practical task implementation and cooperation. It is therefore left to the National Coordination Centres and the Competence Community to design these. The resulting freedom of design offers both sides the opportunity to take into account national, regional or local, thematic and sector-specific circumstances in the design of the cooperation. However, a realistic approach must of course also recognise the danger that independent shaping in the Member States fails and that no cooperation at all or no cooperation sufficient for the promotion of European cybersecurity is achieved. While the National Coordination Centres, as public institutions, have an internal structure and can use traditional forms of action under their national legal systems, the *Competence Community*, contrary to its name, is not (yet) a structured unit that can fall back on common organisational or financial resources and thus enable cooperation. Whether and how cooperation will succeed in practice remains to be seen.[114]

Establishing and Structuring the Community

Considering that the Competence Community - despite or precisely because of the thematic affinity of its members - will include competitors with opposing interests, e.g., with regard to political influence, funding opportunities or expansion of market shares, an "automatic" formation of a community seems far-fetched. Although the Regulation lays down the criteria and procedure for becoming a member of the Community, it does not contain any explicit rules on how a community is to be formed from the registered members and which structures it can actively use to fulfil its tasks. Thus, the tasks of the Community and its members as well as their integration into the control structure of the Regulation, can give at most only clues as to what kind of community the legislator had in mind. As demonstrated, however, no community-forming factors result from the Regulation alone.

The broadly chosen community concept is a good approach to cover as many affected areas and existing competences in the field of cybersecurity in the European Union as possible. Another question, however, is whether this fundamentally broad framework can subsequently be filled at all. Decisive for this is the participation design, i.e., the question whether a structural limitation of the initially broad community concept can be observed in practice. Studies on private standardisation organisations demonstrate that regularly only those stakeholders with the necessary financial, time and personnel resources can exert active influence, because this is what makes active participation possible in the first place. Not all interests therefore have the same chances of assertion,[115] even if in principle everyone can participate[116] . The resulting work therefore only reflects the contributions of the actively involved, assertive stakeholders and is not a consensus of all stakeholders. This effect cannot be ruled out for the Competence Community. Particularly in the field of cybersecurity, with rapid technical developments and effects that reach into every area of society and government, it is undesirable to leave existing competences unused from the outset due to structural deficits.

One objection to a structural disadvantage of smaller institutions could be that the Regulation provides, inter alia, for the promotion and facilitation of the participation of civil society, start-ups and SMEs in cross-

[114] Of course, it would be desirable that the results of the above-mentioned Call for Proposals (see above, fn 43) also contain useful proposals in this regard. According to EC (17) Regulation (EU) 2021/887, with regard to the management of the Community and its representation in the Competence Centre, the experience of, among others, the 4 pilot projects CONCORDIA, ECHO, SPARTA and CyberSec4Europe, which were launched at the beginning of 2019 within the framework of Horizon 2020, shall be drawn upon. CyberSec4Europe has extensively addressed governance design issues for the Community of Excellence, cf. https://cybersec4europe.eu/our-results/deliverables/ (last on 30.06.2022).

[115] *Bolenz,* Technische Normung zwischen Markt und Staat (1987), p. 174.

[116] For example, anyone can submit a standardisation application to DIN and the draft standards produced are published for comment by anyone, cf. *Bolenz*, Technische Normung zwischen Markt und Staat (1987), p. 117; *B. Hartlieb/A. Hövel/N. Müller,* Normung und Standardisierung (2nd ed., 2016), p. 38 ff.

border projects and cybersecurity activities through the National Coordination Centres.[117] This may, in the medium or long term, help such stakeholders develop the resources to actively participate as members of the Competence Community. However, this is by no means assured and a short-term solution is lacking.

The lack of opportunities for participation is not compensated for by ensuring representation of the members with the greatest organisational capabilities. Their resources say nothing about their standing in the community as a whole and their willingness to represent interests other than their own. Moreover, it is not the Competence Community that decides who becomes a member, attends board meetings, gets involved in working groups or becomes part of the Strategic Advisory Group. Instead, all these decisions are made by the Governing Board, possibly with the involvement of the National Coordination Centres. True representation, on the other hand, would require that Community members can choose their own representatives.

Conclusion
There are no recognisable advantages from mere membership in the Competence Community. The integration into the structure of the Competence Centre does not offer any incentives either. The Community is characterised by a top-down approach that offers only very limited opportunities for participation and cannot be expected to have any community-building effects. Nonetheless, a certain amount of freedom is given to the National Coordination Centres regarding cooperation with the Community. If used wisely, it could create an incentive for membership and participation in the Competence Community. In order to achieve this, however, National Coordination Centres would have to overcome the lack of existing interfaces and the inclination to have only their respective national community in mind.

Furthermore, despite the broad concept of community, the Regulation has an exclusive participation design which structurally only allows those members of the Competence Community to benefit who are already well networked and have established contacts with public institutions. This can not only disadvantage other members, but also perpetuates the status quo and contradicts the aims of the Regulation.[118] Furthermore, the Community and the influence of the practical actors there could also be weakened by the fact that the other EU institutions are also represented in the Community and can exert influence. This dilutes the voice of the practitioners even more, even though they are hardly heard as it is and are hardly integrated institutionally.

In order to activate and effectively use the wealth of expertise and experience in cybersecurity research, technology and industrial development that exists in the Union,[119] it is crucial to harness the potential that lies within the Competence Community. This entails ensuring cooperation opportunities, collaboration, knowledge sharing and financial opportunities within the Community. However, the purely top-down approach and the limitation to observing or advisory roles without real opportunities for influence have so far offered little incentive for the Competence Community and its members to get actively involved, while the exclusive participation design makes it even more difficult to exploit existing competences.

4.3. Conclusions

In summary, the analysis of the Regulation allows for the following conclusions:

4.3.1. European Competence Centre

- The number of Union representatives has been reduced and voting rights as well as majority rules have been adapted. A closer look, however, still reveals complicated decision-making rules with a pro-Commission effect and a de facto veto right in most areas of responsibility.

[117] Art. 7 para. 1 lit. c) Regulation (EU) 2021/887.
[118] Cf. Recitals of the Regulation.
[119] Recital (7) Regulation (EU) 2021/887.

- From a rule of law point of view the design of the decision-making process in the Governing Board is still unsatisfying. Neither the Regulation nor the Rules of Procedure of the Governing Board provide for the collection of information, preparation of decisions, whether and how detailed decisions have to be reasoned and how conflicts of interest have to be dealt with.
- The Strategic Advisory Group has replaced the Industrial and Scientific Advisory Board. Apart from minor changes in the number of members, their selection and working methods, the advisory and support tasks have remained largely unchanged. The Advisory Group has no voting rights and in contrast to the Regulation Proposal there is no longer any provision for the members of the Advisory Group to attend the meetings of the Governing Board.

4.3.2. National Coordination Centres

- The position of the Council, which in the legislative process had advocated an obligation for Member States to designate only public institutions as National Coordination Centres, has prevailed. Given their role and tasks, this requirement is adequate.
- The Regulation introduces two categories of National Coordination Centres, basic ones on the one hand and Coordination Centres with funding management tasks on the other. The latter have to fulfil additional requirements in order to achieve such status.
- A call for proposals for the establishment and implementation of the tasks of the National Coordination Centres and the Network has been issued by the European Commission. The further development remains thus to be seen.
- The term 'Network' in the Regulation has the character of a summary designation for the National Coordination Centres as a group in relation to the European Competence Centre. It is probably not a description of a specific line of action of national and European administrative units.
- The network term only applies to the National Coordination Centres. The Regulation does in no way provide for the implementation of *one* European Cybersecurity Network with equal actors or any bottom-up structures.

4.3.3. Cooperation with other EU Cybersecurity Institutions and Networks

- Despite the EU's intention to overcome fragmentation, the new framework introduces a new set of actors in an already complex web of European cybersecurity institutions and networks without clarifying the relationship between them.
- The Regulation does not provide any organisational structure for the public-private and the inter-institutional collaboration between the Community members. It is therefore unlikely that the Community will achieve the aim of overcoming the fragmentation of EU cybersecurity stakeholders.

4.3.4. Competence Community

- The analysis was focused on the Competence Community and how the Regulation integrates its potential into the European Competence Centre and the National Coordination Centres and the Network of National Coordination Centres respectively.

- The Regulation defines a broad notion of Competence Community in terms of potential members and how they deal with or are affected by cybersecurity challenges. It envisages a multidisciplinary Competence Community and additionally requires the members' representatives to have expertise related to industry, technology or research in the field of cybersecurity.
- Obtaining membership follows a staged procedure in which potential members do not only have to apply for a registration but also have to fulfil certain criteria for the membership. Under certain conditions, the membership can be revoked by the European Competence Centre.
- The Regulation remains silent on the question, how possible members, that are not already well networked and informed should learn about the possibility of application and registration.
- There is no evident benefit or added value for possible members to increase their interest in going through the application and registration procedure.
- The Regulation does not specify how or by what means the Community should accomplish the task of promoting, sharing and disseminating cybersecurity expertise throughout the Union. Due to the lack of an internal structure of the Community, however, an organised division and execution of these tasks is just as little possible, at least within the framework of the Regulation, as a subsequent self-monitoring with regard to the success or failure of the performance of tasks and possible need for improvement.
- The Governing Board can invite Community members to attend their meetings. However, neither the Regulation nor the Governing Board's Rules of Procedure offer any rules on selection criteria for the Community members. This should be changed. Attending a meeting possibly conveys impressions and information that Community members not participating in the respective meeting do not receive at all, only incompletely or only at a much later point in time and which in turn would have an influence on their own strategic or economic decisions, for example. Even the appearance of favouring certain members or interest groups should therefore be avoided.
- The Competence Community is not involved in the selection of the Strategic Advisory Group members, so the Advisory Group is not a Community representation in the structure of the European Competence Centre.
- The degree of participation of the Advisory Group in the work and decisions of the Governing Board is weak overall: Their advice or recommendations are not binding, members can be invited to Governing Board meetings, but have no permanent observer status and have no voting rights.
- The Regulation missed the opportunity to create a real incentive not only for participation in the Advisory Group, but also for membership in the Competence Community.
- The rules on the establishment of Working Groups leave room for improvement. Especially procedural rules or selection criteria would not only be desirable from a rule of law perspective, but also from a community building point of view. By ensuring a certain plurality and diversity of Working Group members the Community networking, dissemination of expertise, research and development could be enhanced.
- By defining Community related tasks for the National Coordination Centres and, conversely, tasking the Community with involving the National Coordination Centres in its work the Regulation creates "meeting points" between the Coordination Centres and the Community. However, the Regulation does not lay down structures for practical task implementation and cooperation.
- While the National Coordination Centres, as public institutions, have an internal structure and can use traditional forms of action under their national legal systems, the Competence Community, contrary to its name, is not (yet) a structured unit that can fall back on common organisational or

financial resources and thus enable cooperation. Thus, the role of the National Coordination Centres is crucial and it has to be taken into account, that there will be differences in the potential of the National Centres in the Member States.

