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

Project start: February 1, 2019
Project duration: 42 months

Cyber Security for Europe

D2.1

Governance Structure v1.0

Document Identification	
Due date	31st of January 2020
Submission date	28th of January 2020
Revision	1.0

Related WP	WP2	Dissemination Level	CO
Lead Participant	TUD	Lead Author	Natalia Kadenko (TUD)
Contributing Beneficiaries	TUD, GUF, UNITN, TLEX, UMU	Related Deliverables	D2.2, D2.3, D4.1, D6.1

Abstract

The existing and emerging cybersecurity threats require new models of organization in order to tackle them efficiently. The ultimate goal of CyberSec4Europe as a project is to design the governance structure that will answer the main challenges faced by the field of cybersecurity today. The EU 2018/0328 Regulation Proposal of the Commission contains ideas for the governance design, yet it still leaves a lot of options open. The role and the structure of Cybersecurity Competence Community, which has been left open for interpretation in the Regulation Proposal, will be crucial due to its potential in resolving the issue and helping realize the outlined goals.

CyberSec4Europe has elicited stakeholder and legal requirements and best practices to inform the design of the governance model. Together with partners in WP6, WP2 conducted a governance pilot on MOOC quality assurance and extracted lessons for the governance model. The deliverable presents the draft governance structure based on these inputs. We are exploring a bottom-up approach realized through local cybersecurity hubs, such as the Toulouse hub that we describe in our overview of existing governance models. This bottom-up approach is a strategy to answer the stakeholders' demands and to give a boost to cybersecurity research and development in Europe. This deliverable assesses the best governance practices, analyses governance proposals for the different levels and diverse approaches to cybersecurity governance, tests them against the input required by the relevant stakeholders, and draws conclusions about the desired characteristics of the governance model that is adequate for answering the identified challenges.

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

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

In order to meet these challenges, the European Commission proposes to set up a Network of National Coordination Centres, a Cybersecurity Competence Community and a European Cybersecurity Industrial, Technology and Research Competence Centre. It has initiated four pilots to test potential designs for the Network and its central node at the EU level, the Competence Centre.

The current EU 2018/0328 Regulation Proposal of the Commission, sent to the EU parliament, describes the elements mentioned above (the network of national centres, the community and the central competence centre). It still leaves a lot of options open, however. Moreover, the proposal does not fully address the underlying challenges, and thus additional governance mechanisms are needed. This document reports on the first draft of a wider governance structure, and the inputs on which it is based, as developed in WP2 of CyberSec4Europe, one of the four pilots.

In order to design the governance model capable of addressing the identified challenges, it is essential to take into account the stakeholder views and current best practices. In order to collect these inputs, we have gathered views from more than 80 stakeholders via survey, interviews, and workshops. We have also studied best practices in research collaboration, data sharing, and initiatives to create cybersecurity competence hubs.

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

- Stakeholders express widespread support for the objectives of cybersovereignty, independence, and control, combining this with a view that the focus of the network of competence centres should be broader than only stimulating R&D, and also include capability-building and policy interventions.
- In terms of governance structures, there was support for a combination of a hierarchical and a network model, as well as for a governance structure that is open to a diverse set of actors, initiatives and collaborations.
- The low level of collaboration between academia and industry in the EU is a systemic problem that is visible in the leading cybersecurity research venues where innovative work is published. The new governance structure, therefore, cannot just be a platform, but has to also address the lack of focused investment if Europe wants to better capitalize on the synergies from joint R&D by academia and industry.

- From examining different types of governance structures, we have identified a number of elements that could provide valuable lessons for the governance design for NCCC (Network of Cybersecurity Competence Centres). The synergy between formal and informal, top-down and bottom-up structures can be achieved by integrating informal structures, thus leading to a more efficient stakeholder engagement throughout all societal levels. Transparency is another key element for facilitating trust in an organization.

Based on these findings, CyberSec4Europe is developing a draft governance model for the NCCC. As part of this development, CyberSec4Europe conducted a governance pilot focused on MOOC (Massive Open Online Course) quality assurance. We have learned that applied decision-making processes should take place on the level of the Community and below. This ensures that the process is flexible, while including a clear voting system that facilitates agreement on quality criteria and the relevance of applied elements. However, our pilot also demonstrates that the process should receive feedback from evaluators and verticals (via the different representative bodies and boards). Although the MOOC case was not completely representative for the structure of membership, board and decision process in the NCCC, we propose to use this feedback mechanism and integrate representative bodies into the NCCC structure.

The next pilot will focus on implementing a Community Hub of Expertise in Cybersecurity Knowledge as suggested in this document. Our pilot will be based on the existing Toulouse security hub OcSSImore, which emerged as a suitable candidate from the survey of existing governance structures. Our case study on the Toulouse security hub shows that successful projects can thrive due to an agile governance model of case-by-case decisions on funding and innovation, which is possible if the hub is separate from the actual investments in security innovations. This separation of the platform investments from the actual R&D investments means the hubs could work with a modest amount of resources to function as a platform, ensuring the model can be open to participation of stakeholders of various kinds and with different resource constraints, such as SMEs and non-profits.

The overall approach of CyberSec4Europe is to explore a community-driven approach for the governance model, to complement – and marginally adjust – the Commission's EU Regulation Proposal 2018/0328, within the legal requirements. At the core of the model are regional and sectoral cybersecurity hubs, as seen in the hubs in Toulouse and in Basque country. The hubs have successfully enabled collaboration between industry and academia, brought security innovations to firms and the market, and helped to build capabilities in the area. That being said, the current hubs do not directly solve the observed problem of investment gap. This means that a governance model based on community hubs will still need accompanying mechanisms to increase funding and investment. (This is not yet part of the first version of the governance model presented in this report.)

In short, we propose a network of Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs). To make the bottom-up approach work with the Commission Proposal, we put forward the introduction of a sub-structure for the central Competence Centre, the introduction of a Stakeholder Council, and a modification of the existing governance structure for the proposed NCCC under the Regulation Proposal. The next deliverables offered by the project will test and improve the suggested governance structure, ensuring that it remains up-to-date, flexible and capable of accommodating the ever-adjusting list of challenges and demands.

Document Information

Contributors

Name	Partner
Tobias Fiebig	TUD
Michel van Eeten	TUD
Natalia I. Kadenko	TUD
Wolter Pieters	TUD
Indra Spiecker gen. Döhmann	GUF
Dirk Müllmann	GUF
Christina von Wintzingerode	GUF
Robin Henrich	GUF
Pierantonia Sterlini	UNITN
Fabio Massacci	UNITN
Chan Nam Ngo	UNITN
Dorien Surinx	TLEX
Jos Dumortier	TLEX
Edwin Jacobs	TLEX
Antonio Skarmeta	UMU
Antonio Ruiz	UMU

Reviewers

Name	Partner
Fabio Massacci	UNITN
Simone Fischer-Hübner	KAU
Josef Vyskoc	VaF

History

0.1	11-11-2019	TUD, UNITN, TLEX	1st Draft, incl. Chapter 2, 4, and 5
0.2	29-11-2019	UMU	Chapter 7 contribution
0.3	01-12-2019	GUF	Contribution to the section on legal requirements
0.4	10-12-2019	TUD	Added Chapter 3 and Figures
0.5	16-12-2019	TUD	2nd Draft uploaded to SVN for the high-level review
0.6	21-12-2019	UMU	Update Chapter 7
0.7	25-12-2019	TUD, GUF, TLEX	Draft first review addressing high-level review comments
0.8	15-01-2020	TUD, GUF, TLEX, UNITN	Comments first review integrated for second review
0.9	24-01-2020	TUD, GUF, UNITN	Integrated comments of second review round
1.0	28-01-2020	TUD	Final version sent to PC

This page has been intentionally left blank.

List of Contents

This page has been intentionally left blank.

List of Figures

List of Tables

This page has been intentionally left blank.

List of Acronyms

A	**AC**	Audit Committee
	ACM	Association for Computing Machinery
	ANSSI	Agence nationale de la sécurité des systèmes d'information
B	**B2B**	Business-to-Business
	BSI	Bundesamt für Sicherheit in der Informationstechnik
C	**CCN**	Cybersecurity Centre and Network
	CCS	Conference on Computer and Communications Security
	CeDEM	Conference for E-Democracy and Open Government Conference
	CEN	Comité Européen de Normalisation
	CENELEC	Comité Européen de Normalisation Électrotechnique
	CEO	Chief Executive Officer
	CERN	Conseil européen pour la recherche nucléaire
	CERT	Computer Emergency Response Team
	CHECK	Community Hubs of Expertise in Cybersecurity Knowledge
	CISO	Chief Information Security Officer
	COM	European Commission
	cPPP	Contractual Public-Private Partnership
	CyberSec4Europe	CyberSec4Europe
	CSIRT	Computer Security Incident Response Team
D	**DG CNCT**	Directorate-General for Communications Networks, Content and Technology
	DIS	Dipartimento delle Informazioni per la Sicurezza
	DMP	Data Management Plan
	DoA	Description of Action
	DPIA	Data Protection Impact Analysis
E	**EC**	European Commission
	ECHA	European Chemical Regulation Agency
	ECSEL	Electronic Components and Systems for European Leadership
	ECSO	European Cyber Security Organisation
	EEA	European Economic Area
	EFTA	European Free Trade Association
	eGov	Electronic Government
	EIB	European Investment Bank
	EIT	European Institute of Innovation and Technology
	EMPIR	European Metrology Program for Innovation and Research
	ENISA	European Union Agency for Cybersecurity
	EP	European Parliament
	ePart	Electronic Participation
	ETSI	European Telecommunications Standards Institute
	EU	European Union
	EURAMET	European Association of National Metrology Institutes
	EUROJUST	European Union Agency for Criminal Justice Cooperation
	EUROPOL	European Union Agency for Law Enforcement Cooperation

F	**FRONTEX**	European Border and Coast Guard Agency (Frontières extérieures)
G	**GDPR**	General Data Protection Regulation
	GUF	Johann Wolfgang Goethe-Universität Frankfurt am Main
H	**HREC**	Human Research Ethics Committee
I	**ICA**	International Cooperation Agreement
	ICT	Information and Communication Technology
	IEEE	Institute of Electrical and Electronics Engineers
	IFIP	International Federation for Information Processing
	IPR	Intellectual Property Rights
	ISOC	Internet Society
	IT	Information Technology
J	**JIT**	Joint Technology Initiatives
	JU	Joint Undertakings
K	**KIC**	Knowledge and Innovation Communities
M	**MNC**	Multinational Company
	MOOC	Massive Open Online Course
	MoU	Memorandum of Understanding
N	**NCCC**	Network of Cybersecurity Competence Centres
	NCCyber	National Cybersecurity Centre Poland
	NDSS	Network and Distributed Systems Security Symposium
	NGO	Non-Government Organization
	NIS	Network and Information Systems
	NLO	National Liaison Officer
	NNI	Net National Income
	NSA	Nation State Actor
	NSPW	New Security Paradigms Workshop
P	**PRIMA**	Partnership for Research and Innovation in the Mediterranean Area
	PSG	Permanent Stakeholders Group
	PUPP	Public-Public Partnership
Q	**QC**	Quality Criterion
R	**R&D**	Research and Development
	RDM	Research Data Management
	ReNEUAL	Research Network on EU Administrative Law
S	**S&P**	Symposium on Security and Privacy
	SMEs	Small and Medium Enterprises
	SPRI	Agencia Vasca de Desarrollo Empresarial
	SRIA	Strategic Research and Innovation Agenda
T	**TFEU**	Treaty on the Functioning of the European Union
	TLEX	TIME.LEX

	TREF	Tripartite Employment Conditions Forum
	TUD	Technische Universiteit Delft
U	**UMU**	Universidad de Murcia
	UNITN	Universita Degli Studi de Trento
	USENIX	USENIX – The Advanced Computing Systems Association
W	**WG**	Working Group
	WP	Work Package

This page has been intentionally left blank.

Glossary

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

Accountability
Requirement to justify and explain actions to an independent authority or, in case of government organisations, the general public

B **Best Practices**
A widely accepted set of rules and procedures for operating given a concrete situation or application case.

Bottom-Up
Actions and activities originating emergently from stakeholders without being initiated by a higher authority.

C **Commission Proposal**
EU Regulation Proposal 2018/0328 (COD) on a Network of Competence Centres, a suggestion for a binding regulation, i.e., applicable law, which does not have any legal binding apart from signalling future intent of regulation.

Community
The interacting set of all stakeholders.

Competence Centres
Entities that host several stakeholders from academia or industry to develop cybersecurity competencies in one or more verticals.

Competencies
Ability to address technical and societal challenges.

Cooperation
Interaction between multiple stakeholders for their mutual benefit.

Cybersecurity Hubs
See: Competence Centres

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

G **Governance**
The rules, regulations, and operational entities that shape the interaction of public and private actors.

Governance Model
The codified set of rules describing the governance of a social system with public and private actors.

Governance Structure
See: Governance Model

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

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

L **Law**
: The set of applicable law and regulations of all member states and the EU combined.

Lower Governance Layers
: Governance for entities acting below the member state level in the European Union.

M **Massive Open Online Courses**
: Educational offerings on the Internet participants can join without the necessity to visit a certain location or institution.

Member State
: A nation state that is part of the European Union.

Network Model
: A governance model where participants interact on the basis of equal rights and responsibilities while pertaining autonomy in their internal operation.

P **Pilot**
: A small-scale (in comparison to the final result) test of a proposal or artefact.

Policy
: Codified rules and procedures for a specific case.

Policy Makers
: Elected and non-elected officials that prepare, define, and decide generally applicable policies.

R **Region**
: An area in the European Union which does not necessarily correspond to a single member state; It might overlap parts of several member states, or be a sub-set of a single nation state.

Regional Hub (see: CHECK)
: A competence centre associated with a region.

Regulation Proposal
: See: Commission Proposal

S **Scientific**
: Results obtained and communicated according to academia's best-practices

Sovereignty
: The ability to independently act and prevent external intervention in an institution's operations.

Stakeholder
: A party that has an interest, concern, or influence in certain area.

Strategic Objectives
: A set of long-term objectives that have to be completed to reach an overarching goal, relevant for all member states.

Substructures
: Structures of an organisation that are not visible to other organisations interacting with the organization in a network model.

T **Top-Down**

Actions and activities that are mandated from a higher authority, e.g., by applicable law or decisions of the European Commission.

Transparency

Ability to trace and understand all decisions of an organization by its members, or, constituents in case of government organizations.

V **Vertical**

A set of applications of cybersecurity questions united by an overarching industrial context, e.g., the aviation vertical, which contains all cybersecurity actors involved with aviation safety and security.

Voting

A procedure to democratically reach a decision.

W **Workshop**

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

This page has been intentionally left blank.

1 Introduction

With the societal shift from industrialization to digitalization, new questions of sovereignty and the role of traditional nation states emerged. The challenges of computer security issues affecting private data of hundreds of millions of citizens, nation-state actors trying to influence federal elections, and attacks on critical infrastructures transcended traditional borders and shifted the international balance of power. In this environment, it is the European Union's ambition to maintain its sovereignty by becoming a leading digital economy, guided by both democratic values and the capabilities to be resilient when it comes to cybersecurity threats.

To accomplish these goals, the European Commission outlined two multiannual strategic objectives: (i) Creating a connected and internationally independent digital single market, and, (ii) Facilitating economic growth and investment to incentivize the creation of an economic environment, which provides the right opportunities to retain and employ the highly trained professionals already graduating within Europe.

1.1 Challenges

Aiming to accomplish its goals in terms of cybersecurity, the Commission has identified four major challenges that need to be overcome:

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

As one of the instruments to address these challenges, the European Commission has decided to investigate a network model of cybersecurity competence centres. The Commission is funding four pilot networks within Europe, to explore how the identified challenges can be overcome and how public and private actors can work together in doing so. This network-based model of international cybersecurity cooperation may hold the answer to the challenges of cybersecurity, similarly to the way that the EU and its predecessors were the answer to the challenges of peace building in post-war Europe. A common European goal may be best realized in a network model as described by Powell – "indebtedness and reliance over the long haul"[1]. A successful network model facilitates the exchange of data and knowledge, for which an environment of trust and sense of unity is essential.

CyberSec4Europe is one of the four pilots that will develop a roadmap and recommendations for the implementation of the European Cybersecurity Competence Network. The project will consolidate

[1] W. W. Powell, "Neither market nor hierarchy: Network Forms of organisation", *Research in Organizational Behaviour* 12 (1990): 295-336.

existing capabilities and develop new models for cybersecurity, ensuring the readiness of Europe to tackle the challenges of the rapidly-changing global cybersecurity environment.

A governance structure is needed to not only create such a network, but also to ensure its sustainability after the funded project ends. To guide and instruct the network pilots in the creation of the governance structure, the European Commission issued a draft regulation that outlines the Commission's high-level view and requirements. Figure 1 visualizes the design as described by the EU Regulation Proposal 2018/0328. (Chapter 4 will explain the figure in more detail.) This EU Regulation Proposal 2018/0328, sent to the EU parliament, envisions making Europe more secure and more competitive, "a global leader in cybersecurity"[2]. However, this ambitious goal, accompanied by the elements for the governance design, still leaves a lot of options open, while not addressing the underlying problems in their entirety.

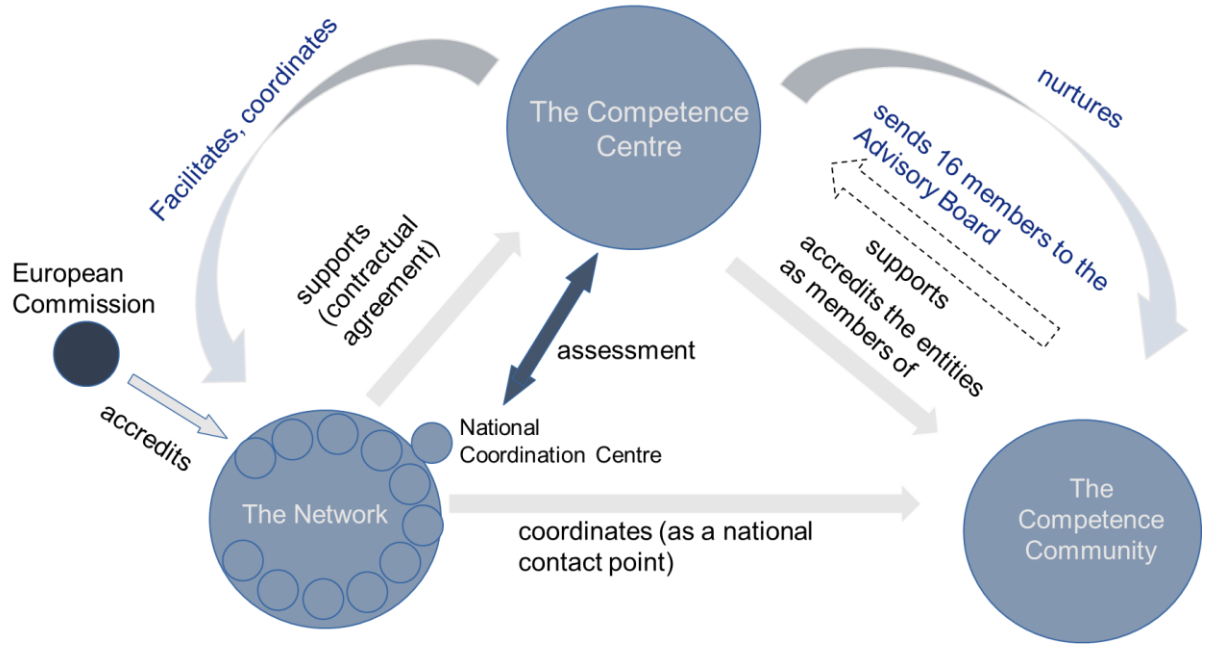

Figure 1: EU Regulation Proposal 2018/0328 draft governance structure overview

When we take the growing body of additional policy documents (see Figure 2) into account, as well as the nation-level legislative acts contributing to cybersecurity governance, several challenges become apparent. The EU-wide issue of maintaining balance between national freedoms and supranational regulations remains problematic. In the cases of cyber threats, the distinctions between these domains become even less clear. From the identification of the attacker to developing the most efficient responses, cybersecurity increasingly requires intra- and international cooperation, as well as cross-domain policy responses (justice, international security and harmonization of education are some examples).

[2] COM(2018) 630 Final 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: 2

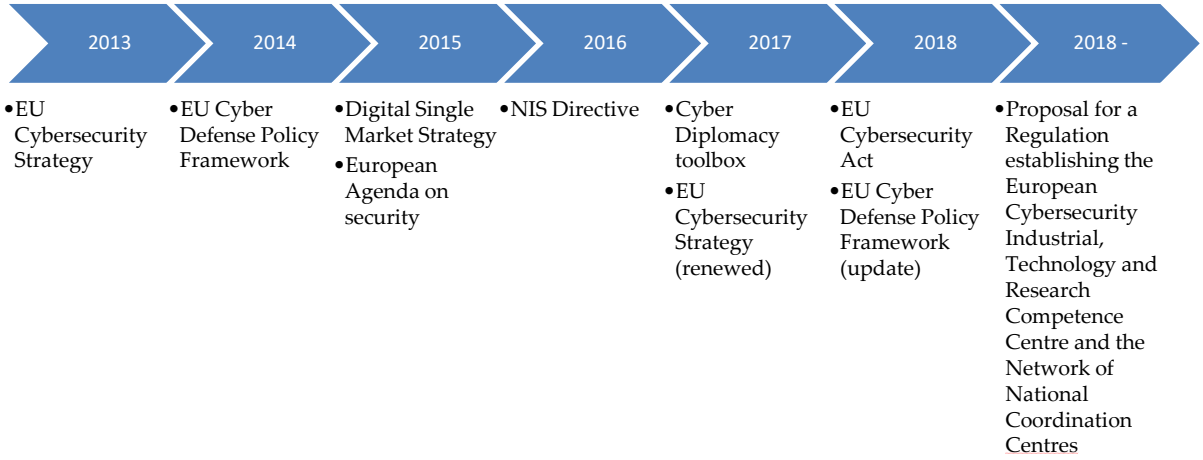

Figure 2: Overview of EU Cybersecurity regulation

Hence, the emerging multi-national, multi-stakeholder cybersecurity network model, while correctly identifying the existing challenges and aiming for transparency, accountability, sufficient development potential and resources allocation, may suffer from challenges to efficiency, overlapping competencies, and independence concerns. The governance process is further complicated by the nature of the inter-institutional cooperation between the EU bodies. Like many domains that require intense and timely cooperation, it should avoid falling into a state of disequilibrium by producing short-term solutions and sacrificing long-term stability for immediate political gains[3].

In order to meet these challenges, the commission wants to set up a Network of National Coordination Centres, as described in the EU Regulation Proposal 2018/0328. Identifying and addressing these challenges is one of the core tasks of the four pilots. They should test potential designs for the Network and its central node at the EU level, the Competence Centre (European Cybersecurity Industrial, Technology and Research Competence Centre), in order to align the existing capacities across Europe.

Hence, the ultimate goal of CyberSec4Europe as a project is to design the governance structure that will complement the Commission's proposal so as to provide a more comprehensive answer to the challenges outlined by the Commission itself (summarized at the beginning of this Chapter). The role and the structure of Cybersecurity Competence Community, which has been left open for interpretation in the EU Regulation Proposal 2018/0328, will be crucial due to its potential in helping to realize the outlined goals. We are exploring a bottom-up approach, realized through the local cybersecurity hubs, as a strategy to answer the stakeholders' demands and to give fresh boost to the cybersecurity development in Europe.

[3] D. Hodson and U. Puetter, "The European Union in disequilibrium: new intergovernmentalism, postfunctionalism and integration theory in the post-Maastricht period," *Journal of European Public Policy* 26 (2019): 1-19.

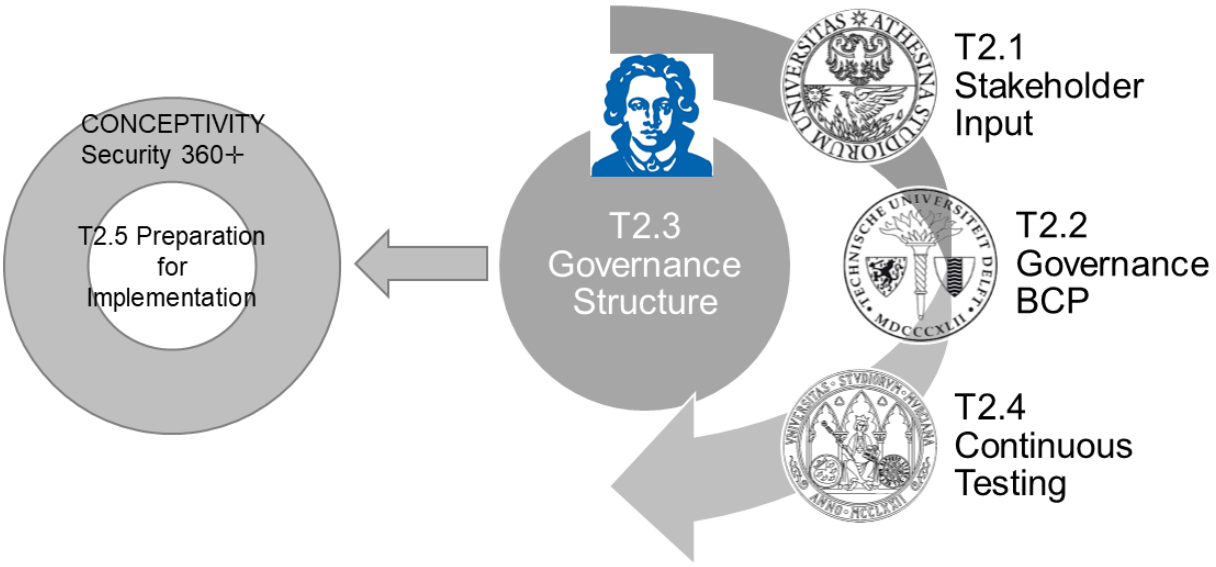

Figure 3: Agile governance development cycle

1.2 Approach

In this deliverable, we outline the first findings of WP2 (Work Package 2) in the period leading up to M12, on how to design a governance model that enables capabilities for addressing the current challenges, see Figure 3. To accomplish this, we follow an agile development process, in which stakeholder input is continuously collected (Task 2.1), refined with best practices (Task 2.2), integrated into the Governance model (Task 2.3), and finally evaluated (Task 2.4.) Furthermore, Task 2.5 ensures that our governance model is put on a sustainable basis for future implementation by the EC (European Commission).

We take stakeholders' views and current best practices into account first. In order to collect these inputs, we have gathered views and requirements from more than 80 stakeholders via surveys and interviews, including contributions from WP4. We also studied best practices in research collaboration, data sharing, and existing governance models in cybersecurity research, innovation and practice. To connect the governance design process with the EU Regulation Proposal 2018/0328, we carefully study the draft regulation and identify aspects to extend and improve it. We then outline a governance approach that covers also the lower governance layers, which so far have been omitted in the EU draft regulation. Together with WP6, we evaluate one of the lower-level governance mechanics we propose in a small-scale pilot based on MOOC (Massive Open Online Course) quality assurance. Although this pilot was not fully representative of the membership structure of the future NCCC, it highlighted the importance of including its representative bodies and boards into a feedback-loop based decision making process. Hence, we propose to incorporate this into the future NCCC's governance structure, to ensure that especially the verticals can contribute their feedback early and effectively.

Based on the stakeholder input, we structure our improved governance structure proposal around the following four core paradigms:

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

The overall approach of CyberSec4Europe is to explore a community-driven approach for the governance model, to complement – and marginally adjust – the Commission's EU Regulation Proposal 2018/0328, within the legal requirements. At the core of the model are regional and sectoral cybersecurity hubs, as seen in the hubs in Toulouse and in Basque country, which were discussed in our survey of existing governance structures. The Toulouse hub will be the focus of the upcoming governance pilot in CyberSec4Europe.

In summary, this deliverable lays a foundation for answering the main challenges of the European cybersecurity future. In order to develop an organizational principle that gives the cybersecurity research community a common European goal, the pilot is collecting input from diverse stakeholders. Examining best practices will contribute to designing a governance model based on the organization principle that is in line with the interests and the legal framework of EU, its member states and third countries, as well as to building and testing a robust and durable governance structure for European cybersecurity cooperation.

1.3 Document Structure

In Chapter 2, we present the results of collecting and analysing input and requirements for a governance model from stakeholders via diverse means, including qualitative semi-structured interviews, online survey, workshops and discussions, some of which were conducted by partners in WP4. We discuss data sharing practices employed for joint research in academia and industry. In a similar fashion, we outline the method and describe the proceedings of the workshop and small survey. We find that participants are open to the plans of an NCCC, but are cautious about a pronounced top-down approach, and would appreciate a more bottom-up vision that includes stakeholders across the board.

Chapter 3 provides an overview of existing governance models and analyses the potential takeaways that are relevant for the goals of the project. We find a landscape of successful projects, and identify transparency as a key contributor to a successful governance structure. Furthermore, in regional hubs we find existing capabilities for a distributed bottom-up approach informed and inspired by the existing accomplishments in the Toulouse and Basque country regions.

Next, we present the EU Regulation Proposal 2018/0328 in Chapter 4. We also outline requirements and aspects of regulation. This chapter serves as a point for comparison for our later suggestions on how to improve the Proposal 2018/0328.

Chapter 5 is dedicated to the presentation of a draft governance model to improve upon the existing regulation. The key aspect of our proposal is a vision for better integrating stakeholders across the board by using a lower-level governance approach involving sub-committees for dedicated tasks.

In Chapter 6, we outline the governance pilot conducted with WP6 to investigate the applicability of our governance proposal. For this purpose, we investigate the quality assurance process for MOOCs under our proposed governance regime. For completeness, we also specifically spell out how our governance proposal applies to the case study.

Next, in Chapter 7, we discuss the results of our governance evaluation. We find several aspects where the initial proposal has to be further refined. Hence, based on the input from this experimental process, we adjust our governance proposal. Furthermore, we find that our approach of evaluating our governance proposal using specific aspects as case studies is viable. Therefore, we will continue utilizing and scaling this process, by proceeding with the evaluation of our governance structure on the suggested regional centres and hubs for the next version of our governance structure.

Finally, we summarize and present our conclusions in Chapter 8.

2 Stakeholder Viewpoints and Best Practices

Considering the goals and challenges outlined in the introduction, the optimal governance model for the European Cybersecurity Competence Network of cybersecurity centres of excellence needs to be tied to the up-to-date practices and qualifications of the stakeholders in various fields. Hence, this input has to be collected and made available to policy makers. Aiming to develop an organizational principle that gives the cybersecurity research community a common European goal, the first question to clarify should be the vision of this goal through the lens of practitioners from various governmental and non-governmental sectors. It is also important to understand the key challenges in each area, such as possible inefficiencies of the allocation of resources, as well as the potential counter-measures. In order to adhere to the organizational principle that is in line with the interests and the legal framework of the EU, as well as its member states and third countries, it is important for the policy makers to envision the structure that provides a clear action plan in case of overlapping (national and supranational) competencies. Considering the wide diversity of stakeholders involved, ranging from government officials to hacktivists, policy makers should be interested in how these groups see their role in the decision-making process, as well as their possible cooperation with the existing bodies, such as ENISA.

When trying to create governance frameworks for cybersecurity, policy makers often lack guidelines and "user requirements". Proposing more (or less) centralized regulations and certifications is always an option but it is not always the most effective one[4]. For example, when deciding whether to prioritize research or skill development, they need to have a ground-truth on the needs and requirements of existing stakeholders in the cybersecurity domain. Imposing an impractical framework might inhibit existing collaboration, therefore being counterproductive. The diverse, distributed, evolving, and global nature of cyber threats requires integration of existing partnerships.

Both the desired degree of specialization and possible funding priorities are bound to arise as the key issues for the future common governance model, and thus it is important to collect the stakeholders' input on these. Furthermore, in order to ensure the consistency of the governance design, it is important that the stakeholders are approached again in order to evaluate the suggested governance model, preferably in a form of a number of pilots. Ensuring the sustainability of the governance model includes, next to the validation by the stakeholders, close cooperation with the responsible EU bodies, such as the European Commission.

Within CyberSec4Europe, we approached national and international stakeholders via three different paths. First, we conducted a combined survey and interview study among high- and mid-level European stakeholders: CEOs, Vice-Presidents, Privacy Commissioners, Academics, Hacktivists. Next, we conducted a workshop with experts from the eGovernance field, and participants of the New Security Paradigms Workshop (NSPW). These are a diverse population of experts, especially in terms of future developments in cybersecurity.

[4] F. Massacci, R. Ruprai, M. Collinson, J. Williams. "Economic impacts of rules-versus risk-based cybersecurity regulations for critical infrastructure providers", *IEEE Security & Privacy* 14(3) (2015): 52-6

2.1 Stakeholder Overview

In order to collect stakeholders' opinions on the cybersecurity requirements and on the governance of the NCCC, the CyberSec4Europe consortium compiled a list of relevant stakeholders and their key competencies, see Figure 4. We insured within the consortium that representatives of all groups are reachable via the network, either due to the direct inclusion of them as partners, or by adding them as associated partners.

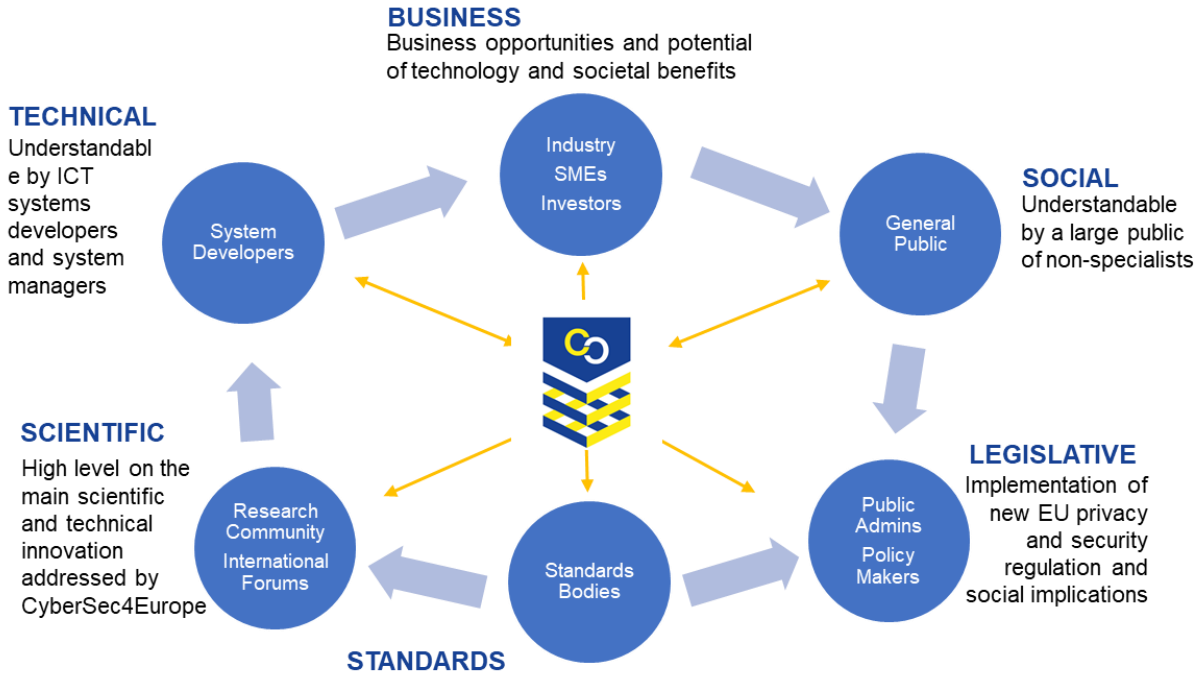

Figure 4: Overview of involved stakeholder groups

In total, we identified six distinct clusters of stakeholders. These are:

- **Technical stakeholders:** This includes ICT operators and developers, as well as system managers, not necessarily in their capacity as employed personnel, but as professionals. We decided on this distinction, as they might otherwise mostly reflect their employers' perspective, which we consider as its own stakeholder category.
- **Businesses:** Businesses have a distinct perspective on cybersecurity and the challenges and impact of related governance. Hence, we include stakeholders from a range of businesses, starting with SMEs, up to large scale enterprises, and investment bodies.
- **Social/Societal stakeholders:** Ultimately, all actions of the government should be for the benefit of the general public. In the past, we often saw regulation and governance proposals suffering from public dissent, mostly due to insufficient involvement of the general public in the underlying decision-making and design process. Hence, we explicitly include the general public in our stakeholder model.
- **Legislative stakeholders:** While, in general, legislative bodies are not stakeholders, but rather the entities making decisions, the federal environment of the European Union changes it insofar that we also have to consider the national government and legislative perspective in our stakeholder model.

- **Standards bodies:** Technical standards can often have a far more lasting impact on the implementation of technological progress and the governance of these processes. Hence, we include standards bodies in our stakeholder model to ensure early alignment with their requirements.
- **Scientific stakeholders:** In classical innovation cycles, scientific researchers inhabit the instrumental first phase of progress. Especially in terms of cybersecurity, European researchers are world-leading. Nonetheless, there is an inherent issue with retaining these capabilities, and we often see researchers being recruited abroad, e.g., by the U.S. academic institutions. To understand their requirements and build a future of cybersecurity in Europe that caters towards retaining these competencies, we also include researchers in our stakeholder model.

Due to the aforementioned inclusion of partners from all elements of our stakeholder model in the CyberSec4Europe network, we have access to a recruitment infrastructure for our subsequent surveys. In addition, we also conduct additional surveys with stakeholders outside of our network to increase the external validity of our findings.

2.2 Combined Stakeholder Questionnaire and Interview Study

In this section, we present the results of our combined interview and questionnaire survey. The survey was conducted between mid-March and the end of August 2019, recruiting European stakeholders and policy experts, as well as the industrial and academic members of the pilots (with an audience of around 200 potential respondents); 57 completed answers were collected. The survey is a joint effort between WP2 and WP4. The ethical and data management related aspects of this questionnaire are described in D4.1 of WP4[5].

In order to collect further requirements for the NCCC from the key stakeholders, a number of semi-structured interviews with the stakeholders from the key cybersecurity fields has been conducted by the CyberSec4Europe partners UNITN and TU Delft. The collected qualitative data included interview recordings and pseudonymized transcripts. The ethical and data management related aspects of the interviews are documented in ‘Annex A: Research Data Management and Ethical Considerations’.

2.2.1 Questionnaire Design

For our first survey, we started out from a questionnaire to be filled in by stakeholders. Each identified stakeholder group had a specific interest in the project (or on a part of it), which is related to the stakeholder’s key area of expertise, geographical area, business etc., see above. The complete questionnaire can be found in ‘Annex B: Interview and Survey Supplements’.

The survey included both open questions and multiple choices questions to provide a quantitative analysis of the results. The expected time it would take the respondents to answer 24 questions was around 15-20 minutes.

Both survey and interviews featured a few key questions to elicit answers in a terminology close to stakeholders’ own interests (see ‘Annex B: Interview and Survey Supplements’ for the full list of questions, recruitment procedure and data management protocol). We have combined the results from the questionnaire with the open-ended questions related to the respondents’ field of specializations, in order to obtain the most broad and detailed vision on the future of cybersecurity governance in Europe.

[5] “D4.1: Requirements Analysis from Vertical Stakeholders”, Ferreira et al., Deliverable of CyberSecurity4Europe, Proposal No. 830929, Call H2020-SU-ICT-03-2018

We did not expect all of them to be well-versed in governance theory, and thus we omitted the "generic questions" on governance, while providing the space to express their opinion on what capabilities Europe should develop and who should be in charge of achieving them. The respondents were encouraged to share their own experiences on cooperation, both domestic and international. Our questions started with the overall goal in cybersecurity that Europe should achieve (e.g. coordination of policies, technological independence, or protection of citizens and state actors from non-EU countries). The question of what should change was followed by the key capabilities that, according to our respondents, would be required by systems, people, institutions, etc., to achieve that change. Research and technological innovation were among the options, but professional knowledge and skills could also be selected. With regard to the key players, participants were asked to choose up to eight players out of a broad list. Then we focused on the decision- making aspects of the CCN. We expected the question on specialization (i.e. funding a particular research area only in one Member State) to be an issue that would prompt strong opinions. In terms of mandate we asked whether the CCN should push towards mandatory security certification at European level. In the initial EC text, there was a provision for identifying areas for mandatory security certification. Industry lobbying effort has weakened the wording: at the time of writing only voluntary certification schemes are considered in the legislative texts. Additionally, we have inquired about the future role of ENISA as envisioned by our respondents.

2.2.2 Interview and Survey Results

To collect the opinions of stakeholders we took a two-pronged approach: a structured survey with over 50 stakeholders to collect suggestions and opinions about the governance model was supplemented by conducting additional 20 person-to-person interviews based on the notion of "grand tour interviews"[6]. See Table 1 for a list of interview participants. The collected data was analysed iteratively.

When asked about what Europe should achieve as an *overall goal* in cybersecurity, *coordination* was identified as the most important goals together with independence from non-EU countries with regards to technology and protection of citizens, businesses and state actors.

Concerning the *desired change* to improve the situation (e.g. better resilience, transparency, trustworthiness, security metrics etc) the respondents considered transparency of cybersecurity decisions, trustworthiness, and resilience as challenges. Authority supervisors and industry managers [#4, #7, #9, #17] highlighted *the need for knowledge and education* to be *constantly updated to meet the dynamic changes in cybersecurity*: cybersecurity needs a new generation of experts trained through an interdisciplinary approach mastering the security of systems and understanding how cybersecurity affects the business. Some participants raised the issue of making sure that the *EU taxpayer money in cybersecurity research* through open calls *does not benefit US companies* through their EU subsidiaries as pointed out by an ENISA's senior manager [#1] and a board member of European Trade Org. [#3]. In general, according to some authority board members, university professors, and hacktivists, the goal was to achieve *cyber sovereignty, independence, and control* [#1, #3, #11. #14, #15, #16], clearly expressing preference for *the broader focus*; only 32% of the participants to the *survey* consider the developments of better security technologies as essential and another 35% consider it of major

[6] M. Halaweh, "Using grounded theory as a method for system requirements analysis," *Journal of Information Systems and Technology Management* 9(1) (2012): 23-38.

importance. Less than half of them (42%) considered new or improved technical standards of major importance. In contrast, almost half of the respondents consider new professional or academic skills as essential to achieve cybersecurity capabilities (46%). Also, half of them also consider policy interventions of major importance (51%).

ID	Role	Organization
1	Senior Manager	ENISA
2	Board Member	ENISA
3	Board Member	European Trade Org.
4	Board Member	EU Data Protection Supervisor
5	Senior Manager	European Consumer Org
6	Ethical Hacker	Self-Employed
7	Senior Manager	Semiconductor MNC
8	Vice President	Re-Insurance MNC
9	President	Critical Infrastructure Org.
10	CISO	Big Pharma and Energy MNC
11	Professor	University
12	Policy advisor	Cybersecurity for industry and government
13	Government official	National government, IT Security
14	Professor, entrepreneur	University, small company in security
15	Ethical hacker	Security industry
16	Professor	University
17	Vice President	Software MNC
18	Senior Manager	Financial institution
19	Government official	National government
20	Instructor	University, Cybersecurity Training

Table 1: Participants of the stakeholder interviews

Interviewees from authorities and industry agreed that *one of its objectives was R&D funding* [#1, #2, #3, #7, #10] but they also *widely diverged on whether it was the only task* (as advocated by an EU actor [#2]). For example, three very diverse stakeholders, authority board members [#3], ethical hacker [#6], and CISO [#10], raised the critical importance, shared by the EU Parliament, of *supporting SMEs to bring research to the market*, others [#1, #4, #8, #9, #17] focused on *professional skills and education*. The certification of infrastructures, service, and products were also indicated as the aspects that should

change (major importance for one-third of the respondents). In this respect half of the participants agreed that the CCN should support mandatory security certification.

The idea of *specialization of a particular area of research* in each national centre was not supported by the stakeholders. Less than a third (28%) supported the option, while a quarter of them considered it possible only in special cases, while the rest expressed a negative opinion. Indeed, the *feeling of potential duplication* was mostly felt only by *stakeholders with a European responsibility* (e.g. board members of ENISA and European Trade Org. [#2, #3]), who explicitly mentioned wasted resources). Other stakeholders who saw it as potentially backfiring did not share this view. For example, diverse stakeholders from authorities, industry and academics [#4, #6, #10, #17] all identified this policy as effective only in the short term, since it is not possible to predict in advance where new innovation would take place. Others from the similar diverse backgrounds [#4, #10, #11, #12, #13 #16] stated that specialization will occur naturally, and should be capitalized rather than enforced.

Another interesting policy question raised was whether the Network should push towards *mandatory security certification at European level.* Indeed, in the initial text of the Regulation proposed by the Commission there was a provision for identifying areas where security certification was to be mandatory. A strong lobbying effort from industry has *significantly weakened the wording*: at the time of writing only voluntary certification schemes are considered in the legislative texts. In this respect the majority of participants (51%) agreed that the Network and Centre should push towards mandatory security certification at European level, while the 7% expressed a negative opinion.

With regard to the *key players*, participants were asked to indicate at most 8 players out of a broad list of players to choose from (see 'Annex B: Interview and Survey , Online Questionnaire').

The majority of the participants consider the European Commission (60%) as a *key player* as well as ENISA (61%). However, 18% indicated only the EC as a key player without considering ENISA, and some of them were confused about the exact role of ENISA. On the other hand, a similar number of respondents (19%) indicated ENISA without mentioning the EC. Of those respondents who expressed an opinion, most assigned to *ENISA only an "orchestration role"*, underlining the need of a harmonization between organizations [#17]. The board member of ENISA [#3] and CISO of Big Pharma and Energy MC [#10] noted that anything effective have not and would not come out of ENISA due to lack of resources. Most interviewees argued that *such decision should be left at Member State levels* and that a balance between different stakeholders is desirable. As authority managers [#3, #4, #5] observed, different Member States would have different sensibilities and different agencies in charge of national security (e.g. BSI in Germany, ANSSI in France, and DIS in Italy, each referring to a different `kind' of Ministry). Indeed, eventually cybersecurity will always have a key role for national security and such role cannot be disregarded by purely considering market issues as pointed out by some authority managers [#3, #4, #9].

What emerged as a surprise was the role of the CCN as a first point of contact to support society at large (from SMEs to individual citizens) when seeking cybersecurity advice. For example, the majority of the participants (68%) assigned a key role to academia, which is expected for a Centre in charge of research funding. Yet, almost a half of respondents pointed to the Computer Emergency Response Teams (CERTs, CSIRTs) to have an advisory role, which would create confusion if the activities of the Centre

were limited to the distribution of funding for R&D. Several interviewees, mostly authority managers [#1, #4, #8, #9], highlighted that CCN could *promote mechanisms for sharing of attack data* in a way that *safeguards the anonymity of the victim*, while *allowing other actors to protect themselves*. Others [#1, #4, #5, #9] also pointed how normal citizens or ethical hackers could turn to CCN for responsible disclosure of the security issues to the corresponding regulator of each vertical domain, as the company which has the security issues would have clearly a conflict of interest. Also, more than a half (58%) of the respondents attributed the key role to Data Protection Authorities, a proportion comparable to the number selecting the European Commission, thus showing the key importance that privacy protection has for European citizens.

In general, *there is no convergence on the relative importance of R&D vs. skill development*. Given the diverging viewpoints of our participants, we recommend allocating resources evenly in both directions. There is also clearly a *preference for an informed network model (academics) with some elements of hierarchy (EC and ENISA)*. The presence of CERTs among the stakeholders in charge of advising on funding and education shows the clear importance of incident management in a cyber security governance framework. This is also relevant in terms eventual funding and educational skills should go (which only play a minor role in today's educational charters). Additionally, there seems to be *a general consensus that the flexibility of the network model seems to be most appropriate to cope with the challenges of cyber security and to provide the flexibility to adapt to the different states economic and policy conditions*. Such flexibility also implies that there should be no top-down decision on the form for the individual national centres or on their "specialization". This has broad consequences also for the Atlantic Council proposal for the US. In terms of operational and decision-making rules another broad consensus exists on promoting information sharing about security issues and possibly coming to unifying technical standards about cyber security.

Eventually, if *research funding remains the core of the network approved by the EU institutions*, the broader ambitions for the CCN could be accommodated via incentives that reward linking research with societal impacts. The incentive embedded in the funding schemes would strengthen the need for researchers to work with CERTs, industry partners, NGOs etc., and to improve the actual security of services and solutions in the European Union.

2.3 Stakeholder Interaction in Cooperation and Data Sharing

Breakthroughs in security research are often tied to the availability of valuable data. This makes data sharing a key driver for increasing the impact and value of research for the Digital Single Market. This sharing of data goes from academia to industry, from industry to academia, and among academics. In real life, however, the practices of data sharing are still in their formative stage, with every research group or business unit having to consider the benefits and drawbacks of data-sharing in light of their own objectives, as well as having to navigate a complicated set of legal provisions around data protection and privacy. There is a growing body of research on incentives for data-sharing and cooperation[7]. Some

[7] See C. Werker and W. Ooms, "Substituting face-to-face contacts in academics' collaborations: modern communication tools, proximity, and brokerage", *Studies in Higher Education* (2019): 1-17; W. Zenk-Möltgen, E. Akdeniz, A. Katsanidou, V. Naßhoven, E. Balaban. "Factors influencing the data sharing behaviour of researchers in sociology and political science", *Journal of Documentation 74(5)* (2018): 1053-1073; Y. Kim and P. Zhang, "Understanding data sharing behaviours of STEM researchers: The roles of attitudes, norms, and data repositories", *Library & Information Science Research*,37(3) (2015): 189-200.

research focuses specifically on the data sharing between industry and academia[8]. The authors apply theory of planned behaviour and social capital theory in order to understand the motivation behind data sharing.

Some authors[9] explore the concept of open innovation and open science and outline the trends of their development. In particular, they note the increasing role of open access publication and research institutes assuming the role of "knowledge brokers" rather than jealous guardians of knowledge. The industries, accordingly, are increasingly open to cooperation, outsourcing of research and financing, interdisciplinary approaches. Others[10] examine the difference between academia-based and industry-based bio-scientists. Group identification seems to play a role; industry-based scientists are less likely then academics to share in general, but more likely to share if they expect reciprocity – on the other hand, these are academics that will more likely share high-value information if they expect to benefit from the similar exchange in the future.

The above-mentioned papers, while offering relevant insights that could be extrapolated to various fields, do not specifically focus on cybersecurity and related areas. In the field of cybersecurity, analysis of academic publications provides interesting insights into the best practices around the alignment of research competencies. In order to gain understanding of the state of field, we have compiled a database of the conference papers accepted to the traditional "Big 4" top conferences (ISOC NDSS, IEEE S&P, USENIX Security, ACM CCS). While other researchers examined the complete dataset of papers dating back to 1981[11], we have focused on the recent sample (2015-2018) of the "European" subset of papers – i.e., the papers containing, at least, one author affiliated with a European institution (EU Member States, Switzerland and the UK) – since we found this approach to possess better relevance for the goals of the project, and namely, for studying best practices of the research activities. We have labelled the affiliation of each author according to one of the categories (Academia, Industry, Government, Other), and thus placed each paper in one of the five groups according to the affiliation of its authors: Academia, Industry, Academia+Industry, Government, Academia+Government, Other). The total amount of papers we have processed is 488. We utilized quantitative data in order to provide strength and background to the stakeholders' input; as a result of our analysis, some interesting insights have emerged, presented in the Figure below.

To begin with, the total amount of accepted European papers has been increasing during the observed time period – however, the share of European papers remains small, and the US still dominates the field. The latter is also reflected in the fact that the "Big 4" are all US-organized venues. The US also is the leading co-author affiliation for European authors (see 'Annex F: Geography of Existing Collaboration Within the EU' for more information). Academics co-authoring with other academics (the A group) consistently account for the biggest group, followed by A+I (Academics co-authoring with the industry-affiliated scientists) that remains a stable, if less sizeable, group. The respective shares of other groups have consistently remained tiny.

[8] S. Friesike, B. Widenmayer, O. Gassmann, and T. Schildhauer, "Opening science: towards an agenda of open science in academia and industry", *The Journal of Technology Transfer*, 40(4) (2015): 581-601; C. Haeussler, "Information-sharing in academia and the industry: A comparative study", *Research Policy*, 40(1) (2011): 105-122.
[9] Friesike et al, "Opening science", 581-601.
[10] Haeussler, "Information-sharing", 105-122.
[11] A. Baset, T. Denning, "A Data-Driven Reflection on 36 Years of Security and Privacy Research", In *CSET'19. Proceedings of the 12th USENIX Conference on Cyber Security Experimentation and Test* (Santa Clara, CA: USENIX Association, 2019).

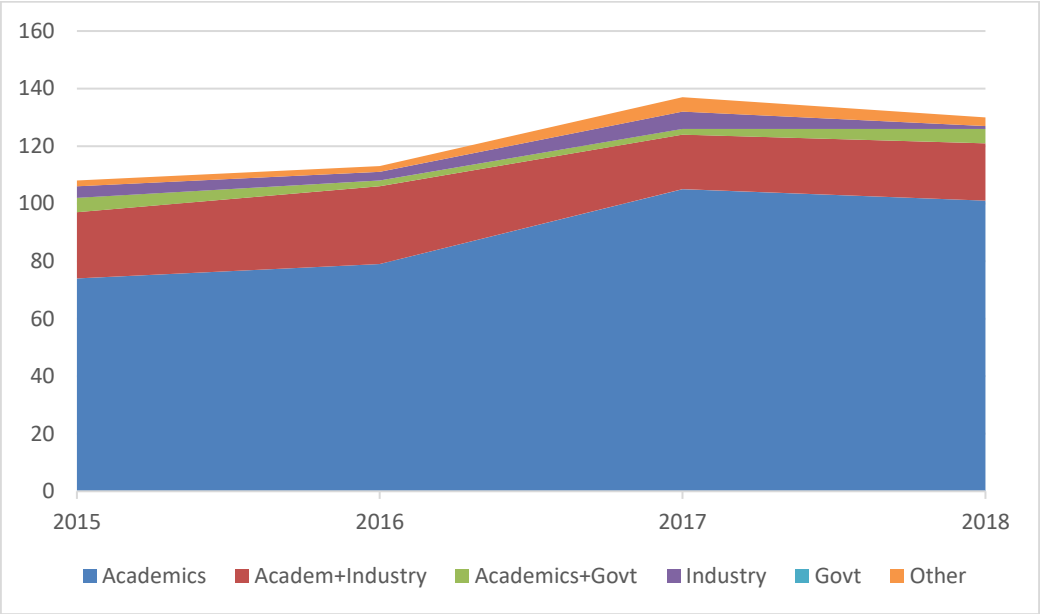

Figure 5: The current state of data-sharing between academia and industry

While the respondents did not get asked direct questions on data sharing, the semi-structured format of the interviews allowed to bring it up among the number of important issues for security research. Both academic and non-academic respondents had clear views on cooperation and data-sharing. For example, while the respondents generally agreed on the importance of cooperation between academia and industry, one of the respondents pointed out the difficulty in cooperating with industries due to the different planning horizon (#11). According to that respondent, industries were focused on the short-term goals, in particularly, on the profit, which did not align with the academic research values. Gathering and properly systematizing data on the existing cybersecurity issues, as well as maintaining open data principle, including open and transparent data formats, were named as important issues for booking progress in cybersecurity research. A different respondent with the industry affiliation (#18) pointed out that industries would benefit from having access to academic research to solve a particular problem, while academia could use the substantial data accumulated by industries. In his/her experience, which extended to the whole country of residence, there was always general readiness to cooperate: from industries providing sponsorship and involving students to suggesting new research directions.

Another respondent, affiliated with the national government structure (#19), talked about the valorisation chain and the role of the companies in it to establish resilience, which is the ultimate goal. Unlike the previous industry-affiliated respondent based in the same country, this one was somewhat more pessimistic about the knowledge transfer between academia and industry.

Another respondent with policy-advisory role and industry affiliation (#12) emphasized the responsibility of keeping the data safe; in fact, several respondents have mentioned (and generally positively evaluated) GDPR in the context of data management. Likewise, they emphasized the importance of trust and transparency in sharing data and knowledge on cybersecurity issues. The EU taking the leading and/or facilitating role in information exchange, including reducing the “transaction costs” for academics seeking cooperation, was another important topic (#11). The explicit obligation to share knowledge and research outcome was mentioned by one of the respondents in the context of the

possible specialization of the member states (#20); the others, while not making it an explicit requirement, were nevertheless worried on the negative outcomes of not having data/knowledge in certain areas as a result of specialization.

Another respondent with non-academic background, while discussing the lack (and loss) of talent in the cybersecurity field, pointed out that industries, and namely, top companies, play crucial role in attracting talent by providing sufficient challenge (#15). This insight could be interpreted as the desirability of industry-academia cooperation as such that is capable of solving one the EU's shortage of talent.

While the factors mentioned by the interviewees are very informative, we can see that certain factors are missing, or at least underrecognized. If we take a longer-term view, as was done by Baset and Denning, then we see that (1) the ratio of A+I has been going down since the nineties and that (2) this decline also took place in the US, not only in the EU.[12] In other words, there are more macro-level forces at work that need to be acknowledged. In terms of the time frame, this decline in the EU and US coincides with the decline of dedicated R&D labs in industry and with the reduction on longer-term research and innovation. This means fewer resources and incentives to collaborate with academia.

Some conclusions can be drawn from the research presented in this section. For one, propagating the open data culture would be in line with facilitating bottom-up approach; reputational gains could be an incentive for academics to engage in cooperation and share data to enable such initiatives. The path to enabling reciprocity lies is facilitating cooperation through both formal structures and informal networking. While there is a possibility to capitalize on the existing perception that cooperation is mutually beneficial, more qualitative and quantitative research into the concerns of academia- and industry-based scientists is clearly needed.

2.4 Brainstorming Workshop

Next to the interviews and surveys, we were aware of the importance of participating in live discussions with groups of stakeholders. The workshop format, while delivering less structured data in comparison with the interviews and surveys, is a valuable source of original insights and feedback. In order to engage the stakeholders directly, TUD (Delft University of Technology) and GUF (Johann Wolfgang Goethe-Universität Frankfurt am Main) conducted a workshop on September 2, 2019, at the IFIP EGOV-CeDEM-ePart Conference hosted by University of Camerino in San Benedetto del Tronto. The ethical and data management related aspects of the workshop are documented in 'Annex A: Research Data Management and Ethical Considerations'.

The format allowed to approach not only the members of the academic community, but also other groups, such as industry representatives. We were aware that, taken separately, the workshop format would not provide the representative selection of stakeholders. However, we decided that, despite the limitations, the workshop method would provide added value as a complementary means to collect stakeholders' input.
In course of preparation for the workshop, it has been opted for the format of a free discussion. Instead of presenting the findings from the interviews and surveys, the participants were given the general introduction to the governance theory and encouraged to contribute their original perspective as the specialists in their own fields.

[12] A. Baset, T. Denning, "A Data-Driven Reflection on 36 Years of Security and Privacy Research", In *CSET'19. Proceedings of the 12th USENIX Conference on Cyber Security Experimentation and Test* (Santa Clara, CA: USENIX Association, 2019).

The findings from the workshop were obtained in the form of two kinds of input: the verbal (discussion) input and the graphical (drawing) input. The verbal input was recorded in course of the workshop by the note takers, based on which the minutes were created subsequently. The graphical input was based on the governance design graph provided on the slides, which was subsequently transferred to the whiteboard and modified in course of the discussion. After the workshop, it was transferred into electronic format, and a drawing was made, see Figure 6.

The workshop participants were offered to express their opinion on the governance structure for the European Network of Cybersecurity Centres. After the introduction to the governance theory, the workshop participants got enlightened on its practical application as realized by the CyberSec4Europe project. The participants were given the option either to improve or to reinvent entirely the proposed governance model for the European Cybersecurity Centre and Network. One of the biggest challenges identified by the present experts was working with formal vs. informal governance, as well as dealing with the hierarchical dimension. The participants agreed that governance should be close to users and capitalize on the relevant knowledge through informal networking and involving the specialists in order to ensure the diversity of expertise and the possibility to include the opposite views.

Subsequently, the participants pointed out that "becoming a leader" is a vague goal for Europe; it would be more beneficial to define clear agenda and vision ("first man on the moon" type), as well as to redefine success (for example, "becoming the most cybersecure according to certain criteria"). The issue of moral leadership in cybersecurity as a possible goal for Europe was discussed. As an example of one of the moral dilemmas that such leadership would entail the participants mentioned protecting users' privacy against NSA (National Security Agency), as well as adherence to the norms of GDPR (General Data Protection Regulation). The outcome of this workshop helped us to restructure the governance model presented in the EU Regulation Proposal 2018/0328 in order to capitalize on bottom-up approach, according to the stakeholders' needs. While the basic governing bodies, such as the Centre, the Network, and the Community, were kept intact, the relations between them were upended, in order to involve the experts as a part of the community, and generally operate in more flexible, less centralized, and less rigidly hierarchical manner. Figure 6 shows the result of the workshop.

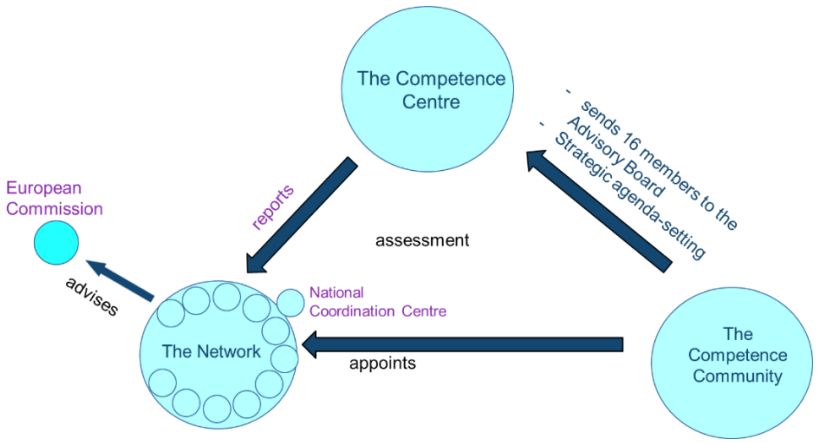

Figure 6: European Cybersecurity Governance structure suggested by workshop participants.

2.5 Survey of NSPW Participants

NSPW (New Security Paradigms Workshop) is a conference targeted at the researchers with "unconventional" ideas on cybersecurity[13], offering the platform for critique and potential paradigm shifts. NSPW papers often involve non-obvious cooperation between disciplines and institutions, which generates new perspectives contributing to innovation in the field. We have approached the participants in order to see whether the alternative or complementing perspective can be gained by studying their experiences. We designed a number of multiple-choice and open-ended questions that required some elaboration. The full list of questions and the detailed results are available in 'Annex C: NSPW Survey Questions and Outcomes'. The ethical and data management related aspects of the survey are documented in 'Annex A: Research Data Management and Ethical Considerations'. Regarding network governance, participants emphasized the importance of the right incentives, commitment from stakeholders, in-person meetings, and diversity. Some funding could be dedicated to "risky" ideas with (radical) innovation potential, and awards could be given for breakthroughs.

2.6 Conclusions on Stakeholder Input

In this section we have set out to collect and analyse the stakeholder input from diverse channels (surveys, semi-structured interviews, workshops) and complement it with quantitative research. Our goal was to collect "user requirements" for the future cybersecurity policy of Europe. In total, we have engaged more than 90 participants representing different groups. We intended to find out how diverse stakeholder groups (Technical stakeholders, Businesses, Social/Societal stakeholders, Legislative stakeholders, Standards bodies, Scientific stakeholders) see their role in the future governance structure for NCCC and how they envision interaction between the different groups.

In particular, the Data Protection Supervisor, along with the other respondents, has outlined the need for knowledge and education to be constantly updated to meet the dynamic changes in cybersecurity: cybersecurity needs a new generation of experts trained through an interdisciplinary approach mastering the security of systems and understanding how cybersecurity affects the business. In other words, professional skills and education were considered the key. A CISO (Chief Information Security Officer) from the big pharma, along with a number of respondents, highlighted R&D funding, supporting SMEs (Small and Medium Enterprises).

The idea to dedicate financing to the "risky" ideas with the breakthrough potential, voiced by the NSPW participants group, found no reflection in the opinions of the other groups.

Overall, transparency of cybersecurity decisions, trustworthiness, and resilience were considered challenge items by diverse stakeholders. Sovereignty, independence and staying in control were defined as key tasks for Europe, which included, in particular, the necessity to safeguard that the projects paid by the EU taxpayers' money don't benefit the US companies through their EU-registered subsidiaries. Collaboration between industry and academia was seen as desirable, and likely beneficial in the long-term; the more efficient and accessible funding system facilitating research and innovation was also indicated as necessary. The responses received reflected some existing confusion about the governance

[13] New Security Paradigms Workshop, https://www.nspw.org/2019

design ideas, which was likely the result of the diversity of stakeholders operating in the area; however, the general preference steered towards the network model and bottom-up approach. The respondents found it essential that the existing resources, networks, and organizations are involved and actively consulted, rather than subjected to the top-down governance mode.

The conclusions for the governance design, drawn from the stakeholders' input, can be summarized into three main dimensions: overall organization, policy, and funding priorities.

In terms of the overall priorities of the organization, we can outline the following:

1. Coordinating EU countries to achieve cybersecurity independence from non-EU countries.
2. Supporting the constant evolution of cybersecurity knowledge and education.
3. Having a broad reach on the different aspects of cybersecurity (developments of better security technologies, new or improved standards; new professional or academic skills, and support of policy interventions).
4. Providing a framework for data- and knowledge-sharing among academia and industry (see point 2 and 3), while making sure that transparency and data safety are guaranteed, in order to develop trust inside the sharing community.

In terms of funding policies:

1. Supporting SMEs to bring research to the market.
2. Supporting professional skills and education.
3. Supporting R&D towards certification of infrastructures, service, and products with the final goal of making cybersecurity certification mandatory.
4. Making sure such funding is actually beneficial to EU communities (beware of direct or indirect transfer to US companies and their EU subsidiaries).

In terms of organizational policies:

1. EC and ENISA should be key players, focusing primarily on the orchestration roles, so that channels to provide bottom-up priorities would be visible and actionable in the organizational structure.
2. Harmonization between different organizations and different levels of stakeholders is desirable – in particular to leverage on existing cooperation activities (e.g. CERTs, standardization bodies, regional or sectoral centres).
3. Governance structures for the National Centres and their interaction with the European Centre must be flexible by supporting different national models rather than providing one-size fits all.

This page has been intentionally left blank.

3 Existing Governance Models

Having analysed the stakeholders' views on governance, collaboration and data sharing, we move on to looking into the existing governance models and their possible relevance as best practices for the future CCN. In order to understand the underlying processes and frameworks, we start by analysing theoretical background of various governance models.

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

The *hierarchical model*, with its vertical chain of command, clear task distribution and specialization, and the underlying skeleton of bureaucratic rules, is according to Powell[14] suited for high-speed mass production. It compensates with stability and predictability for the uncertainty of market mechanisms. The backside of stability is lack of flexibility that is necessary to react to the changes, let alone to anticipate them. Desire of predictability also generates tendencies toward compliance and 'box ticking' instead of proper risk analysis and secure products and services. Unfortunately, for reacting to rapidly-shifting cybersecurity environment, high-speed flexibility is crucial. Hierarchical organizations also require a back-up of joint resource pool to safeguard for inevitable insufficient responses. Yet, the request to pool additional resources by organizations in charge of security is always vulnerable to threat inflations. The hardest challenge is that this model requires the commitment of a large group of actors, not just industries, consumers and civil society groups, but also representatives of various national and supranational political bodies, to align within a singular comprehensive hierarchical structure.

One of the ways to realize an ambition for "cyber moon shot" is to act within the framework of what started out as an institutional moon shot of sorts – and namely, within the structures of the EU. A unifying goal of international cybersecurity cooperation answers the modern challenges of policy-making, similarly to the way that the EU predecessors were the answer to the challenges of peace-building in post-war Europe. A common European goal is best realized in the *network governance model* as described by Powell – "indebtedness and reliance over the long haul"[15]. A key feature of a successful network model is reciprocity, which fits well with the facilitated exchange of data and knowledge. An environment of trust and the feeling of being interdependent is essential. Pupillo also mentions that "trust-based relationships are essential to cybersecurity and resilience policy"[16], elaborating on the inherent contradictory market incentives (private costs versus shared benefits). In other words, leaving cybersecurity to the domain of market-based relationships will likely fail to create the conditions necessary for realizing the Commission's objectives, while hierarchical structures with their rigid

[14] Powell, "Neither market nor hierarchy: Network Forms of organisation", 295-336.
[15] Ibid.
[16] L. Pupillo, "EU Cybersecurity and the Paradox of Progress,", *CEPS Policy Insight* 6 (2018): 1-6.

division of authority, tasks and responsibilities lack the adaptivity and innovation that is needed from the cybersecurity research community, both in academia and industry. The network model has its own challenges, such as perceived loss of independence, unclear responsibilities, encapsulation. It is important to not disregard these challenges in designing the governance model that involves various European stakeholders. Like many domains that require intense and timely cooperation, network governance should avoid falling into the trap of enhancing its state of disequilibrium by producing short-term solutions and sacrificing the long-term stability for immediate political gains.[17] Collaborative governance, i.e., "attempts to bring all the relevant stakeholders together for face-to-face discussions during which policies are developed"[18] will help tackle the additional challenges, such as attracting talent and drafting the governance structure that would incorporate input from multiple stakeholders. The latter will ensure sustainable development of the governance model.

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

3.1 ENISA

One such example of an existing governance structure in the field of cybersecurity is ENISA, the European Union Agency for Network and Information Security. ENISA is a European agency with the mission to contribute to secure Europe's information society. Its activities are conducted based on a European Regulation of 2019[19]. It is one of the agencies closest to a future NCCC and intended to complement NCCC[20]. The **mission** of ENISA is to achieve "a high common level of cybersecurity across the Union, including by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. ENISA shall act as a reference point for advice and expertise on cybersecurity for Union institutions, bodies, offices and agencies as well as for other relevant Union stakeholders. [21]"

ENISA has outlined a number of strategic objectives:[22]

- Expertise: monitoring, updating, and making the relevant information available in order to increase efficiency of facing the upcoming cybersecurity challenges;
- Policy: promoting network and information security as an EU policy priority;
- Capacity: supportive role in maintain network and information security capacities for the EU Member States and bodies;

[17] D. Hodson and U. Puetter, "The European Union in disequilibrium", 1-19.
[18] M. Bevir, *Governance: A very short introduction* (OUP Oxford, 2012)
[19] Regulation (EU) 2019/881
[20] COM(2018) 630 final: 4
[21] Article 3(1) of ENISA Regulation (EU) No 2019/881
[22] ENISA Strategy 2016-2020, https://www.enisa.europa.eu/publications/corporate/enisa-strategy [last accessed 30 November 2019].