- Despite the broad Community definition and explicit inclusion of civil society, start-ups and SMEs it has to be noted that such actors are at a structural disadvantage compared with larger institutions and companies. Active participation largely depends on financial and human resources. Limited resources thus mean limited participation opportunities, e.g., in Working Groups or in the Strategic Advisory Group, which in turn leads to lacking visibility. It has to be ensured that cybersecurity knowledge and expertise of such Community members do not get lost in the rather exclusive participation design.
- Overall, the Regulation does not yet offer recognisable advantages from a Competence Community membership and little to no incentive for an active involvement of a member.

5. Looking at the Community

In the cybersecurity domain there are many communities and sub-communities, with various degrees of overlapping and interconnections that are forming multiple networks. One can distinguish, for example, industrial and academic communities, crypto or cyber-resilience communities, financial or telecom sector cybersecurity communities, Member State or regional communities etc.

With our definition of cybersecurity ecosystem, we also acknowledge the existence of related resources (e.g., testbeds, datasets), practices (e.g., awareness building, certification of skills) or technologies so that the definition of an "ecosystem" includes all cybersecurity communities, networks and resources.

The community in Europe is primarily comprised of six different key components:

1) The European Citizen and Society (the key stakeholder, the customer and the end user)
2) European Solutions Providers and the Cybersecurity Industry as a whole
3) Government actors, regulators, standards bodies, and European institutions
4) Research and academic institutions focused on cybersecurity
5) European public sector and private sector users (often represented by Chief Information Officers (CIOs))
6) European Investors and Financial Institutions

Ultimately, a number of organisations already exist that are addressing the issue of ensuring the best possible network and results in the realm of European Cybersecurity. And as such, we will be covering two of these important focal elements, namely the Four Pilot Projects (CONCORDIA, CyberSec4Europe, ECHO and SPARTA) and the European Cyber Security Organisation (ECSO). In this section we also look at the conclusions and recommendations from our Deliverable D2.2 in which we present the concept and the execution of the CHECKs. The CHECKs are a unique opportunity built up from the grassroots, so that these represent the constituent components rather than a top-down approach.

5.1. Community Hubs

In CyberSec4Europe deliverables D2.1 and D2.2, the CHECK-based governance model was described and validated through specific implementation of this model in Toulouse. It was built with bottom-up inputs and assumed to address the main challenges of stakeholders in a heterogeneous community. In addition, each partner contributed with a short analysis of cybersecurity communities in their own countries, partially based on the comparison with the CHECK model.

All results revealed priorities such as capability-building or collaborative strategy, policy making and R&D roadmap input building. Although there was a clear support for bottom-up approach and openness to a diverse set of actors, initiatives and collaborations, validation and inputs from external initiatives also revealed the need to have both top-down and bottom-up approaches, leading to a more efficient stakeholder engagement throughout all levels. The conclusion was that the governance model needs to be flexible, oscillating between formal and informal, when it comes to stakeholder engagement, processes, and actions. From our initial model, we concluded in D2.2 that at least two types of CHECK could exist, depending on its financing and business model, for the similar types of services. One is part of the public administration and financed as a public good, while the other could be self-sustainable. These should construct economic models based on diversified financial resources, the foundation of which would come from major programs in the area, proposed by local authorities in a first step, before being completed by e.g. inter-alia (i) membership fees paid by its constituting members, (ii) access fees for consultation of its expertise, (iii)

consultancy fees related to the facilitation of participation in calls for proposals, as well as through (iv) bonus schemes on the results.

The mistrust that could exist between these two types of hubs, related to their perimeter of action and influence, is a separated governance challenge. There are, for example, specific services that hubs should offer, related to the economic development of a region, country, or specific sectors, which should be done in close partnership with solution providers and the research and higher education communities. One important activity of CHECK could be to provide the community-based assessments, whether these are for products (e.g., MOOC), services (e.g., training) or organizations (e.g., new members). Assuming the existence of CHECK networks, which could be a basis to constitute the EU Competence Community, the flexible governance model should align EU, national and regional interests, but also common research agendas. Interface mechanisms would thus be necessary to avoid any kind of duplication and limit overlap in tasks performed, as well as to make periodic alignments.

To quickly ensure the feasibility and relevance of the approach chosen for a specific territory, it is recommended to go through a phase of formal "pre-configuring" of the hub, favoring legal support by an actor in the territory with a certain notoriety in the targeted ecosystem. It enables CHECK to attract funds and to deploy a structuring project that would demonstrate the robustness and sustainability. This "seed" approach has also been also applied in the existing hubs and communities, even at the EU level, for example with ECSO which was a spin-off from EOS (European Organisation for Security).

Types for membership and representation should be defined, for example full member, associated member, and observers, before decision support rules could be set accordingly. The reputation of a core group, as well as early members, and trust relationships should be considered. Ensuring transparency of and fostering trust-based cooperation between diverse stakeholders is essential in this early stage.

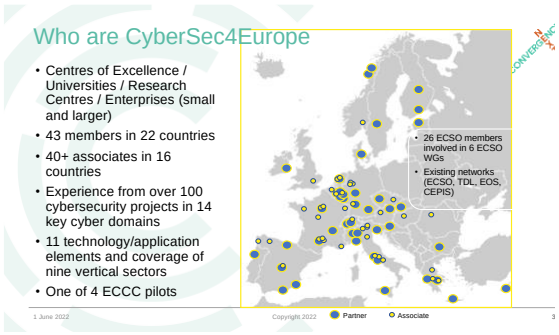
The main added value of a CHECK-like structure is the capacity to coordinate and orchestrate exogenous and diverse skill resources. The development of effective training practices should become an early priority action, specifically concerning end users, to improve the general awareness towards cybersecurity issues. The management of research and innovation capacity of CHECK is also considered as a priority, as well as the sector specific use cases, which are strategic for the region. Mentoring aspects and seed capital investment strategies were not highlighted, while testbeds and other resource sharing, such as space for experimentation, were also not prominently mentioned during the validation with stakeholders in Toulouse.

5.2. Four Pilots

5.2.1. Overview

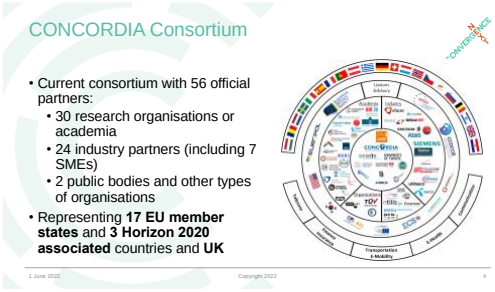
The European Commission selected four consortia to pilot the Cybersecurity Competence Network in Europe (CONCORDIA, CyberSec4Europe, ECHO and SPARTA).

The latest snapshot picture of the activities, efforts and results of the 4 pilot projects can be found in our CyberSec4Europe deliverable D10.3, which covers the key CONVERGENCE NEXT Event held in June 2022. CONVERGENCE NEXT was the concertation event which enabled the demonstration of the key results from all of the pilots and ECSO and represented the culmination of the joint pilot project efforts.



CyberSec4Europe Pilot Project Consortium[120]

ECHO Pilot Project Consortium[120]



CONCORDIA Pilot Project Consortium[120]**Error! Bookmark not defined.**

SPARTA Pilot Project Consortium[121]

Figure 1. Four Pilot project consortiums

Detailed information about each pilot project and their key results can be found on their individual websites (see below):

- ECHO Pilot Project - https://echonetwork.eu
- CONCORDIA Pilot Project - https://www.concordia-h2020.eu
- SPARTA Pilot Project - https://www.sparta.eu
- CyberSec4EuropePilot Project - https://CyberSec4Europe.eu

The four pilots have conducted extensive work on identifying stakeholders needs and common objectives, focusing on the ways of (formal) community involvement. The respective pilots' governance approach evolution has demonstrated the dynamically evolving cybersecurity landscape.

ECHO (Figure 2) conducted extensive research and design work to identify and agree upon the best fitting governance model which will ensure sustainability and effective exploitation of the project achievements and assets. Discussions have been held throughout the ECHO network, resulting in selecting a CNO model, with a Central Hub, National Hubs and Service Groups. Key processes were designed and tested through simulation games.

[120] From presentation given at CONVERGENCE NEXT 2022
[121] From presentation given at CONVERGENCE 2020

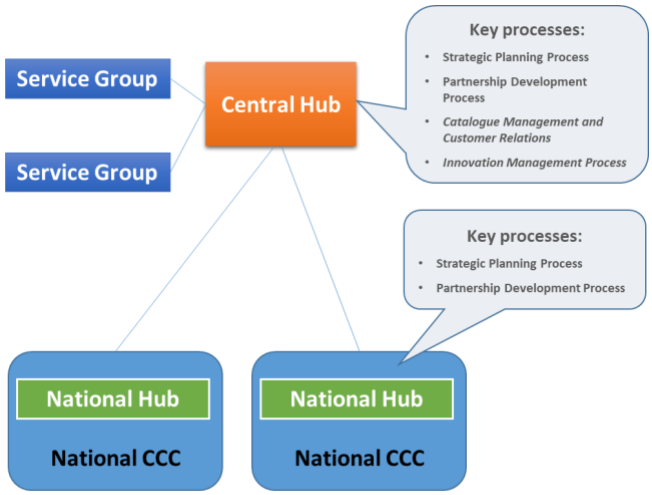


Figure 2. ECHO Governance Model[122]

Upon decision to proceed with a "bottom-up" approach, ECHO is now piloting the establishment of one National Hub (Bulgaria) and one Service Group - Governance Consultancy Services (E-GCS). The Governance Consultancy Services (E-GCS) builds upon the experience of the team involved in research and design of the post-project ECHO CNO. The first consulting project is internal – E-GCS will support the implementation of the pilot National Hub in Bulgaria thus showcasing and improving the methodology developed. E-GCS developed its Catalogue of Services and is now working on finalizing its Exploitation Strategy. The business model envisaged is customer-funded. E-GCS will work with the other ECHO assets to provide integrated services, and will cooperate with National Hubs to extend its offering.