- Community: nurturing the European network and information security community by encouraging cooperation between diverse stakeholders;
- Enabling: increasing ENISA's impact through efficient management and efficient engagement.

3.1.1 Membership

The members are appointed for the term of four years and are subject to renewal. The Board takes its decisions by an absolute majority of its members. A two-thirds majority of all Management Board members shall be required for the adoption of the Management Board's rules of procedure, the Agency's internal rules of operation, the budget, the annual and multiannual work program, the appointment, extension of the term of office or removal of the Executive Director, and the designation of the Chairperson of the Management Board. The Agency is managed by its Executive Director, who is, amongst other tasks, responsible for the administration of the Agency and for implementing the decisions adopted by the Management Board.

The Management Board is assisted by an Executive Board, which prepares decisions to be adopted by the Management Board on administrative and budgetary matters only. It is made up of five members appointed from among the members of the Management Board. The Management Board, after a proposal by the Executive Director, sets up an Advisory Group (formerly - Permanent Stakeholders' Group) for 2.5 years. It is composed of 33 recognized experts representing the relevant stakeholders. The experts are recruited in the following way[23]. First, there is an open call with expression of interest; based on its results, the Executive Director draws a list of experts, representing the following stakeholders:

- The ICT industry
- Consumer groups
- Providers of electronic communications networks or services available to the public
- Academic experts in network and information security
- Representatives of national regulatory authorities, law enforcement and privacy protection authorities, nominated under Directive 2002/21/EC[24]

The members may resign on their own initiative, or be dismissed based on their non-attendance of the meetings. However, the Decision on the establishment and operation of PSG does not specify how often the meetings should be convened. Additionally, no quorum is required for the meetings to be valid.

The ENISA Advisory Group is responsible for the contact with stakeholders, focusing on the issues that are relevant to stakeholders and bringing them to the attention of ENISA. The idea is that the ENISA Advisory Group should be consulted on ENISA's draft annual work program[25]. The composition of the ENISA Advisory Group and the tasks assigned to it should ensure sufficient representation of stakeholders in the work of ENISA.

The formal structures outlined above are complemented by the semi-formal bodies, such as the NLO (The National Liaison Officers) Network, which initially served as an informal point of contact between

[23] Decision No MB/2014/7 of the Management Board of ENISA on the Establishment and Operation of the Permanent Stakeholders' Group, https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/mb-decision-no-mb-2014-7-on-internal-rules-of-operation-of-psg [last accessed 3 December 2019].
[24] Article 12, paragraph 1, (EU) No 526/2013
[25] ENISA Advisory Group, https://www.enisa.europa.eu/about-enisa/structure-organization/advisory-group [last accessed 9 December 2019]

the Member States and ENISA. The NLO Network meets annually to discuss, among other, emerging initiatives, legal updates and national developments. Currently its role is facilitating the exchange of information between ENISA and the Member States, and supporting ENISA in disseminating its activities, findings and recommendations to the relevant stakeholders across the Union.[26] This element of the governance structure is interesting to consider for the governance structure design for NCC: after being set up in 2004, this body was formalized in 2019. Such development clearly shows the need for lower-level, decentralized contact points and interactions. This needs to supplement and, to certain extent counteract, the top-down governance approach, providing the member States and national-level bodies with direct contact and exchanges.

Financing is done through contributions from the Community. Currently ENISA is in the process of implementing a new regulatory framework. The design of ENISA illustrates how a governance structure can be built, with different levels, different tasks assigned and various degrees of formal and informal bodies incorporated into the governance structure.

3.1.2 Governance Structure

The central governance body of ENISA is the Management Board. It defines the general direction of the Agency and is responsible for the decision-making process. The Board is composed of 30 delegates, consisting of two representatives of the EU Commission and one representative of each Member State[27].

Figure 7: Governance structure of ENISA

3.2 ECSO

The European Cybersecurity Organisation (ECSO) is a fully self-financed non-for-profit organization. ECSO is the "private counterpart to the European Commission in implementing the contractual Public-Private Partnership (cPPP) on cybersecurity"[28] that aims to unite diverse European cybersecurity

[26] ENISA National Liaison Office Network, https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office [last accessed 9 December 2019].
[27] See Article 4 et. Seq., (EU) No 526/2013, for more detailed information.
[28] ECSO webpage, https://ecs-org.eu/ [last accessed 9 December 2019].

stakeholders across the EU Member States, the European Free Trade Association (EFTA) and H2020 Program associated countries.

The mission of ECSO is "to develop a competitive European cybersecurity ecosystem, to support the protection of the European Digital Single Market with trusted cybersecurity solutions, and to contribute to the advancement of the European digital autonomy"[29].

3.2.1 Membership

In order to become a Member, the party should be either legal entity established at least in one ECSO Country (EU/EEA/EFTA country or a country participating in Horizon 2020), or a physical person (a civil servant) on behalf of national Public Authorities from an ECSO Country[30]. Furthermore, this entity should possess "a significant footprint and decision centre in an ECSO Country (creation of jobs) in cybersecurity activities for research and development and / or manufacturing and / or providing services, as determined by the Board of Directors of and whose management have the capacity to support decisions in favour of a European interest for security" [31], demonstrate prominent R&D capacities and a genuine interest in developing European cybersecurity market. The Bylaws foresee the following types of members: Large companies, National and European Organisations/ Associations, SMEs, Users / Operators, Regional / Local public administrations, national-level Public Authorities, Research Centres, Academies / Universities, and others. In order to support self-financed and independent character of the organization, the members may be required to contribute annual membership fee; other sources of financing include grants, contracts, donations and testamentary provisions, as well as other legal sources. ECSO has come up with a number of low-level initiatives, such as ECSO Cybersecurity Business Matchmaking events, aimed at bringing European start-ups and SMEs closer to funding opportunities. Additionally, it publishes ECSO Cybersecurity Market Radar, which maps European cybersecurity products and services providers.

3.2.2 Governance Structure

The Board of directors is composed by the First Directors for the first three years of the Association and by representatives of other Members appointed at the Annual General Assembly (maximum 36 members, representatives of different stakeholders; the candidates are voted for at the General Assembly). There are various criteria outlined concerning the representation of different stakeholders, with non-binding quotas. The General Assembly is composed of the Members that possess voting rights. External experts may be invited by the Chairperson of the Board of Directors for the Advisory purposes.[32] During the Annual or Extraordinary General Assembly (convened either at the initiative of the Board of Directors, or at the request of one-third of the Members), each member is entitled to one vote, with the Chairperson possessing the right to cast the decisive vote in case of an equal number of votes. The minutes and the voting outcomes, with the exception of the decisions concerning the Statutes and their modifications; the mandates of directors', ECSO representatives, and day-to-day management; the nomination of a liquidator and the liquidation of the Association are not made publicly available.

[29] Ibid.
[30] European cybersecurity organisation (ECSO) ASBL – bylaws https://www.ecs-org.eu/documents/uploads/bylaws-dec-2019.pdf [last accessed 9 December 2019].
[31] Ibid, Art. 3.3.
[32] ECSO Statutes: 6

Coordination and Strategy Committee, National Public Authorities Committee, Scientific and Technology Committee, Financial Committee. The daily management is conducted by the Secretariat and the Secretary-General. The action takes place through the Working Groups (WGs), which are established or dismissed by the Board of Directors. Each WG chooses for one or more Chairs, elected "ad personam" with a renewable mandate. [33] WGs perform advisory and/or mediating roles. Decisions in the Working Groups and are preferably taken by consensus, or by a two- thirds majority vote by the representatives of Member States if the consensus is not reached.

Figure 8: Governance structure of ECSO[34]

3.3 CERN

CERN was founded in 1954 with the ambitious goal to rejuvenate European science, develop leading research and unite the world-class professionals, which is not dissimilar to the goals of CyberSec4Europe. The **main task and mission** of the organization is best expressed in their own words: "Our work helps to uncover what the universe is made of and how it works" and "unite people from all over the world to push the frontiers of science and technology, for the benefit of all".[35] The emphasis

[33] General rules and working guidelines for the participation, functioning and governance of ECSO Working Groups and Task Forces, https://www.ecs-org.eu/documents/uploads/wg-governance-rules.pdf [last accessed 9 December 2019].
[34] ECSO webpage, https://ecs-org.eu/about [last accessed 9 December 2019].
[35] CERN webpage, https://home.cern/about/who-we-are/our-mission [last accessed 9 December 2019].

lies on the scientific excellence combined with nurturing robust professional community through investment and training.

3.3.1 Membership

The key players in the CERN governance structure are the Member States. There are several degrees of relationship with CERN that the states can choose from: the institutional ones (membership, associate membership, observer status) and non-institutional ones (ICA – International Cooperation Agreement and MoU – Memorandum of Understanding). Membership and Associate Membership are available to States only, regardless of their location. The decision of acceptance is made by the CERN Council[36] in accordance with the criteria outlined in the CERN Convention[37] and CERN Council Resolution[38]. In particular, while geographical limitations no longer apply as membership criteria, it has been established that the majority of Member States must remain EU/EFTA members, in order to maintain the European foundation of the organization. The Council expresses interest in considering the application; afterwards, Associate Membership is an obligatory pre-membership status that has to be maintained for at least two years. The final decision has to be unanimous.

Member States are granted access to scientific and technical programs, may employ staff and participate in training programs, as well as access industrial return. They get full voting rights in the Council. Members annually contribute to the budget in proportion to their Net National Income (NNI). Next to that, new members are asked to make a special contribution of varying and negotiable amount.

The membership criteria are divided into two parts: those verified by the Council, and those verified by the member States themselves according to their competencies.

In accordance with the Convention, each Member State may submit a written notice certifying its wish to withdraw to the President of Council; the withdrawal takes place at the end of the financial year or later. A member State can also lose membership in case of failure to fulfil its obligations. This decision is also adopted by a two-thirds majority. A Member State loses its right to vote in case of failure to fulfil its financial obligations for a particular programme, unless such failure is recognized by a two-thirds majority of all the Member States as being beyond the State's control.

3.3.2 Governance Structure

Since CERN is an organization focused on scientific research, its governing process contains a number of provisions and details directly tied to the scientific programs and projects. For instance, participation in one of the basic programs of CERN is obligatory; similarly, the Council has the competence to determine a minimum initial period of participation in any program for a certain period, as well as to change it. The initial period is established by a two-thirds majority of votes, while the later changes have to be approved unanimously. [39] Another provision maintains that the States generally are not entitled to

[36] Participation in CERN, https://international-relations.web.cern.ch/stakeholder-relations/Participation-CERN [last accessed 9 December 2019].
[37] Convention for the Establishment of a European Organization for Nuclear Research, https://council.web.cern.ch/en/convention [last accessed 9 December 2019].
[38] Council Working Group on the Scientific and Geographical Enlargement of CERN, "Report on Geographical Enlargement of CERN", https://cds.cern.ch/record/1289091/files/001289091_English.pdf [last accessed 9 December 2019].
[39] Convention on the Establishment of CERN, https://council.web.cern.ch/en/convention [last accessed 9 December 2019].

vote on the matters, unless they directly concern one of the scientific programs that these States participate in. The cases requiring approval by the Council unanimously or by a two-thirds majority of all the Member States are the exception.

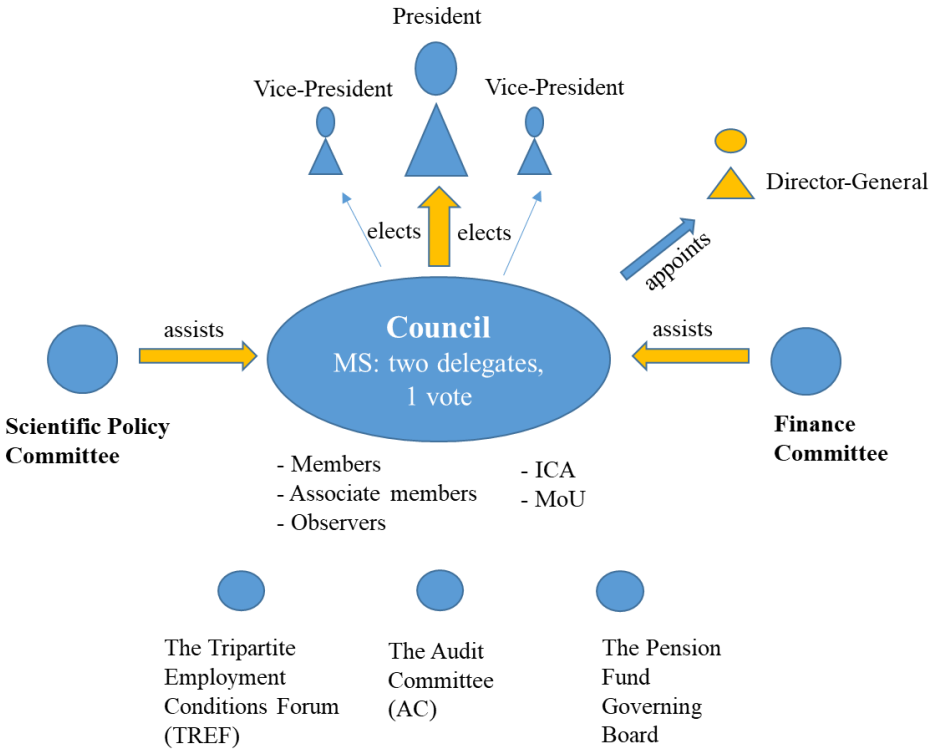

Figure 9: Governance structure of CERN

CERN Member States (currently 23 in total) send two official delegates each to the CERN Council. One of the delegates acts as a representative of the government administration, while the other delegate represents national scientific interests. Each Member State has a single vote. While most decisions are made by a simple majority, the practice is in to aim for "a consensus as close as possible to unanimity"[40].

The CERN Council is the most important governance organ of CERN that is in charge for taking the main decisions, as well as general control over the main activities, such as approval of budget and activities. It elects a president and two vice-presidents for the term of one year who may be re-elected for two consecutive terms maximum; the Council meets four times a year. The Council appoints (and dismisses) by a two-thirds majority of votes a Director-General, assisted by a directorate, who is in charge of running one of the Laboratories. This appointment lasts for a defined period. The Council is assisted by two advisory bodies: The Scientific Policy Committee and the Finance Committee that meet before the Council sessions. Additional structures are The Tripartite Employment Conditions Forum (TREF), The Audit Committee (AC), which includes external experts, and the Pension Fund Governing Board.

[40] CERN webpage: Our Governance, https://home.cern/about/who-we-are/our-governance [last accessed 9 December 2019].

While CERN is not an organization that specifically deal with cybersecurity, there is a historical reason why it should be considered as one of the examples in this document: it was CERN that developed the World Wide Web in the 1990s. On April, 30, 1993 CERN voluntarily relinquished its intellectual property rights to the web's software: the basic client, basic server, and library of common code. The memo containing this decision was addressed "To Whom It May Concern", thus also, perhaps, setting foundation to the modern dimension of open data policy. The underlying motivation was to "further compatibility, common practices, and standards in networking and computer supported collaboration". [41] CERN was founded on the premises of fostering unity based on scientific collaboration, as well as on providing employment conditions that would encourage European talent to remain; additionally, it has early on adopted the culture of transparency, which made the above-mentioned release of the web's software possible. Currently, comparatively to many other bodies, CERN's website provides one of the most detailed overviews of the governance structure, financing mechanisms etc. With transparency and trust being outlined by the stakeholders as one of the most important components of success for the European cybersecurity policy, the example of CERN is noteworthy and needs to be taken into consideration for the governance design.

3.4 OcSSImore (Toulouse hub)

Next to the governance models of the existing high-level international organizations, it is interesting to examine the governance model for a regional cybersecurity hub. One such example is a hub that is being set up in Toulouse, France. The Toulouse hub prototype was founded 4 years ago as an association driven by the security vision of its vertical stakeholders (public sector, finance, transport, health), becoming a dedicated brand designed to ease communication in the field of security. It is based within the OcSSImore association[42], which is a non-profit organization aimed at designing new innovations and businesses, while not actually participating directly in running those businesses. It is a small and agile structure designed to facilitate cooperation. Next to the above-mentioned stakeholders, it provides platform for cooperation between R&D laboratories, start-ups, academic institutions and cybersecurity providers, with the involvement of institutional sponsors.

3.4.1 Membership

The idea behind the development of the Toulouse hub is fostering a community that will shape the vision and provide the necessary expertise in order to create innovative, trustworthy and trusted, digital services. In practice, it means that the hub will operate in the space where diverse stakeholder needs have to be satisfied before the face of various cybersecurity challenges. The key players within the Toulouse hub structure are users (the above-mentioned vertical stakeholders), academic institutions (R&D labs), industries (cybersecurity service providers), and regional governmental institutions. Through the involvement of diverse actors, the balance is achieved.

The main challenge faced by the **users/vertical stakeholders** is the issue of sharing; in particular, sharing security challenges in the conditions of trust. Trust has been mentioned as one of the key issues by the stakeholders as described in Chapter 2, and the Toulouse hub places emphasis on it. Identifying and formalizing cross-sector needs and priorities, which is also considered crucial, is an essential point

[41] "CERN's ultimate act of openness", *CERN Courier*, 11 March 2019, https://cerncourier.com/a/cerns-ultimate-act-of-openness/ [last accessed 9 December 2019].
[42] OcSSImore webpage, https://www.ocssimore.net/ [last accessed 5 December 2019].

in forming joint security vision and ensure successful cooperation. The other envisioned tasks of vertical stakeholders involved in the joint endeavour within the hub (sub-)structure are engaging innovation providers on ROI guaranteed collaborations, providing community with security4digital expertise to develop co-business actions, as well as creating a common brand to communicate the joint vision. The tasks **of academic institutions (R&D labs)** in the envisioned structural sub-unit of the Technology Centre would be sourcing and prototyping innovative technologies, ensuring access and promotion of European expertise and capabilities, building and implementing the training Road Map, as well as monitoring European R&I developments.

The main challenge is to focus on use cases. Next to the academic input, European cooperation would be also addressed by the **industries**, the challenge for which is thinking long-term. The long-term goals are best realized by facilitating European high-level consortium building. Turning innovations into fully supported solutions, as well as creating innovative business and intellectual property sharing models would be other focal points for the industries. The **regional institutions** could focus on facilitating economic development, with economic growth and job creation as the goal. The ways to achieve these goals could be sourcing innovative SMEs, providing deployment capabilities, fostering final user adoption, as well as making innovations usable and affordable for SMEs and developing regional attractiveness for talents and skilled workforce.

Thusly structured, the Hub would combine diverse valuable inputs from various stakeholders: cybersecurity expertise, technical capabilities built upon innovative technologies, use cases valuable for businesses, as well as business and digital innovation expertise.

3.4.2 Governance Structure

The Toulouse hub is going to be set up as a new entity, coming out of the OcSSImore association. The latter is a non-profit organization aimed at designing new innovations and businesses, while not actually participating directly in running those businesses; in other words, investment in innovation remains separate from funding. This Hub connects itself with an existing private-public initiative in which individualized cybersecurity problems are identified. A governing board of few partners then decides in a unanimous voting rule which problems to pursue further in a solution-oriented research approach. Other members who are not partners may decide to join in the further research.

In other words, the Hub is a platform that itself does not invest in the projects. It is just a structure for industry and research to meet and conduct projects that they see as beneficial and, potentially, marketable. The partners in such a project bring their own funding, typically in terms of people and time. Whether other agreements are in place, such as for IPR, is left to the project partners. So far, projects have worked towards innovations without prior contracts for IPR in place. This is likely to have made the projects much more nimble and easier to get off the ground, allowing more innovative ideas to be explored without major upfront hurdles and investment. Also, this approach avoids the high cost of setting up prior contracts, which allows these resources to be used for actual innovation. In sum, the original setup of the hub foresees that innovation is kept separate from the structure.

As of now, neither the financing setup of the hub nor its future governance structure have been developed. Currently, the partners in OcSSImore pay a fixed yearly fee to allow OcSSImore to function. How this will be set up in the new Hub is still an open question. Since the cost of the Hub are quite modest, due to it being separate from the innovation itself, this does not need to become a major

stumbling block. The industrial partners with the relevant interests and expertise can join the hub; membership fee has to be paid annually. In order to ensure balanced development of the multi-stakeholder structure, academic institutions could be charged lower fee, or no fee at all. The implication for the governance design is the following question to address: where does innovation money come from? The challenges identified so far include formalizing the diverse needs of the vertical stakeholders, as well as the need for support of public authorities.

3.5 Tecnalia (Basque country hub)

Tecnalia is a Research and Technological development Centre based in the Basque Country in Spain, with a network within and outside Europe. Due to the significant level of autonomy that the Basque country enjoys in various policy areas, such as education and industry, additional possibilities exist in organizing the cybersecurity cooperation based on bottom-up approach.

3.5.1 Membership

The mission of Tecnalia is defined as "We transform technology in GDP". [43] It was initially created within the Basque Agency of Business Development (SPRI); in the value chain it places itself within the fields of applied research and technological development. Next to investment and entrepreneurship, the hub focuses on development, education, security, eGovernment, investment, and forming research network. This hub fosters collaborations and alliances with the universities, research centres, cooperative research centres, private companies, as well as other organizations.

3.5.2 Governance Structure

There is no detailed information available about the governance structure of Tecnalia. The CEO is assisted by a Sub-Directorate General of Market and a Sub-Directorate General of Technology. The hub is comprised of a number of committees: Executive committee, Appointments and patrons committee, Audit committee, Tecnalia+ committee, and Strategy committee. Supervisory Board exists alongside a Boards of Division (Chairpersons) and a Board of Directors. Sources of funding are mixed, coming from private donors and both competitive and non-competitive public grants.

While Tecnalia has developed an extensive international network, its main priority remains regional development. This includes a number of activities aimed at attracting talent; dual vocational training programs tuned to the local industry needs; supporting start-ups and SMEs; extensive contact with the (foreign capital) companies established in the region. Tecnalia is one of the partners in the Basque Digital innovation Hub, which is a part of the pan-European network of Digital Innovation Hubs[44]. This network aims at assisting SMEs in integrating digital technologies; its ultimate goal is to even out the level of digitalization across the EU.

This hub is clearly focused on developing local ecosystems and channelling resources towards them, with minimal regulatory intervention from the centralized state governing bodies. It recognizes that regional-, national- and European-level bodies can have different priorities that need to be reconciled and structured for optimal cooperation. The hub envisions that the latter can be achieved by combining

[43]Tecnalia, "Strategic Vision", https://www.tecnalia.com/en/tecnalia/strategic-vision/strategic-vision.htm [Last accessed on December 1, 2019]

[44] Pan-European network of Digital Innovation Hubs (DIHs), https://ec.europa.eu/digital-single-market/en/digital-innovation-hubs [last accessed 9 December 2019].

top-down and bottom-up approaches, while capitalizing on the communities that are already in place. Interregional cooperation can be key to reducing technological dependency, exchanging knowledge and furthering trust.

3.6 Conclusion

Having examined different types of governance structures, and keeping the stakeholder requirements in mind, we have identified a number of elements that could provide valuable lessons for the governance design for NCCC. An overview of the identified strength and weaknesses can be found in Table 2.

We find that the synergy between formal and informal, top-down and bottom-up structures as found in ENISA can be beneficial to the overall success of an institution. By integrating informal structures participation borders are reduced, leading to a more efficient stakeholder engagement throughout all societal levels. This ties in with the model of membership opportunities for societal stakeholders of different levels and foci, which we found in ECSO. Furthermore, we find that transparency is a key element for facilitating trust in an organization. The effects of a transparent organizational construct can be seen well in CERN.

While, in general, rules for eventual procedures are an essential aspect of a complete governance structure, our case study on the Toulouse security hub (initiated by OcSSImore) shows that successful projects can thrive because of a nimble governance model. OcSSImore adopted an agile concept of case-by-case decisions on funding and innovation, at a project level, by the project partners. This is possible because the hub is separate from the actual investments in security and innovation. It ensures that—often time critical—decisions on funding innovative and novel ideas and research proposals are not inhibited by elongated funding procedures that ultimately prevent timely innovation. Additionally, the Toulouse hub structure that is currently undergoing its evolution demonstrates an overall promising development for the future structure of the NCCC and the Competence Community.

Specifically, we selected OcSSImore as a potential pilot, because its agile stakeholder engagement allows a quick integration of their needs during the pilot, to ensure translation from science to practice is quick and provides competitive solutions. This will foster innovation and increase competitiveness of this European endeavour. Furthermore, the transparent structure enables us to effectively capitalize on the local networks and resources already present, to ultimately foster a vibrant cybersecurity community as a role-model for the future structure of the NCCC.

Further chapters of this document will examine the possibilities concerning the incorporation of this and similar structures into the governance structure proposal. Similarly, we find that including existing local resources and capabilities can be instrumental for realizing the full potential of an institution. For example, capitalization on the existing local resources has been instrumental in ensuring the success of the Basque hub Tecnalia.

Governance Example	Positive	Negative
ENISA	The synergy between formal and informal, top-down and bottom-up structures as found in ENISA can be beneficial to the overall success of an institution and interactions. By integrating lower-level, decentralized informal structures participation borders are reduced, leading to a more efficient stakeholder engagement throughout all societal levels.	Despite the formalization of the lower-level structures, ENISA remains a top-down-institution; in the field of cybersecurity, it creates challenges for reaching out to the stakeholders and in reacting to stakeholders' demands.
ECSO	ECSO is based on a model of membership opportunities for societal stakeholders of different levels and foci, which enables bottom-up approach and diversity of engagement. ECSO has come up with a number of low-level initiatives, such as ECSO Cybersecurity Business Matchmaking events, aimed at bringing European start-ups and SMEs closer to funding opportunities.	ECSO is currently in progress regarding the issues of governance transparency.
CERN	Transparency is a key element for facilitating trust in an organization. The effects of a transparent organizational construct can be seen well in CERN. There is a rigorous system in place to ensure the prevention of (financial) free-riding and the maximal involvement of the member states in the projects relevant to them. The development of vibrant scientific community in Europe and ensuring its prominence on the world stage is given clear priority.	The CERN governance is specific to its goals of fostering research and cooperation, and is insufficient for the goals of fostering multi-stakeholder and multi-sectorial approach.
Tecnalia	Tecnalia is a good example of capitalizing on the existing local resources and networks.	The strength is also a weakness: despite a growing amount of international cooperation, the character of activities remains local, thus creating challenges for the possible long-term planning and broader strategy.
OcSSImore	OcSSImore is a unique example of an agile concept of case-by-case decisions on funding and innovation, at a project level, by the project partners. This is possible because the hub is separate from the actual investments in security and innovation. It ensures that—often time critical—decisions on funding innovative and novel ideas and research proposals are not inhibited by elongated funding procedures that ultimately prevent timely innovation.	The challenges identified so far include formalizing the diverse needs of the vertical stakeholders, as well as the need for support of public authorities.

Table 2: Overview of positive and negative aspects in the analysed governance examples.

This page has been intentionally left blank.

4 Presentation of EU Regulation Proposal 2018/0328 (COD)

In this chapter, we present the EU Regulation Proposal, which is a draft 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. The chapter carries out a comprehensive in-depth legal analysis of the EU Proposed Regulation 2018/0328, presenting the general context, the legal requirements and content of the Proposal. At the end of the chapter, an itemized summary of the Proposal and the main takeaways will be presented.
The proposal contains core elements for a potential legal framework in which a later NCCC could be managed that on itself could be managing cybersecurity research, funding and innovation within the EU. Since the proposal is still subject to discussion, it is neither binding nor definite yet. There does not yet exist a binding legal structure of a NCCC as of now; and even if the regulation was passed there would still be ample room for legal analysis and research due to a certain vagueness and lack of content as will be shown below.

4.1 Legislative Process

On 12 September 2018 the Commission presented a proposal for a Regulation (the "Proposal", the "Proposed Regulation")[45] which will establish (1) a European Cybersecurity Industrial, Technology and Research Competence Centre (the "Competence Centre"), [46] (2) a Network of National Coordination Centres (the "Network" of "Coordination Centres") and a (3) Cybersecurity Competence Community (the "Community"). The proposal builds on previous initiatives such as the 2013 Cybersecurity Strategy[47] and the Directive on security of network and information systems of 2016 (the "NIS Directive")[48] and aims to scale-up the Cybersecurity Contractual Public-Private Partnership (cPPP) between the European Commission and the European Cybersecurity Organisation ("ECSO").[49] The Cybersecurity cPPP is a contractual partnership between ECSO, an industry-led association of stakeholders, and the European Union, that was established in 2016 in order to create a dialogue between them and foster cybersecurity research and development in the Union.[50]

[45] 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, 2018/0328 (COD).

[46] The Council of the European Union wants to exclude "competence" in the name of the entity, which means that the name would be the European Cybersecurity Industrial, Technology and Research Centre (proposal and remark 4, Interinstitutional File 2018/0328 (COD)).

[47] European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 7 February 2013, JOIN(2013) 1 final.

[48] Directive (EU) 2016/1148 of 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).

[49] European Commission, Decision of 5 July 2016 on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organization, C(2016) 4400 final).

[50] The goal of the cybersecurity cPPP is to increase development and innovation of cybersecurity solutions in Europe, increase the European cybersecurity competitiveness, strengthen cybersecurity awareness and training and align the investments and research with the cybersecurity demand (C(2016) 4400 final). Compared to the cybersecurity cPPP, however, the explanatory memorandum to the Proposal claims that the added value of the Proposal lies in the larger scale of investment and the establishment of an efficient framework for pooling knowledge and stimulating development.

The Proposal is in line with the need to secure the Digital Single Market, as was pointed out in the Joint Communication of the Commission and the High Representative of the Union for foreign affairs and Security Policy of 2017.[51] It aims to strengthen the European position in the cybersecurity market as well as to ensure European cybersecurity independently from third countries by combining knowledge and experience available in the Member States.[52]

So far, the Proposal already went through the European Economic and Social Committee, which gave an opinion,[53] and afterwards through the European Parliament, which made several amendments.[54] After the first and the second trilogue discussions, respectively on 13 March 2019 and 20 March 2019, three technical meetings were held in order to make progress on the text. After the last technical meeting on 26 March 2019, a text was published that displays the initial proposal of the European Commission, the amendments of the European Parliament and the position of the Council of the European Union, as well as a representation of the possible compromises between the three institutions.[55] Trilogue negotiations on the basis of articles 288, 289 paragraph 1 and 294 TFEU are being continued at the time of writing in order to come to a decision on the basis of article 294 paragraph 3 TFEU.

4.2 Purpose of the Proposal

In broad terms, the Proposal aims on the one hand to secure Europe digitally and on the other hand to increase Europe's cybersecurity competitiveness. These are goals that originate in the changing economy and society, and the historic backlog of Europe on cybersecurity solutions in comparison to third states such as the United States.

The establishment of a true Digital Single Market, i.e. an online market where goods, persons, services, capital and data can freely move, requires taking away regulatory barriers and fragmentation. Considering the exponentially increasing presence of online interactions and commerce in modern society and economy, it is of great importance to secure the Digital Single Market against cybersecurity threats. Yet Europe has a history of relying on non-European products and solutions for doing so, because of a lack of marketed European cybersecurity products. This is illustrated by the low level of competitiveness of Europe in the field of cybersecurity, the main players being the United States and China.

In order to determine the reasons for this deficit, we can firstly point out the political barriers, namely the complex inter-state climate of the EU and the Member States' political and industrial considerations involved in security and cybersecurity, and the regulatory barriers created by fragmented legislations. These barriers are however slowly removed through Member State cooperation, such as the European

[51] European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, 13 September 2017, JOIN(2017) 450 final.

[52] Article 3, 2018/0328 (COD).

[53] European Economic and Social Committee, *Opinion on 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 – 2018/0328 (COD)], 23 January 2019, TEN/684-EESC-2018.

[54] European Parliament, *Amendments adopted by the European Parliament on 13 March 2019 on 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)0630 – C8-0404/2018 – 2018/0328(COD)), P8_TA-PROV(2019)0189.

[55] Interinstitutional File 2018/0328 (COD).

Defence Agency and the Permanent Structured Cooperation, and regulatory initiatives such as the recent NIS Directive and the Cybersecurity Act,[56] that strengthen the role of the European Union Agency for Cybersecurity ("ENISA").

On an operational level, a first (1) important obstacle to the increase of cybersecurity innovation and marketable products is the isolation of research and development, as a result of the lack of cooperation between Member States, industries and actors. As mentioned above, states have a nationalistic approach to cybersecurity, resulting in research and development activities running parallel to one another, duplicating effort and not using capacities and capital in an efficient manner.[57] Furthermore, public, private and academic actors are often also reluctant to cooperate for reasons of data and innovation ownership, competitive advantages and underlying contradictions of goals.[58] Moreover, there is an information dissymmetry between the supply and demand industries, as it appears that cybersecurity products do not always answer the real-life requirements and challenges that arise on the end-user side.[59] Finally, because of the historical dichotomy between civilian and defence applications, research on these topics also runs parallel to each other.[60] With the appearance of hybrid threats however, cooperation on dual use applications will become increasingly important and will result in a more efficient use of knowledge and resources.[61]

A second obstacle is sub-scale investment in cybersecurity in Europe. To illustrate this, in 2019 the estimated investments in Europe in cybersecurity were limited to 1-2 billion Euro, while in the United States for example the investments are budgeted at 21 billion dollar, which seems to be a staggering difference.[62] While there is innovation, there is a lack of easy access to funding, venture capital and an overall limited budget to spend, which results in the existing innovation not living up to its full potential and experts and innovative businesses moving out of Europe in search for investments.

[56] Regulation (EU) 2019/881 Of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act).

[57] European Court of Auditors, Briefing Paper: Challenges to effective EU cybersecurity policy, March 2019, https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf [last accessed 5 November 2019]; European Commission, Commission Staff Working Document, *Impact Assessment accompanying the document 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} - {SEC(2018) 396 final} - {SWD(2018) 404 final}, 12 September 2018, SDW(2018) 403 final, Part 1/4, p8-9.

[58] European Court of Auditors, *Briefing Paper: Challenges to effective EU cybersecurity policy*, March 2019, https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf [last accessed 25 October 2019]; SDW(2018) 403 final, Part 1/4, p9-10.

[59] SDW(2018) 403 final, Part 1/4, p8.

[60] European Court of Auditors, *Briefing Paper: Challenges to effective EU cybersecurity policy*, March 2019, https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf [last accessed 6 November 2019].

[61] The proposal includes provisions on enhancing the cooperation between civil and defence spheres with regard to dual-use technologies and applications in cybersecurity (see article 4(7), 2018/0328 (COD)). This is however, a major point of disagreement in the negotiations as the trilogue document suggests (proposal and remark 131 ff., Interinstitutional File 2018/0328 (COD).

[62] European Court of Auditors, *Briefing Paper: Challenges to effective EU cybersecurity policy*, March 2019, https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf [last accessed 25 October 2019]

Third, there is an increasing demand for cybersecurity know-how, skills and facilities, but unfortunately access thereto is limited.[63] The lack of know-how and skills results on the one hand from the brain drain caused by the sub-scale investment referred to in the previous paragraph and the fragmentation of profiles across the EU. On the other hand, there are not enough profiles trained in cybersecurity, and curricula are not aligned with the actual skills that are needed in practice ("the skills gap"). Cybersecurity facilities are also scarce, since they are often too costly for one entity or a Member State to acquire. This is regrettable, given that the facilities that enable cybersecurity testing, experimentation and operation are essential for the development of cybersecurity products.

In order to overcome these obstacles and make up for the EU's lost ground, the Proposal essentially focusses both on stimulating and coordinating cooperation and on retaining and developing cybersecurity and industrial capacities.

4.3 Requirements and Aspects of Regulation

The NCCC aims to connect institutions from different disciplines all across Europe, creating a consortium of specialists that pool expertise with the best possible use of existing resources.[64] As a system of different companies, business models, practitioners, member states and their institutions, EU institutions, cross-border-cooperation, international actors, administrative agencies and bodies, academic and research institutions, societal movements and all other potential stakeholders, the success of such a network depends in a special way on the successful cooperation of the parties involved. As a basis for the internal structure of such an institution, it is precisely the task of successful governance to facilitate and organize this cooperation in a meaningful way.

The legal framework of any type of cooperative endeavour depends on numerous factors. The most important one are the actors involved: Whether or not private partners are part of the cooperation, whether EU institutions such as the EU Commission or the EU parliament as well as national member states participate, whether separate public and state entities in the individual member states act – these and many more factors make the legal framework in itself highly complicated and complex.

The NCCC is not one single organization according to this draft regulation, but – as any network – combines several institutions and cooperations in operation and communication at different levels. It aims at cooperation between all actors involved in a loose connection of interchange and communication with only few regulatory boundaries and settings.[65] Within the NCCC, the overall cooperation is one between public entities on the one hand (i.e. the Competence Centre as EU entity even if the exact legal nature is still under discussion, potentially the National Coordination Centres performing public service, public entities within the Cybersecurity Community) and private actors (i.e. practitioners, businesses and research institutions as part of the Cybersecurity Community; potential National Coordination

[63] European Commission, Commission staff working document, *Executive summary of the 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} - {SEC(2018) 396 final} - {SWD(2018) 403 final}, 12 September 2018, SWD(2018) 404 final.

[64] Recital 6, 2018/0328 (COD), Amendment 7 to Recital 6, P8_TA(2019)0189, http://www.europarl.europa.eu/doceo/document/TA-8-2019-0189_EN.html , latest visit on 29th July 2019.

[65] Article 4(1) (7) and (8), 2018/0328 (COD).

Centres if designed under private law and not considered to be fulfilling public tasks, other private actors).

This is also reflected in all the cooperation taking place within the institutions of the NCCC, e.g. the Network of the National Coordination Centres or the Community where both private and public actors are members. It will depend on the exact structure and the exact partners in these sub-institutions of the NCCC whether the private or the public partners are in the majority. At least for the Community, it is likely that due to the concentration of the regulation proposal on business and enterprises, private actors will outweigh the public actors and other practitioners. Parts of the cooperation are intended to take part only between public entities, so especially true for the cooperation between the Competence Centre and the Network of National Coordination Centres, which according to the Commission shall be established in the form of a Public-Public governance structure[66].

4.3.1 Legal Framework of Cooperation

Not every cooperation deserves the assessment as a legally relevant cooperation, however. Often, especially between private parties, there is no desire of the parties to bind each other and oneself. Loosely connected interaction is not legally framed; no legal obligations shall arise of the contact. One might argue that at least parts of the NCCC are based on this level, particular the interaction of the Community as it is designed presently. The tasks of the Community as formulated in art. 9 all describe un-enforceable missions which do not create claims against or obligations for individual members of the Community.

It can be debated whether the entire NCCC is based on such loose connections without legal binding. After all, typically a network consists of information interaction rather than regulated interactions and decisions. However, the Commission has expressed the understanding that at least the collaboration between the Competence Centre and the Network of National Coordinating Centres shall be regulated by a Public-Public governance structure. Also, the exact description of a Board of Governance, of tasks and means of interaction, of roles and even of legal consequences (such as accreditation) speaks the language of a legal formality, which contradicts an understanding of the NCCC as a loose interaction without any legal intention. Therefore, legal binding is desired at least in parts of the NCCC. This raises the necessity to ask for the legal framework of cooperations into which the NCCC would potentially have to be integrated.

4.3.1.1 Private Cooperation Law

Private cooperations between two and more private partners can rely on a well-established, long-standing legal framework on cooperations, i.e., corporate law. This has also been extended to cross-border cooperations in the course of establishing the EU internal market. Private cooperations can choose between a variety of legal instruments on the legal form which depend on the level and the purpose of cooperation. This framework makes available a number of different legal forms of cooperation and establishes a default system on which private cooperations may rely. Corporate legal forms typically provide for the governance structure, i.e. the members of the cooperation, the duration of the cooperation, whether it has legal personality, who acts as representative, how decisions are made or how contributions and extractions of funds are decided. Numerous governance issues need not be addressed for this reason because corporations law provides a legal default; and if the partners in a

[66] SDW(2018) 403 final, Part 1/4: 33.

private cooperation decide to deviate from the forms of corporate law, the freedom of contract and the liberty to act usually protect any of the chosen and agreed-on special rules of the individual cooperation. This typically allows private parties in cooperations to refrain from establishing their own governance structures. They may rather define and discuss those issues where individual agreements reflect the particularities of the cooperation better than the standard solution of the law. It should be remarked, that such standard rules by law also are resource-saving instruments and that some – although few - governance structures are binding depending on the legal form.

4.3.1.2 Public Cooperation Law

However, a similar extensive legal framework does not exist for cooperations where public entities are involved, whether it is a public-public-cooperation or a public-private cooperation. There exists no comparable differentiation and systematization in public law with corresponding requirements on the legal forms and variety of cooperative behaviour. Public-public- and public-private-cooperation regulations are already scarce at member state level[67]; in EU law even less, formal legal guidance exists. Exact specifications for legal structures are missing. Even though contractual relations are possible, they are not protected under freedom of contract or similar legal discretion on the side of the public partners in such cooperations but rather fall under restrictions due to the rule of law and other principles governing and restricting the action of states and public entities.

In the case of the NCCC, the EU has expressed the desire not to leave the establishment to existing parties but to create the NCCC and its institutions by law, namely the proposed regulation. Any legal obligation or design of governance structure is thus binding if not else declared.

This might lead to the conclusion that the EU aims at creating the organizational form of a "European Agency" as an administrative institution. European agencies are institutions within the Union which fulfil a specific task. They are, unlike the institutions of the European Union, legitimized not by the Treaties as primary law but by secondary EU legislation.[68] They are based on the legislative act of a regulation that set out the basic organization of the institution. The European Union Agency for Cybersecurity (ENISA) is such an example, ECHA, the European Chemical Regulation Agency another. However, re-constructing any of the proposed NCCC institutions or the overall NCCC as a European Agency would be in clear contradiction to the idea of the network. There exists no clear administrative task for the NCCC; typical attribution norms are lacking. The entire structure of the NCCC is designed opposite to an administrative agency with its clear structure and clear task. Thus, the lack of a general cooperation governance structure by law requires an individual approach which is found in the proposed regulation.

The simplicity of this approach of no clear legal framework for public cooperations, however, is diminished by the fact that there is no offset law or any default governance structure on which the involved parties may rely on if the regulation has not regulated some issues in full. Therefore, for reasons of legal clarity, the parties of such cooperations should typically find a normative ground for their actions in an agreement.

[67] Richter and Spiecker gen. Döhmann, in Durner, Reimer, Spiecker gen. Döhmann, Wallrabenstein (Eds), "Das sinnvoll Denkbare denken, das davon Machbare machen" , *Festschrift Arndt Schmehl*, 2019.
[68] Typically, the foundation of this competence of the EU is seen in art. 352 TFEU.

It is obvious that the legal construction, e.g. as a chartered corporation or a society or a club, each require a different set of governance structures. This also has consequences for the formalities required. Any type of network like the NCCC is very complex in these aspects due to the large number of organizations involved and their legal classification, as both private and public structured organizations will participate in this cooperation. This fact significantly restricts the possibilities of legal formality and can most easily be achieved through contractual agreements between the parties involved. However, with the proposed regulation, the EU Commission has taken a significant step towards establishing a single system of public and private interaction and cooperation on several levels under which existing and future cooperations could then be classified.

4.3.2 Overlapping Legal Requirements from Substantive Law

This situation is complicated furthermore in the type of situations in which the NCCC will act: When public entities and private actors cooperate, they do this on a variety of levels, content and binding power. This is also true for a NCCC: Its broad task of furthering cybersecurity and in particular research and education leaves a lot of space for wide and narrow activities alike in many concrete areas of law. Thus, the proposal of a regulation for a NCCC is only a first step to establish a cooperation. Respect has to be paid also, beyond the cooperation issue, towards content-specific law which may bind the parties of the cooperation further. Substantive matters on which a cooperation decides in such a governance structure may oppose the liberties promised by the lacking cooperation law.[69]

These substantive law rules may have a decisive influence on the potential of cooperation: Whether there is a seller-buyer-relationship or a B2B-relationship, whether there is public procurement at issue or whether there is an educational or other specific content in relation to Cybersecurity may change the legal framework in which the cooperation may act. This will – in addition to the cooperation as such – be another backbone of legality of the cooperation and its decisions. In all of these areas, there may be existing legal rules to which a NCCC would have to adhere to when taking decisions in these matters in the area of cybersecurity.

The test case of CyberSec4Europe of MOOCs serves as an illustration of this abstract finding (See Chapter 6): Here, typically public and private actors are involved, e.g. public universities and private research institutions. Sometimes only public actors take part, e.g. public universities. As no public-public or public-private cooperation law exists, the parties are in a first step generally free to design a governance structure to their individual needs. They may agree on a majority rule by which all partners are bound.

However, if the cooperation decides to grant credits towards a degree for courses taken at any of the involved universities, this might violate the educational and academic laws of some of the member states where the universities are incorporated. Thus, the cooperation would have to adhere to the educational law within each of the involved universities' member states and potentially also further EU law in regard to the exchange of education. The procedural, governance-oriented decision rules of the cooperation could not overcome this substantive binding. Naturally, MOOCs which are organized on a lower level – e.g. not granting credits – will have to adhere to lesser regulation.

[69] It should be mentioned that this is also true for private cooperations: their governance structure does not assist them in the overcoming of substantive law.

Thus, the validity and liberty of the decision-making processes in a governance structure also always depend on the exact topic of decision. This has to be integrated into the NCCC's governance structure: The NCCC may only decide where it is competent to do so, and this depends on the attribution of competences to the EU on the one hand and to the NCCC on the other hand.

4.3.3 Summary

In summary, the Regulation Proposal is an important step in establishing a legally functioning NCCC beyond the non-existing public cooperation legal framework and thus the lack of a default setting. However, it should be noted, that effective cooperation legally depends on more than a governance structure for the NCCC: Each decision of the NCCC will also have to take into account the boundaries of substantive law.

4.4 EU Competence

As the NCCC is proposed by the EU, the special requirements of EU law also apply to the design of the NCCC. The EU is bound by the treaties, by its secondary law and also by the principle of subsidiarity. When proposing legislation and establishing bodies, The EU is bound by the limitations of its competence as enshrined in the Treaties and its secondary law.

4.4.1 General Perspective on EU Competence

The Treaties determine the areas in which the EU can act and the modalities and limitations of such actions. If the Union wants to intervene, e.g. to establish the Competence Centre and the Network, a legal basis should be found in the Treaties.

Furthermore, when a competence is non-exclusive, meaning that the Member States can also act in this area, the EU needs to respect the principle of subsidiarity which entails that the Union can only act when the intended action cannot be sufficiently achieved by the Member States on a central, regional or local level, and when it, by reason of the scale or effects of the proposed action, can be better achieved at Union level.[70]

Finally, the Union should respect the principle of proportionality when acting. This principle entails that the intervention by the Union should always be suitable to achieve the predefined goal and should be necessary to achieve that goal. An intervention by the Union is considered necessary when it is the only action able to achieve the goal without there being a valid alternative which has fewer negative effects on other interests or goals.

4.4.2 Legal Basis

The Commission proposed to establish the Competence Centre and the Network on the basis of article 173, paragraph 3 TFEU and article 187 of the TFEU.

Article 173(3) TFEU falls under the EU's competence with regard to "Industry", a competence which should, according to article 6(b) TFEU, be limited to supporting, coordinating or supplementing the actions of the Member States. In other words, the centre of gravity regarding industry policy remains at the Member State level. In the area of industry, the TFEU created the open-coordination method, i.e. a flexible and non-binding promise of coordination between the Member States and the Commission

[70] Article 5, paragraph 3 TEU.

where necessary. Nevertheless, Article 173(3) TFEU opens up the possibility for the Union to take specific measures to foster competitiveness of the Union's industry, by for example encouraging an environment favourable to cooperation between undertakings and by fostering better exploitation of the industrial potential of policies of innovation, research and technological development. It is in this regard that the Competence Centre would be established to create an environment for cooperation and to offer support in order to increase cybersecurity competitivity.

The Proposal of the Commission is also based on article 187 TFEU, an article which is part of the Union's competence on "Research and technological development and space". Although, this competence is not limited to coordination, support or supplementing the Member States, as is the case for industry, article 4(3) TFEU limits EU competence in this area to intervention which does not prevent Member States from exercising their competence. Specific EU activities the TFEU refers to under this competence are defining and implement research and technological development programmes. The legal basis itself creates the possibility to establish joint undertakings or *any other structure necessary* for the execution of European research, technologic development and demonstration programmes.

The legal bases mentioned above are however not a perquisite to determine the legal form that the Competence Centre will adopt, several forms are possible as will be described below.

The Proposal stipulates that the Competence Centre will be a *union body with legal personality* and continues by stating that the Competence Centre is proposed as a *European Partnership* under the proposed Regulation establishing the new Horizon Europe programme.[71] Such a European Partnership is a cooperation between the Union and Private and or Public Partners, for which the proposed Horizon Regulation refers to examples such as bodies with a public service mission at local, regional, national or international level or civil society organisations including foundations. The partners should jointly support the development and implementation of a programme of research and innovation activities.[72] The proposed Horizon Regulation stipulates that these partnerships can be or co-programmed, co-funded or established as an institutionalised partnership on the basis of article 185 (public-public) or 187 TFEU (joint undertakings (public-private) and other structures).[73]

Besides the conditions for the European Partnerships also the conditions of the EU Financial Regulation should be taken into account when determining which entities can implement EU funding. With relevance to the Competence Centre and the Network, bodies which can implement EU funding are public law bodies, including Member State organisations; bodies governed by private law, provided that they have adequate financial guarantees; bodies governed by private law of a Member State that are entrusted with the implementation of a public -private partnership and provided with adequate financial guarantees; bodies set up under the TFEU, such as joint undertakings; and public-public partnership bodies.[74]

[71] Proposal for a Regulation of the European Parliament and of the Council establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination Horizon Regulation, 2018/0224 (COD).
[72] Article 2(3), 2018/0224 (COD).
[73] Article 8, 2018/0224 (COD).
[74] Article 62(1)(c), Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 (1).

4.4.3 The Structure of the Competence Centre and the Network.

Keeping in mind that the Commission proposed to establish the Competence Centre and the Network as a European Partnership, which by definition appears to be a public-private partnership when established on the basis of article 187 TFEU (i.e. the basis for establishing joint-undertakings and other structures), the intention of the Commission seems to be to establish the Competence Centre and Network as a public-private partnership. This would then be an institutionalised public-private partnership, since the proposal states it will be an EU body with legal personality.

The question that arises here is whether this is an appropriate structure and legal ground as the Competence Centre and the Network have a public-public nature, since its members are the EU and the Member States. It is true that the stakeholders will be involved through the Community, the Advisory Board and the Network, thereby bringing the private component to the table. However, they are not established at the outset of creating the Competence Centre and the Network and are not as such involved in the negotiation process.

Public-public partnerships are usually based on other legal grounds, such as article 185 TFEU that provides for the Member States and the Union to participate on research and development programmes and participation in structures created for the execution of such programmes. A sui-generis EU body which is also established on the basis of article 173 TFEU is the Institute for Innovation and Technology, to which the Proposed Regulation refers. The difference between the Competence Centre and the EIT however, is that the EIT is not a partnership between the Union and the Member States, but an initiative from the Union that includes private experts and private partnerships in its governance.

It is therefore interesting why the Commission has preferred a combination of article 187 and 173 to establish a European Partnership as described by the proposed Horizon Regulation, rather than establishing an executive agency or an institutionalized public-public partnership on other grounds.

4.4.4 Tasks of the CC and the NCCC: Is the EU Overstepping its Competence?

Linked to the unclarity of the legal structure is the uncertainty of whether the Competence Centre and the Network do not overstep EU competence in the area of cybersecurity, industry and research and technological development.

When it comes to cybersecurity, the complexity of EU action is illustrated by the lengthy journey it took to give ENISA its status of a permanent agency. ENISA is established on the basis of article 114 TFEU with its main objective to ensure the proper functioning of the internal market through approximating Member State laws. Cybersecurity touches on matters of national security, defence, public security and criminal law, areas which belong to the sovereignty of the Member States and in which the union can only act when it does not impact Member State competence. However, since cyberthreats are a cross-border issue and are difficult to be tackled on an isolated national level, it is of collective importance to cooperate at the Union level and secure the internal market. These objectives of cooperation and support are reflected in ENISA's competences, which have been the result of a lengthy negotiation process to make them solely complementary to the Member States' competences.

As mentioned above, the competences with regard to industry, research and technologic development are limited to supporting, coordinating or supplementing the actions of the Member States and not hampering them in exercising their own competences. Important to know is that the Competence Centre

is tasked with setting up a strategic research agenda, in order to direct cybersecurity funding towards the research mentioned on the agenda. The initial Proposal stipulates that the Competence Centre would be funded 50/50 between the Union and the Member States this would entail the *de facto* steering of national cybersecurity research, which could be considered as going beyond mere support and coordination. Furthermore, the Competence Centre would be tasked with enhancing access to cybersecurity capabilities, knowledge and infrastructures by acquiring, upgrading, operating and making available testing and experimentation infrastructures, a task which might also go beyond merely providing support and coordination to the Member States.

4.4.5 CHECKs

Under Section 5 of this deliverable, the CyberSec4Europe consortium will propose an additional structure to that of the Competence Centre, Network and Community. The Community Hubs of Expertise in Cybersecurity Knowledge or CHECKs will function as regional centres of expertise which gather regional expertise, i.e. regional members of the Community, and stimulate cooperation between the Community.

For the establishment of the CHECKs similarities could be drawn from the Knowledge and Innovation Communities (KICs) under the EIT. These communities are partnerships between higher education institutions, research organisations, companies and other stakeholders in the innovation process, in the form of a strategic network, that are selected by the EIT.[75] The proposed Horizon Regulation refers to the KICs as a programme in which the union might participate in the form of a European Partnership.[76]

Similarly, to what has been done for the EIT and the KIC's, the Proposed Regulation could create the possibility for the Competence Centre to appoint CHECKs and lay down some ground rules for the governance of these CHECKs. The relationship between the Competence Centre and the CHECKs could then be based either on a contract, on the basis of article 187 TFEU, creating a joint undertaking, or on the basis of a European Partnership. The latter would mean that the CHECKs itself would also have competences to implement EU Horizon funding.

4.5 The Structure Proposed by EU Regulation Proposal 2018/0328 (COD)

The proposed Regulation establishes the Competence Centre, which is composed of a Governing Board, an Executive Director and an Industrial and Scientific Advisory Board, three bodies which will be discussed in detail below. Initially, the Commission planned to establish the Competence Centre in Brussels.[77] However, in its amendments, the Parliament proposed to delete this provision[78] and the Council proposed to add a provision reserving the decision on the seat of the Competence Centre to the Representatives of the Governments of the Member States.[79]

[75] Regulation (EC) No 294/2008 as amended by Regulation (EU) No 1292/2013.
[76] Article 8, 2018/0224 (COD).
[77] Article 1(3), 2018/0328 (COD).
[78] Amendment 46, P8_TA-PROV(2019)0189.
[79] Proposal and remark 18, Interinstitutional File 2018/0328 (COD).

On the level of the Member States a network of National Coordination Centres will be established. The Coordination Centres will be (existing) national (public) entities nominated by the Member States and accredited by the Commission.[80]

Thirdly, the proposed Regulation creates the Community, a network of cybersecurity stakeholders, defined by the Proposal as industry representatives from the demand and supply-side, academic and non-profit research organisations, associations of users, public entities and other entities dealing with operational and technical matters in the area of cybersecurity.[81] Besides the stakeholders, the National Coordination Centres and the relevant Union institutions and bodies will also be involved. The Parliamentary amendment also explicitly proposes to add SME's, individual experts, European Digital Innovation Hubs and European Standardisation Organisations to the Community. The possible inclusion of European Standardisation Organisations is very much welcomed by Elena Santiago from CEN-CENELEC, as she has stressed at a panel discussion on the proposal hosted by CyberSec4Europe.

4.6 The Competence Centre

In order to meet the objectives of the Proposal, the Competence Centre and the Network will be responsible for pooling and connecting efforts and expertise and putting them to use in an efficient manner. In order to do this, the Competence Centre will play a key role in facilitating and coordinating cooperation between all actors involved.[82] Remarkable in this context is the fact that the Proposal does not elaborate on the relationship between the Competence Centre and the Cooperation Group, a group without legal personality established under the NIS Directive.[83] This Cooperation group, consisting of representatives from the Member States, the Commission and ENISA, after all, has tasks that might overlap with those of the Competence Centre. Similar to the facilitation and cooperation role of the Competence Centre, the Cooperation Group of the NIS Directive focuses on facilitating strategic cooperation between all actors involved in the implementation of the NIS Directive and is a platform for the exchange of information and best practices on research and development relating to the security of network and information systems.[84] It is therefore striking that the Proposal does not stipulate how these two entities relate to one another.

Another important role of the Competence Centre is situated on the level of financial support, that originates from both the Union and an efficient pooling of investments.[85] In this regard, the Competence Centre will perform a pivotal role in the implementation of the funding through the European Union's Horizon Europe Programme and the Digital Europe Programme.[86]

[80] Article 6, 2018/0328 (COD). The Council stipulates in its position that it wants the National Coordination Centres to be appointed by the Member States and registered by the Governing Board, taking away the role of the Commission and deleting the accreditation process (Proposal and remark 162-163, Interinstitutional File 2018/0328 (COD)).

[81] Article 8, 2018/0328 (COD).

[82] Article 4(1) (7) and (8), 2018/0328 (COD).

[83] Article 11, NIS Directive.

[84] Article 11, NIS Directive.

[85] Article 5, 2018/0328 (COD).

[86] Article 4(2), 2018/0328 (COD). The Horizon program will be the successor of the Horizon 2020 program, aimed at funding research and innovation (Proposal for a Regulation of the European Parliament and of the Council establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, 7 June 2018, COM(2018) 435 final. Digital Europe will be a new funding mechanism which aims to develop and reinforce the

Moreover, the Competence Centre envisages to enhance access to cybersecurity capabilities, knowledge and infrastructures by acquiring, upgrading, operating and making available testing and experimentation infrastructures, or providing support to entities in doing so.[87] It will furthermore facilitate access to the existing and future expertise across the Union by promoting cybersecurity education and reducing the skills-gap.[88]

The general idea is to develop a Union wide cybersecurity industrial strategy, intended to foster wide deployment of European cybersecurity products.[89] Part of this strategy will involve supporting research and innovation for standardization in cybersecurity technology.[90] In the Parliament's view, besides supporting research and innovation for standardization, there should also be support for actions in the area of certification. Furthermore, the Parliament stipulates that the Competence Centre should cooperate with European Standardization Organizations and ENISA while carrying out these tasks. The Council's position added that the activities in the field of standardization and certification should be done in accordance with the Cybersecurity Act.[91]

4.6.1 Governance of the Competence Centre

The Competence Centre will be a new European entity with legal personality. The form of the entity, and whether it should have legal personality or not, is however still a point of disagreement in the negotiations.[92] The Proposal states that the Centre will be created on a double legal basis, namely article 187 TFEU and 173 TFEU,[93] thereby giving the Centre a broad mandate to pool knowledge and actors, but also to take steps towards coordination and strategy for market deployment. The Commission's view is to establish the entity in the form of a Public-Public governance structure.[94] The creation of such Public-Public Partnerships (PUPP) is foreseen in the proposed Horizon Regulation.[95] Examples of PUPP's implementing Horizon 2020 funding are the Eurostars partnership, the European Metrology Program for Innovation and Research (EMPIR) and the Partnership for Research and Innovation in the Mediterranean Area (PRIMA).[96] However, unlike the Competence Centre created by the Proposal, these partnerships do not create a European entity.

European strategic digital capacities and increase European competitiveness in this area. For cybersecurity, the programme will invest in infrastructure and equipment and the development of the necessary skills and knowledge. (European Commission, *EU budget: Commission proposes €9.2 billion investment in first ever digital programme,* Press release, 6 June 2018, IP/18/4043, https://europa.eu/rapid/press-release_IP-18-4043_en.htm [last accessed 31 October 2019])

[87] Article 4(3) 2018/0328 (COD). The task of facilitating the acquisition of cybersecurity infrastructures and capabilities proves a controversial point in the trilogues, with the Council being of the opinion to fund this aspect solely through voluntary contributions from Member States and Union funding for joint actions (proposal and remark 147, Interinstitutional File 2018/0328 (COD)).

[88] Proposal and remark 149 and 189, Interinstitutional File 2018/0328 (COD)).

[89] Article 4(4), 2018/0328 (COD).

[90] Article 4(6)(c), 2018/0328 (COD).

[91] Proposal and remark 146, Interinstitutional File 2018/0328 (COD)).

[92] Proposal and remark 499-501, Interinstitutional File 2018/0328 (COD).

[93] According to which the Union can set up Joint Undertakings or any other structure necessary for the efficient execution of Union Research, technological and demonstration programmes (Article 187, Treaty on the Functioning of the European Union (TFEU)) and actions can be taken to stimulate the competitiveness of the Union's industry (173 TFEU).

[94] SDW(2018) 403 final, Part 1/4, p33.

[95] Article 8, Proposal for a Regulation of the European Parliament and of the Council establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, 2018/0224(COD).

[96] These examples will be discussed further below in the section regarding the voting rules in the Governing Board.

In order to determine the form of the Competence Centre, it proves interesting to look at another entity established on the same legal basis. There is, for example, the European Institute of Innovation and Technology (EIT), an entity also established on the basis of article 173 TFEU. Similar to the Proposal, the EIT Regulation also created a community in support of the EIT, namely the Knowledge and Innovation Community (KIC).[97] The EIT is tasked with promoting higher education, research and innovation in the EU, in order to increase economic growth and competitiveness in the Union.[98] The entity is established as a Community body and identified by the Union itself as being part of the group of *"other EU organizations"*, that differ from decentralized or executive agencies.[99] It is therefore to be expected that the Competence Centre will be established in a similar form. Nevertheless, the matter is still under negotiation.

The Proposal stipulates that the 'members' of the Competence Centre will be the Member States (financially participating or not) and the European Union, which will be represented by the Commission.[100]

The Competence Centre will work together with relevant Union institutions, bodies, offices and agencies, including ENISA, CERT-EU, the European External Action Service, the Joint Research Centre of the Commission, the Research Executive Agency, the Innovation and Networks Executive Agency and the European Cybercrime Centre at Europol. Furthermore, the Centre will work with the European Defence Agency on dual-use projects, services and competences.[101] Again, it is interesting that the Proposal does not mention the Cooperation Group under the NIS Directive here. A possible explanation for this could be that the Commission expects the same representatives to take part in both the Cooperation Group and the Competence Centre.

The cooperation will be carried out under a framework of working arrangements[102] which will have to be preapproved by the Commission.[103] Such working arrangements could be useful in determining the synergies between the Competence Centre and other Union bodies, in particular ENISA, to avoid duplicating work and joining forces on for example the dissemination of information.

4.6.2 Financing of the Centre

According to the Proposal, the operational and administrative costs of the Competence Centre are divided 50-50 between the Union and the Member States that decide to participate financially.[104] As the

[97] Article 7, Regulation (EC) No 294/2008 of the European Parliament and of the Council of 11 March 2008 establishing the European Institute of Innovation and Technology.

[98] Article 3, Regulation (EC) No 294/2008.

[99] European Union, Agencies and other EU bodies, https://europa.eu/european-union/about-eu/agencies_en [Last accessed 29 October 2019]

[100] Article 11, 2018/0328 (COD).

[101] Article 10(1), 2018/0328 (COD). The Parliament adds to this the relevant European Digital Innovation Hubs (amendment 120, P8_TA-PROV(2019)0189).

[102] Working arrangements are a common instrument to determine the conditions for cooperation between European institutions, agencies, bodies and organizations. For example, Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation, opens up the opportunity for EUROPOL to conclude working agreements with other Union bodies.

[103] Article 10(2), 2018/0328 (COD). The Parliament stipulates that these working arrangements should be adopted by the Governing Board (amendment 121, P8_TA-PROV(2019)0189).

[104] Article 22, 2018/0328 (COD).

Parliament rightfully pointed out through an amendment, there is no definition of financial contributions by Member States. The Parliament suggests that such a definition would be adopted by the Governing Board.[105] The Council added to this that instead of a definition, the Governing Board should adopt a methodology to calculate the amount of voluntary contributions.[106]

Unsurprisingly, the financial contributions to the Competence Centre are a major hurdle in the negotiations on the legislative text, with Member States not accepting the obligation to double the amount put in by the Union, which are resources that essentially also originate from the Member States. The Council is suggesting an important change in this regard, by stating that the operational and administrative costs of the Competence Centre should be borne by the Union.[107] The Member States on their part, would in the Council's view be able to participate voluntarily by delivering financial contributions for Joint actions with the Union. The Council suggests these contributions to be paid in instalments and in-kind contributions, the latter consisting of costs incurred by the national Coordination Centres and beneficiaries in implementing actions which are not reimbursed by the Centre.[108] Another suggestion made by the Council to reduce the financial burden of the Centre is to redeploy staff from the Commission and the European bodies to meet the staffing requirements of the Centre.[109]

4.7 The Governing Board

Members of the Competence Centre are represented in the Governing Board, which determines the direction of the Centre and makes sure that the Proposed Regulation is complied with when carrying out its tasks. The Board establishes the budget and sets up its own rules of procedure for the decision making and rules to prevent and avoid conflicts of interest.[110] Furthermore, the Board adopts the Centre's annual work plan and the multiannual strategic plan after preparation thereof by the Executive Director.[111] [112] According to the Council, the annual work plan should focus on implementing the relevant Union funds, notably the cybersecurity parts of the Horizon Europe and Digital Europe programmes, in the framework of the multi annual strategic plan and the strategic planning process of Horizon Europe. Furthermore, in the Council's opinion, the annual work plan should contain the allocation of funds from the Union budget to joint actions between the Union and the Member States, for which the conditions also have to be established by the Governing Board.[113] In order to make decisions on a certain cybersecurity topic, the Governing Board can set up working groups with members of the Community.[114] Finally, the Governing Board is also in charge of accrediting the Community Members.

[105] Amendment 134, P8_TA-PROV(2019)0189.

[106] Proposal and remark 265, Interinstitutional File 2018/0328 (COD)

[107] Proposal and remark 368 and 389, Interinstitutional File 2018/0328 (COD).

[108] Proposal and remark 82 and 376, Interinstitutional File 2018/0328 (COD).

[109] Proposal and remark 453, Interinstitutional File 2018/0328 (COD).

[110] Article 42, 2018/0328 (COD).

[111] Which, according to the Council, has to contain a common strategic, industrial, technology and research roadmap (proposal and remark 242, Interinstitutional File 2018/0328 (COD)).

[112] The Parliament added to this that it should take into account the advice of ENISA before adopting the work plan and the multi-annual plan (amendment 127, P8_TA-PROV(2019)0189).

[113] Proposal and remark 246-247, Interinstitutional File 2018/0328 (COD)

[114] The Parliament stipulates that the Board should take into account the advice of the permanent observers before it forms working groups (amendment 131, P8_TA-PROV(2019)0189). The Council however wants to delete this provision (Proposal and remark 255, Interinstitutional File 2018/0328 (COD))

A question that arises here is how the Governing Board will deal with all the specific issues and topics related to cybersecurity competence, as well as the elaboration of the financing schemes, both tasks that require a lot of effort and specific expertise. This void leaves room for the establishment of substructures that work continuously in a specific area or are established ad-hoc when certain issues arise. This idea would be in line with the possibility for the Cooperation Group under the NIS Directive to set up sub-groups for specific questions.[115]

The Proposal already creates a possibility for such a substructure, by giving the Governing Board the power to establish working groups made up of Community members. This is in line with ENISA's structure, that confers strategic decision powers upon the Management Board, which is assisted by the Executive Board, which can also establish working groups.[116] The Council suggested that, when setting up such working groups, the Competence Centre should consider replications of existing structures, such as the cybersecurity Public Private Partnership and the cybersecurity pilots under Horizon 2020.[117]

Another possibility lies at the level of the National Coordination Centres, that can deploy the Network to establish Member State cooperation on certain themes. Nevertheless, as will be elaborated upon further, the governance of the Network itself is still to be determined.

4.7.1 Membership

The Governing Board is composed of one representative of each Member State and five representatives of the Commission.[118] This formation is slightly adjusted by the Parliament's amendment to include an observer for the Parliament at the cost of one of the Commission's representatives (which number is consequently pushed back to four).[119] The Council's position however is to push the number of Commission representatives back to two.[120]

Representatives are ought to be appointed in light of their knowledge in the field of technology and managerial, administrative and budgetary skills for a renewable term of 4 years.[121] The Board selects its Chairperson from among the members with voting rights for a period of two years, renewable for one term.[122]

The Proposal appoints ENISA as a permanent observer to the Board (without voting rights), and stipulates that the Executive Director and, upon invitation of the Chairholder, the Members of the Advisory Board can take part in the deliberations (both without voting rights).[123] The Parliament has done an important amendment to the Proposal in this regard, by including the Advisory Board as a

[115] Article 8, Commission Implementing Decision (EU) 2017/179 of 1 February 2017 laying down procedural arrangements necessary for the functioning of the Cooperation Group pursuant to Article 11(5), NIS Directive.

[116] Article 20, Cybersecurity Act.

[117] Proposal and remark 55, Interinstitutional File 2018/0328 (COD).

[118] Article 12, 2018/0328 (COD).

[119] Amendment 122, P8_TA-PROV(2019)0189.

[120] Proposal and remark 230, Interinstitutional File 2018/0328 (COD)

[121] Article 12, 2018/0328 (COD). The Council's position is that Member States appoint employees of the relevant public authorities as these representatives (proposal and remark 232, Interinstitutional File 2018/0328 (COD)).

[122] Article 14, 2018/0328 (COD). The Council wants to push the number of years to three (proposal and remark 271, Interinstitutional File 2018/0328 (COD)

[123] Article 12(7), 14(3) and (4), 2018/0328 (COD).

permanent observer to the Governing Board, alongside ENISA. This amendment is important in the light of stakeholder representation, a topic which will be dealt with in detail further on. Furthermore, the Parliament opened up the possibility to invite members of the Community.[124]

4.7.2 Voting

An important part of the Centre's governance are the voting rules in the Governing Board, as set out by article 15 of the Proposal. 50 percent of the votes are reserved for the Commission, the other 50 percent being held by the financially participating Member States. Decisions are taken by 75 percent of all votes, including those of absent members. Furthermore, these 75 percent of votes should also represent at least 75 percent of the total financial contributions to the Competence Centre, which are calculated based on the estimated expenditures proposed by the members and based on the value of the contributions of the participating Member States.