ECHO sees high potential of applying their expertise in supporting the structuring of the European Cybersecurity Community (our partnership development process being only one example). The transition to a sustainable cybersecurity community involves transition and change management challenges which they are preparing to support.

CONCORDIA has been focused on the main challenges in the form of practical implementation of the pilots' ideas for the bottom-up low-level governance, stressing the importance of trust and related trustworthiness as the main enablers, also in any of the cyber/cyber-physical domains, any community and any information sharing. Knowing and understanding the ecosystem & communities is key for these communities to thrive and to collaborate efficiently (Figure 3).

[122] From presentation given at CONVERGENCE NEXT 2022

Figure 3. CONCORDIA Governance Model[123]

SPARTA's evolution of governance approach from the internal evaluation to the larger model has resulted in the following main governance objectives (see Figure 4):

- Setup the processes and governing instances for Cybersecurity Competence Networks
- Animate the strategic direction at board and working group level
- Ensure all stakeholder groups represented interact
- Continuous assessment of performance and strategic direction

Table 1: Typology of innovation agencies

	Radical innovation Shielded from interference	**Incremental improvements** Embedded in industries	
Targeted objectives	**State-led disruptors** *Radically innovative technological breakthroughs along a narrow, focused approach* Examples: DARPA, ITRI Governance goals: design new domain-specific technologies up to the level of early stage products with key industries	**Directed Upgraders** *Incremental innovation mobilizing resources around a relatively narrow range of industries and activities, facilitating large-scale change* Examples: A*Star, CORFO Governance goals: steer technological development, attract investments in key sectors	Mission-oriented and prize- driven innovation Significant resources Targeted technology fields
Wide-ranging objectives	**Transformation enablers** *Radically innovative, large number of small-scale experiments* Examples: OCS, Sitra Governance goals: develop clusters of innovative, high-productivity, research-intensive enterprises	**Productivity facilitators** *Small-scale, incremental product and process innovations across a wide range of established industries* Examples: GTS Institutes, IRAP Governance goals: creating local networks and organizing R&D communities	Delegated innovation objectives and R&D Modest resources Maximized application fields

Figure 4. SPARTA Governance Model[124]

[123] From presentation given at CONVERGENCE NEXT 2022

[124] Ibid.

5.2.2. Cross-Pilot Focus Group on Governance

The structural community-building efforts have manifested themselves in the Governance Focus Group initiative. The underlying idea for FG Governance setup was to work together and see how different governance approaches can be complementing, in order to help achieve the joint goal of setting up and maintaining the living and vibrant European cybersecurity community. The efforts undertaken between four pilot projects ECHO, SPARTA, CONCORDIA and CyberSec4Europe were aimed at identifying the umbrella governance approach for effective and efficient coordination in the institutional framework established by ECCC/NCCs. The joint efforts have manifested in the Governance FG sessions and joint panels at the Convergence and Concertation events by Cyber Competence Network of four H2020 pilots CyberSec4Europe, SPARTA, CONCORDIA and ECHO. Next to that, the joint White paper is being prepared at the time of writing of this deliverable to combine findings from the different approaches implemented by the different pilots on regional and functional (sectoral) principles.

With the preliminary results of the Governance FG being presented during the joint Convergence event in June 2022, it can be concluded that the pilots have arrived at the different forms of cyber regions, regional/sectorial hubs, or similar as a form of cybersecurity community organization. Involving underrepresented actors and incorporating grassroots initiatives has been identified as an important priority. The following recommendations have been outlined:

- Proceeding with the ongoing concepts/tests of the hubs
- Proceeding with stakeholder mapping
- Maintaining contact in order to work out our respective priorities
- Making sure that the cooperation experience and the established connections don't get lost after the pilots conclude
- Ensuring long-term strategic cooperation and coordination
- Keeping focus on trust as a key component.

5.3. ECSO

The European Cyber Security Organisation (ECSO) represents a significant cross section of the European Cybersecurity Community, including, but not limited to: solutions providers, users, public sector (including regulators), research and academia, as well as investors and financial institutions. In fact, it can be considered the most diverse cybersecurity community organisation in Europe representing the broadest set of stakeholders.

It is described by ECSO itself as:

> *"The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.*
>
> *ECSO is the privileged partner of the European Commission for the implementation of the Cybersecurity Public-Private Partnership, as well as a recognised actor in the European institutional landscape, A pan European, multi-stakeholder and cross sectoral partnership organisation working on cybersecurity with a holistic approach, ECSO federates the European Cybersecurity public and private sector, including large companies, SMEs and start-ups, research centres, universities, end-users and operators of essential services, clusters and associations, as well as the local, regional and national public administrations across the European Union Members*

States, the European Free Trade Association (EFTA) and H2020 Programme associated countries."[125]

ECSO has more than 270 members from 29 European countries with a large percentage of SME members (25%). ECSO key activities are focused upon the efforts of 6 active working groups:

1) Working Group 1 - Standardisation, Certification and Supply Chain Management
2) Working Group 2 - Market Deployment, Investments and International Collaboration
3) Working Group 3 - Cyber Resilience of Economy, Infrastructure & Services
4) Working Group 4 - support to SMEs, coordination with countries and regions
5) Working Group 5 - Education, Training, Awareness, Cyber Ranges
6) Working Group 6 - Strategic Research and Innovation Agenda and Cyber Security Technologies

ECSO has created a significant set of cybersecurity investment events, cybersecurity days, cybersecurity summits, and community events which foster networking, investment, advocacy and dialogue among all of the actors, stakeholders and players related to cybersecurity in Europe and beyond.

The uniqueness of ECSO is the fact that it is a supranational community of stakeholders covering extensively the communities of users, solutions providers, the private sector, the public sector, and the research and academic communities. Furthermore, ECSO brings together the cybersecurity investor community and the community of European CIOs with important offerings in both realms.

ECSO has developed a confidential secure platform for CIOs to share information in a way that clearly limits access to those who are vetted and who have a need to know such that the information can be kept confidential and will not be shared with a wider audience. This represents the first comprehensive European cybersecurity sharing platform which is for the benefit of the CIO community specifically.

ECSO also has secured the commitment of cybersecurity investment community to develop a "fund of funds" for cybersecurity investment, and as such this will be the first financing facility of this kind for addressing cybersecurity investment in Europe.

[125] www.ecs-org.eu

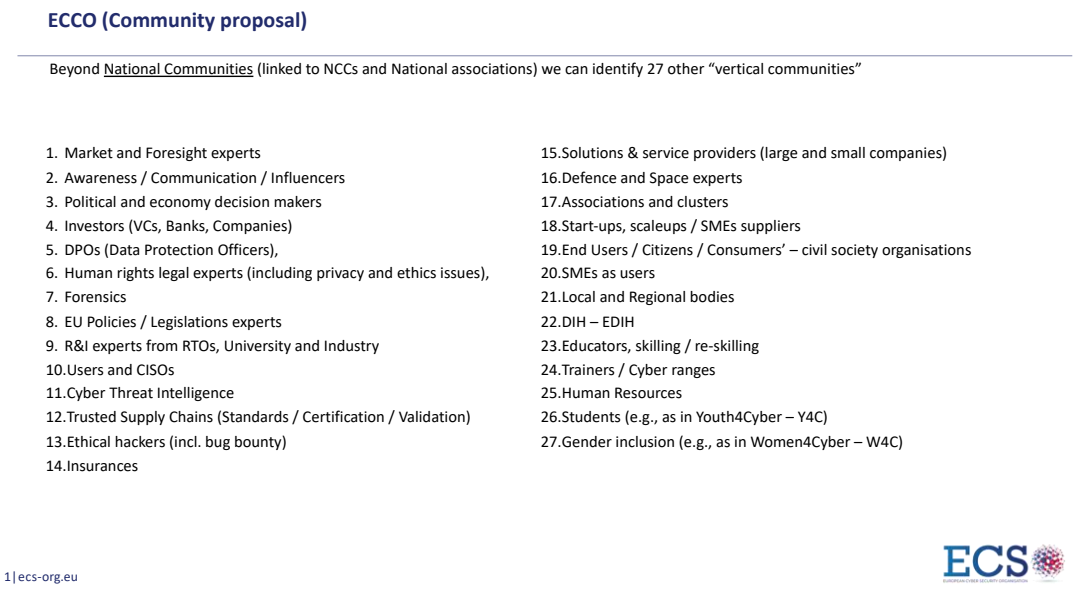


Figure 5. ECSO – 27 vertical communities[126]

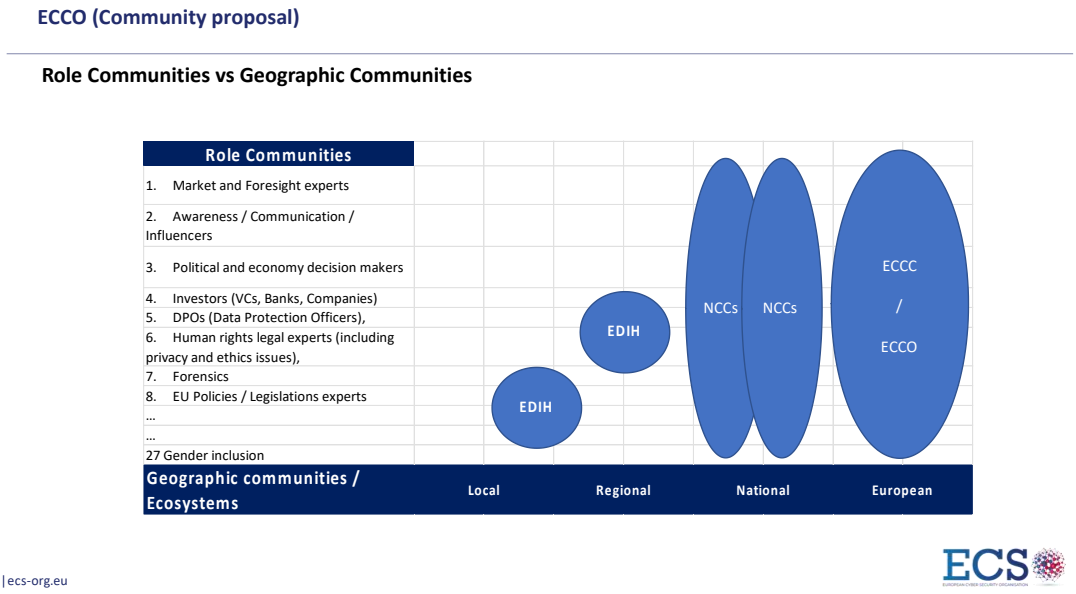


Figure 6. ECSO Role Communities vs Geographic Communities[127]

In the evolution to the next phase of the implementation of the European Cybersecurity Competence Centre (or ECCC), it is envisaged that ECSO and it's working groups will form the core of the community along with the 4 pilot projects.

[126] www.ecs-org.eu
[127] Ibid.

5.3.1. ECSO role in European Competence Community

Since the initial discussions for the creation of the cPPP in 2013 and then with the official development of such public private partnership, we have strongly cooperated with the European Commission and the other European Institutions, well beyond the formal cPPP objectives. As non-for-profit organisation, ECSO members consider that the role of this association is to provide all the possible support for the growth of the European competence and market. This objective is embracing activities going well beyond the identification of initial R&D priorities as in traditional cPPPs but, first of all, in the development of a European cybersecurity community and network for a stronger cooperation across countries, sectors and communities. With the development of the network and of the communities, the development of the market in a wider cooperation will follow more easily.

Community-Building

In the first six years of ECSO we have seen the different levels of maturity in the digital transition of the different countries and sectors. We have helped them, as much as possible, to grow and possibly cooperate. We have identified the different kind of stakeholders and we have supported the development of communities at local, regional and national level. We have also created new organisations / networks to boost the gathering of experts (e.g. CISOs) or of sectors of the community (e.g. women) to better understand their needs and help them participating actively in the protection of the digital transformation. These activities of "community building" are fundamental in the growth of the society and market and in the growth of ECSO as well. A lot has been done since 2016, but a lot remains to do.

Awareness, Education and Training

ECSO has contributed to a cybersecurity education and training capacity building effort in Europe with papers on Gaps in Education and Professional Training[128], Understanding Cyber Ranges: From Hype to Reality[129] (includes use cases for education purposes), and Minimum Reference Curriculum[130] for universities. In addition, initiatives such as Youth4Cyber and ECSO's monthly awareness calendar have helped raise awareness among the European youth and general public on key cybersecurity topics. In gathering several education and training providers within its membership (and beyond). In building up a community of providers, trainers, and industry experts, ECSO in direct collaboration with the European Commission (DG CNECT), ENISA and the four Pilot projects has worked to implement scalable solutions and the most appropriate tools and learning methods to develop applicable capability. This includes the organisation of awareness workshops and toolkits, the definition of academic and professional cybersecurity curricula, and showcasing of relevant European exercise and training opportunities (cyber ranges, MOOCs, hands-on learning methods, micro-credentialing, etc.).

Cybersecurity Skills

With papers on Cybersecurity Professional Certification[131], Simulation-based Competence Development, and Understanding European Cybersecurity HR Recruitment Processes[132] (based on surveys from its European Human Resources for Cyber (EHR4CYBER) initiative and the Pilots), ECSO has leveraged the expertise of its members and outcomes from the four Pilot projects to bridge the gap between academia and industry for skills and competence development for the future cybersecurity workforce and brought increased awareness on the needs of the job market. ECSO has also been an active contributor in the ENISA

[128] https://ecs-org.eu/documents/publications/5fdb282a4dcbd.pdf
[129] https://ecs-org.eu/documents/publications/5fdb291cdf5e7.pdf
[130] https://ecs-org.eu/documents/publications/6283b1eb9bce9.pdf
[131] https://ecs-org.eu/documents/publications/60101ad752a50.pdf
[132] https://ecs-org.eu/documents/publications/6202804a65a70.pdf

Ad Hoc WG on developing a cybersecurity skills framework, helping to define the professional profiles (particularly the CISO, CTI specialist, and educator roles) and leading the work on integrating soft skills within the framework itself and in the wider EU policy discussion (I.e. as member of the European Commission's Pact for Skills and Large-scale Partnership for the Digital Ecosystem). The Women4Cyber Foundation has also become a significant player in the European skills capacity-building effort, with the facilitation of trainings for women, establishment of mentorship programmes, and development of a Women4Cyber Academy (online one-stop shop for cybersecurity courses, trainings, etc.).

R&I roadmaps

As counterpart of the European Commission for the implementation of the contractual Private Public Partnership (cPPP), ECSO has delivered a comprehensive R&I roadmap[133] as input for 2017-2020 Work Programme. Leveraging its unique membership and on the initial work, the ECSO Working Group 6 (WG6), has defined the cybersecurity R&I roadmap for trusted technologies addressing the challenges of digitalisation of the society and industrial sectors to foster EU digital autonomy. This has resulted in two documents[134],[135] as inputs to the Horizon Europe and Digital Europe Programme (ECSO 2021-2027 vision). The documents identify some strategic areas for investment in order to develop a Capability Development Plan to increase digital autonomy and respond to the needs of our industrial sectors, while protecting the European fundamental rights.

ECSO has also engaged with other initiatives and cPPPs at the European level and contributed to their R&I roadmaps to ensure a close cooperation and alignment on the relevant cybersecurity challenges in key technological areas such Artificial Intelligence or 5G and beyond. ECSO is one of the initiators of the Trans Continuum Initiative (TCI)[136], with the ambition to elaborate joint recommendations for R&D to be carried out in EU- or JU-funded work programmes addressing challenges in the digital continuum.

Finally, the ECSO WG6 has worked on a number of technical papers, such as on Internet of Things (IoT) and Blockchain, to define cybersecurity challenges encompassing different aspects from technology to policy and application to vertical sectors.

Dedicated Forum for Civil and Defense Sectors

ECSO has a dedicated forum to discuss the synergies between the civil and defence sectors. This initiative has been launched to structure the dialogue with the European Defence Agency (EDA) and to understand how the already available and soon-to-be- commercialised technologies developed for civilian or industrial applications can be used in the cyber defence domain. The main motivation behind is to increase cyber resilience in the defence domain and ensure synergies between civil and defence sectors to better use and leverage the respective investments in Research and Innovation (R&I). The objective is to define the challenges for the cyber defence sector to identify potential gaps in cybersecurity technologies and what are the collaborative actions needed to sustain long-term European cybersecurity and cyber defence capability development strategies. This is resulted in the publication of a document identifying the "Initial Areas of Interest for Cyber Security for Dual Use Technologies".

[133] ECSO Strategic Research and Innovation Agenda. https://ecs-org.eu/documents/publications/59e615c9dd8f1.pdf

[134] Input to the Horizon Europe Programme 2021-2027: Priorities for the definition of a Strategic Research and Innovation Agenda in Cybersecurity https://ecs-org.eu/documents/publications/5fdc4c5deb6f9.pdf

[135] Input to the Digital Europe Programme 2021-2027: Priorities for supporting the implementation of policy, technology, competitiveness, and competence-building https://ecs-org.eu/documents/publications/5fdc4ca16dde0.pdf

[136] https://ecs-org.eu/newsroom/8-european-associations-and-projects-commit-to-the-trans-continuum-initiative

Vertical Industries – CISOs

Since its establishment, ECSO has gathered its members (industry, academia, and users/operators) and sectoral associations to elicit an understanding of the functionalities and needs of different vertical industries in order to provide recommendations for needed R&I, investment, operational requirements, and regulatory considerations for different sectors. With the development of Sector Reports for Industry 4.0 and ICS[137], Energy[138], Transport[139], Finance[140], Healthcare[141], and Smart Cities[142], a state-of-the-art and definition of needs and priorities has been performed, in close consultation with relevant sectoral representatives. Sector-specific work conducted also includes an analysis of the needs for different ISACs[143] and policy / legislative recommendations such as on the review of the NIS Directive[144].

ECSO has also successfully launched the operations of the first European Community of Chief Information Security Officers (CISOs), gathering security leaders from European countries to cooperate on the most pressing cybersecurity topics in a trusted, secure and time-sensitive way. ECSO's CISOs European Community (CEC) currently counts around 190 CISOs and is open for membership requests from European CISOs. With the CEC, ECSO is adopting a broad approach by hosting CISOs from both the public and private sector and ranging from SMEs to large companies. The CEC allows its Members to share lessons learned and other operational information through an instant messaging platform, receive daily briefings on the latest and most pressing cybersecurity news and vulnerabilities, facilitate the interaction with European Institutions on policy and legislative priorities (e.g., NIS 2), and have access to monthly presentations and webinars held by peers. CISOs currently exchange in a dedicated chat group run on Signal, while preparing for a migration to a more structured Community platform that will enable sector-specific discussions on sensitive issues and threat information sharing. The rapid growth of CISOs adhering to this initiative shows the importance of such a tool which allows them to exchange lessons learned and best practices, share information on operational issues, develop positions and link with the European institutions, through regular networking and meetings on specific issues. ECSO is organising the first physical CISO Meet Up event in Brussels in Autumn 2022.

Supply Chain Management and Certification

The activities of ECSO on standardisation and certification are coordinated by Working Group 1 (WG1) that has contributed to the Cybersecurity Act with a Meta-scheme approach for the EU Cybersecurity Certification Framework. ECSO considers standardisation and certification as important areas to develop a European industrial strategy and strategic autonomy. One of the main objectives of ECSO is to establish trusted supply chains at European level, also via international cooperation, and reduce the (technical and business) impact of cybersecurity attacks to improve resilience for the increasing digitalisation of society and industrial sectors.

ECSO has also published several key documents including a State-of-the-Art Syllabus (SOTA) which helps identify potential gaps in standardisation based on the analysis of the market needs and priorities for certification schemes (EU rolling work programme). Another relevant one is the Security Assessment Option document which explains how to benefit from the right mix of security assessments, and what constraints stakeholders should be aware of. To contribute to the roll-out of certification scheme, ECSO has

[137] https://ecs-org.eu/documents/publications/5fdb2628a0318.pdf
[138] https://ecs-org.eu/documents/publications/5fdb2673903c6.pdf
[139] https://ecs-org.eu/documents/publications/5fdb2791553ac.pdf
[140] https://ecs-org.eu/documents/publications/5fdb25077e039.pdf
[141] https://ecs-org.eu/documents/publications/5fdb26b99d089.pdf
[142] https://ecs-org.eu/documents/publications/5fdb27182b472.pdf
[143] https://ecs-org.eu/documents/publications/5fdb27584719d.pdf
[144] https://ecs-org.eu/documents/publications/5fd24425bc74c.pdf

published the Product Certification Composition document, which serves as a high-level set of guidelines when seeking a certification by composition under the requirements defined by the EU Cybersecurity Act. Lately, ECSO has published the System Security and Certification Considerations as a high-level awareness document on the system lifecycle security and relevant certification information when applicable. This document aims to have a level of simplification that fits most stakeholders, including non-system security experts.