In its amendments, the Parliament has proposed to change these voting rules. First of all, the amendments set out the decisions subject to a vote, distinguishing between (a) decisions on the governance and organization of the Centre and the Network, (b) the allocation of the budget and (c) the joint actions by several Member States. The Parliament maintains the 75 percent majority rule in its reading of the Proposal for all these decisions. This majority is supplemented by additional rules depending on the type of decision. For the decisions under (a) all Member States are represented and have the same equal right of vote, regardless of their financial participation. The Union holds the remaining votes, which should be at least 50 percent corresponding to its financial contribution. For the decisions under (b), (c) and other decisions the Union will hold at least 50 percent of the voting rights according to its financial contribution, and only financially participating Member States will hold a vote, which will correspond to their financial contribution.

The difficulty of agreeing on the voting rules is reflected in the position of the Council, whose viewpoint differs from that of the Commission and the Parliament. It stipulates that a vote should only be held if the members of the Governing Board fail to find a consensus. Decisions should furthermore be taken by a majority of at least 75%. For decisions on the Joint actions, the contributing Member States and the Commission shall hold votes proportional to their relevant contribution on that specific action. For all other actions every Member State and the Commission shall hold one vote.[125]

Apart from setting up a very complicated voting system, dependent on the size of financial contributions – a concept which is left ambiguous – the Proposal's voting rules are drawn up entirely in favour of the Union. Since 50 percent of the votes go to the Commission, and the representatives of the Commission can only vote unanimously, the Commission will have a de facto veto on all the decisions in the Governing Board, since decisions can only be taken with 75 percent of the votes. Moreover, in that 75 percent majority, 75 percent of the financial contributions have to be represented. This strengthens the veto right of the Commission even more, since the Competence Centre is 50 percent funded by the Commission.

[124] Amendments 124 and 125, P8_TA-PROV(2019)0189.

[125] Proposal and remark 280-284, Interinstitutional File 2018/0328 (COD).

In this regard, it proves interesting to look at the institutions and bodies that currently implement Horizon 2020, to look for similarities with regard to the applicable voting rules, assessed in light of the funding arrangements, since funding arrangements always have a large impact on the voting rules. Implementation of Horizon 2020 funding is not located at one single European body or agency, but involves five Commission Directorate-Generals, including DG CNCT, executive agencies, public-public partnerships, public-private partnerships, the European Institute of Innovation and Technology (EIT) and the European Investment Bank (EIB).

Particularly relevant are the public-public partnerships, since the Competence Centre and the Network of National Coordination Centres will have elements of these partnerships.[126] Eurostars is an example of such a PUPP, in which the European Commission cooperates with states (also non-EU), in order to support international innovative projects that are led by small- and medium-sized enterprises that perform research and development. The budget of this partnership consists on the one hand of contributions of the participating Member States and on the other hand of funding by the Union under Horizon 2020, but with the limitation that at least 1/3 of the contributions should come from the participating states. Eurostars' key decision-making body is the High-level Group, in which the European Commission is an observer, but does not have any voting rights.[127]Another example of a PUPP is The European Metrology Programme for Innovation and Research (EMPIR), which provides coordination for research projects to develop fundamental measurement science in the fields of energy, health, environment and industry. The EMPIR PUPP is funded 50-50 between the European Union and the Participating States.[128] EMPIR is managed within the framework of EURAMET, and decisions on the annual work plan, calls for proposals and the projects to be funded are made by the EMPIR Committee. The Commission is an observer without voting power in this Committee, except for decisions on the annual working plan, which the Commission must approve prior to adoption.[129] Another PUPP where funding is divided 50-50 between the Union and the participating states and where the annual working plan has to be pre-approved by the Commission is the Partnership for Research and Innovation in the Mediterranean Area (PRIMA).[130]

The differences between the abovementioned PUPP's and the Proposal are situated primarily on the level of the intended scope and expected impact of the initiatives, since the Proposal covers all domains of cybersecurity, aims to bring together all relevant public and private stakeholders across Europe and has far-reaching goals for the European market and its competitivity. Moreover, the Proposal stipulates that the Centre will be a European entity as opposed to an intergovernmental entity. Furthermore, the initiative to create the Centre and the Network comes from the Union itself, whereas the PUPP's are partnerships the Union wished to participate in. Taking these factors into account, the voting rules in the PUPP's cannot merely be applied to the Competence Centre.

[126] See Section 3.2.

[127] Decision No 553/2014/EU of the European Parliament and of the Council of 15 May 2014 on the participation of the Union in a Research and Development Programme jointly undertaken by several Member States aimed at supporting research and development performing small and medium-sized enterprises.

[128] Decision No 555/2014/EU of the European Parliament and of the Council of 15 May 2014 on the participation of the Union in a European Metrology Programme for Innovation and Research (EMPIR) jointly undertaken by several Member States.

[129] Decision No 555/2014/EU, Annex III.

[130] Decision (EU) 2017/1324 of the European Parliament and of the Council of 4 July 2017 on the participation of the Union in the Partnership for Research and Innovation in the Mediterranean Area (PRIMA) jointly undertaken by several Member States.

Since the Proposal claims as an aim to scale up the contractual Public Private Partnership, it is also interesting to look at the current PPP's that are implementing Horizon 2020. In this area several Joint Technology Initiatives (JTI) have been set up between the European Union and the private sector, initiatives which are implemented through legal entities called Joint Undertakings (JU). These JU's are funded both by the public and private sectors. Decisions are made by a governing board, in which the Commission has a seat. Once the JTI members decide upon an annual or multiannual work programme, the JU will implement the strategic innovation and research agenda that the JTI set out. An example of such a JTI that is relevant for the area of cybersecurity is ECSEL, or in full: Electronic Components and Systems for European Leadership. ECSEL funds research, development and innovation projects in order to increase Europe's competitiveness in the sector of Electronic Components and Systems. ECSEL is funded partly by the Union, participating states and private members. The most important decision-making body within ECSEL is the Governing Board, where the Commission, the participating states and the private members meet. Voting rights in ECSEL are divided equally between the three groups. Within each of these groups, additional rules on the division of votes can be drafted, for example depending on financial contribution. Consensus is the principle, however, when no consensus is reached, decisions are taken with a 75% majority.[131]

Finally, also the EIT and the European Investment Bank (EIB) are implementing the Horizon 2020 programme. The EIT is financed mainly through Horizon 2020.[132] What is interesting however, is that strategic decisions are taken by simple majority by a governing board composed of experts in business, higher-education and research, appointed by the Commission, and representatives of the KIC community.[133] There is thus no Member State vote in the decision making and the experts making the decisions are appointed by the Commission.

As a result of a delegation agreement between the Commission and the EIB, the latter implements Horizon 2020 funding through Innovfin. This programme supports entities with financing for research and innovation, in the form of loans, guarantees and equity products.[134] The decision on whether an entity receives funding or not, is taken by the Board of Directors, consisting of 28 Directors appointed by the Member States and 1 Director appointed by the Commission. The Board of Directors votes with a majority of 1/3, representing at least 50% of the subscribed capital to the EIB.[135] Since the share of every Member State in the capital of the Bank is calculated according to their economic weight within the European Union, the votes of states such as Germany, France and Italy carry more weight.

It follows from the above that one cannot simply conclude that the voting rules of the above partnerships and entities are always dependent on the financial contribution of the participating entities and that the Union always has a decisive vote. It is therefore surprising, in a way, that the Commission has taken the

[131] Council Regulation (EU) No 561/2014 of 6 May 2014 establishing the ECSEL Joint Undertaking, Annex.

[132] Article 14 and 19, Regulation (EC) No 294/2008.

[133] Section 2 and 3 of the Statutes of the European Institute of Innovation and Technology, Regulation (EC) No 294/2008, Annex.

[134] European Commission, *Access to risk finance*, https://ec.europa.eu/programmes/horizon2020/en/h2020-section/access-risk-finance [last accessed 31 October 2019].

[135] EIB, Board of Directors, https://www.eib.org/en/about/governance-and-structure/statutory-bodies/board_of_directors/index.htm [last accessed 31 October 2019].

risk, in the context of a sensitive subject such as cybersecurity, to assign itself a leadership role, especially since the funding essentially comes from the Member States.

4.8 The Executive Director

The Executive Director is responsible for the operations and day-to-day management of the Competence Centre and is the legal representative of the Centre. He or she prepares the annual work plan and the multiannual strategic plan, after consultation of the Governing Board and the Commission.[136] Furthermore, the Executive Director approves the list of actions selected for funding.[137] The Executive Director will also prepare, negotiate and conclude the agreements with the National Coordination Centres.[138]

The Director is appointed by the Governing Board from a list of candidates proposed by the Commission, for a term of 4 years, which can be renewed once.[139] He or she can be removed from office only after a decision by the Governing Board, which follows a proposal by the Commission.[140] The appointment will be based on grounds of expertise and high reputation in the areas where the Competence Centre operates.[141]

4.9 The Industrial and Scientific Advisory Board

The Industrial and Scientific Advisory Board aims to create a dialogue between the private sector, consumer organizations and other relevant stakeholders.[142] In order to represent the stakeholders and advise the Governing Board on the relevant issues it will organize public consultations and collect feedback on the work plan and multi-annual strategic plan of the Competence Centre.[143]

The Board will meet twice a year and will be composed of maximum 16 members, being representatives of entities of the Community which are appointed by the Governing Board for their cybersecurity expertise, and a chair, which will be elected amongst the members.[144] According to some stakeholders,

[136] The Parliament adds to this consultation of the Industrial and Scientific Board and ENISA (amendment 144, P8_TA-PROV(2019)0189). The Council however, proposes to delete this addition (proposal and remark 326, Interinstitutional File 2018/0328 (COD)

[137] Article 17, 2018/0328 (COD). The Parliament adds that the Industrial and Scientific Board and ENISA should be consulted prior to approving the list (amendment 146, P8_TA-PROV(2019)0189).

[138] Article 17, 2018/0328 (COD).

[139] The Parliament wants to change the term to 5 years (amendment 141, P8_TA-PROV(2019)0189).

[140] The Parliament adds that this should also be possible on proposal by the members of the Governance Board (amendment 141, P8_TA-PROV(2019)0189). The Council added to this that this should be a proposal of at least 50% of the Member States (proposal and remark 310, Interinstitutional File 2018/0328 (COD)).

[141] Article 16, 2018/0328 (COD).

[142] Recital 27, 2018/0328 (COD). The Parliament proposed to interpret stakeholders under the Regulation as "*the industry, public entities and other entities dealing with operational and technical matters in the area of cybersecurity, as well as civil society, inter alia trade unions, consumer associations, the Free and Open Source Software community, and the academic and research community"* (amendment 10, P8_TA-PROV(2019)0189).

[143] Article 19 and 20, 2018/0328 (COD).

[144] Article 18 and 19, 2018/0328 (COD). The Parliament wants to adjust the number to 25 members and adds to the criteria for appointment that the representatives should be part of entities which are not controlled by a third-country or a third-country entity except from EEA and EFTA countries (amendment 149, P8_TA-PROV(2019)0189). The Council wants to delete the establishment requirement (proposal and remark 343, Interinstitutional File 2018/0328 (COD)). Furthermore, the Parliament and the Council added that a minimum number of seats should be allocated to each category of industry stakeholders, with

having a high-level of cybersecurity expertise is a very important requirement for the appointment of members of the Advisory Board, since valuable advice with regard to the industrial and research strategy can only come from the most prominent members of the Community. Besides the members and the chair, representatives of the Commission and ENISA are invited to participate in the Advisory Board.[145]

Since the Advisory Board will be established in order to create a dialogue between the stakeholders and the public entities and the Proposed Regulation claims as its greatest value *"scaling-up the cybersecurity contractual Public Private Partnership (cPPP), both on an investment level as well as on a structural level"* it proves interesting to compare both collaborations in terms of stakeholder representation.

In the cybersecurity cPPP, the Commission and ECSO are represented in a Partnership Board, that takes the decisions for the operation of the partnership. It agrees for example on a Strategic Research and Innovation Agenda (SRIA) and a Multi-Annual Roadmap. [146] In the Proposed Regulation, stakeholders are represented in the Advisory Board and through the Community. There is however a clear lack of inclusion of the stakeholders in the decision-making process, since the Advisory Board can only issue non-binding advice to the Executive Director and the Governing Board and there is no obligation for these bodies to seek such advice.[147]

Considering the importance of the stakeholder position and the expertise stakeholders bring to the table with regard to cybersecurity matters, not giving the stakeholders a real voice might result in the Proposal not reaching its full potential.

This point of view is followed by the European Economic and Social Committee, that emphasized being in favour of including the industry in the Governing Board, thereby making the public-public partnership into a private-public partnership at the highest level. In its opinion, the Industrial and Scientific Advisory Board might not be able to ensure an ongoing dialogue between the businesses, consumers and other relevant stakeholders.

4.10 Role of the European Commission

As was already touched upon, the Commission holds several responsibilities and decision-making powers in relation to the Competence Centre. In addition to those, the amendments of the Parliament confer on the Commission the power to adopt delegated acts in relation to the Proposed Regulation and the Competence Centre. More specifically, according to the Parliament the Commission should adopt a set of harmonized general conditions for the contracts with the National Coordination Centres and establish the criteria for the selection of Community members.[148] It is however to be expected that the powers of the Commission will be limited in light of the Council's position.[149]

particular attention paid to the representation of SMEs (amendment 37, P8_TA-PROV(2019)0189; Proposal and remark 345, Interinstitutional File 2018/0328 (COD)).

[145] Article 18, 2018/0328 (COD).

[146] C(2016) 4400 final.

[147] The Council's opinion however, is that the representation should be built upon the experience from the cybersecurity cPPP and the 4 pilots under Horizon 2020 (proposal and remark 55, Interinstitutional File 2018/0328 (COD).

[148] Amendment 185, P8_TA-PROV(2019)0189.

[149] Proposal and remark 167, 200 and 541-546, Interinstitutional File 2018/0328 (COD).

4.11 Relationship to ENISA

The recent Cybersecurity Act strengthens the position of ENISA as the European Union Agency for Cybersecurity.[150] With the Proposed Regulation creating a Competence Centre as an additional European cybersecurity entity, it is particularly relevant to determine how these two entities will exist next to each other.

So far, the Proposal mentions ENISA on two occasions. Firstly, when performing its task to improve understanding of cybersecurity and reducing the skills gap, the Competence Centre will support the development of cybersecurity skills, where appropriate together with ENISA.[151] Secondly, the Proposal appoints ENISA as a permanent observer in the Governing Board.[152] It is interesting in this regard to note that ENISA is given an entirely different weight in the Proposal and the NIS Directive. While here, ENISA only plays a secondary role, in the NIS Directive ENISA is a full member of the Cooperation Group and is considered to provide essential support.

Looking at the Cybersecurity Act, there are several tasks of ENISA which could overlap with the activities of the Competence Centre. First of all, the Cybersecurity Act stipulates that ENISA shall be the centre of expertise on cybersecurity that will support capacity-building and preparedness to develop skills and competencies in the field of cybersecurity.[153] The explanatory memorandum to the Proposed Regulation however defends the complementarity of the two entities when referring to the "core activities" of the Competence Centre, namely stimulating development and deployment of technology in cybersecurity and complementing the cybersecurity capacity building efforts at the European and Member State level.[154] Tasks which are, as the above mentioned reference to the Cybersecurity Act proves, activities which are also mentioned in ENISA's mandate.

Furthermore, ENISA has been given the objective to support and promote operational cooperation through information sharing and coordination among Member States, Union Institutions, bodies, offices, agencies and stakeholders.[155] This is, however, also one of the main objectives the Proposed Regulation aims to achieve.

Another overlap is situated on the level of ENISA's tasks in the area of research and innovation, where it will advise Member States on research needs and priorities in the field of cybersecurity, participate in the implementation phase of research and innovation funding programmes and contribute to the strategic research and innovation agenda.[156] In the explanatory memorandum to the Proposal it is pointed out that the mandate of ENISA focusses on tasks that are crucial for strengthening cybersecurity resilience in the Union, which in a way puts the advisory role in the background.[157]

[150] Regulation (EU) 2019/881.

[151] Article 4(5)(a), 2018/0328 (COD). The Council's position is to delete this provision (proposal and remark 120, Interinstitutional File 2018/0328 (COD).

[152] Article 12(7), 2018/0328 (COD).

[153] Article 4, Cybersecurity Act.

[154] Explanatory memorandum, 2018/0328 (COD).

[155] Article 4 and 7, Cybersecurity Act.

[156] Article 11, Cybersecurity Act.

[157] Explanatory memorandum, 2018/0328 (COD).

Finally, also dissemination of cybersecurity information to the public is on the agenda of both ENISA and the National Coordination Centres.[158]

According to the Parliamentary amendments, the Competence Centre should act as the operational body in cybersecurity, while ENISA will continue to fulfil its strategic objectives.[159] In practice, the Parliament suggests that the Competence Centre provides support to ENISA in its tasks under the Cybersecurity Act and the NIS Directive. ENISA, on its part should use its insights in the Cybersecurity sector to provide input to the Competence Centre for its task of defining funding priorities.[160] Furthermore, the amendments stipulate that the Competence Centre should consult ENISA because of its cybersecurity expertise, specifically on the matter of research.[161] Also for the development of cybersecurity skills, the Competence Centre should align with ENISA, according to the Parliament.[162] Finally, the Competence Centre should cooperate with ENISA in order to support research and innovation for standardization in cybersecurity technology.[163]

4.12 The Network and the Community

The National Coordination Centres will take on the role of national contact point under the Proposed Regulation and will build a bridge between the Competence Centre and the Community by coordinating the Community and by facilitating participation of the relevant national stakeholders in cross-border projects.[164] They will accordingly provide relevant input to the Competence Centre.[165] An important task of the National Coordination Centres will be allocating grants through cascading grant agreements.[166]

The Parliament proposes two additional tasks in its amendments, namely (1) the cooperation with National Standardization Organizations, to involve relevant stakeholders in setting new standards, and (2) the promotion and dissemination of common minimal cybersecurity educational curricula.[167]

4.12.1 Governance

The Proposal is rather concise on the role and governance of the Network of National Coordination Centres, but determines that they will have a contractual relationship to the Competence Centre.[168] This

[158] Article 9, Cybersecurity Act; Article 7, 2018/0328 (COD).

[159] Amendment 31, P8_TA-PROV(2019)0189.

[160] Amendment 22, P8_TA-PROV(2019)0189. This is reflected in the obligation to take into account the advice of ENISA on the multi-annual strategic plan, work plan, annual accounts and balance sheet and annual activity report (amendments 126, 127, 144, 146, P8_TA-PROV(2019)0189). The Council, however, wants to limit the involvement of ENISA (proposal and remark 317, Interinstitutional File 2018/0328 (COD)).

[161] Amendment 29, P8_TA-PROV(2019)0189.

[162] Amendment 79, P8_TA-PROV(2019)0189.

[163] Amendment 87, P8_TA-PROV(2019)0189.

[164] Article 7, 2018/0328 (COD). According to the Parliament, the National Centres should also establish the Cybersecurity Community (amendment 101, P8_TA-PROV(2019)0189).

[165] Article 7, 2018/0328 (COD).

[166] Recital 13, 2018/0328 (COD).

[167] Amendments 105 and 107, P8_TA-PROV(2019)0189.

[168] Article 6(5), 2018/0328 (COD).

contract will determine their tasks and will, in the Parliament's opinion, govern the relationship between them and the Competence Centre.[169]

Looking at other European bodies and agencies, we cannot identify a common practice of concluding such agreements in structures that are similar to the Competence Centre and Network. The NIS Directive, for example, creates the Network of national CSIRTs, which will cooperate with ENISA without there being any requirement to conclude a basis for the relationship. Also, organizations such as EUROPOL, FRONTEX and EUROJUST cooperate with national authorities. The difference however being that these authorities are not separate public agencies, but part of the Member States as such. Overall, it should be noted that the focus of the above-mentioned organizations is cooperation, whereas the focus of the Network lies, in addition to cooperation, in the implementation of Union funding. Looking from this perspective, putting in place a contractual agreement with the national entity distributing funding could provide additional safeguards to the Union.

When taking a look at other Union agencies involved in the distribution of funding, contracts are sometimes used to govern the relationship with entities implementing such funding. The EIT, which was mentioned above already, has agreements in place with the KICs, which are partnerships of universities, research organizations, companies and other stakeholders that put the funding to use in order to reach the EIT objectives.[170] However, contrary to the National Coordination Centres, such KICs are not public agencies.

An example of a contract between a national agency and the Union with regard to funding, can be found in the ERASMUS+ scheme that aims to provide funding for educational and training opportunities for citizens of the European Union. In order to implement the funding on a national level, the authorities of the Member States have to appoint national agencies, which will have a contractual relationship with the Commission. The ERASMUS+ Regulation stipulates the requirements for these contractual relationships.[171] Another example of a contractual relationship between a national agency and a Union agency is the ones between the European Food Safety Authority and the (public) organizations appointed by the Member States as being competent in this field. These contracts will stipulate conditions for the performance of the tasks of the appointed organizations.[172] Nevertheless, it should be stressed that the contractual relationship between the National Coordination Centres and the Competence Centre is still under negotiation at the time of writing, partly because the Council is not in favour of this provision.[173]

How the Network itself is supposed to operate is not determined in the Proposal, leaving the Member States free to decide on how the National Coordination Centres will be connected to one another and how they will interact. It is in this regard unclear how the Network of Coordination Centres will relate to the network of CSIRTs, created by the NIS Directive.[174] This CSIRT network was established to

[169] According to Parliament, the Commission should provide a set of harmonized general conditions for these contracts in delegated acts, with the possibility to supplement the contract with special conditions tailored to the particular Coordination Centre (amendment 99, P8_TA-PROV(2019)0189).

[170] Article 6(3), Regulation (EC) No 294/2008.

[171] Article 29, Regulation (EU) No 1288/2013 of the European Parliament and of the Council of 11 December 2013 establishing 'Erasmus+': The Union programme for education, training, youth and sport and repealing Decisions No 1719/2006/EC, No 1720/2006/EC and No 1298/2008/EC.

[172] Article 6(2), Regulation (EU) No 1288/2013.

[173] Proposal and remark 166, Interinstitutional File 2018/0328 (COD).

[174] Article 12, NIS Directive.

facilitate operational cooperation between the Member States under the NIS Directive, including, inter alia, sharing information on risks and threats and cooperating on specific cybersecurity incidents. Since both networks will have an operational objective, they could benefit from an interplay or even a cooperation.

For the governance of the Network, inspiration can be drawn from EUREKA, an intergovernmental network that facilitates cooperation and funding for research, development and innovation.[175] The decision making in EUREKA is left to a ministerial conference and a high level group consisting of representatives of the participating states, two bodies which are comparable to the Governing Board.[176] However, at the operational level, EUREKA is governed through a group of national project coordinators, that oversee the activities of thematic cooperation and individual projects under the EUREKA framework.[177] The Network of Coordination Centres could establish a similar body in which operational and thematic issues are dealt with by representatives of the National Coordination Centres.

4.12.2 Appointment

The National Coordination Centres are selected on the basis of their capability to support the Competence Centre and the Network. This capability is assessed by taking into account their technological expertise or their access to such expertise and the possibilities the Centres have to engage and coordinate with all relevant stakeholders.[178]

The Proposal provides for the National Coordination Centres to be appointed by the Member States. It does not, so far, determine how these Centres should be selected. Moreover, there is no obligation for Member States to appoint a public entity as the National Coordination Centre, but nevertheless, the Council position expresses that these entities should be public sector entities or entities performing public administrative functions.[179] This position of the Member States did not come as a surprise, given that the National Coordination Centres will have an important role in the allocation of European funding.

When looking at the national public bodies and entities responsible for cybersecurity, it is clear that the designation of the Coordination Centres will not be self-evident. In several Member States, such as Cyprus and Slovakia, there is no dedicated public cybersecurity entity. Rather, the cybersecurity competencies are divided over several state bodies. Furthermore, taking the specific example of Belgium, there is no clarity on whether the mandate and the resources of the Cybersecurity Centre allow for this body to take on the role of National Coordination Centre. In Belgium, and evidently in other Member States as well, the existing cybersecurity entity is not involved in the funding of scientific and technical research and development activities, rather these competencies are regionalized. In other

[175] Eureka, Eureka Regulatory Corpus Between the EUREKA Full Members, 30 June 2017, EUREKA doc. MC35-08, https://www.eurekanetwork.org/sites/default/files/eureka-regulatory-corpus.pdf [last accessed 31 October 2019].

[176] As is also expressed above with regard to Eurostars, which is a program between Eureka member states and the European Union.

[177] Eureka, Eureka Regulatory Corpus Between the EUREKA Full Members, 30 June 2017, EUREKA doc. MC35-08, https://www.eurekanetwork.org/sites/default/files/eureka-regulatory-corpus.pdf [last accessed 31 October 2019].

[178] Article 6(4), 2018/0328 (COD). The Parliament stipulates that the Commission should issue guidelines on the selection procedure and application of the criteria for assessment (amendment 98, P8_TA-PROV(2019)0189).

[179] Proposal and remark 27, Interinstitutional File 2018/0328 (COD). The Council also explicitly mentions that in its opinion these National Centres can be entities that also fulfil other functions created by European Law, such as national competent authority and/or single point of contact in the meaning of the NIS Directive, any other EU Regulation, or digital innovation hub in the meaning of the Digital Europe Programme (proposal and remark 28, Interinstitutional File 2018/0328 (COD).

Member States, Cybersecurity Centres are formed on the basis of a Public Private Partnership, such as NCCyber in Poland. It remains to be seen which entities the Member States will appoint or whether new entities will be created.

4.13 The Cybersecurity Community

Under the coordination of the National Coordination Centres, a Cybersecurity Community will be established. The Proposal rather vaguely describes the role of the Community, as it stipulates that the Community will contribute to the mission of the Competence Centre, enhance and disseminate cybersecurity expertise and participate in activities, working groups and specific projects.[180]

The uncertainty of the involvement of the Community in the Competence Centre, also illustrated by the role of the Industrial and Scientific Advisory Board, raises concerns as to the level of stakeholder involvement and representation in the Centre. The Parliament has proposed to expand the tasks of the Community to also include enhancing, pooling and sharing cybersecurity expertise.[181] Furthermore, they create the opportunity for the Community to provide technical expertise and stakeholder insights to the Competence Centre, for example on cybersecurity vulnerabilities,[182] which could indicate that they are in favour of a more bottom-up-approach. Regarding the expertise on vulnerabilities in particular, the Parliamentary amendments stipulate that the Centre should take into account the vulnerabilities discovered by the Community and accordingly facilitate the development of solutions.[183]184

4.13.1 Membership

Only entities that are established within the Union and demonstrate cybersecurity expertise in the domains of research, industrial development and/or training and education can be appointed as a Community Member.[185] Such criteria, however, would lead to the possible exclusion of stakeholders that are established within the Union, but have a non-European parental background. It is hard to imagine that industrial players that invested in the Union and have a wealth of expertise should be refused from becoming a member to the Community, especially because their valuable input could be needed to achieve the Proposal's goals.

The assessment on the membership conditions will be carried out by the National Coordination Centre of the Member State in which the entity is established. Once the National Coordination Centre presents

[180] Article 8(1) and 9, 2018/0328 (COD).

[181] Amendment 111, P8_TA-PROV(2019)0189.

[182] Amendment 119, P8_TA-PROV(2019)0189

[183] Amendment 83, P8_TA-PROV(2019)0189.

[184] Amendments 124 and 151, P8_TA-PROV(2019)0189.

[185] Article 8(3), 2018/0328 (COD). The Parliament adds to this that also entities and individuals established in the EEA or the EFTA should be able to be accredited (amendment 113, P8_TA-PROV(2019)0189). Moreover, it proposes to add academia, ethics and standardization to the domains of expertise (amendments 114 and 115, P8_TA-PROV(2019)0189). As mentioned above, the Parliament stipulates that the Commission should provide details on the selection criteria in delegated acts (amendment 118, P8_TA-PROV(2019)0189). The Council, to the contrary, wants to limit Community Membership to entities and individuals established in the Union, including those with cybersecurity expertise in the areas of product development, information security and/or incident response operations and scientific or technical partnerships or cooperation with academic and/or public authorities (proposal and remark 191-198, Interinstitutional File 2018/0328 (COD)).

a candidate, the Competence Centre will accredit them as a member of the Community.[186] The Competence Centre can furthermore also accredit Union bodies, agencies and offices as Community members.[187]

As the assessment procedure is carried out by the National Coordination Centres and followed by an appointment by the Competence Centre, a lot of decision power is left at the Member State and Union level in deciding whether an entity is relevant or not. Furthermore, the Proposal is unclear on whether an entity that wishes to be part of the Community can apply for this status or whether assessments can only be conducted at the initiative of the National Coordination Centres.

Moreover, the Proposal is not specific on whether the entities concerned have to be individual stakeholders or whether also groups of stakeholders can be appointed. Most likely, groups of stakeholders will also have to be allowed to participate in the Community, since it is unclear how national centres of excellence and associations could otherwise fit in the Community.

In addition, there are also groups of stakeholders of which the scope extends beyond Member State boundaries. It consequently seems very unnatural to connect such organizations to one National Coordination Centre.

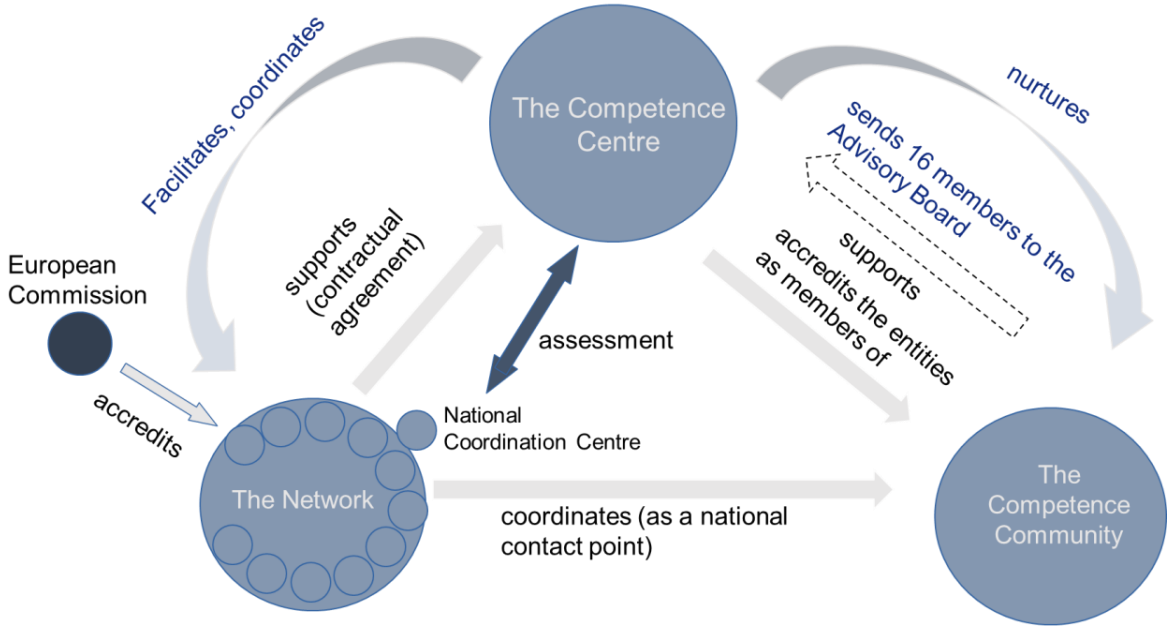

Figure 10: Overview of the Governance Structured proposed in the regulation draft.

[186] Article 8(4), 2018/0328 (COD). The Parliament provides for the Competence Centre to not only do the accreditation but also determine the assessment procedure (amendment 117 and 128, P8_TA-PROV(2019)0189). The Council wants to change the wording of the proposal from accreditation by the Competence Centre to registration and deletes the power of the Competence Centre to determine the assessment procedure (proposal and remark 199 and 249, Interinstitutional File 2018/0328 (COD))

[187] Article 8(5), 2018/0328 (COD).

Name	Type of entity	Members	Role
Cybersecurity Industrial, Technology and Research Competence Centre	PPP on the basis of articles 187 TFEU and 173 TFEU. Form and legal personality are still under negotiation.	European Union and the Member States.	• Facilitate and coordinate cooperation; • Implement Horizon and Digital Europe funding • Enhance access to cybersecurity capabilities, knowledge and infrastructures by acquiring, upgrading, operating and making available testing and experimentation infrastructures; • Facilitate access to existing and future expertise.
Governing Board		One representative per Member State and five of the Commission. The composition is still under negotiation[188].	Decision-making body that: • Decides on the annual work plan; • Decides on the multi-annual strategic plan; • Decides on the budget; • Sets up working groups with Community members; • Accredits the members of the Community.
The Executive Director		Appointed by the Governing Board based on a list of the Commission for a 4-year term.	Day-to-day management and legal representative, who: • Prepares the annual work plan and the multi-annual strategic plan; • Approves the list of actions selected for funding; • Negotiates and concludes the agreements with the National Coordination Centres.
Industrial and Scientific Advisory Board	Stakeholder representation in the Centre.	16 representatives of entities of the Community, which are appointed by the Governing Board for their cybersecurity expertise.	Aims to create a dialogue between the private sector, consumer organizations, and relevant stakeholders by: • Organizing public consultations; • Collecting feedback on the work plan and multi-annual strategic plan; • Issuing non-binding advice to the Governing Board.
Network of National Coordination Centres	A network of national (public) entities connected to the Centre on the basis of a contractual agreement.	National (public) entities selected on the basis of their capability to support the Competence Centre and the Network. Selected by the Member States.	• National contact point and bridge between the Competence Centre and the Community: Coordinating the Community and facilitating participation of the relevant national stakeholders in cross-border projects; • Input to the Centre; • Allocating grants.
Cybersecurity Competence Community	A network of cybersecurity stakeholders dealing with operational and technical matters in the area of cybersecurity, see Chapter 2.1.	**1.** Entities established in the EU demonstrating cybersecurity expertise in research, industrial development and/or training and education, appointed by the NCC of the Member State where the entity is established and accredited by the Competence Centre. **2.** Union bodies, agencies and offices.	• Contribute to the mission of the Competence Centre; • Enhance and disseminate cybersecurity expertise; • Participate in activities, working groups and specific projects.

Table 3: High-level overview of EU Regulation Proposal 2018/0328 (COD).

[188] ENISA will be a permanent member, the Parliament also wants to include the Advisory Board as a permanent observer.

Finally, as pointed out by the EC in its opinion, it is unclear which role the cybersecurity cPPP with ECSO, the predecessor of the Competence Centre and Network, will have in the Network and Community.

4.13.2 Coordination

Since the Proposal only fixed the accreditation of the Community members by the Competence Centre, there still is room to decide on the management of the Community[189], the connection of the Community members to the National Coordination Centres and the basis for cooperation between the different members of the Community.

However, together with the opportunity to establish a governance structure on the level of both the National Coordination Centres and the Community, also come uncertainties as to how relationships will be governed and how tasks are to be divided. This could have a negative effect on the main objective of cooperation that the Proposal wishes to achieve, as stakeholders might not be willing to cooperate without there being a fixed framework for cooperation. Possible reasons for such reluctance could be issues regarding the ownership of the research and the intellectual property rights. When organizing their relationship, stakeholders could define their cooperation based on a contract, for which perhaps a standard version could be provided under the Network or, taking inspiration from the cPPP's, stakeholders could reach an agreement with the National Coordination Centres to establish a cooperation on a certain development or research project.