Start-ups and SMEs

ECSO has developed several market-oriented and ready-to-use tools to help European cybersecurity start-ups and SMEs develop their business outside their traditional home markets and scale at the European level. The CYBERSECURITY MADE IN EUROPE Label has been created as a marketing tool to promote European cybersecurity companies and increase their visibility on the global market[145]. ECSO has gathered 19 European entities, ranging from industry associations to public agencies, to successfully issue the Label in Europe. Since its launch in late 2020, a hundred European cybersecurity industry players have applied for the Label. Companies have been using the Label to promote their European origins and added value among international business partners, investors, and customers.

The Cybersecurity Market Radar and the Cybersecurity Marketplace is another flagship initiative by ECSO dedicated to helping Europe's cybersecurity start-ups and SMEs to establish themselves on the market. The Radar was launched to display the products and services of the European cybersecurity companies in a competitive non-biased way, segmented by solution category[146]. The companies were categorised and presented based on the cybersecurity market taxonomy developed by ECSO to increase market transparency and provide a shared understanding of the cybersecurity market[147]. The Radar proved to be popular among European SMEs with 125 companies joining the Radar. Its success has led ECSO to enlarge the scope of the project with the development of a Cybersecurity Marketplace to provide European cybersecurity providers with a more dynamic and interactive online platform where they can showcase their products and services. They can also find potential business partners or investors. On the other hand, investors and end users can discover companies for potential investments, solution integration and purchases.

ECSO also launched the European STARtup Award in 2020 to recognise the next European champions in cybersecurity and further incentivise investments in European cybersecurity technologies[148]. The Award is built around a shared belief that European cybersecurity companies delivering ground-breaking cybersecurity solutions need recognition and investment support to be able to scale up and develop their business in Europe. The Award leverages ECSO Cyber Investors Days, a well-established cybersecurity business matchmaking event. Several Cyber Investor Days are organised by ECSO together with its members and partners each year, where nominees are selected. The selected nominees meet at the final contest where the winner is chosen by the judging panel composed of European cybersecurity industry experts and thought leaders.

[145] CYBERSECURITY MADE IN EUROPE Label, link: https://www.cybersecurity-label.eu/

[146] Cybersecurity Market Radar, link: https://ecs-org.eu/initiatives/ecso-sme-hub

[147] 'A Taxonomy for the European Cybersecurity Market Facilitating the Market Defragmentation', by ECSO Working Group 2 on Market Deployment, Investments, and International Collaboration, February 2021. Link: https://ecs-org.eu/documents/publications/605de1e3a768a.pdf

[148] 'PHYSEC Crowned Winner of ECSO's European Cybersecurity STARtup Award', 3rd February 2021. Link: https://ecs-org.eu/newsroom/physec-crowned-winner-of-ecsos-european-cybersecurity-startup-award and 'Celebrating European innovation: ECSO announces the winner of the 2021 European Cybersecurity STARtup Award', 7th April 2022. Link: https://ecs-org.eu/newsroom/celebrating-european-innovation-ecso-announces-the-winner-of-the-2021-european-cybersecurity-startup-award

These tools aim to alleviate the challenges of the still fragmented European cybersecurity market and are fine examples of the market-oriented tools that bring added value to Europe's cybersecurity market players.

Regional Ecosystems

Soon after its inception in 2016, ECSO has started closely working with the European regions specialising in cybersecurity and contributed to the initiatives that aim to enhance their role in strengthening Europe's cybersecurity posture. ECSO recognises the role of the regions in supporting the implementation of the EU cybersecurity policy by linking the local users, research centres and suppliers of cybersecurity solutions with the national and European levels.

ECSO has been developing and implementing the Interreg Europe CYBER project (2018-2023), together with seven European regions and the Brittany Development Innovation agency[149]. As an Advisory and Communication Partner, ECSO has provided strategic policy support to the project partners in sharing their regional good practices, defining policy changes and actions plans, which aim to improve regional cybersecurity ecosystem and support its cybersecurity companies. ECSO has been disseminating the results and achievements of the project to the EU policy maker and other cybersecurity stakeholders.

ECSO has also coordinated the 'Cybersecurity Smart Regions' pilot action, aiming to enhance cooperation among European regions specialising in cybersecurity[150]. One of the key deliverables was the mapping of cybersecurity capabilities provided by 470 regional cybersecurity players from four European regions with some of the most mature cybersecurity ecosystems: Estonia and the regions of Castilla y León (Spain), Brittany (France) and North Rhine-Westphalia (Germany). The 'Cyber Smart Regions' presented the practical case of how the increased cooperation among the regions can help to reduce market fragmentation. ECSO has been working on the creation of the network of the European Digital Innovation Hubs (EDIHs) specialising in cybersecurity. Given its expertise in Europe's cybersecurity market and its experience in federating regions and local ecosystems, ECSO has been recognised by the candidates of the EDIHs as the best-positioned organisation to establish and coordinate the network of cybersecurity EDIHs. The main goal of the network is to facilitate collaboration among cybersecurity EDIHs. The ongoing collaboration is key to ensuring that EDIHs will provide well-informed technical expertise and advisory services. As the coordinator of the EDIHs network, ECSO will provide a defined list of services to support the functioning of EDIHs. The network of cybersecurity EDIHs is under finalisation and is expected to be officially launched in autumn 2022.

Matchmaking Events Series (Cyber Investors' Days)

ECSO established a matchmaking event series for cybersecurity in 2017, also known as Cyber Investor Days. Cyber Investor Days aim to address the profound lack of access-to-finance and access-to-market opportunities for European cybersecurity start-ups and SMEs, looking for funding or expansion of sales channels[151]. The initiative also provides investment and business opportunities for investors and integrators, looking for new portfolio companies and solution providers based in Europe.

To reach out to different European cybersecurity ecosystems, each edition of the event is organised in a different European city in close cooperation with the local ecosystem. The ECSO's Cyber Investor Days already took place in Tallinn (September 2017), Paris (March 2018), Milan (September 2018), Berlin (November 2018), Madrid (May 2019), Luxembourg (October 2019), Brussels (May 2020, digital), Bochum (November 2020, digital), Porto (June 2021, digital), Helsinki (December 2022) and Dublin (June 2022).

[149] Interreg Europe CYBER. Link: https://projects2014-2020.interregeurope.eu/cyber/

[150] S3 Industrial Modernisation Partnerships – Cybersecurity link: https://s3platform.jrc.ec.europa.eu/cybersecurity

[151] Cyber Investor Days link: https://www.ecs-org.eu/initiatives/cyber-investor-days

Since 2020, several local Cyber Investor Days were organised by ECSO's members and partners, namely eurobits (Germany), Brittany Region and Sopra Steria (France), SECURITYMADEIN.LU (Luxembourg), Polish Cybersecurity Cluster #CyberMadeInPoland (Poland) and Cybersecurity Agency of Catalonia (Spain).

The initiative has been growing in popularity and the industry scene would indicate that this is set to continue throughout the upcoming years. Since its launch, Cyber Investor Days have received more than 700 participants and hosted more than 900 B2B meetings. The number of the European cybersecurity start-ups and SMEs applying to the event has increased by nearly five times: from 11 applications received for the Tallinn edition to 40-50 applications received for the latest editions. The event also experienced growing recognition among European and international investors. More than 240 investors from Europe, the United States and Japan have participated in the ECSO Cyber Investor Days to date. At least four cybersecurity investment deals by Telefónica-Wayra (Spain), eCapital entrepreneurial Partners AG (Germany), ITrust (France) and Sonae IM (Portugal) were initiated and successfully closed as a result of the cybersecurity matchmaking events organised by ECSO. Some companies are still in funding negotiations.

Market and Investment Funds Community

ECSO has successfully built an active and knowledgeable community of European and international investors specialising in cybersecurity, which will be further developed under the Invest4Cyber name. ECSO has been leveraging its successful Cyber Investor Days to bring together European and international venture capital (VC) and private equity (PE) funds to accelerate the cooperation and joint investments into leading European cybersecurity start-ups and scale-ups. Several joint investments were made because of this initiative. Nine major VC funds specialising in cybersecurity belong to the ECSO's community of investors.

Recognising the threats of the persisting cybersecurity market fragmentation and the investment gap in Europe's cybersecurity market, ECSO has proposed the creation of the European Cybersecurity Investment Platform (ECIP) of at least €1 billion EUR. The proposal was endorsed by 49 European cybersecurity players[152]. The ECIP, structured as an equity fund, would strengthen the investment capacities of the existing cybersecurity investment funds and facilitate the emergence of the pan-European cybersecurity investment. The ECIP would also provide a focus on Series A and growth-stage companies to offer a level playing field for early-stage companies which currently constitute the majority of investments in Europe. It would also create a more specialised investment capacity to attract large international limited partners (LPs) to invest in the European market.

To create such a pan-European investment instrument, a feasibility study on the design and set-up of the ECIP has been launched[153]. The European Investment Advisory Hub – a joint initiative of the European Investment Bank (EIB) and the European Commission – has carried out the study, in cooperation with the EIB and the European Commission experts, leading European cybersecurity investors and ECSO. The results of the study will help to define the next strategic steps toward creating a robust and competitive investment landscape in Europe amidst the increased global competition in the technology sector.

Engagement of the Community / Promotion Activities

[152] 'ECSO to launch a European Cybersecurity Investment Platform', November 2020, link: https://ecs-org.eu/newsroom/ecso-to-launch-a-european-cybersecurity-investment-platform

[153] 'European Investment Advisory Hub and ECSO announce first step towards a new pan-European cybersecurity investment instrument', October 2021, link: https://www.ecs-org.eu/newsroom/european-investment-advisory-hub-and-ecso-announce-first-step-towards-a-new-pan-european-cybersecurity-investment-instrument

As Europe's unique public-private partnership for cybersecurity, it is in ECSO's DNA to bring together and engage the cybersecurity community via marketing activities which disseminate not only ECSO's results, but also the work carried out by ECSO and its Members (via ECSO's six Working Groups, two Task Forces and nine initiatives), as well as the cybersecurity community at large. Promotional activities range from organising physical or online events and workshops (e.g., ECSO'S workshop on the need for cybersecurity experts in Europe, the workshop on System security and certification considerations and the webinar on Log4J), to cooperating with Europe's top cybersecurity events (e.g. it-sa, FIC, European Cybersecurity Forum – CYBERSEC etc.), disseminating information via newsletters (including ECSO's bi-weekly newsletter, and newsletters by ECSO Members and DG CNCT), social media channels (ECSO and Women4Cyber's LinkedIn and Twitter profiles, including ECSO's YouTube channel) and press activities, as well as coordinating promotional work with our strong network of Members (e.g. Cyber Investor Days). ECSO also fosters engagement and cooperation with its Members and the cybersecurity community at large via its CYBERSECURITY MADE IN EUROPE Label website and own communication plan, which is greatly based on engaging with existing and new companies who have obtained the Label, as well as with the European press, which has expressed strong interest in such initiative.

EU Policy Areas

Since its creation in 2016, ECSO has worked on different policy areas to support the work of European institutions with ideas and insights coming from the European cybersecurity community. At the same time, ECSO has informed its members the EU policies in the cybersecurity domain. With its impartial position and its diverse member base, ECSO was able to establish itself over the years as a reliable and non-lobby partner for the European Institutions. The uniqueness of ECSO proved to be an added value for the entire cybersecurity ecosystem and made ECSO the perfect place for policy makers, civil society, and industry to meet, exchange ideas, and collaborate. Between 2017 and 2018, ECSO provided valuable inputs to the Council on the certification scheme of the Cyber Security Act that were instrumental during the during the negotiations of the legislative file. Between 2016 and 2020, ECSO maintained an ongoing dialogue with the European Parliament, DG CNECT, and several permanent representations of EU Member States. In that period ECSO consulted with policy makers on different legislative files including the NIS2 directive, the eIDAS regulation, the ECCC regulation and the EU Cybersecurity Strategy.

By leveraging on its large community and stakeholders' base, ECSO has provided policy makers with data and instruments to understand transversal issues like the gender and skills gaps in cybersecurity and intervene to balance them. ECSO and its sister association Women4Cyber engaged with a variety of stakeholders including Members of the European Parliament, DG CNECT, the cabinet of the European Commission Vice President Margaritis Schinas and the civil society at large, to exchange solutions and act both on the gender dimension of cybersecurity and the need for skilling, up-skilling, and re-skilling towards cybersecurity the European workforce.

Since its creation, ECSO has also produced, within its working groups, a number of position papers on several cybersecurity topics that provide food for thoughts and informed opinion to the EU institutions and the general public[154]. To support its members in understanding the impact of EU cybersecurity policies and have a structured dialogue with European Institutions, ECSO set up a Legal and Policy Task Force to provide transversal support to all its WGs. The Policy Task Force was given a new impulse in March 2022 with the presence of a permanent person in charge of helping ECSO Members to navigate the legislative mechanisms around cybersecurity legislation in the EU. Through the Policy Task Force, ECSO will continue to provide an informed and impartial opinion to policy makers from its community of cybersecurity and political experts.

[154] https://ecs-org.eu/publications

Since its founding in 2016, ECSO has been the partner of the European Commission in the contractual Public Private Partnership (cPPP) on cybersecurity and has started since 2017 an informal dialogue at the highest level to discuss how to develop a network of cybersecurity competence centres in Europe. ECSO has then continued in the years to support the Pilots, H2020 projects like Cyberwatching.eu and to discuss with European and National institutions on how to develop the European Cybersecurity Competence Centre (ECCC) approach.

From the beginning, ECSO has developed and operated several working groups and task forces to tackle dynamically the most urgent issues requested either by the European Institutions in the frame of the cPPP or by its members. Even beyond the objectives of the cPPP, ECSO has informally provided the European Commission with market analysis and categorising the main European players. We have also developed efficient mechanisms of cooperation among stakeholders that in certain cases took several years (e.g. for users / CISOs) due to the distance, the complexity, the drivers, and the effective barriers between the vision in traditional research projects and effective market operational needs.

To support the objectives of the cPPP, ECSO developed first a community of research (mainly technology) experts to define the R&I priorities for H2020 (and then Horizon Europe and DEP), also providing visibility of relevant funding opportunities for cybersecurity research and innovation for H2020 and more recently for Horizon Europe and DEP through brokerage events.

It has then developed a community on Trusted Supply Chains (including Standardisation / Certification / Evaluation experts) to support the definition of the Cybersecurity Act and the cooperation with ENISA and the European Standard Developing Originations, CEN/CENELEC and ETSI. ECSO has progressively developed links with the defence (EDA) for identification of dual use technology priorities and potential synergies with the space sector (ESA).

One of the major challenges (and now present major strengths) has been for ECSO to start an effective dialogue with users / operators. The European network of CISOs from different sectors and countries (we are now at 200 active CISOs members from 26 different European countries) is now providing an invaluable contribution to effectively understand the threats, the needs, and the evolution of the market, beyond traditional approaches and participation of some technical experts from users in research projects.

ECSO has also tackled and innovated the approach to support start-ups and SMEs, initially organising matchmaking events between its community of investors (VCs, banks etc.) and selected startups / scaleups. We have then triggered the initiative to set up a "fund of fund" of 1 bln € dedicated to cybersecurity, work ongoing with the European Investment Bank (EIB). The ECSO activity to support SMEs has also benefitted from the cooperation with national, regional, and local bodies that are strongly supporting the growth of their economy and local companies, an approach that will be further developed in the European Digital Innovation Hub (EDIH) scheme with matchmaking events between suppliers and buyers from users as well as with accelerator services.

ECSO has not only tackled market or technology issues but also human factors issues (skills, education, training, ranges) developing links with communities of students (via the Youth4Cyber initiative), educators (in particular at university level), job structures (with the Human Resources community of its members). Of particular importance, it has been the creation of the Women4Cyber Foundation, now swarming into national chapters to support inclusion of women into the cybersecurity market also via concrete actions like mentorship, a European Academy and a Job platform.

Support to the ECSO working groups has been provided by internal task forces like the one analysing EU policies and or those for defining position on SOC and CTI of for sovereignty and strategic autonomy.

A unique ECSO feature has also been given by the informal dialogue with National Public Administrations via a dedicated committee (NAPAC) to discuss acceptability at country level of ECSO working groups findings and recommendations.

ECSO has also used the competence and views developed in its working groups and task forces to establish links and cooperation with other European and international bodies (Europol, ITU / UN; WEF; US CISA; Japanese Ministries, etc.).

Thus, ECSO is uniquely qualified to address the key areas as follows:

- Supporting the European Cybersecurity Competence Centre and the Network of National Coordination Centres in fostering knowledge-sharing and networking between national, regional and local ecosystems specialised in cybersecurity;
- Support to the development and growth of an internal market in Cybersecurity products and services in the EU. Where relevant and appropriate, activities shall be in line with the JRC Cybersecurity taxonomy and Atlas;
- Support to Cybersecurity start-ups and scale-ups in all Member States, including with a view to attract investment to the EU;
- Support to education, training, and gender balance in cybersecurity, in line with relevant actions promoted by organisations, including ENISA;
- Support awareness raising, including supports for national outreach and engagement to underpin cohesion of the Union in the field of cybersecurity.

Furthermore, ECSO already has key working groups in place addressing a broad set of requirements:

- R&I Road-mapping: continuous development and update of a European Cybersecurity Strategic Research and Innovation Agenda, encompassing the whole cybersecurity value chain and building on the work initiated by the four H2020 Pilots (ECHO, SPARTA, CONCORDIA, CyberSec4Europe), ENISA, ECSO.
- Deployment/uptake in vertical domains: how to best address Cybersecurity Challenges in critical domains such as, for example, eHealth, finance, infrastructures, telecommunications, smart cities and transportation.
- Analysis and recommendations for potential synergies between the civilian and defence spheres of cybersecurity.
- Start-ups/SMEs support: development of operational strategies at national and European level to support the Start-ups/SMEs ecosystem in Europe and benefit from its innovations.

5.4. Conclusions

This chapter has looked into the current forms of the cybersecurity community organization. The first sub-chapter outlines the community setup recommendations based on the previous work of WP2 of CyberSec4Europe. With evidence for clear support for bottom-up approach and openness to a diverse set of actors, initiatives and collaborations, the need to have both top-down and bottom-up approaches became clear in the process of research and validation. The conclusion was that the governance model needs to be flexible, oscillating between formal and informal, when it comes to stakeholder engagement, processes, and actions. From our initial model, we concluded in one of the previous deliverables D2.2 that at least two types of CHECK could exist, depending on its financing and business model, for the similar types of services. The main added value of a CHECK-like structure is the capacity to coordinate and orchestrate exogenous and diverse skill resources.

The chapter proceeds to present an over view of the selected four consortia selected by the European Commission to pilot the Cybersecurity Competence Network in Europe (CONCORDIA, CyberSec4Europe, ECHO and SPARTA). The four pilots have conducted extensive work on identifying stakeholders needs and common objectives, focusing on the ways of (formal) community involvement. The respective pilots' governance approach evolution has demonstrated the dynamically evolving cybersecurity landscape. With the preliminary results of the Cross-Pilot Governance Focus Group being presented during the joint Convergence event in June 2022, it can be concluded that the pilots have arrived at the different forms of cyber regions, regional/sectorial hubs, or similar as a form of cybersecurity community organization. Involving underrepresented actors and incorporating grassroots initiatives has been identified as an important priority.

Finally, the chapter present ECSO and its rich landscape of diverse assets, as well as the role it is currently playing an could potentially play for the Community due to its positioning, organization, initiatives, and resources. ECSO policy work and involvement in regional ecosystems are some of the examples of valuable contributions.

The H2020 pilot projects (CyberSec4Europe, ECHO, Sparta and Concordia) and their focus groups, as well as the European Cyber Security Organisation (ECSO) and its working groups represent a rich connected community. The majority of relevant stakeholders are involved in the cybersecurity ecosystem through the four pilots and ECSO, forming an ecosystem with different focusses, maturity stages, and objectives. Therefore, dedicated funds should be provided, e.g. under the Horizon/Digital Europe Programmes, to deepen the cooperation and coordination of such stakeholders, alongside dedicated funds to set up CHECKs in all Member States.

6. Conclusions and Recommendations

With no active institutional and funding efforts towards ensuring the cohesion of the European cybersecurity community, the rich existing potential of research, skills-building, and market applications is in danger of not getting exploited. The new structure based on the European Centre, the NCCs, and the Community pillars needs to include more tangible actions for nurturing and structuring the Community. A cohesive European cybersecurity ecosystem is essential to further develop and enhance the European innovation potential, as well as to ensure European digital sovereignty. Based on the findings of D2.1, D2.2, D2.3, D2.4, we offer the following main policy recommendations:

- **Institutionalize the Cybersecurity Competence Community**

It is key that the National Coordination Centres have a systematic approach to registering communities and hubs. With the Regulation providing no guidelines on how possible members, that are not already well networked and informed, should learn about the possibility of application and registration, it is important to develop mechanisms to do so. The benefits and added value for possible members to get acknowledged as members of the Community through the application and registration procedure should be made clear.