In any case, in the event that the cooperation was based upon a grant under Horizon 2020 or Digital Europe, the National Coordination Centres and the stakeholders will be connected through a grant agreement.

4.14 Summary

An overview of the EU Regulation Proposal 2018/0328 can be found in Table 3, and a visualization in Figure 10. In summary, the main takeaways of the EU Regulation Proposal 2018/0328 are:

1. The Proposal stipulates that the Competence Centre and the Network are a scale-up of the **Cybersecurity contractual Public-Private Partnership** (cPPP) between the European Union and ECSO, which was established in 2016.
2. The **goals** are to secure the EU digitally and to increase cybersecurity competitiveness through coordination, cooperation and investment.
3. Points of **unclarity** in the proposal:
    - Form of the Centre: will it be an EU agency?
    - Relation to and cooperation with other EU bodies and agencies, such as the Cooperation group under the NIS Directive and ENISA.
    - Funding: Commission proposed a 50/50 split between the EU and the Member States. The Council suggests voluntarily Member State participation.

[189] The Council suggests that the management of the Community should build upon the experience of the cPPP in cybersecurity and the cybersecurity pilots under Horizon 2020 (proposal and remark 55, Interinstitutional File 2018/0328 (COD).

- Voting in the Governing Board: The Proposal creates a *de facto* veto right for the Commission, voting rules that show no similarities to other Public-Public Partnerships or Joint undertakings implementing EU Horizon funding.
- Stakeholder representation:
  - The Cybersecurity Community is represented in the Industrial and Scientific Advisory Board, which issues non-binding recommendations and decisions and has got observatory role in the decision-making process of the Competence Centre, without voting rights.
  - The role of the Cybersecurity Community in the Competence Centre is described by the Proposal very broadly and vaguely.
- The Network of National Coordination Centres:
  - It is unclear which (type of) national entities will be appointed.
  - The (contractual) relationship to the Competence Centre is not yet defined.
  - The governance of the network itself, i.e. the cooperation between the National Coordination Centres, is left to the Member States.
- The Cybersecurity Competence Community:
  - Selection procedure: can stakeholders apply to become a member and can groups of stakeholders, such as centres of excellence, become members?
  - The Proposal does not stipulate how the Community should cooperate with the Network of National Coordination Centres and the Competence Centre.
  - There is room for determining the governance of the Community and setting up sub-structures, yet, within the framework of cooperation and substantive law.

In summary, the EU Regulation Proposal 2018/0328 presents a complete governance structure for the European Network of Cybersecurity Coordination Centres and the Cybersecurity Community. However, given the legal requirements analysis in Chapter 4.3, the stakeholder requirements from Chapter 2, and insights from our analysis of existing governance structures of similar bodies in Chapter 3, we have identified several points for improving the EU Regulation Proposal 2018/0328. These points we include in our proposal for a bottom-up cybersecurity governance network in the next chapter.

5 Proposal for a Bottom-Up Cybersecurity Governance Network

On the basis of the afore developed insights, the vision of CyberSec4Europe, the open structure of the proposal and the vision for a NCCC as outlined by the EU Regulation Proposal 2018/0328, a complementary bottom-up approach is desirable to create an effective governance structure. This includes a more precise and enlarged integration of the stakeholders and civil society as well as strengthening of the EU as a harbour for human rights and a purveyor of democratic and freedom-oriented society.

Top-down as well as bottom-up approaches each have specific advantages and disadvantages. While a pure top-down approach in general serves well to establish command-and-control structures and allows for quick reactions and binding decision-making, such an approach is limited in time and requires specific knowledge resources. A pure bottom-up approach, on the other hand, lacks the ability of binding decision-making on relevant issues and is limited in establishing control mechanism. The power of bottom-up approaches rather results from their possibility to provide broad expertise and knowledge of industry, academia and stakeholders in specific areas by organising information gathering and distribution. It is, thus, an appropriate way of activating research and development capacities. By combining top-down and bottom-up approaches it is possible to balance advantages and disadvantages and, hence, to enable the synergetic potential of approaches in order to create a tailored governance design for an individual field of action, e.g. to ensure a strong performance of the NCCC.

Therefore, CyberSec4Europe proposes five major amendments:

1. Introduction of a sub-structure for the Competence Centre.
2. Introduction of Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs).
3. Introduction of Stakeholder Council.
4. Modification of the existing governance structure for the proposed NCCC under the EU Regulation Proposal 2018/0328.
5. Establishment of a strong and vibrant community.

5.1 Substructures for Competence Centre

Presently, the Competence Centre is designed to act solely through the Governing Board. This Governing Board shall decide all relevant matters of the Centre. No other decision-making organ is established; also, any type of substructure is missing. This, however, should be changed to accommodate quick decision-making for specific sub-tasks, e.g., for the MOOC case we use in Chapter 7 to evaluate first aspects of the proposed governance structure.

5.1.1 Connection to Prior Insights

The Regulation does not take into account the different levels on which decisions with regard to cybersecurity are being made. It can be assumed from the governance structure and the involved parties that it will be on the well-regulated level of the Competence Centre that the decision will be made concerning the questions of fundamental importance, such as the general orientation of the organization, or the accreditation of individual institutions as members of the Competence Community.[190] The structure of the Governing Board can only function if it does not deal with individual and small-framed

[190] Compare Article 4, paragraph 1 and Article 8, paragraph 4 and 5, 2018/0328 (COD).

content issues related to individual topics. It would not be possible to take up for considerations on individual concepts and actions on a level this high; their initiation and implementation cannot be accompanied by the tasks of the Competence Centre. Instead, the Governing Board should concentrate on the main guidelines and strategic decisions. This leaves room for additional substructures that could be laid down in the codes of conduct, or by means of establishing sub-committees on special issues. One good example for such special issues are MOOCs (which will be explained in more detail in Chapters 6 and 7). It cannot be imagined that a MOOC would be designed and enacted by the Governing Board of the Competence Centre. Rather, on this level one would expect decisions on the general desirability and potential start-up funding for MOOCs, with the exact enactment decided on a different level. Similarly, decisions like the quality criteria of MOOCs would be ill-placed within the Competence Centre. On cybersecurity issues on this level, the EU Regulation Proposal 2018/0328 contains no suggestions.

In the case of the MOOCs, the inaugural decision on cooperation between different institutions will be on a lower level than the Competence Community, since the partners who are not accredited could pursue the offer and distribution of MOOCs. Thus, the Governing Board and the Competence Centre would typically not be involved, as this is a bottom-up approach to cooperation.

For this level of action in the field of cybersecurity, the Regulation Proposal contains no regulative ideas. It remains on an abstract level with little guidance for the concise design on cybersecurity-related research, education, development and competitiveness starting from among the partners cooperating on education. This leaves room and calls for a legal design, on the one hand, altering the structure of the NCCC to allow – together with the top-down approach of the present Regulation Proposal – a bottom-up approach as well as, on the other hand, for substructures of the Competence Centre itself.

It has to be noted that also from the point of membership it can be advisable to establish different decision-making processes, which will not always include all partners on all issues.

5.1.2 Proposal for Substructures of Competence Centres

One has to distinguish between two settings: one concerns day-to-day decisions and decisions where superior experience and knowledge is demanded; the other concerns situations where a bottom-up approach from the Community, the National Network or the Stakeholder Environment needs inclusion in the regulation. Stakeholder Environment includes all of the above-mentioned stakeholders accredited to the Community, but also the numerous further stakeholders that didn't undergo this procedure or didn't fulfil all of the criteria. This includes individuals, NGOs and other forces of the civil society; additionally, it encompasses political parties, non-institutionalized groups, general research institutions without a distinct cybersecurity focus, and also small and medium-size enterprises. Finally, it also includes public entities such as agencies or other institutions on state level. One might think here, in particular, of the supervisory authorities in data protection and regulatory agencies in telecommunications. They all would be part of a larger environment of cybersecurity with potentially high interest, but lacking resources or the power to contribute to the Community for numerous reasons.

One way to achieve a detachment of the members and thus the Governing Board from the day-to-day decisions could be the establishment of an executive organ below the Governing Board proposed by the Regulation, e.g. an executive board or a single executive person. This executive organ would have the power to bindingly decide issues of lesser importance and value to the cooperation, while the core decisions would remain with the members. Routine decisions could then be delegated.

Similarly, a bottom-up approach of topics into the Governing Board can be achieved by creating relevant substructures. Looking at the chances of bottom-up structures, a general openness for small and medium-size institutions and corporations would be desirable. This includes the possibility of agreements between individual parties as long as these endeavours are shared within the community. Aside from the institution of CHECKs and a Stakeholder Council, which will be introduced in the following two subchapters, relevant sub-committees staffed with institutions and individuals with special expertise in specific areas would be a suitable solution.

5.2 Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs)

One of the core characteristics of the Regulation is its top-down approach. This approach is established by several tools, mainly by creating the Competence Centre at the core of the NCCC and furnishing it with the most tasks, as well as assigning to it an almost exclusive right to make important decisions. The establishment of the other institutions, such as the Network of National Centres and the Community, but also the Advisory Board, serves to foster the decisions of the Competence Centre rather than diversify the decision-making process. In other words, the other institutions are designed to assist the Centre; the Centre is created as the decisive part within the NCCC. This is also reflected by the weight the Regulation puts on the description of the functioning of the Competence Centre in comparison to the other institutions – beyond the restrictions due to competence.

In a field of many players in diverse functions that possess a variety of interests, a top-down approach is suitable in order to quickly react to present challenges and to organize a new network such as the NCCC in a fast and efficient manner. It also serves well to distribute funds and to quickly establish procedures for control.

However, such an approach neglects the power of a bottom-up-approach, in particular in a developing market with a variety of approaches that could be considered. With ENISA, the EU has already created a top-down-institution in the field of cybersecurity; the difficulties of ENISA lie in reaching out to the stakeholders and in reacting to stakeholders' demands. NCCC should not follow this line exclusively, in particular because the field of research and education is much more volatile and much less directly governable than other fields which ENISA typically regulates. Also, the NCCC has no command-and-control instruments to directly influence cybersecurity research and education and thus has to rely much more on the interaction and collaboration with the stakeholders.

Thus, the EU's power of funding and furthering cybersecurity should be established by applying both a top-down- and a bottom-up-approach together. This combines the effects of both approaches to achieve the best results. After all, the special power of the NCCC lies in accumulation, distribution and organization of information about problems and solutions and by fostering straightforward and meaningful research after the identification of core issues.

Another problem which the EU Regulation Proposal 2018/0328 does not address is the interconnection within the NCCC. With the proposed structure, there is no direct interaction between the members of the Community other than via the Network of National Centres. It would be desirable, however, to understand a European cybersecurity strategy not as a national, member-state oriented strategy, but to think in larger terms of cross-border cooperation and communication.

5.2.1 Proposal for Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs)

Therefore, CyberSec4Europe increases the exchange of information by installing additional regional and cross-border networks on the Community level in order to further a bottom-up-approach and thus create a stringent design of a future cybersecurity strategy within the EU. As one element to achieve this goal, CyberSec4Europe proposes the introduction of CHECKs into the regulation. Thus, the network structure is significantly strengthened and advanced into a true network structure that ensures efficient flow of information without just few strong central points.

Such Hubs would be desirable in order to accumulate special expertise and to create sub-networks which can bundle information and interests, as well as to assist in allocating funding by potentially raising additional funding from other sources. The goal of the CHECKs will be to link stakeholders from all areas of cybersecurity and integrate them into the Community and the NCCC, as well as to bring money closer to the researchers/projects and thus to implement the complementing bottom-up approach. Apart from that, the hubs shall promote the scientific exchange, present research and produce and facilitate novel and practically meaningful research. Considering the limitations of primary EU law, it might be necessary to design CHECKs in particular ways in order to be able to legally include their framework of governance in the regulation.

The CHECKs thus function as a source of continuous information which can be passed on to the Network of National Centres and the Competence Centre in order to generate new input and new directions for renewed strategies in a demand-driven outset. This allows, on the one hand, for low-level cooperations, ideas and strategies in different areas of cybersecurity which may, at the same time, be quickly integrated into the NCCC if these produce important findings or advantageous solutions. The CHECKs are as such the low-level, easy-to-access points of accumulation of regional interests and information, and they can serve as accelerator to demands and problem identification as well as solution mechanisms.

In addition to this, CHECKs may also play an important role in accreditation. The regulation provides for an accreditation to the Community as an important tool to distinguish the overall Stakeholder Environment from the more advanced Community. By accreditation, the Community is designed to be of superior expertise in comparison to the many players in the Stakeholder Environment. The accreditation within the EU Regulation Proposal 2018/0328 is restricted to the accreditation of partners within the Community, but does not go further than that. In particular, there is no accreditation for special areas of competence. This could be performed by the CHECKs, which would then play an additional important part within the Community.

These CHECKs serve as network within the NCCC and connect both the Network of National Centres and the Stakeholder Environment as well as the Community. They may also take on the role of a National Centre, e.g. in smaller member states. They also stress the fact that within the EU there exist not only vast differences in orientation in cybersecurity between the member states (which is reflected in the National Centres), but also within several regions and industries. CHECKs react to these differences and turn the variety of cybersecurity interests within the EU into a driving force towards both highly specified and broad in scope cybersecurity. This also reflects the freedom of markets and entrepreneurs as they will be able to address the issues of highest importance to their particular sub-market.

The pilots will function as test for the CHECKs; CyberSec4Europe has facilitated the creation of the "Toulouse Hub of Expertise". This Hub connects itself with an existing private-public initiative in which individual cybersecurity problems are identified. A governing board, comprised of the representatives of the few partners, decides in a unanimous voting rule which problems to pursue further in a solution-oriented research approach. Other members who are not partners may decide to join in the further research.

This model case, however, is constructed in its first step with a limited number of partners and members which is not the typical situation of a CHECK, which connects numerous regional partners of the Stakeholder Environment. However, the to be tested Toulouse Hub of Expertise demonstrates that CHECKs also give the opportunity to fund cybersecurity research and strategies with additional input from interested parties within the CHECKs. They build on prior interaction and enlarge then on further groups of interest.

On the other hand, practitioners will also have an interest in joining and participating in the network effects of CHECKs because of short-range, problem-oriented research on a larger scale than would be accessible in smaller corporations typically accessible to them. Also, industry-wide standards are easier developed if more partners of an industry describe problems and develop solutions together. Thus, CHECKs can also function in bringing together members of the Community and the Stakeholder Environment beyond the direct influence and funding of the Centre.

Finally, it would be profitable for the NCCC to include more direct accessibility of practitioners as the CHECKs might offer interested parties the chance to test academic solutions and strategies with shared risk among all of the parties.

Thus, CHECKs perform a number of functions that set up an efficient network: they connect with the Competence Centre and the Network of National Centres, at the same time interacting with the Community and the Stakeholder environment. Communication on research and exchange of information is thus not designed as a one-way road restricted to singled out problems, but as an interactive continuous process offering a number of alternatives on how to identify, analyse and prioritize problems and find solutions for them.

5.2.2 Further Design

The next deliverable in M24 will present the more elaborated governance design. Such design will describe how CHECKs are selected; as for now, the CHECKs can already be identified within the pilots, such as the Hub in Toulouse. It is likely that centrally involved actors of the pilots, such as the University of Frankfurt that acts as main coordinator, may play an important role as they create a reputation for coordination already in the course of the pilot phase. However, this does not exclude the CHECKs to be a cooperation themselves, e.g. between Universities/Research Institutions and other stakeholders. The Toulouse CHECK is an example of this, as the University and an existing platform, OcSSImore, are jointly testing the structure of a Hub.

Part of this elaboration will also be whether or not CHECKs within a member state should be differentiated according to industries or problems or simply establishment or self-attribution, which still needs to be decided until the M24 deliverable. Also, the contribution to cross-border network should be more specified.

Within the course of the project work, it should also be discussed how to link the CHECKs more to the Network of National Centres, e.g. by installing them as their operational hands, particularly in accreditation of the Community from the Stakeholder Environment as well as in the distribution and public procurement of the funds of the Competence Centre on the national level.

The community organized in CHECKs should not only consist of cybersecurity professionals with a technical background, but also embrace the full interdisciplinary possibilities of the community and the bottom-up approach. The work and projects organized and conducted in the community hubs should, therefore, also include the requirements and research results of other disciplines, e.g. usability research, psychology, sociologist, law and economics. By pooling expertise, it will be possible to execute interdisciplinary research and projects, which not only consider technical necessities but allow a comprehensive approach.

Participants would learn about the requirements and progresses in other areas and could, by applying this knowledge, improve products. By implementing this approach, the CHECKs could constitute a contact point for the participants where they are able to get answers to questions concerning matters outside of their subject area, e.g., technicians learning about legal requirements.

This way, it is possible to create successful cybersecurity tools in Europe on the foundation of a European understanding of cybersecurity and European core values. The products created do not only fulfil the exact needs of the European Market but also promote European values and a European security culture, which is exported into the world with the product itself.

Finally, finances will play an important role. It should be considered to allow – within public procurement rules – the CHECKs to fulfil smaller projects on cybersecurity research by themselves in order to speed up research and in order to react to particular cybersecurity needs within regions, industries or other special areas.

5.3 Introduction of a Stakeholder Council

Presently, the Community is involved in the decision-making of the Governing Board within the Competence Centre in a limited way. The main tool the EU Regulation Proposal 2018/0328 offers for this task is an Advisory Board. The members of this Advisory Board are determined by the Governing Board itself, but not by the Community. This pre-selection mechanism avoids a bottom-up approach insofar as not the Community decides which players may represent its interests in the best way but the Centre itself. Also, it does not allow the Community to set their own focus and potentially thus complement the focus of the Competence Centre.

One could argue that this procedure is in accordance with the top-down approach the EU Regulation Proposal 2018/0328 follows. However, this would counteract the intention of the regulation to create a demanding and competent market for cybersecurity and to establish European cybersecurity players as competent and competitive in the worldwide situation of ubiquitous IT and continuous volatility to cybersecurity threats. The achievement of such a goal desires – which is the intention of creating the NCCC – a strong network between all players in which information flows freely and in which strategic decisions are made according to the strengths and weaknesses of the existing cybersecurity landscape.

Moreover, cybersecurity also demands a strong inclusion of civil society in order to represent the special human rights approach of the EU in comparison to many other players worldwide and in order to understand the special situations of individual user cybersecurity and include them in the cybersecurity strategy. After all, a net is only as resilient and strong against attacks as its weakest part, and human beings have often been identified as one of the major threats to cybersecurity.

Therefore, CyberSec4Europe strengthens in its proposal the establishment of bottom-up-institutions within the NCCC. It does so by a variety of instruments, among them the establishment of CHECKs (Community Hubs of Expertise in Cybersecurity Knowledge), a more focused approach on the Stakeholder Environment and the introduction of Substructures in the Competence Centre. CyberSec4Europe hereby introduces one further instrument, the Stakeholder Council. It shall complement the Advisory Board; it is also well imaginable to exchange the structure of the Advisory Board with the Stakeholder Council.

The Stakeholder Council shall represent important players of the Stakeholder Environment and thus represent further stakeholders beyond the Cybersecurity Community, and without prior accreditation. It shall consist of 48 persons or institutions from the EU. They are nominated in the following proportion: one-third by the Community, one-third by the CHECKs, and one-third by a free selection process within the Stakeholder Environment. Sub-committees according to the sub-committees of the Governing Board of the Competence Centre shall be established.

In order to assure that all relevant groups of interest in the Community and the Stakeholder Environment are represented, the Stakeholder Council will also assign a certain number of the seats to particular groups of interest. It is important to note that civil society and human rights/data protection organizations shall be represented in a significant number, in all groups of representatives from the Community, the CHECKs and the Stakeholder Environment. Also, for reasons of fair representation, each group shall administer at least half of its representatives on a randomized rotation so that no member remains in the Stakeholder Council for longer than two years, even if she was now a candidate for another institution within the NCCC. Re-election after a pause shall be possible. Members of the Stakeholder Council will receive sufficient compensation for their work, allowing them to have a non-permanent replacement in their position.

The Stakeholder Council will advise the Competence Centre on its future strategy in regard to all topics which the Competence Centre is concerned with. This is done by regular meetings with the Centre and also with all of its sub-committees, at least three times a year. The Stakeholder Council will meet shortly before the meetings with the Competence Centre or the sub-committees.

The Stakeholder Council will give recommendations to the Centre with a simple majority. If recommendations are passed with a two-thirds majority of all members of the Stakeholder Council, the recommendation shall have to be decided upon by the Governing Board of the Competence Centre. The Competence Centre shall follow the recommendation of the Stakeholder Council. If the Governing Board of the Competence Centre refuses to take up the recommendation of the Stakeholder Council in full or partly, the Governing Board shall be required to give sufficient justification why it decided against following the recommendation of the Stakeholder Council.

5.4 Modification of EU Regulation Proposal 2018/0328(COD)

The idea of the NCCC regulation to create a common market for ideas in the field of cybersecurity and to advance EU cybersecurity standards and technology by establishing a closely-knitted network seems not to be optimally represented in the present design, as it has been mentioned already. We maintain that it excludes important potential input, concentrates on a top-down approach rather than including venues for a bottom-up involvement, its network structure is incomplete, and its decision mode gives the EU interests represented by the Commission a wide advantage over the member states by establishing a veto right.

Particularly in a network governance, it should be ascertained that there is a fair participation of public stakeholders, but also of private stakeholders such as industry and academic representatives. It is typical for a network governance model to be able to react to changes in membership quickly; this inherent flexibility should be integrated into the NCCC to a greater extent. Also, majority rules should only be strengthened in special cases in order to prevent one party from becoming the dominant player.

5.4.1 Members, Composition of the Governing Board, and Decision Processes

As a central part of the cooperation, the composition of the Competence Centre and its decision-making plenum deserves special attention. It addresses one of the most important elements of any governance structure, and namely, who is participating in the governance in the first place, and thus gains greatest importance in determining the future decisions, as well as the overall future focus and direction of the NCCC.

A state entity or an entity entrusted with public duties and/or public service, as well as an entity involving state participation, - under the EU law, all of them are bound to democratic principles and rule of law. This requires a decision-making plenum of representation. It is the solid base of a democratically determined process of opinion-forming. Similarly, to a democratically governed state, the plenum of an entity with state involvement – such as the NCCC – plays a key role in securing the democratic legitimacy of the institution and its decisions.

The Competence Centre's membership is determined by EU institutions, namely the member states and the EU Commission; the proposed Governing Board structure defines the influence of each institution further. As far as the decision-making process itself (beyond voting rules), the EU Regulation Proposal 2018/0328 does not regulate much. It leaves room for a more precise definition for the Competence Centre's Governing Board to determine.

5.4.2 Connection to Prior Insights

It is important for the goals of the NCCC to integrate as many interests as possible, and thus to integrate a certain degree of plurality within the process of decision-making. This assures that in a combined top-down and bottom-up approach a multitude of needs, opinions, analytics, research designs and questions, as well as toolboxes and solutions, are integrated. Thus, membership can and should be used as an integral part of inclusion and representation, and this is also true for the decision-making organ – in this case, the Governing Board.

However, there are also other designs possible to include maximal amount and diversity of information, e.g. by including advisory boards and certain procedural safeguards within the decision-making process

through the involvement of experts and stakeholders. In this manner, representation and plurality can be exercised in different ways, ensuring different impacts and outcomes of each group's ideas, information and importance. It has to be stated that equal representation of all stakeholders is not required; a focus on membership of only member states and EU institutions for the new Competence Centre is feasible, although the integration of broad interests should not be neglected. This issue of how to integrate and represent plurality and diversity will be further addressed in the creation of the Stakeholder Council and is also part of the CHECKs.

According to the EU Regulation Proposal 2018/0328, the Governing Board is construed as the central body of the Competence Centre. The proposed structure of the Governing Board follows in its general structure the structure of the EU, i.e. Commission and Parliament as EU institutions and the member states are present. Other institutions of the EU are not represented, ENISA shall be included with an advisory position.[191]

The composition of the Governing Board seems to give particular weight to the member states, as 28 out of 33 members of the Governing Board are representatives of the member states[192]. Only five seats are reserved for EU institutions against four seats for representatives of the European Commission and one seat for a representative of the European Parliament.[193] Also, one can conclude that among the EU institutions, the Commission is granted an outstanding weight as about 1/8 of the seats are assigned to it. This has already been criticized by the EP (European Parliament).

However, a closer look reveals that the influence of the member states is considerably diminished by the distribution of the voting rights in the original EU Regulation Proposal 2018/0328. Despite the involvement of the Member States, their strong representation (and financial contribution) is not reflected in the voting rules within the Governing Board. Contrary to a typical "one-member-one-vote"-rule, 50% of the votes are assigned to the EU Commission. Thus, four members out of 33 control half of the votes. This amount is in reality even higher, as the EU Parliament representative is not given the right to vote; her inclusion into the Governing Board is limited to advisory or observing matters in the original Regulation Proposal. In effect, this decision-making process gives the Commission a de facto veto right, as the Commission can never split its votes and no decision can take place without active confirmation of the Commission. This has also been pointed out by the Parliament, which introduced itself a complicated, and task-oriented voting mechanism which, however, still reflects mostly Commission power.

Additionally, no stakeholders, no private entities, no intermediaries and no other European institutions are considered to be members of this committee, even if the Regulation Proposal concedes the possibility for advisory opinions by the Advisory Board on an institutional level, as is the case for ENISA and the Parliament.

Opportunities for the private sector and civil society to participate directly in any decision-making process of the Governing Board are thus non-existent. The Competence Community or the Stakeholder Environment have no voice in the Governing Board and hence no direct access to the decision-making

[191] According to EP or Council
[192] Article 12, paragraph 1, 2018/0328 (COD).
[193] Amendment 122 to Article 12, paragraph 1, 2018/0328 (COD).

process. This illustrates once more the top-down approach of the Regulation, rather than a bottom-up-approach.

The Competence Community can only influence decisions of the Centre through indirect means – for instance, through the Network of National Centres and – foremost – by the Industrial and Scientific Advisory Board. From among the representatives of the Competence Community, the Governing Board appoints 16 members to as this Industrial and Scientific Advisory Board.[194] The members of this Advisory Board have the task of supporting the Competence Centre with advice and hence have at least an advisory position. However, they do not actively take part in the Governing Board meetings and decisions. Their position is thus reduced in comparison to other merely advisory opinions, such as the EU Parliament which occupies at least one – observing – position in the Governing Board. More importantly, these members of the Advisory Board are also selected by the Competence Centre itself and thus do not reflect the choices of the Community or the overall Stakeholder Environment.

The EU Regulation Proposal 2018/0328 also lacks any type of further regulatory input on the decision-making process as such, how to gather information, whether a decision has to be reasoned and in what detail, how to prevent and avoid conflicts of interest, how decisions are being prepared etc. The EU Regulation Proposal 2018/0328 only grants the Governing Board the right to execute its own rules of procedure for the decision-making.[195] This leaves a wide area of discretion to the Governing Board without giving clear outlines on how it shall govern itself and the NCCC. Such a lack of procedural binding typically leads to wide discretionary decisions with little possibility of control. In an administrative setting with many public partners involved that are bound by the rule of law, such a lack of procedural binding is undesirable.

5.4.3 Implications for Membership of the NCCC

Membership according to financial contributions and to the general structure of the EU are one way of construing membership of the NCCC. This reflects the general outset of the NCCC to further research in the area of cybersecurity and thus to play an important role in allocating funds and determining research agendas, notably the cybersecurity parts of the Horizon Europe and Digital Europe programs, in the framework of the multiannual strategic plan and the strategic planning process of Horizon Europe. Furthermore, in the Council's opinion, the annual work plan should contain the allocation of funds from the Union budget to joint actions between the Union and the Member States, for which the conditions also have to be established by the Governing Board.[196]

Therefore, the membership should remain a reflection of the EU structure, with the Commission and the member states present. However, there should also be a more active integration of the EP by establishing its representatives in a role that is not only advisory, but entails full membership with voting rights for at least two members of the EP. This integrates, in compliance with the role of the EP, a stronger inclusion of the civil society.

Finally, the membership structure should be represented within the enactment of voting rights. This aspect of membership is developed further below.

[194] Article 18, paragraph 1, 2018/0328 (COD).
[195] Article 42, 2018/0328 (COD).

[196] Proposal and remark 246-247, Interinstitutional File 2018/0328 (COD)

As a point of change, CyberSec4Europe also proposes to give the Governing Board clear normative standards on the decision-making process. This should reflect the administrative procedure. Unfortunately, the EU does not yet have a common standard for administrative procedural settings. But there exist a number of proposals on how to establish a common EU administrative law, most prominently probably the ReNEUAL proposal[197]. They can be used as a model for core elements which should be regulated.

Considering the visions of CyberSec4Europe, there should be extensive legal hearing of a variety of stakeholders on decisions of the Governing Board. Furthermore, clauses should be included on potential conflict of interests of the representatives in the Governing Board, on the qualifications of members of the Board and their proxies, an obligation to justify the decisions and how to retract decisions. There should also be included norms on the information gathering process, together with potential obligations to appear before the Board as an expert witness or a stakeholder. This links to further proposals on the introduction of a Stakeholder Council and its integration into the decision process.

Another proposal of the change of decision-making process will be described in more details in Chapter 5.5 with regard to inclusion of a Stakeholder Council and also the integration of sub-committees to the Competence Centre.

5.4.4 Voting

Voting rights, typically, constitute an important means of integrating different membership interests and attributing power. While membership can only be granted to a natural or legal person or entity, voting rights can provide means to differentiate to a greater extent between the different input of diverse members of an institution. So, while all members are construed as equal, the voting rights may be distributed differently.

The EU Regulation Proposal 2018/0328 makes use of this possibility and does not establish the above-mentioned easy voting systems: a majority rule where every member has the exact same weight, i.e. where all of the member states and the Commission each are assigned one vote. Instead, the Commission has proposed a rather complicated structure. Presently, the voting mechanism is still under discussion in several aspects, such as potential differentiation depending on the content of the decision, as the Parliament has proposed a task-dependent voting mechanism. It has also been subject to critique that the proposed voting rights give the Commission a veto right and a dominant position beyond membership participation.

The voting system[198] proposed by the Commission itself increases its own importance and power drastically in comparison to its membership status. In the system suggested by the Commission, only a 75% majority of all votes will lead to a decision. In addition to this, there must also be a majority of 75% of the financial contributions. As the EU Commission has more access to grant EU funding than individual member states, this increases the Commission's dominant position additionally. A funding-oriented approach would centralize the Commission's power within the NCCC; additionally, it has been discussed that the member states' contributions should be diminished, since they are already contributing into the funds that the Commission may invest in the NCCC.

[197] P. Craig, H. Hofmann, J.-P. Schneider, J. Ziller (Eds.), *RENEUAL Model Rules on Administrative Law*, 2017.
[198] Cf. Art. 15 COM (2018) 630 final.

Usually, absolute majorities, veto rights, extra high thresholds etc. are established as an exception to a general majority rule with equal voting shares. They are typically used in the context of particularly important decisions, for example, in cases these decisions would change the general outline or content of an institution and its core governance structures: who may join, who contributes in general, how decisions are made etc. In this manner it is typically safeguarded that the core understanding of an institution is shared by the vast majority, in order to establish acceptance for the possible changes. The original Regulation Proposal, however, creates a one-supermajority-for-all decision-making rule, which is extraordinary. It is particularly noteworthy, since it hands the supermajority to the Commission which already has – because of the funding – a high influence in the actual practice of the NCCC when it comes to steering research and providing incentives in cybersecurity.

It is true that the voting procedure is used to balance the different groups to be represented. But the present Regulation Proposal leaves behind additional possibilities to include further interests and thus balance the voting rights scheme. Therefore, the Stakeholder Environment should be introduced more actively. This is done by the Stakeholder Council.

5.4.5 Implications for Voting in the NCCC

The voting rights as proposed by the Commission reflect neither the division of power the way it is typically distributed within the EU, nor the contributions to the NCCC's programs or the variety of content of the decisions within NCCC. Thus, the NCCC should include a voting mechanism which reflects the funding structure in an adequate way. This need not be an exact reflection of the financial contributions, but it should give some power to those who contribute most.

In addition, if the Parliament is integrated as a full member, it also has to be given full voting rights. This reflects not funding, but the importance of civil society to be integrated by means of a democratically elected EU institution.

Finally, the voting mechanism as such should be changed. Similar to the proposal of the Parliament, difference in content should be reflected in the adjustments of voting mechanism. In general, a majority of more than 50% should be sufficient. If it is found to be of particular importance to create a more consent-oriented voting mechanism, this could be strengthened to a two-thirds majority. Precautions should be taken, however, to ensure that no single institution is granted a veto right.

For the core governance questions – such as a change of voting mechanism, a change of share in contributions, or potential new members with their own voting rights, - generally a two-thirds majority should be laid down. This should also apply for funding, which either exceeds the threshold of funding of individual institutions or projects beyond a certain amount, or which exceeds the overall funding by a certain amount.

5.5 Cybersecurity Community Establishment

The EU Regulation Proposal 2018/0328 provides little information about the estimated governance structure for the Competence Community. Articles 8 and 9 provide information on the entities which can participate to the Community, how they are accredited and what contribution is expected from these members. They contain, however, no information about the inner structure of the Community itself, e.g. how the Community works together, shares its knowledge and comes to mutual and mandatory decisions.

So far, the Regulation proposes an accreditation process which includes the Competence Centre as well as the Network of National Coordination Centres. However, as the Community represents the Stakeholder Environment and requires proof of superior expertise, this accreditation process should be part of the structures without Competence Centre involvement. Such a procedure would assure that expertise and willingness to actively participate in the new strategy of EU cybersecurity is derived from superior expertise itself.

5.5.1 Proposal

Therefore, CyberSec4Europe designates the CHECKs in Cooperation with the National Coordination Centres – if they are different entities – to fully accredit the members of the Community. This shall be done by a procedure which requires interested parties from the Stakeholder Environment to describe their competence and their willingness to participate. The CHECKs then test this according to the standards of the regulation. In a mutual decision of the CHECK and – if existent – the National Coordination Centre by majority vote, accreditation is granted on a non-temporary basis. Regularly, the National Coordination Centres name the latest additions to the Competence Centre. Sufficient funds are provided that the CHECKs and the National Centres may fulfil this task.

5.5.2 Building and Establishing a Vibrant European Competence Community

The NCCC is constructed presently as an insider network. However, in order to influence the worldwide cybersecurity movement and to enhance worldwide cybersecurity strategies with the EU standpoint, it is necessary to create also activities for outreaching. Typical instruments such as newsletters, press releases, presence on social media etc. may well be considered but would not assist the solution-oriented approach of the NCCC.

In order to establish EU cybersecurity as one of the strongholds worldwide on the edge of new topics and research strategies, as well as research agenda and results, the NCCC shall, under the organization and funding of the Centre and at different places within the EU, organize a yearly, three-day-long worldwide cybersecurity conference. This conference should be established as one of the leading scientific cybersecurity conferences worldwide. In order to achieve this, the Centre shall form a sub-committee on this topic. This sub-committee will determine agenda, publication and procedure for presentation of scientific results and set up a structure for participation.