- **Use CHECKs to organise the Community, in order to address the existing challenges, while providing flexibility**

We offer the concept of a collaborative network of local cybersecurity hubs, 'Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs)', which are envisioned as environments for community-level research, innovation, and capacity building in cybersecurity. CHECKs are a bottom-up approach which will not only complement the "top-down" focus from the EU Member States and the ECCC, but can actively contribute to addressing cybersecurity in Europe. Many similar "hub" like structures of communities already exist and we should acknowledge different types and sorts of CHECKs, including those that are created in top-down manner, with the funding from a government. This concept answers concrete stakeholder demands and is based on requirements, empirical best practices, and stakeholder feedback. The existing diversity in the Member States and their connection to the NCCs and to the Community can be integrated through CHECKs (thus resulting in complementary approaches for addressing the same mission).

- **No "one size fits all" approach**

There is an important diversity in the national Member States and the connection between authorities / the NCCs / and the communities (thus resulting in differing approaches to addressing the same mission).

- **Explore practical implications of community decision-making**

There is a need to improve the process of research transfer to industry. New mechanisms could offer solution, such as collaborative ranking of the assets that are exploitable for the market and thus can receive funding. In combating fragmentation in the cybersecurity domain the existence and promotion of "communicating vessels" is of paramount importance. Knowledge should flow where it is needed – i.e., it should be transported between the countries and/or sectors to overcome "the cybersecurity divide" of maturity and funding.

- **Insensivitize collaboration**

Stimulating CHECKs could act as a path towards overcoming organizational divide. Putting new partners in projects is one of the best ways to incentivize collaboration. Controlling mechanisms to accompany the intentions and measuring the results is another important component of collaborative decision-making.
In the NCC and community approach there should be a balance between top-down, bottom-up, peer-to-peer development, methodology and sharing.

- **Dedicate funds to capitalize on the existing community connections and networks**

The H2020 pilot projects (CyberSec4Europe, ECHO, Sparta and Concordia) and their focus groups, as well as the European Cyber Security Organisation (ECSO) and its working groups also represent a rich connected community. The majority of relevant stakeholders are involved in the cybersecurity ecosystem through the four pilots and ECSO, forming an ecosystem with different focusses, maturity stages, and objectives. Thus, deep cooperation, coordination and execution must continue with all of the partners and stakeholders involved. Dedicated funds should be provided, e.g. under the Horizon/Digital Europe Programmes, to deepen the cooperation and coordination of such stakeholders, alongside dedicated funds to set up CHECKs in all Member States.

Europe's cybersecurity potential is not being fully realized due to the existing fragmentation of the cybersecurity landscape and inefficient cooperation and collaboration. One of the ways to overcome the existing fragmentation is by promoting the already existing and functioning structures, especially at the national level, while actively pursuing the aim of a pan-European community through networking.
The concept of CHECKs ('Community Hubs of Expertise in Cybersecurity Knowledge') as a grassroots bottom-up approach was developed by CyberSec4Europe in the course of the past years as a way to provide additional involvement channels and complement the bodies and organisations set up by EU legislation, namely the European Cybersecurity Industrial, Technology and Research Competence Centre, the National Coordination Centres and their network, and the Cybersecurity Competence Community.
These community-level cybersecurity hubs should enable collaboration between industry and academia, bring market security innovations, and help build capabilities in the area by shortening the chain between decision-making and existing needs on the ground. The governance model would benefit from targeted European cybersecurity funding mechanisms in the next decade to build and maintain a pan-European cybersecurity community.

7. References

1. Komorowski, M. (2016). The seven parameters of media clusters: An integrated approach for local cluster analysis. International Journal of Media & Cultural Politics, 12(2), pages 171-191.
2. Komorowski, M. (2017). A novel typology of media clusters. European Planning Studies, 25(8), page 1-22
3. MIDIH project website: https://midih.eu/
4. Morgan J, 2013, The Five-Step Maturity Model for Building a Collaborative Organization, https://www.cloudave.com/27679/the-five-step-maturity-model-for-building-a-collaborative-organization/
5. White, G. (2007). The Community Cyber Security Maturity Model. 99. 10.1109/HICSS.2007.522.
6. Boughzala I. (2014) A Community Maturity Model: a field application for supporting new strategy building, Journal of Decision Systems, 23:1, 82-98, DOI: 10.1080/12460125.2014.857203
7. Smart AgriHubs project deliverable D4.1 "Needs assessment report"
8. DIHNET project Deliverable 2.3 "Maturity assessment Tool"
9. DIHNET project Deliverable 3.4 "Common Approach for Maturity Assessment"
10. Alliance for Internet of Things Innovation (AIOTI), White Paper IoT eDIH Network activities, 2020
11. AI Digital Innovation Hubs Network, Blueprint for cross border collaboration among DIHs, 2020
12. JRC report, DIH as policy tools to boost EU innovation, 2020
13. JRC Practical guidelines on the use of the Digital Maturity Assessment (DMA) tool, https://digital-strategy.ec.europa.eu/en/events/webinar-digital-maturity-assessment-tool
14. National Coordination Centres web site, https://cybersecurity-centre.europa.eu/nccs_en
15. https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/UP-KRITIS/up-kritis_node.html (last 21.08.2022).
16. https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/nationaler-pakt-cybersicherheit/nationaler-pakt-cybersicherheit-node.html (last 21.08.2022).
17. https://bdi.eu/artikel/news/industrie-und-innenministerium-etablieren-buendnis-fuer-cybersicherheit / (last 21.08.2022).
18. https://cyber-security-cluster.eu/ (last 21.08.2022).
19. https://www.teletrust.de/itsmig/ (last 21.08.2022).
20. https://www.teletrust.de/ueber-teletrust/ziele-und-nutzen/ (last 21.08.2022).
21. https://www.it-sicherheit-in-der-wirtschaft.de/ITS/Navigation/DE/Ueber-uns/Initiative/initiative.htm l (last 21.08.2022).
22. https://www.it-sicherheit-in-der-wirtschaft.de/ITS/Navigation/DE/Ueber-uns/Initiative/initiative.html (last 21.08.2022).
23. https://www.wirtschaftsschutz.info/DE/Home/home_node.html (last 21.08.2022).
24. https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Wirtschaftskriminalitaet/InitiativeWirtschaftsschutz/initiativeWirtschaftsschutz_node.htm l (last 21.08.2022).
25. https://www.bitkom.org/Sicherheitskooperation-Cybercrime/Ueber (last 21.08.2022).
26. https://www.bitkom.org/Sicherheitskooperation-Cybercrime/Schuetzen (last 21.08.2022).
27. https://www.cert-verbund.de/index.htm l (last 21.08.2022).
28. https://www.cert-verbund.de/Gruende_CV.html (last 21.08.2022).
29. https://www.cert.sachsen.de/kooperationen-4067.html (last 21.08.2022).
30. https://www.fitko.de/ueber-uns/wer-wir-sind (last 21.08.2022).
31. https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2021-08-04&atto.codiceRedazionale=21G00122&elenco30giorni=false
32. https://www.acn.gov.it/strategia-nazionale-cybersicurezza
33. https://www.cybersecitalia.it/a-cosa-serve-lagenzia-per-la-cybersicurezza-nazionale/12621/
34. https://clusterkb.sk/en/about-us#s0
35. https://cybercompetence.sk/en/
36. https://kyberkomunita.sk/

37. https://foronacionalciberseguridad.es/
38. https://www.agoradih.es/
39. Regulation Proposal (EU) 2018/0328 (COD).
40. On this in detail von Wintzingerode/Müllmann, Ein europäisches Netzwerk für Cybersicherheit, in: Taeger (ed.), Den Wandel begleiten - IT-rechtliche Herausforderungen der Digitalisierung, 2020, p. 475 ff; von Wintzingerode/Müllmann/Spiecker gen. Döhmann, NVwZ 2021, 690 et seq.
41. Art. 15 Regulation (EU) 2021/887.
42. Art. 15 para. 1 of Regulation (EU) 2021/887.
43. Art. 12(1) Proposal Regulation (EU) 2018/0328 (COD).
44. In Art. 15 para. 1-3 Proposal Regulation (EU) 2018/0328 (COD), with a general majority requirement of 75%, a voting share of the European Commission of 50% in each decision was provided for.
45. Art. 15 para. 4 of Regulation (EU) 2021/887.
46. von Wintzingerode/Müllmann, Ein europäisches Netzwerk für Cybersicherheit, in: Taeger (ed.), Den Wandel begleiten - IT-rechtliche Herausforderungen der Digitalisierung, 2020, p. 482 f.; von Wintzingerode/Müllmann/Spiecker gen. Döhmann, NVwZ 2021, 690 (692).
47. Art. 13 para. 2 of Regulation (EU) 2021/887.
48. Decision No GB/2021/1 of the Governing Board of the European Cybersecurity Industrial, Technology and Research Competence Centre adopting its Rules of Procedure, 20 October 2021, available at https://cybersecurity-centre.europa.eu/system/files/2021-11/ECCC%20Decision%20No%20GB20211%20RoP_final.pdf (last access 10.03.2022). The regulations on possible conflicts of interest can be found in Art. 17 of the Rules of Procedure.
49. Art. 13 para. 5 ECCC Decision No GB/2021/1 RoP.
50. Cf. Art. 13 para. 1 and para. 5 ECCC Decision No GB/2021/1 RoP, which use the term "publishable summary" in the original wording.
51. Art. 6 para. 3 Regulation (EU) 2021/887.
52. Art. 6 para. 7 of Regulation (EU) 2021/887. The original English version does not allow for any other conclusion.
53. Art. 6 para. 6 subpara. 1 sentence 1 of Regulation (EU) 2021/887. Art. 6 para. 2 allows Member States to ask the Commission for an opinion on the capacity to manage funds even before the formal application and even before the designation of a National Coordination Centre.
54. Art. 7 para. 2, 3 of Regulation (EU) 2021/887 as well as Communication of the Commission on the Guidelines within the meaning of Art. 6 para. 6 subpara. 3 of Regulation (EU) 2021/887, p. 1 f., available at https://ec.europa.eu/newsroom/dae/redirection/document/80257 (last access 26.04.2022).
55. Cf. Art. 6 Proposal Regulation (EU) 2018/0328(COD).
56. Examples in Schoch/Schneider/Schoch, VerwR VwVfG, Einl. Rn. 542.
57. Schoch/Schneider/Schoch, VerwR VwVfG, Einl. Rn. 541.
58. S. Augsberg, in: J.P.Terhechte (ed.), VwREU (2nd ed., 2022), § 6 marginal no. 53 with further references; R. Schmidt, in: W. Kahl/M. Ludwigs (eds.), Hdb. VerwR, vol. 1: Grundstrukturen (2021), § 9 marginal no. 20 with reference inter alia to S. Groß, in: W. Hoffmann-Riem/E. Schmidt-Aßmann/A. Voßkuhle (eds.), GVwR, vol. I (2nd ed., 2012), § 13 marginal no. 12.
59. Art. 6 para. 7 of Regulation (EU) 2021/887.
60. Art. 7 para. 4 of Regulation (EU) 2021/887.
61. Art. 5 para. 2 lit. d) Regulation (EU) 2021/887.
62. On the network as a mode of action, see Hoffmann-Riem in: Terhechte (ed.), Verwaltungsrecht der Europäischen Union, 2nd ed., 2022, § 3 marginal no. 27 f. with further references.
63. European Centre of Excellence at https://cybersecurity-centre.europa.eu/news/coming-soon-new-call-deployment-network-national-coordination-centres-2022-02-17_en (last access 30.06.2022).