Note that, based on our stakeholder input and analysis of current venues, it is quite unlikely that such a premier event can be started successfully from scratch. Similar efforts, like, for example, the IEEE EuroS&P or ACM AsiaCCS, have not been able to gain sufficient traction to fully compete with the traditional “Big4” top conferences (ISOC NDSS, IEEE S&P, USENIX Security, ACM CCS). Hence, in order to make this proposal work, we offer a different approach.

We suggest that, given the current scaling issues of the traditional Big4, the sub-committee should seek to establish a collaboration with these venues. Authors of the, e.g., top 15% of accepted papers in each of the Big4 could be structurally invited to also publish an extended version of their papers in the to-be-established EU conference. As papers, even accepted and published, usually leave room for improvements and additional material, often based on input received during the conference, authors could be required to add at least 20% of new material to the publication to be included in the proceedings of the conference. The proceedings of the conference could then serve as the ‘archival’ version of

publications, as it is also common in other fields, where authors usually first produce a conference publication, which they then refine to an 'archival' journal publication.

Furthermore, to attract scientists from all over the world, even though it is a relatively new venue, and incentivize successful authors from the Big4 to participate in the event, it should be an invite-only event, exclusively open to the authors of accepted papers, and selected additional participants from the identified stakeholder groups in Chapter 2.1. This model is also suggested as a viable platform by our stakeholder input from Chapter 2.5. Furthermore, the different entities within the NCCC (the Centre, the National Network, the Hub of Excellence, the Community, the Stakeholder Council, the Advisory Board) shall each have slots in which to present topics and participants of their choice for greater variety.

At least one day shall be reserved for social sessions in which EU practitioners present cybersecurity solutions in the setting of the scientific conference, e.g. with Posters, Stands, Discussion Rounds, Panels and Displays in order to give room to EU business solutions.

Also, regular other activities need to be implemented to create a vibrant Community and strong interaction between the different groups. The means of the Hubs to enable short-term research and fast identification of imminent problems may enable this; the Hubs' projects, thus, need to be strongly reconnected to activities within the Community.

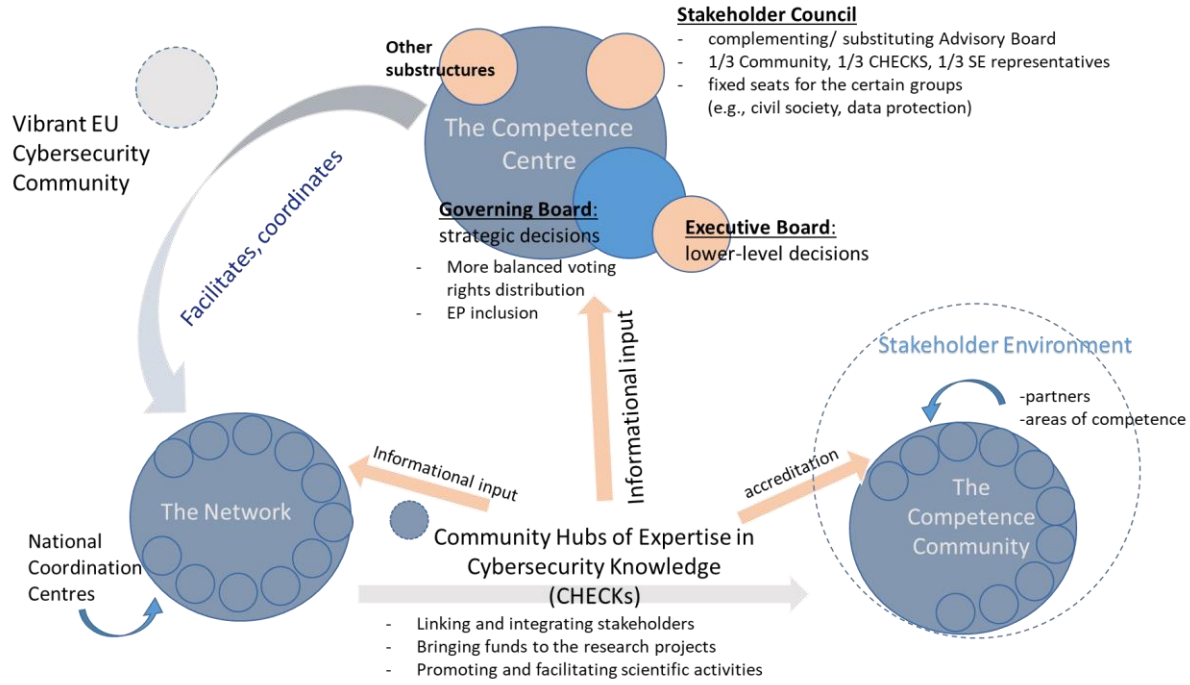

Figure 11: Overview of the adjusted governance structure.

5.6 Conclusion

In this section, we propose five major amendments to the NCCC governance in relation to EU Regulation Proposal 2018/0328(COD). Specifically, we suggest the introduction of Cybersecurity CHECKs, sub-structure for the Competence Centre, a Stakeholder Council, a modification of the existing governance structure for the proposed NCCC under the Regulation Proposal, and the

establishment of a strong community. An overview of our changes in the context of the regulation proposed structure can be found in Figure 11.

In the next chapter, we will validate a first aspect of our envisioned governance structure, on a small case study, i.e., the accreditation of MOOCs. This specifically pertains to the idea of introducing sub-structures for specific action items as outlined in Chapter 5.1.

Note that the Regulation Proposal contains no information about the specific governance structure of the Network or of the several Coordination Centres. This is in accordance with EU law, as the EU does not have competence over the national bodies. Thus, the member states will have to put forward their own governance structures how to construe and enact the network structures. It is clear, however, that the regulation expects the national member states to establish their own contact points for the network and to assign them their own tasks and responsibilities. One possibility might be to introduce the CHECKs as national centres.

The above-outlined proposals bear in mind that the supranational structure of the EU and the limitation of competences, as well as the principle of subsidiarity, require a deeper legal analysis of the individual proposals in order to avoid transgressing legal borders. As is the case with substantive law in the field of cooperation which may bind the parties beyond their cooperation, also EU law may require to adhere to member state law. Also, special requirements such as public procurement or tax law may have to be adhered to.

The proposal, however, takes this in general into account from the legal cooperation standpoint. It proposes tasks and a governance structure for each of the involved institutions which are in accordance with EU law.

This page has been intentionally left blank.

6 MOOC Overview and Governance Pilot

In this chapter, we outline the concept of MOOCs, and how they tie into our governance proposal from Chapter 5. The contents of this chapter were already part of an internal Deliverable in M 6. In this deliverable we describe a governance pilot for the quality assurance process and branding of Massive open online courses (MOOCs) to be developed within CyberSec4Europe. In WP6, quality criteria for MOOCs have been developed. For completeness, we also summarize these criteria in 'Annex D: Stakeholder Requirements Overview'.

In this chapter, we then propose a governance structure for decision-making on quality assurance in Section 6.2 based on the criteria. This is the design for the pilot, which will be evaluated in Chapter 7. In addition to the quality assurance governance pilot, we also develop complementary governance mechanisms for the joint co-production of MOOCs in Section 6.2. This is not part of quality assurance, but a relevant aspect of MOOC provisioning where we also explore and evaluate governance mechanisms. This additional mechanism will briefly be considered in Chapter 7 as well. The deliverable on a "Case Pilot for WP2 Governance" had the objective to provide an initial review of existing offerings and governance structures of European cybersecurity MOOCs in the form of academic, continuous learning and Cyber Range courses. Moreover, the goal was to present a quality assurance process based on quality assurance criteria to be proposed.

The review of MOOC offerings and of their governance structures showed that cybersecurity MOOCs in Europe are mainly offered by academic institutions, but academic MOOCs in cybersecurity awarding credit points for participants are rare and Cyber Range MOOCs are basically non-existent in Europe. Moreover, cybersecurity topic platforms or channels do not exist yet either in wide areas – existent cybersecurity MOOCs are rather offered on dominant learning platforms, such as Coursera, EdX, FutureLearn, Udacity, Udemy, or Canvas. Governance structure aspects identified that need to be addressed by quality criteria include a well-balanced and unbiased course content as well as fairness and transparency of admission for continuous education MOOCs that are offered by commercial organizations. In addition, there is a need for ethical rules for course participants as well as policy rules for a restricted openness to the course content, student admission or course material for Cyber Range MOOCs. Moreover, today's most prominent MOOC platforms are hosted in the US or other international actors outside the EU, which requires attention for achieving compliance with the GDPR's rules allowing data transfers to third countries outside of Europe.

The M6 deliverable also reviewed existing MOOC Quality Assurance and Validation Criteria as related work, which are however not generic in nature, as no cybersecurity course-specific MOOC Quality Assurance Criteria frameworks have been proposed yet. The set of Quality Assurance Criteria that GUF proposed composes of criteria for the qualification of the proposing institution, qualifications of students, qualification of teachers, for course examination, credentialization and recognition, for course evaluation, meeting professional expectations, course structure and content criteria, requirements for platforms and channels, as well as criteria for cyber ranges. In addition, general certification and accreditation models for courses are discussed including the involvement of cybersecurity expert stakeholders, such as ENISA, governmental cybersecurity agencies or contingency as certifiers or accreditation bodies. Finally, this deliverable also concludes with a proposed prioritization of the quality assurance criteria for the pilot of governance structures for cybersecurity MOOCs in Europe to be

designed by Work Package 2. Quality assurance criteria for meeting professional expectations as well as course content and course structure criteria are considered to be of high relevance for the pilot. Moreover, cybersecurity specific quality assurance criteria should be given high priority, including quality criteria for cyber ranges, ethical hacking rules and policies for restricting the openness of courses or course material for Cyber Range courses.

6.1 Definition of Massive Open Online Courses (MOOCs)

Massive Open Online Courses are academically oriented courses on all subjects that are accessible to a very wide audience due to their online design. Often MOOCs are offered by universities both as a substitute and as an extension to traditional learning and teaching methods such as university lectures, but may also be provided by commercial providers. Over the last years MOOCs emerged as an alternative to formal education, as they enable life-long learning to a broad variety of students.

The design of MOOCs can vary – they can provide add-on training, they can substitute existing mandatory courses for a degree or offer post-degree course-work, they can be open to the public or only to a limited audience, they can be designed to be interactive or one-sided, etc. The definition of MOOC Channels as well as criteria for the measurement of their quality are elaborated under 'Annex D: Stakeholder Requirements Overview'.

6.2 Suggested Governance Structure for MOOC Quality Decision-Making

The cooperation between two and more institutions in the field of MOOCs for Cybersecurity can only be governed if the assessments and the – in many regards missing – legal framework above presented are understood and applied properly. This requires each cooperation to assess their individual legal requirements carefully and to design a fitting governance decision process.

6.2.1 Avoidance of MOOC-Specific Governance and Content Regulation

As shown above, the Commission's Regulation Proposal addresses basic requirements for the Network and the Competence Community. However, it does not contain rules on how the cooperation between the individual members of these institutions is legally structured. There are no EU legal requirements regulating this type of cooperation, and even private law with its rules for partnerships or private companies is not applicable due to the involvement of public-law partners. Also, many cooperations are informally designed and grow within time; information exchanges and networks are difficult the rephrase and reformulate in more formal terms. Especially with regard to the number of institutions involved in EU cybersecurity and the complexity of the objectives pursued, together with the many different levels of cooperation, a general legal framework cannot be identified.

Any type of MOOC governance proposal may not contradict the proposed EU regulation – notwithstanding that as a proposal this regulation still may undergo severe changes. This is the case because contradictory or parallel governance structures would complicate the exchange and information flow necessary in a European network of cybersecurity in order to create a strong European cybersecurity movement.

Rather, depending on the individual content of the cooperation in the shadow of the NCCC, the content-specific legal framework has to be attended to. This is even more so the case as the potentially applying content-specific legal framework usually does not explicitly address matters of governance, i.e. it does

not set up a binding governance process for the decision-making process on the channels. There may, nevertheless, be additional rules to adhere to, such as IT-security-regulation (i.e. if a MOOC were to be defined as "critical infrastructure" and as such would fall under strict scrutiny on the basis of IT-security laws), data protection or copyright law.

The cooperative framework may then follow depending on the individual circumstances of the cooperation. In the case of MOOCs, the content-specific law to be adhered to originates from the member states', the involved institutions' legal foundation and potentially also from any EU or other public international treaties. This may vary depending on the partners involved and the exact framing of the legal agreement between the partners.

6.2.2 Legal Agreement as Basis of Cooperation between Equal Partners

As hardly any legal framework governing the MOOC cooperation between European partners exists, cooperation for this purpose could possibly – and due to the individuality – would typically be achieved in the form of legal agreements that are considered binding on all participating cooperation partners. Only then can the cooperating partners rely on the durability and binding power of their cooperation which is the ground for investment and action. It is to be noted, however, that these agreements must address basic governance elements as there is no default legal option on which partners can fall back in the case of disagreement.

6.2.3 Partners of MOOC Cooperation

Taking the governance structure proposed in the EU Regulation Proposal 2018/0328 as a basis with three major actors – the EU Centres, the National Networks and the Community, it becomes clear that a MOOC governance decision-making process should take place on the level of the Community (of accredited members) and below (of non-accredited members). This is, where the relevant actors convene. Taking into account that a bottom-up-approach should not be discouraged, MOOCs on the level of non-accredited, out-of-community members should still be possible. It could prove, however, to be of a special competitive value if only accredited members were allowed to offer a branded MOOC (see below as "community excellence centre").

Only indirectly, some factors of the quality of the partners of a MOOC cooperation can be derived from the Regulation Proposal. One of these elements concerns the selection and accreditation of the participating partners. These partners of a MOOC would stem most probably from the field of the Competence Community, but not from the Centre itself, and only potentially from the National Network. This can be derived from the actors which the proposal puts forward as members of the three structures. MOOCs are typically offered by academic and educational institutions, maybe also by industry. These actors would be typically nationally organized. If they cooperated, they would do so on the level of the Competence Community, but less so on the level of the other two structures.

As stated above, the EU Regulation Proposal 2018/0328 does specify which institutions are eligible for inclusion in the Competence Community. There, the relevant stakeholders will represent the involved industry, society, research and academia as well as other stakeholders. A decision process for a MOOC would typically occur at the level of the Competence Community. What the proposed Regulation does provide for, however, is the necessity of accreditation: under Article 8 No. 4 and 5, the Competence Centre is declared to be in charge of accreditation of the members of the Competence Community. This leads to the situation that there will be members of the Competence Community once there are

accredited, but that there will also be members outside of the Competence Community which are not (yet) accredited. However, the proposed regulation makes no statements about the partners having the individual task assignments.

Transferring these interpretational results to MOOCs, this means that there could well be MOOC cooperation within the Community, but also outside of the Community and also a cooperation between accredited and non-accredited partners. There would not be legal framework by the proposed regulation neither on establishing the partners (nor the decision-making process between them). Under the proposed regulation, it is unclear which institutions can work together to develop a cross-border MOOC; it is equally unclear who decides on the qualification of potential participants. Thus, the requirements would be something the partners would have to draw up among themselves.

6.2.4 Decision-Making Process

The proposed Regulation goes one step further than any existing legal framework as it concentrates on the governance structures of a European-wide network. This network (NCCC), however, is described only in general terms on the upper level. A decision-making process for the lower levels and in particular for specific content such as MOOCs is not explicitly addressed. This is not surprising as the level of abstraction is very high, and it is unlikely that the proposed EU centre could potentially regulate all existing and developing MOOCs according to its decision-making process.

Thus, the decision-making process has to be derived from general rules beyond the particularities of a specific EU-wide cybersecurity network. Given that the Competence Community does not have a general decision-making body, decisions will be up to the partners themselves. This is also true for any MOOC cooperation between non-accredited partners.

Such a legal agreement should then contain rules about the voting rights and the necessary majorities for decisions. They are the institutions contributing to the development of the MOOC. Generally, this will be the case as equal partners in the decision-making process: All parties who contribute to the MOOC will be equal partners in the agreement and in the decision-making process.

However, equality only functions as long as all partners contribute similarly. If there is a leading partner or if there are partners who are generally less contributing, be it by design or by action, it is advisable to detach the decision-making process from the equality rule.

In general, the more partners are involved, the more important becomes a clear rule on the decision-making. Thus, a cooperation having started rather informally can in due course decide to change to a more formal cooperation.

In both cases – unequal contributions or numerous partners – it can be advisable to establish different decision-making processes which will not always include all partners. One of the ways to achieve a detachment of the partners from the day-to-day-decisions could be the establishment of an executive organ, e.g. an executive board or a single executive person. This executive organ would have the power to decide issues of lesser importance and value to the cooperation while the core decisions would remain with the partners.

6.2.5 Majority Rule

Having established such a governance process on the basis of general equality of all partners, the next step for a governance process in regard to decision-making will be the voting rule by which the decisions are taken. This reflects the general decision-making rule – if there is inequality between the cooperation partners, this will and should also show within the majority rule.

The Regulation, again, does not offer assistance, as its complicated voting system is applicable only to the governing board with its special connection to the EU division of power between the EU institutions and the members states. Thus, one will have to look at the general voting rights distribution. From theory as well as from a comparison of other governance structures, e.g. ENISA, federal states, CERN, ECSO, national-level structures or existing MOOC collaborations, one can conclude that there exist two separate types of voting rules: Unanimous decision making and majority rules. In a set of unanimous decision making, all partners share the exact same weight in decision-making. They are all assigned veto-rights as anyone not complying with the proposed decision can successfully hinder the decision. In a majority rule setting, decisions are taken on the majority of the vote – with a high degree of variation in regard to the exact majority possible (e.g. whether the majority of the present partners or the absolute majority needs to be reached). A mixture of both systems is a veto-right of each partner which could be then overcome by a supermajority (e.g. 75% or two-thirds majority).

A unanimous decision mode strengthens the importance of each partner. At the same time, it can often create little flexibility and little efficiency as such a system needs long preparations before votes can take place; the unanimous-rule becomes the more problematic the more partners are involved.

Thus, it is most sensitive to distinguish between types of decision: Decisions regarding the core of the cooperation need to be agreed upon by either a super-majority (75% or two-thirds majority) or all partners. These decisions could be the inclusion of new partners or the core of the cooperation – e.g. if a MOOC offered shall now be turned into a degree. All other decisions on the operative level should then only require a simple majority of all partners present.

This page has been intentionally left blank.

7 Evaluation of the MOOC Governance Structure

This chapter sets out to present the application of the governance structure for MOOC quality assurance. We first select a set of suitable MOOCs to be included in the evaluation in Section 7.1. In Section 7.2 we then conduct the pilot and implement the governance structure developed in Section 6.2 of this deliverable. Note that the work in these two sections was mainly carried out in T6.3 in WP6. Partially, they are already described in D6.1 from WP6[199]. Furthermore, other parts will be the subject matter of future deliverables of the concerned partners. We reflect on the lessons learned from the pilot in Section 7.3 and propose improvements to the governance structure. In that section, we also briefly reflect on the experience with the joint co-production governance mechanisms.

7.1 Selection of MOOCs for the Case Study

We first selected a set of MOOCs from the participating partners within CyberSec4Europe. Within this selection process, we ensured a wide variety of topics and involved partners. Our final selection can be found in Table 4.

Index	Name	Content	Reason for Inclusion	Eval. Partners
A.19	Information Security: Context and Introduction	An introductory course to the basics of information security.	Selected as a basic course for any curriculum on cybersecurity.	6
A.24	Managing Security in Google Cloud Platform	An applied course on permission and control systems available in the Google Cloud Platform.	Selected as a medium level application centred course.	5
A.26	Netzwerksicherheit (#nwsMOOC)	An introductory course for network security.	Selected as a basic, yet more advanced than A.19, course.	5
A.27	Privacy by Design	A design centred course on privacy, enabling participants to build inherently privacy preserving systems.	Selected to not only focus on security, but also include a privacy perspective.	6
A.56	Development of Secure Embedded Systems Specialization	An advanced course on systems, teaching methods of designing system specifications and embedded systems in a secure way.	Selected as an advanced technical course to also include courses with a significant technical depth.	5
CSBFS	Cybersecurity Base with F-Secure	An applied course focusing on product specific capabilities to increase cybersecurity.	Selected as a company provided course, to enrich the academic perspective.	6

Table 4: Overview of selected courses including their inclusion criteria.

[199] "D6.1: Case Pilot for WP2 Governance", Fischer-Hübner et al., Deliverable of CyberSecurity4Europe, Proposal No. 830929, Call H2020-SU-ICT-03-2018

In total, we selected six MOOCs, including both academic and professional courses. Furthermore, the course selection covers introductory topics as well as MOOCs with an extended technical depth.

7.2 Evaluation Process

Subsequently, we evaluated all MOOCs according to the criteria described in 'Annex D: Stakeholder Requirements Overview' following the governance structure outlined in Chapter 6.2. For this purpose, each selected MOOC has been evaluated by the board of experts formed by 5-6 partners. These partners have examined the MOOCs to diverse criteria that were relevant to them, both for academic education and continuous education (also known as professional learning). However, due to feasibility constraints in evaluating all MOOCs completely, we decided to base the pilot solely on the *publicly available information* provided by the MOOC's authors. This means that MOOCs may score low on items they actually *do* fulfil, simply because that information was not available in the execution of the pilot. We decided to follow this approach, as the objective of the pilot was not the evaluation of the MOOCs themselves, but of the process to evaluate them. Hence, we explicitly caution that the results presented on the individual MOOCs are *not* an objective assessment of the full course, but instead the results of a governance pilot restricted for feasibility reasons, and should be understood as such.

According to Chapter 6.2, we then subjected each MOOC to a decision-making panel from industry and academia. The number of involved partners can be seen in the last column of Table 4. In order to ensure consistency, the results of the evaluation of each MOOC have been consolidated by a single partner.

Finally, the selection and the evaluation have been analysed by the consortium partners from WP5. After the consolidation process was complete, the results for each MOOC have been presented in the table, showing the percentage of the positive evaluation of the correspondence to the criteria (answered "Yes" when asked about the correspondence of the criteria and presented the following options: "Yes", "Partly", "No") for both academic and professional learning, see Table 5.

MOOC	Yes, for Academic education	Yes, for continuous education
A.19	56 %	64 %
A.24	29 %	33 %
A.26	27 %	36 %
A.27	82 %	82 %
A.56	50 %	41 %
CSBFS	29 %	19 %

Table 5: Results of the consolidated evaluation.

According to our initial concept, the consolidation process was supposed to provide final result that would indicate whether any of the selected MOOCs can be considered for being branded as a CyberSec4Europe (CyberSec4Europe) MOOC. This initial assessment, however, should be subsequently customized or adapted to the vertical where it is being applied, and the possibility exists

that the assessment for the vertical could be different from the initial assessment. On the other hand, we consider that, as a result of the consolidation process, the MOOC should receive an assessment on whether it is satisfying the general criteria to become a branded CyberSec4Europe MOOC for academic or continuous education.

In order to determine whether the MOOC gets branded or not, one possibility would be to consider the percentage share of "Yes" received and define whether a MOOC is branded when it is above 50%-60%, leaving some room for variation. This is a simple way of assessment; however, we consider that it is ineffective. A MOOC could obtain the percentage of "Yes" required to pass the criteria with a few lesser categories, while receiving negative assessment in some other important categories. As an example, let us suppose that MOOC is considered branded if the percentage of "Yes" is above 50%. Under these conditions, we could see that MOOC A.19 is branded for continuous education. However, if we examine the category "Meeting professional expectation", the positive evaluation on correspondence to criteria is 0%. Therefore, we might consider that the course is not suitable for continuous education. Another example we could put forth is that a MOOC could be failing to obtain the necessary percentage because of the qualification of the institution (e.g., it is a new institution which is entering into the cybersecurity world), but the quality of the instructors or contents could be excellent.

Accordingly, we deem that in order to award a MOOC a status of a branded CyberSec4Europe MOOC, we should take into account, on the one hand, the percentage of "Yes" obtained in the different categories, and, on the other hand, a set of thresholds for the different categories (e.g., each MOOC for continuous education should have, at least, a 60% value of "Yes" in the category "Meeting professional expectation"). These thresholds could vary depending on whether the assessment is for academic education or continuous education. An additional option would be establishing compensation mechanisms between categories, e.g., we could establish that for an academic MOOC the result in the categories of "Qualification" of the proposing institution should be higher than 60%, but we could also establish a compensation rule: if the qualification of the proposing institution is between 40% and 60%, we could compensate it in case the quality of the instructors is above 80%. We could also modify the percentage assessment considering some criteria that are evaluated as "partly satisfying". Therefore, these criteria should be the baseline that any CyberSec4Europe-branded MOOC should accomplish. Once this baseline has been satisfied, the MOOC could be evaluated by verticals or in specific contexts. We also consider that vertical should follow a multifactor evaluation based on thresholds, and this could be different from the baseline.

By reviewing the evaluations, we have seen that there are some cases (e.g. in MOOC A.19 the evaluation of criteria QC41 or QC42; in MOOC A.26 - QC43; in MOOC A.27 - QC37; in MOOC A.56 - QC25), where either the criteria to evaluate the category as "Yes", "Partly" or "No" are not clear or the information the evaluators have used is different[200]. We consider that evaluators could, in some cases, have different opinions on the degree of satisfaction (which would result in the borderline evaluation for a MOOC in that category). However, there should not be contradictions between evaluations or a broad range of evaluations. In order to address this issue, we could consider different actions. First, during the consolidation process, for those cases where there is a broad disparity of evaluations, the partner that is performing the consolidation process could check with the evaluators the reasons (or based on the explanations provided) why each evaluator has made their decision. Based on the information received,

[200] See CyberSec4Europe D6.2, "Education and training review" for the full list of criteria.

the evaluation would be modified. Another alternative is to meet to establish a consensus among partners. Independently of the action taken, a report should be made by indicating the criteria that have generated this dissimilar evaluation so that the governance committee would consider whether the conditions under the category should be evaluated. This data is essential to establish a well-structured decision-making process.

Another issue that we should consider is whether all the CyberSec4Europe-branded MOOCs should be mandatorily evaluated regarding, e.g., the treatment of privacy issues or the report of vulnerabilities. We note that, while all courses have to be evaluated on their privacy conformance in terms of the systems used to teach the MOOC, privacy handling and ethics in the teaching material can be subject to the courses' contents. This means that only courses teaching activities with a possible ethical impact or privacy implications should be judged on whether they discuss this in the course.

We also consider that as part of partners' evaluation for a MOOC, apart from the evaluation that they provide for each category, each partner should provide a report indicating whether the evaluations of the MOOC regarding the categories established are suitable for the general evaluation of the MOOC and whether the criteria for each category are clear or if there are inconsistencies. The partner could also provide, based on its expertise, an overall assessment of the MOOC considering whether MOOC should be branded or not, and whether the categories and criteria have helped them to achieve this assessment. The partner could also classify the MOOC as a cybersecurity topic taxonomy. This could be later used to see the correlation and evolution of the categories and see if for specific topic different criteria should be considered and to establish the common criteria background for all cybersecurity MOOCs. A similar process should be made by partners that are evaluating vertically the MOOC.

Finally, once a MOOC has been awarded the status of a branded CyberSec4Europe MOOC, a monitoring process should be established to check its success and quality with the aim of determining whether the categories established were suitable. For example, we could have considered a MOOC suitable for continuous education but, in the end, the MOOC is not being useful for this purpose and professional are not interested in it.

7.3 Reflections on MOOC Governance

Based on our observations during this process, we find that several parts of the proposed governance structure have to be adjusted to ensure a more seamless process. We understand that the process should be flexible and based on thresholds and not on a unanimous decision-rule. While the general equality between the partners of MOOCs calls for a unanimous decision-rule, which would give every partner full control over the content of the decision by establishing a veto-right which cannot be overturned by the other partners, not all decisions need to be agreed on by all partners. Partners can well identify general content where a majority (50%) suffices. They can agree that this should be the case with the quality criteria and the channels as they are not of general importance to the consortium (such as who can become a member etc.). The larger a consortium of cooperating partners gets, the more important it becomes to establish a governance procedure in formality in order to integrate new partners. Then, it become even more important to establish not only fields of content where a simple majority suffices for a decision, but also to establish a representative body such as a governing board in order to assure that the cooperation may be executes in a manner that is fast and efficient.

7.3.1 NCCC Structure Changes

On the basis of first findings, CyberSec4Europe developed a first change of the regulation governance structure in the MOOC case. However, as MOOCs are typically organized by university bodies or other educational institutions on a case-by-case relationship and the task focused on the decision-making process, and as the Competence Community or the Stakeholder Environment do not have a general decision-making body, decisions will be up to the partners themselves. This is also true for any MOOC cooperation between non-accredited partners. We maintain that the process should receive feedback from MOOC evaluators and verticals (the different representative bodies and boards) and, based on this feedback, this meta-level process should be revised accordingly. Although the MOOC case was not thoroughly applicable to the structure of membership, board and decision process, CyberSec4Europe proposes some changes for the NCCC on this basis to avoid similar problems under a NCCC. In spite of its limitation the MOOC case was able to point some interesting issues, and enables us to address them early in the governance model design process.

The MOOC case decision-making process has to be derived from general rules beyond the particularities of a specific EU-wide cybersecurity network on public-public partnerships or public-private partnerships, or even private-private partnerships. It is often the case that the MOOC cooperative basis will not even be formally acknowledged but handled on a student-by-student case. Where MOOCs are practiced on a more institutionalized level, there will be an understanding between the involved partners, typically including everyone who participates. Further procedural bindings are typically not discussed and cleared before entering into MOOCs, but will be adjusted along the need. Third parties, e.g. other public institutions or civil society partners, are normally not included; their interests are usually only indirectly addressed.

7.3.2 Changes to Voting in the Context of the NCCC

The MOOC case does not reflect the special structure within the EU, therefore, its construction of voting rights only presented indirect experience on voting rights and mechanisms to CyberSec4Europe. In the MOOC case, the partners for MOOCs usually do not have a legal setting such as that provided by the regulation. Thus, the decision-making process has to be derived from general rules beyond the particularities of a specific NCCC. Given that the Competence Communities do not have a general decision-making body, decisions will be up to the partners themselves. This is also true for any MOOC cooperation between non-accredited partners outside the Competence Community in the Stakeholder Environment.

In general, the more partners are involved, the more apparent is the necessity of clear rules on the decision-making. In this manner, a cooperation that had started rather informally can in due course morph into a more formal cooperation, should the need arise. Such a legal agreement on the decision-making should then contain rules about the voting rights and the necessary majorities for decisions. They are the institutions contributing to the development of the MOOC. Generally, all parties who contribute to the MOOC will be will be equal partners in the agreement and participating as equal partners in the decision-making process.

7.4 Summary

In summary, we find that our proposed governance structure is already applicable to the case of MOOC accreditation, even though minor adjustments are necessary. However, the pilot case immediately highlighted shortcomings and points for improvements, enabling us to address these issues right away. Hence, our evaluation approach for the overall governance structure, i.e., implementing parts and evaluating them there, is feasible. We will hence continue with this implementation and evaluation approach as outlined in the updated Description of Action.

8 Conclusion

In the beginning, we have outlined a number of key cybersecurity goals for the EU: becoming the leading digital economy, guided by democratic values, while developing self-reliance and independence. In order to accomplish these goals, and with an eye to the two multiannual strategic objectives outlined by the European Commissions, CyberSec4Europe has identified four major challenges:

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

The project has set out to resolve these issues by designing the governance model for the network of cybersecurity competence centres. The desired governance model would not only address the current challenges, enable the development of the necessary capabilities, and successfully counteract the existing fragmentation of resources and capacities; it would also possess the needed flexibility to adapt to the emerging cybersecurity challenges. This deliverable has presented the results of the first year of CyberSec4Europe work towards realizing that goal.

We have set out by analysing the governance theory in order to start shaping the governance model that would be optimal for the goals of the project. We have arrived at the conclusion that the network model is best suited to create a European network of cybersecurity centres, with its flexibility, potential for bottom-up initiatives, and incorporation of non-market incentives and motivations, such as a single unifying goal and trust. Next to that, we have studied best practices in research collaboration and data sharing. Our conclusions were that the inter-sector collaboration between academia-based scientists with the other groups, notably with industry-based scientists, has been steadily decreasing, which is not a positive trend. Armed with this theoretical understanding, we have set out to collect input that would determine the shape of the future cybersecurity Network.

We have agreed early on that it was essential not to lose sight of the existing problems and concerns. For the new governance structure to work, it was vital that we go out into the field and listen to the opinions of the stakeholders. As “another European project”, we had to overcome a certain degree of prejudice and reluctance to contribute, but we have also received reassurances that a more efficient European cybersecurity cooperation was sorely needed and anticipated. And thus, we were even more determined to create the blueprint for the structure that would make it work for all the different stakeholders: academia, businesses, industries, civil societies, and national governments. We have gathered these stakeholders’ opinions via interviews, we have conducted surveys and workshops, and presented at the conferences. This way we have collected diverse feedback from various audiences. In both confidential one-on-one interviews and lively group discussions we have asked what the main cybersecurity goal of Europe should be, and what the governance structure for the network of cybersecurity centres should look like. The stakeholders’ input can be summarized in the following paradigms:

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

Subsequently we have looked at what we could learn from the existing governance structures. We have selected a number of big European organizations for analysis, in order to see how the cooperation between different members states and stakeholders can be structured. We also found it essential to look at the low-level initiatives aimed at creating cybersecurity hubs. All of the examples that have been analysed contained a number of valuable lessons to learn, with regard to the goals, community-building and nurturing trust, but also more practical considerations such as governance design and membership criteria. We have discovered a lot of variety concerning the formalization of, for example, membership criteria and voting, but also very different conceptual approaches. In particular, the Toulouse hub and its novel approach to funding innovation and case-by-case flexible decision-making system looked promising as we were considering the possible options for governance design.

We have extensively analysed the Regulation Proposal of the European Commission and the governance structure contained in it. We have provided critique on the provisions that, in our opinion, do not optimally contribute to realizing EU cybersecurity goals. In particular, the power distribution and the lack of representation of the European Parliament as a democratic structure in the Governing Board resulted in the centralized top-down character of the whole governance structure, which contradicted both the stakeholders' wish and our own findings. Meanwhile, the mechanism for the civil society involvement was not explicitly provided, and the structure of the Community, which could have been made into a possible outlet of exercising such power, was omitted entirely. In order to examine how the new network of cybersecurity centres will fit into the existing legal base, we have analysed the private and public cooperation law and the challenges of incorporating such network, or a similar envisioned structure, into the frames of existing legal structures. Any type of network in this respect presents a challenge due to the large number of organizations involved and their legal classification, as both private and public structured organizations will participate in this cooperation. While contractual agreements between the parties involved would normally provide the necessary degree of flexibility, establishing a single system of public and private interaction and cooperation on several levels has no known precedent, and thus would present another challenge to be figured out.

The CyberSec4Europe project started with the idea to utilize a small-scale pilot based on the governance structure for evaluating MOOCs in order to develop the broader governance structure. Initially we focused on presenting a quality assurance process based on quality assurance criteria to be proposed. However, in course of the project's unfolding and developing, it became clear that the MOOC case does not address the proposed tasks adequately. The MOOC testing case, however, has already demonstrated, among others, that such hubs would be desirable in order to accumulate special expertise and to create sub-networks that could bundle information and interests, as well as to assist in allocating funds by potentially raising additional funding from other sources.