64. European Commission's Funding & Tenders Portal at https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2022-cyber-02-nat-coordination (last access 30.06.2022).
65. M.P. Schwind, Netzwerke im Europäischen Verwaltungsrecht, 2017, p. 131 f. It should be taken into account that the term network is used with different meanings and different compositions are possible depending on the network term.
66. Cf. Art. 1 para. 1 p. 2, Art. 8 f. VO (EU) 2021/887.
67. European Commission, Impact Assessment accompanying the 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, COM(2018) 630 final.
68. Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.
69. Article 11 of Directive (EU) 2016/1148 f the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive),
70. Recital 7 Regulation (EU) 2021/887. The dimension of the objective is further clarified by EC 8, 9 and 12.
71. Translation of definition in Duden online, available at https://www.duden.de/Rechtschreibung/Gemeinschaft (last access 21.06.2022).
72. Art. 8 para. 2 sentence 1 Regulation (EU) 2021/887.
73. According to Art. 8 para. 3 sentence 1 of Regulation (EU) 2021/887, the only restriction is that only institutions established in the Member States can be registered as members. This is only consistent if one considers that the Regulation has cybersecurity in the Union in mind. In addition to the competitiveness of the European internal market, it is also about the ability to secure oneself and independence from non-European suppliers of cybersecurity products.
74. Art. 8 para. 2 sentence 2 of Regulation (EU) 2021/887.
75. Art. 8 para. 3 sentence 2 lit. a) - f) Regulation (EU) 2021/887.
76. Art. 8 para. 8 sentence 2 of Regulation (EU) 2021/887.
77. Art. 8 para. 4 p. 1 f. VO (EU) 2021/887.
78. Art. 8 para. 4 p. 3 f. VO (EU) 2021/887.
79. Art. 8 para. 1 subpara. 2 of Regulation (EU) 2021/887.
80. Art. 8 para. 2 sentence 3 of Regulation (EU) 2021/887 refers to the National Coordination Centres, among others.
81. Art. 8 para. 9 of Regulation (EU) 2021/887.
82. Art. 12 para. 6, 14 para. 5 Regulation (EU) 2021/887.
83. Art. 11 para. 2 lit. c) Regulation (EU) 2021/887. The selection of members for the Strategic Advisory Group is provided for in the Single Programming Document 2022-2024 of the Governing Board in the period up to and including 2023 (p. 14), available at https://cybersecurity-centre.europa.eu/system/files/2022-03/GB%20decision%20No%202022_6_ECCC%20SPD%202022-2024_Budget%202022.pdf (last access 05.07.2022).
84. Art. 18 para. 1-2 Regulation (EU) 2021/887.
85. Cf. Art. 18 para. 1 p. 5-6 Regulation (EU) 2021/887.
86. Art. 18 para. 3 of Regulation (EU) 2021/887 in conjunction with Art. 20 of the Rules of Procedure of the Governing Board. Art. 20 of the Rules of Procedure of the Governing Board (see fn. 17 above).
87. Art. 19 para. 5 of Regulation (EU) 2021/887.
88. Cf. Art. 20 of Regulation (EU) 2021/887.
89. Art. 20 lit. c) Regulation (EU) 2021/887.

90. Art. 12 para. 7 sentence 2 Regulation (EU) 2021/887.
91. Council of the European Union, Mandate for negotiations with the European Parliament, 9 March 2020.
92. von Wintzingerode/Müllmann, Ein europäisches Netzwerk für Cybersicherheit, in: Taeger (ed.), Den Wandel begleiten - IT-rechtliche Herausforderungen der Digitalisierung, 2020, p. 483; von Wintzingerode/Müllmann/Spiecker gen. Döhmann, NVwZ 2021, 690 (693).
93. Art. 13 para. 3 lit. n) in connection with Art. 8 para. 9 and Art. 9 lit. b) of Art. 8 (9) and Art. 9 (b) of Regulation (EU) 2021/887.
94. Art. 19 para. 2 sentence 2 of Regulation (EU) 2021/887.
95. Cf. wording in Art. 19 para. 2 sentence 1 of Regulation (EU) 2021/887.
96. Cf. wording in Art. 8 para. 9 of Regulation (EU) 2021/887.
97. Cf. Art. 7 para. 1 of Regulation (EU) 2021/887.
98. Art. 3 para. 2 of Regulation (EU) 2021/887.
99. Art. 7 para. 1 lit. a) Regulation (EU) 2021/887.
100. Art. 7 para. 1 lit. h) Regulation (EU) 2021/887.
101. Art. 7 para. 1 lit. c) Regulation (EU) 2021/887.
102. Art. 8 para. 2 sentence 3 Regulation (EU) 2021/887.
103. Art. 9 lit. a) Regulation (EU) 2021/887.
104. Art. 9 lit. c) Regulation (EU) 2021/887.
105. https://cybersec4europe.eu/our-results/deliverables/ (last on 30.06.2022).
106. Bolenz, Technische Normung zwischen Markt und Staat (1987), p. 174.
107. Bolenz, Technische Normung zwischen Markt und Staat (1987), p. 117; B. Hartlieb/A. Hövel/N. Müller, Normung und Standardisierung (2nd ed., 2016), p. 38 ff.
108. Art. 7 para. 1 lit. c) Regulation (EU) 2021/887.
109. Cf. Recitals of the Regulation.
110. Recital (7) Regulation (EU) 2021/887.
111. Presentation given at CONVERGENCE NEXT 2022
112. Presentation given at CONVERGENCE 2020
113. www.ecs-org.eu
114. https://ecs-org.eu/documents/publications/5fdb282a4dcbd.pdf
115. https://ecs-org.eu/documents/publications/5fdb291cdf5e7.pdf
116. https://ecs-org.eu/documents/publications/6283b1eb9bce9.pdf
117. https://ecs-org.eu/documents/publications/60101ad752a50.pdf
118. https://ecs-org.eu/documents/publications/6202804a65a70.pdf
119. ECSO Strategic Research and Innovation Agenda. https://ecs-org.eu/documents/publications/59e615c9dd8f1.pdf
120. Input to the Horizon Europe Programme 2021-2027: Priorities for the definition of a Strategic Research and Innovation Agenda in Cybersecurity https://ecs-org.eu/documents/publications/5fdc4c5deb6f9.pdf
121. Input to the Digital Europe Programme 2021-2027: Priorities for supporting the implementation of policy, technology, competitiveness, and competence-building https://ecs-org.eu/documents/publications/5fdc4ca16dde0.pdf
122. https://ecs-org.eu/newsroom/8-european-associations-and-projects-commit-to-the-trans-continuum-initiative
123. https://ecs-org.eu/documents/publications/5fdb2628a0318.pdf
124. https://ecs-org.eu/documents/publications/5fdb2673903c6.pdf
125. https://ecs-org.eu/documents/publications/5fdb2791553ac.pdf
126. https://ecs-org.eu/documents/publications/5fdb25077e039.pdf
127. https://ecs-org.eu/documents/publications/5fdb26b99d089.pdf
128. https://ecs-org.eu/documents/publications/5fdb27182b472.pdf

129. https://ecs-org.eu/documents/publications/5fdb27584719d.pdf
130. https://ecs-org.eu/documents/publications/5fd24425bc74c.pdf
131. CYBERSECURITY MADE IN EUROPE Label, link: https://www.cybersecurity-label.eu/
132. Cybersecurity Market Radar, link: https://ecs-org.eu/initiatives/ecso-sme-hub
133. 'A Taxonomy for the European Cybersecurity Market Facilitating the Market Defragmentation', by ECSO Working Group 2 on Market Deployment, Investments, and International Collaboration, February 2021. Link: https://ecs-org.eu/documents/publications/605de1e3a768a.pdf
134. 'PHYSEC Crowned Winner of ECSO's European Cybersecurity STARtup Award', 3rd February 2021. Link: https://ecs-org.eu/newsroom/physec-crowned-winner-of-ecsos-european-cybersecurity-startup-award and 'Celebrating European innovation: ECSO announces the winner of the 2021 European Cybersecurity STARtup Award', 7th April 2022. https://ecs-org.eu/newsroom/celebrating-european-innovation-ecso-announces-the-winner-of-the-2021-european-cybersecurity-startup-award
135. Interreg Europe CYBER. Link: https://projects2014-2020.interregeurope.eu/cyber/
136. S3 Industrial Modernisation Partnerships – Cybersecurity link: https://s3platform.jrc.ec.europa.eu/cybersecurity
137. Cyber Investor Days link: https://www.ecs-org.eu/initiatives/cyber-investor-days
138. 'ECSO to launch a European Cybersecurity Investment Platform', November 2020, link: https://ecs-org.eu/newsroom/ecso-to-launch-a-european-cybersecurity-investment-platform
139. 'European Investment Advisory Hub and ECSO announce first step towards a new pan-European cybersecurity investment instrument', October 2021, link: https://www.ecs-org.eu/newsroom/european-investment-advisory-hub-and-ecso-announce-first-step-towards-a-new-pan-european-cybersecurity-investment-instrument
140. https://ecs-org.eu/publications