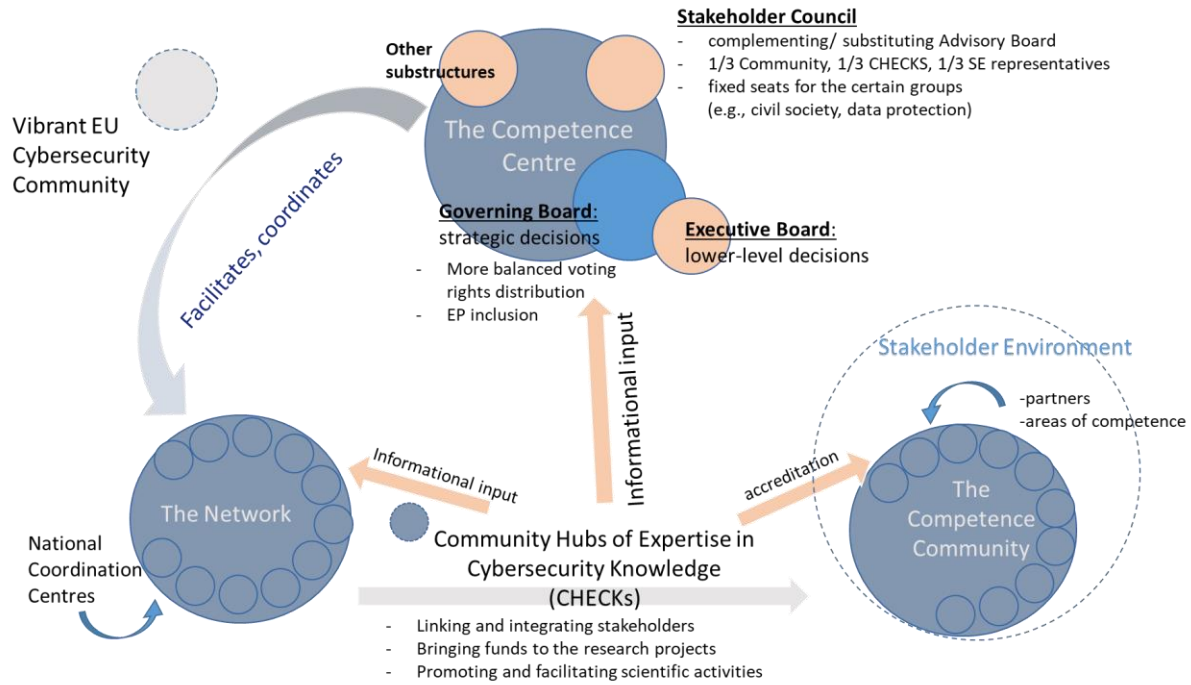

Figure 12: Overview of the adjusted governance structure.

We have outlined a governance proposal based on the approach that covers also the lower governance layers, so far omitted in the EU draft regulation (see Figure 12). In particular, we paid attention to the CHECKs as the new structures that could contribute to the goals of the project. We have consequently proposed to introduce a number of substructures to the Competence Centre, a flexible voting system for the issues of the diverse level, and other measures that would ensure that the complementary bottom-up approach gets implemented. As a form of practical input, we have provided the evaluation approach for one of the lower-level governance mechanics that we had proposed in a small-scale pilot based on MOOCs.

Overall, we have gained understanding about the field and outlined the direction of our future work. Our next deliverables will further explore governance design and test the hubs as potential inclusions into our governance model. Most important, we'll keep our hand on the pulse of emerging cybersecurity challenges, ready to timely respond and adjust our input when necessary – for the safety of Europe's nation states and citizens, and for the future of Europe in the world cybersecurity field.

This page has been intentionally left blank.

Annex A: Research Data Management and Ethical Considerations

In this Annex, we outline the ethical requirements and procedures applicable to our interviews and surveys in Chapter 2 for each directly involved partner.

TU Delft (TUD)

TUD uses two dedicated structures to handle ethical concerns of research and proper data management of research data. For ethical concerns, TUD instituted an HREC (Human Research Ethics Council), which enforces appropriate procedures for ethical approval of research. To ensure proper data management practices are followed, each faculty hosts a data steward, who works with researchers to set up a data management plan for each research project.

Ethical Procedure

For the ethics clearing process at TUD, there is a distinction between research directly involving human subjects, e.g., interviews, and research indirectly involving them, e.g., surveys, which we describe below.

Interviews

As interviews involve direct contact to human subjects, they have to go through a full ethics review at TUD. During this review, the HREC checks the correct implementation and communication of data privacy issues, ensures that the participants are aware of the scope of the study, their rights, e.g., in the context of anonymization, implementation of informed consent and the possibility of later retraction of consent, and the ethical viability of the asked questions. For this purpose, the HREC reviewed the interview supplements, see ‘Annex B: Interview and Survey Supplements’. The HREC of TU Delft considered the survey supplements to be sufficient, and the overall content and scope of the research to be ethically viable.

Surveys

As surveys do not directly involve interaction with human subjects, the HREC of TU Delft offers a fast-track procedure to decide whether a survey has to undergo a full ethical review or not. For the research conducted by TUD, the authors followed this fast-track procedure. As the survey does not collect personally identifiable information, required informed consent to participate, and is fully anonymous, fast-track clearance was granted.

Data Management Plan

TUD developed a data management plan for the data collected within the project together with the data steward of the faculty. For this, we used the tool DMP Online provided by TU Delft. Our data management plan accounts for data storage in secured and contracted data facilities, including appropriate backups. Furthermore, we account for the proper archiving of our research data, within the privacy limitations set out by the ethical considerations. This includes ensuring that no PII is stored together with the research data, i.e., consent forms are stored independent of the research data.

University of Trento (UNITN)

The Human Research Ethics Committee of the University of Trento is in charge of the evaluation and drafting of opinions on the experiment proposals involving human beings submitted by experts and research teams working at UNITN.

Ethical Procedure

The project research team contacted the Human Research Ethics Committee as well as the Research office for the Data protection which concluded that a detailed procedure was not applicable and an informed consent to the participants was sufficient given that no personal data were collected for research purposes and that participants joined in their capacity as experts rather than experimental subjects. The detailed process dealing with ethical considerations for surveys and interviews has been described in D11.2.

Data Management Plan

As for the DMP, the data have been collected for the sole research purpose of collecting stakeholders' opinions on cybersecurity requirements and the governance of the network of cybersecurity centres. Such opinions have not been attributed personally to the stakeholders according to the "Opinion on Anonymisation Techniques" WP216 05/2014 by Article 29 Working Party. The stakeholder's opinions have been reported as overall findings described in scientific reports (e.g. deliverables). All data have been kept confidential, stored safely and pseudonymised.

Annex B: Interview and Survey Supplements

Questionnaire Recruitment and Execution

As outlined in the previous section, CyberSec4Europe has established a methodology to identify and reach stakeholders (i.e. experts, academics, policymakers, etc.). Hence, we disseminated our survey via the communication channels within CyberSec4Europe (see Work Package 9). Furthermore, based on the preliminary stakeholders list from the institutional contacts of the CyberSec4Europe partners, the outreach was extended through the "snowball" method by asking the respondents to provide further contacts of their colleagues and scanning the websites of the relevant organizations. In order to reach a wider range of stakeholders, the survey has been conducted on the online survey tool "EUSurvey", the European Commission's official survey management tool. In total, we had over 50 participants in our survey.

Participation in the survey has been voluntary. The data has been collected for the sole research purpose of collecting stakeholders' opinions on cybersecurity requirements and the governance of the network of cybersecurity centres. Such opinions have not been attributed personally to the stakeholders according to the "Opinion on Anonymization Techniques" WP216 05/2014 by Article 29 Working Party. The stakeholders' opinions have been reported as overall findings described in scientific reports (e.g. deliverables). All data has been kept confidential, stored safely and pseudonymized. Stakeholders participating in the survey have been provided an Information Sheet on the research, which also included the privacy regulation applying to the data collection, see 'Annex A: Research Data Guidelines'. Once the stakeholders consented to the terms indicated in the Privacy Policy and Consent, they proceed to fill in the survey on the online survey tool. Participants have been free to withdraw their consent and to leave or end the survey at any point without explanations.

Online Questionnaire

CyberSec4Europe - **European Network of Centres of Cybersecurity Expertise.**

Fields marked with * are mandatory.

EUROPEAN NETWORK OF CENTRES OF CYBERSECURITY EXPERTISE.

YOUR OPINION MATTERS

Introduction

Who We Are

CyberSec4Europe is one of the pilots funded by the European Union to explore common European Cybersecurity Research & Innovation Roadmaps beyond 2020 and European cybersecurity strategies for industry.
Mariya Gabriel, Commissioner for Digital Economy and Society, said: "These projects will assist the EU in defining, testing and establishing the governance model of a European Cybersecurity Competence Network of cybersecurity centres of excellence."
The competence centre is supposed to become the main body that would manage EU financial resources dedicated to cybersecurity research under the two proposed programmes – Digital Europe and Horizon Europe – within the next multiannual financial framework, for 2021-2027.

More info: http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2019)635518

Why We Ask You

This survey will elicit both cybersecurity requirements in your area of activities and suggestions about governance models for the Competence Network.
Your expert opinion is of utmost importance for correctly shaping the European cybersecurity landscape of the future.

Privacy Policy & Consent

Participation in this survey is completely voluntary. Your data will be used for the sole research purpose of collecting stakeholders' opinions on cybersecurity requirements and the governance of the network of cybersecurity centers.
Such opinions would not be attributed personally to you along the "Opinion on Anonymisation Techniques" WP216 05/2014 by Article 29 Working Party and will be reported as overall findings described in scientific reports (e.g. deliverables to the European Union).

See the full provacy policy in PDF:
CS4E_Interview-_Full_privacy_policy.pdf

☐ I agree to the survey

Information about the respondent

Country

- ○ Austria
- ○ Belgium
- ○ Bulgaria
- ○ Croatia
- ○ Cyprus
- ○ Czechia
- ○ Denmark
- ○ Estonia
- ○ Finland
- ○ France
- ○ Germany
- ○ Greece
- ○ Hungary
- ○ Ireland
- ○ Italy
- ○ Latvia
- ○ Lithuania
- ○ Luxembourg
- ○ Malta
- ○ Netherlands
- ○ Poland
- ○ Portugal
- ○ Romania
- ○ Slovak Republic
- ○ Slovenia
- ○ Spain
- ○ Sweden
- ○ United Kingdom
- ○ Other

If other please specify

* You are employed in:

at most 1 choice(s)

- [ ] Industry
- [ ] Academy
- [ ] European Agency
- [ ] National Agency
- [ ] European Regulator
- [ ] National Regulator
- [ ] Law Enforcement
- [ ] Standardization Body
- [ ] Other

Other (please specify):

* What is your area of work?

between 1 and 1 choices

The following sectors are taken from the statistical classification of economic activities in the European Community (NACE). They will be used to associate your response to the different stakeholders communities.

Agriculture, Forestry, Fishing
Mining, Quarrying, and Oil and Gas Extraction
Utilities (electricity, gas and water supply, waste management, etc.)
Construction
Manufacturing
Wholesale Trade
Retail Trade
Transportation and Warehousing
Information and communication
Finance and Insurance
Real Estate and Rental and Leasing
Professional, Scientific, and Technical Services
Management of Companies and Enterprises
Administrative and Support Services
Education
Research and Higher Education
Health Care and Social Assistance
Arts, Entertainment, and Recreation
Accommodation and Food Services
Public Administration
Defense
International organizations
Other

Other (please specify)

What is your position?

at most 1 choice(s)

- [ ] President/CEO/Member of Board
- [ ] Senior administrator/head of department
- [ ] Manager/professor/head of group
- [ ] Officer/Researcher/Administrator/Member of Staff
- [ ] Consultant/self-employed/
- [ ] Other

Other (please specify)

* Are you directly involved in one of the EU pilot projects launched to prepare the European Cybersecurity Competence Network?

- ( ) Yes
- ( ) No

* Are you involved in CyberSec4Europe?
  - ( ) Yes
  - ( ) No

* Which of the following Cybersecurity Vertical Sectors is your main area of expertise?
  - [ ] Energy
  - [ ] Financial
  - [ ] Health/Medicine
  - [ ] Digital Infrastructure
  - [ ] Transportation
  - [ ] Public Safety
  - [ ] Defense
  - [ ] Space
  - [ ] Other

If other, please specify:

* Which of the following verticals of the pilots is your main area of expertise:
  - Finance and E-Commerce
  - Supply Chain Security Assurance
  - Privacy-preserving Identity Management
  - Incident Reporting
  - Maritime Transport
  - e-Health and Medical Data Exchange
  - Smart Cities

Main goal

What Europe should achieve as an overall goal in cybersecurity?

* In your specific area of expertise, what is the key cybersecurity situation that must change (e.g. better resilience, transparency, trustworthiness, security metrics...)? If possible, explain also the motivations behind your indications.

The European Cybersecurity Competence Network will have to indentify its key priorities to drive the cybersecurity technological agenda and access to cybersecurity expertise.

Capabilities

* In your area, what key capabilities are required by systems, people, institutions, etc, to achieve that change?

The Competence Centre and its Network will become the main implementation mechanism for activities in support to Member States and the cybersecurity industry (including deployment, investments and research) in the 2021-2027 period.

What is needed to achieve the capabilities you just mentioned?

	Not Essential	Of Minor Importance	Of Major Importance	Essential
Novel Technologies	○	○	○	○
New professional or academic skills	○	○	○	○
Policy interventions (regulations and fines)	○	○	○	○
New Certification and Audit procedures	○	○	○	○
New or improved technical standards	○	○	○	○
Other	○	○	○	○

Other (please specify):

* Please describe some specific technologies or technical standards that you have in mind, otherwise add N/A.

* Please describe some specific organisational measures (e.g. skill sets, regulation, liability) that you think are important. Otherwise add N/A.

Should the Network and Centre push towards specialization of Member States and prioritize funding the development of different technologies in different Member States?

at most 1 choice(s)

- [ ] No
- [ ] Only in special cases
- [ ] Yes

Should the Network and Centre push towards mandatory security certification at European level?

at most 1 choice(s)

- [ ] No
- [ ] Only in special cases
- [ ] Yes

Decision Makers in the Network

The upcoming regulations of the European Cybersecurity Competence Network of cybersecurity centres establish that the main European centre will be governed by the European Commission and the Member States. However, the participants to Advisory Committee and the Individual National Centres are not yet defined. The purpose of the Pilots is to suggest the European Commission on their composition and their decision making process.

* Who should be the key players in the *European Cybersecurity Competence Network of cybersecurity centres of excellence* to achieve those capabilities?

between 1 and 8 choices

"The people" are sovereign; "the people's will" must prevail; but who are "the people"? Who gets to belong to this group, and who decides? How do individuals coalesce into a collective "people", and what other communities are formed in the same way?

- ☐ European Commission
- ☐ ENISA (European Network and Information Security Agency)
- ☐ National cybersecurity agencies
- ☐ Other national Government Representatives
- ☐ Industry
- ☐ Academia
- ☐ Industry associations
- ☐ Consumer associations
- ☐ Data Protection Authorities
- ☐ Computer Emergency Response Teams (CERTs, CSIRTs)
- ☐ Formal standards and/or certification organizations (e.g., ISO, ITU)
- ☐ Community standards and/or certification organizations (e.g., IETF)
- ☐ Community professional organizations (e.g., NANOG, community around RIRs like the RIPE NCC)
- ☐ Open Source software communities (e.g., the Linux foundation or the community around FOSDEM)
- ☐ Hacker communities (e.g., the German CCC or members of European Hackerspaces)
- ☐ Other

If other please specify:

* In your expert opinion, what should be the key role of the entities you have selected above in the *Network*? (Decision making on Financial allocation, advisory to Member States, etc.)

The Competence Centre and its Network will become the main implementation mechanism for activities in support to Member States and the cybersecurity industry (including financial distribution of EU funds, deployment and research) in the 2021-2027 period.

What type of accreditation process would be appropriate for those players in the *Network* ?

What do you think should be the relationship between ENISA (European Network and Information Security Agency) and the *Network*?

Has your national legislation given a coordination role on cybersecurity to a national agency?

- YES
- NO

If yes: what do you think should be its relationship with the *Network*?

Any Other Issue

What additional information you would like to give us and that we forgot to ask for?

Would you like to/prefer to be interviewed in person? (If YES, please leave your contact details below).

- Yes
- No

More information on the personal interview session:

CS4E-_Interview_information.pdf

Name

Email

Interview Leaflet Page 1 (Context)

EUROPEAN NETWORK OF CENTRES OF CYBERSECURITY EXPERTISE:
YOUR OPINION MATTERS

Who We Are

C yberSec4Europe is one of the pilots funded by the European Union to explore common European Cybersecurity Research & Innovation Roadmaps beyond 2020 and European cybersecurity strategies for industry.
Mariya Gabriel, Commissioner for Digital Economy and Society, said: "These projects will assist the EU in defining, testing and establishing the governance model of a European Cybersecurity Competence Network of cybersecurity centres of excellence." The competence centre is supposed to become the main body that would manage EU financial resources dedicated to cybersecurity research under the two proposed programmes – Digital Europe and Horizon Europe – within the next multiannual financial framework, for 2021-2027.

Why We Ask You:

This survey will elicit both cybersecurity requirements in your area of activities and suggestions about governance models for the Competence Network. Your expert opinion is of utmost importance for correctly shaping the European cybersecurity landscape of the future.

If you want to give your opinion on cybersecurity requirements in your area of activities and on the governance models for the European Competence Network and the national cybersecurity centres of excellence you can participate to the survey at the following link on the side: https://ec.europa.eu/eusurvey/runner/CyberSec4Europe_Survey Thanks for your support to the research!	

We would like to interview you in person if possible. Please contact our representative in [country]

[a short bio of the interviewer]

Interview Leaflet Page 2 (Interview Questions)

If you are interested in a one-to-one personal interview, below you will find the interview template.

Who are you?

1. Broadly describe your role (e.g. European or National Agency, National or European Regulator, Industry Representative, Law Enforcement, Standardization Body etc.) Which is the key domain in which you are working on?

Main Goal

2. What Europe should achieve as an overall goal in cybersecurity?
3. In your specific area of expertise, what is the key cybersecurity situation that must change (e.g. better resilience, transparency, trustworthiness, security metrics...)? If possible, explain also the motivations behind your indications.

Capabilities

4. What key capabilities are required by systems, people, institutions, etc., to achieve that change in your area?
5. What other measures do you think are needed to achieve the capabilities you just mentioned (novel technologies, training, policy intervention, new professional, improved technical standards, etc.)?
6. Should the Network and Centre push towards specialization of Member States and prioritize funding the development of different technologies in different Member States?

Decision Makers

7. Who should be the key players (e.g. national governments, industry, academic experts, Consumer associations, Hacker communities, etc.)?
8. What type of decision making and accreditation process do you think would be appropriate for those players for the Network?
9. The upcoming legislation will give a clear role to ENISA. What do you think should be the relations between ENISA and the network?

Any Other Issues

10. Any other questions that we should have asked and we didn't?

Your Privacy Rights:

Your data (name and email) will be processed according to Article 89 of the General Data Protection Regulation 2016/679 and it will not be transferred to third parties. It will be used for the sole research purpose of collecting stakeholders' opinions on the requirements and governance of the network of cybersecurity centres. Such opinions would not be attributed personally to you along the "Opinion on Anonymisation Techniques" WP216 05/2014 by Article 29 Working Party and will be reported as overall findings described in scientific reports (e.g. deliverables to the European Union). The data controller for this research activities for the Governance roadmap are the University of Trento, via Calepina 12, 38122 Trento, Italy and TU Delft, Mekelweg 5, 2628 CD Delft, The Netherlands. The researchers in charge are [name] [contact details]

This interview is part of a project that has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 830929.

Qualitative Interviews: Data Management

The following criteria for selecting the participants were applied, in order to comply with the applicable regulations and legislation in the countries of the collecting parties:

- All participants were of age (18 years and older) and provided informed consent;
- All participants joined in their capacity as experts in diverse relevant fields (academia, industry, government institutions, ethical hackers), see 'Stakeholder overview';
- Diversity and balance in terms of gender and member state representation were strived for.

As a result, we have been able to collect input from the stakeholders with diverse perspectives that originated from their professional activities and affiliations.

During the recruitment procedure the prospective study participants received information sheet (see 'Annex A: Research Data Management and Ethical Considerations') prepared by UNITN and TU Delft, containing the following information:

- A short description of the CyberSec4Europe project;
- The purpose of the interview and data collection;
- A link to the online questionnaire;
- A short biography of the person(s) conducting the interviews;
- The questions that will serve as a base structure for the interview;
- A legal disclaimer on data processing, privacy, and the participants' rights;
- A list of the responsible data controllers.

Additionally, every participant has been explicitly informed on the procedure of handling transcripts and on their right to withdraw their consent to participate at any time. The participants have given their verbal consent on- and off-record. The participants have received the pseudonymized transcripts and had the opportunity to verify that their opinions had been transcribed faithfully and that their anonymity had been protected, and only after that step the transcript was shared with the partners. All the references to nationality, place and country of work, biography, gender, and professional connections has been edited in order to ensure anonymity.

The challenge for the data management process manifested in the necessity to balance the needs of the project, open data commitment, and protecting the privacy of the research subjects. No sensitive personal data needed to be gathered, such as political preferences, sexual orientation and details on family members; however, interview recordings qualified as identifiable personal data, since the voices of the respondents could be potentially used to identify them. Furthermore, even in the pseudonymized form the transcripts hypothetically contained the potential for de-anonymization by someone familiar with the experts in the field. Therefore, to safeguard privacy of the respondents, it has been decided that anonymized/pseudonymized data collected by TU Delft and UNITN would not be published as open data. Considering potential ethical issues that might arise from secondary use of data, as well as application of Open Data principle, in consultation with the Data Steward, a plan has been agreed upon. For both data collectors, the voice recordings, being the data that is the most vulnerable for identification, will be destroyed after the transcript approval has been granted. The storage of the transcripts is managed in the following way:

- TU Delft: The transcripts are stored in the TU Delft online data repository in pseudonymized form. In course of research, the files are stored on the password-protected computer accessible only to the researcher in charge of interviews (copy 1), as well as on the TU Delft-authorized online storage service SurfDrive (copy 2) shared with multiple members of the research team. In compliance with Research Data Guidelines (see 'Annex A: Research Data Management and Ethical Considerations'), the files are stored on two different media types, one of which is off-site. The transcripts in their anonymized form are shared with UNITN in a safe way via protected link to the SurfDrive folder.
- UNITN: The transcripts in anonymized form are stored in a Secure backed up storage space and located in a safe.

Upon the completion of the project, the data will be archived with proper supporting documents describing the steps of data processing.

Annex C: NSPW Survey Questions and Outcomes

We developed a security cooperation and innovation survey, and asked NSPW 2019 participants as well as steering committee members to participate. The survey included questions about cooperation and innovation in the field of security. Nine persons filled out the survey. All participants except one were working in the research sector, with some having additional affiliations in government and/or industry.

Regarding collaboration, all participants had worked together with others from at least the research and industry sectors, most also with government, and some with NGO or other sectors. The most successful forms of cooperation are indicated to be joint research, case studies, and prototype development. Regarding success factors for cooperation, most participants selected good personal contact, similar interests, and available funding or other incentives. Most participants had shared their (organization's) data with government and researchers, as well as had used data shared by researchers, government, and industry. Regarding success factors for data sharing, eight participants selected (open) data policies of organizations, seven participants picked protection of rights of data owners and subjects, seven selected reputation / recognition, and three selected availability / conditions of funding. No other factors were suggested. According to the participants, actions to facilitate data sharing could include recognition that data sharing is a matter of public good, strong deidentification and data sharing rules, protection from bad actors, mechanisms to ensure privacy of raw data, even from researchers, clear statement of policy of conditions for sharing, and communications.

Regarding critical features of successful governance models, all participants selected openness and transparency, eight participants picked flexibility and strategic leadership, and five selected capitalizing on existing capacities. Participants expect strong legal agreements and information protection rules in the network. Nonetheless, the network should also provide a structure that encourages friendship with international colleagues and collaboration between communities. Collaboration between communities; cybersecurity is usually a distributed responsibility in most governments Suggested key activities in developing and maintaining a cooperation network are, incentives, commitment, and a strong community focus by encouraging regular meetings.

The security cooperation survey developed for and distributed at NSPW provided useful input from experts that are used to thinking outside the box. Some of the ideas put forward by the respondents may be used in developing governance structures and events for a network of excellence, contributing to (radical) innovation. The survey can be reused in other contexts, to increase the number and diversity of responses.

Security Cooperation and Innovation Survey

Fields marked with * are mandatory.

Opening Statement and Consent

You are being invited to participate in a research study titled **Cybersecurity cooperation and innovation survey**. This study is being done by Wolter Pieters, Tobias Fiebig and Natalia Kadenko from the TU Delft. The study was approved by the Human Research Ethics Committee of the TU Delft.

The purpose of this research study is to gather information on successful cooperation leading to innovation / new paradigms in cybersecurity. The survey will take you approximately 15 minutes to complete. The data will be used as input to the design of a governance structure for a network of excellence around cybersecurity in Europe. This research is part of the CyberSec4Europe project (https://www.cybersec4europe.eu/).

Your participation in this study is entirely voluntary and you can withdraw at any time. You are free to omit any question.

We believe there are no known risks associated with this research study; however, as with any online related activity the risk of a breach is always possible. We will minimize any risks by not collecting any personal data or specific demographics and storing the survey data securely.

The European Commission requires data gathered in funded project to be made publicly available for further research (open data). This means that your (anonymous) answers will be included in a publicly available dataset when results of this study are published. **Please do not reveal your identity by referring to specific persons, places, organisations, etc. in your answers to the open questions.**

Contact: w.pieters@tudelft.nl

☐ I have read and understood the above information and I agree to participate in this survey.

In which context were you invited for this survey?

- ○ New Security Paradigms Workshop (NSPW)
- ○ Other

Part I: Cooperation

Which sector are you working in? (multiple answers possible)

- ☐ Research
- ☐ Industry
- ☐ Government

- [ ] NGO
- [ ] Other

With people from which sectors have you worked together on cybersecurity? (multiple answers possible, including your own sector)

- [ ] Research
- [ ] Industry
- [ ] Government
- [ ] NGO
- [ ] Other

Which sectors have been most important to you in successful cooperation on cybersecurity? (multiple answers possible)

- [ ] Research
- [ ] Industry
- [ ] Government
- [ ] NGO
- [ ] Other

Which forms of cooperation do you consider most successful in the cybersecurity domain? (multiple answers possible)

- [ ] Joint research
- [ ] Case studies
- [ ] Prototype development
- [ ] Other

Could you please specify other successful forms of cooperation?

Which factors characterise successful cooperation in the cybersecurity domain? (multiple answers possible)

- [ ] Similar (research) interests
- [ ] Geographical proximity
- [ ] Good personal contact
- [ ] Available funding / other incentives
- [ ] Other

Could you please specify other success factors for cooperation?

Part B: Data sharing

With which sectors have you shared cybersecurity data collected by yourself or your organisation in the past? (multiple answers possible, including your own sector)

- [ ] Research
- [ ] Industry
- [ ] Government
- [ ] NGO
- [ ] Other

From which sectors have you used shared data on cybersecurity in the past? (multiple answers possible, including your own sector)

- [ ] Research
- [ ] Industry
- [ ] Government
- [ ] NGO
- [ ] Other

Which factors characterise successful data sharing in the cybersecurity domain? (multiple answers possible)

- [ ] Availability/conditions of funding
- [ ] Protection of rights of data owners and subjects
- [ ] (Open) data policies of organisations
- [ ] Reputation / recognition
- [ ] Other

Could you please specify other success factors for data sharing?

What actions should be taken to facilitate data sharing / open data on cybersecurity?

Part C: New solutions

Have you been involved in developing cybersecurity innovations / new paradigms?

- ( ) Never
- ( ) Once
- ( ) A few times
- ( ) Often

Which properties characterise cybersecurity innovations / new paradigms as compared to incremental improvements?

Which are the critical factors contributing to the development of successful cybersecurity innovations / new paradigms?

Part D: New products/services

Have you been involved in translating cybersecurity innovations / new paradigms into practice (new products/services)?

- ○ Never
- ○ Once
- ○ A few times
- ○ Often

Which are the critical factors contributing to successful translation of cybersecurity innovations / new paradigms into practice?

Which cybersecurity products/services do you find most innovative? Why?

Part E: Capacity building

What are critical features of governance models for successful cybersecurity cooperation and innovation? (multiple answers possible)

- ☐ Openness and transparency
- ☐ Flexibility
- ☐ Strategic leadership
- ☐ Capitalising on existing capacities
- ☐ Other

Could you please specify other critical features of governance models?

What activities are key in developing and maintaining a cooperation network in cybersecurity?

How could funding mechanisms stimulate non-incremental progress / new paradigms in cybersecurity?

What should be done to stimulate successful cooperation and innovation in cybersecurity?

Part F: Additional remarks

The results of this survey will be used for developing a governance structure for a network of excellence in cybersecurity. Do you have any additional remarks on cooperation and innovation in cybersecurity that would be relevant for this purpose?

End of the survey

This is the end of the survey. Please do not forget to click "Submit". Thank you for participating!

Annex D: Stakeholder Requirements Overview

Stakeholder Groups	Requirements
ALL	Coordination within EU and independence from non-EU countries with regards to technology and protection of citizens, businesses and state actors.
LS + B	The need for knowledge and education to be constantly updated to meet the dynamic changes in cybersecurity.
S	EU taxpayer money in cybersecurity research through open calls does not benefit US companies through their EU subsidiaries.
LS + ST + SS	The goal was to achieve cyber sovereignty, independence, and control: clearly expressing preference for the broader focus; only 32% of the participants to the survey consider the developments of better security technologies as essential and another 35% consider it of major importance. Less than half of them (42%) considered new or improved technical standards of major importance. In contrast, almost half of the respondents consider new professional or academic skills as essential to achieve cybersecurity capabilities (46%). Also, half of them also consider policy interventions of major importance (51%).
LS + SS + B	One of its objectives was R&D funding [#1, #2, #3, #7, #10] but they also widely diverged on whether it was the only task (as advocated by an EU actor [#2]). For example, three very diverse stakeholders, authority board members [#3], ethical hacker [#6], and CISO [#10], raised the critical importance, shared by the EU Parliament, of supporting SMEs to bring research to the market, others [#1, #4, #8, #9, #17] focused on professional skills and education.
ALL	In this respect, half of the participants agreed that the CCN should support mandatory security certification.
ALL	The majority of the participants consider the European Commission (60%) as a key player as well as ENISA (61%).
ALL	Most interviewees argued that such a decision should be left at Member State levels and that a balance between different stakeholders is desirable.
ALL	What emerged as a surprise was the role of the CCN as a first point of contact to support society at large (from SMEs to individual citizens) when seeking cybersecurity advice.
ALL	Yet, almost a half of respondents pointed to the Computer Emergency Response Teams (CERTs, CSIRTs) to have an advisory role, which would create confusion if the activities of the Centre were limited to the distribution of funding for R&D.
LS	Highlighted that CCN could promote mechanisms for sharing of attack data in a way that safeguards the anonymity of the victim, while allowing other actors to protect themselves.
LS + B	Also pointed out how normal citizens or ethical hackers could turn to CCN for responsible disclosure of the security issues to the corresponding regulator of each vertical domain, as the company which has the security issues would have clearly a conflict of interest.
ALL	More than half (58%) of the respondents attributed the key role to Data Protection Authorities, a proportion comparable to the number selecting the European Commission, thus showing the key importance that privacy protection has for European citizens.
ST (2.3)	Gathering and properly systematizing data on the existing cybersecurity issues, as well as maintaining open data principle, including open and transparent data formats, were named as important issues for booking progress in cybersecurity research.
B (2.3)	Pointed out that industries would benefit from having access to academic research to solve a particular problem, while academia could use the substantial data accumulated by industries.
LS (2.3)	Valorisation chain and the role of the companies in it to establish resilience, which is the ultimate goal.
B (2.3)	Responsibility of keeping the data safe; in fact, several respondents have mentioned (and generally positively evaluated) GDPR in the context of data management. Likewise, they emphasized the importance of trust and transparency in sharing data and knowledge on cybersecurity issues.
WORKSHOP (2.4)	That governance should be close to users and capitalize on the relevant knowledge through informal networking and involving the specialists in order to ensure the diversity of expertise and the possibility to include the opposite views.
WORKSHOP (2.4)	It would be more beneficial to define clear agenda and vision (“first man on the moon” type), as well as to redefine success (for example, “becoming the most cybersecure according to certain criteria”).
WORKSHOP (2.4)	While the basic governing bodies, such as the Centre, the Network, and the Community, were kept intact, the relations between them were upended, in order to involve the experts as a part of the community, and generally operate in more flexible, less centralized, and less rigidly hierarchical manner.

Table 6: Extracted Requirements from Chapter 2

Legend: TS → Technical stakeholders; B → Business; SS → Social Stakeholders; LS → Legislative Stakeholders; S → Standard Bodies; ST → Scientific Stakeholders;

This page has been intentionally left blank.

Annex E: Definition and Quality Criteria for MOOCs

Definition of MOOC Channels

T2.3's task description demands the development of specific governance process for the MOOC case in regard to two aspects. One of them is the design of a decision process for the selection of MOOC "channels". This raises the question what is understood by a "channel", as the open formulation of "channels" leaves space for interpretation.

The task description concretizes the meaning in its first sentence by defining the task as an "identification of top ten topic channels". This definition suggests an understanding of "channels" as different cybersecurity topics i.e. content that might be part of a CyberSec4Europe MOOC course. However, in a conference at June 13th in 2019 of WP6 T6.3, the participating verticals agreed that there are no such streamed topics in cybersecurity education. T6.3 concluded that "channels" means a wide variety of channels in which a MOOC and a set of MOOCs could be distributed. The understanding of "channels" would then be oriented on the different platforms that offer distribution of courses, and the task would be to analyse their strength and weaknesses such as GDPR compliance or user accessibility. This type of definition is consistent with the understanding in the D6.1 deliverable of WP6.

Thus, "channels" means the variety of platforms that offer distribution of courses. A decision-making process on this issue would then mean the agreement which platform(s) are being used for the offer of a MOOC, see D6.1 Chapter 1 by Task 6.3.

Definition of Quality Criteria for MOOCs

The following quality assurance criteria have ultimately been used in the MOOC evaluation:

- **Qualification of the proposing institution:** This criterion relates to the topic specific qualification of the institution proposing a corresponding MOOC. For example, a University renowned for their computer security research will score higher here, than a company whose main business focus so far was not on cybersecurity.
- **Qualification of instructors:** In this criterion, reviewers will assess the qualification of the involved teachers, including but not limited to, teaching certifications held, courses taught so far, and how these have been evaluated.
- **Course examination, credentialization and recognition:** This includes what kind of credits or course certificates are awarded for successful participants, and how assessment is performed. Additional points might be gained, for example, if the proposing institution awards ECTS for students, which these can then use in one of the traditional degree programs of the institution.
- **Meeting professional expectation:** With this criterion, the decision-making body evaluates whether the proposed MOOC or channel conforms to the practical requirements of industry stakeholders.
- **Course structure and content criteria:** These criteria pertain to the relevance of topics and content, the proposed learning outcomes, and the evaluation of learned skills. Furthermore, a MOOC may follow a diverse set of formats to facilitate student engagement. In this criterion the format of the MOOC will be evaluated based on the specific fit for the case at hand.

- **Openness:** While openness is an integral part of the term ‘MOOC’, parties may try to restrict access for monetary or other reasons. Hence, openness might be limited. This criterion evaluates this aspect.
- **Ethics & Privacy - Ethical Considerations for Teaching Cybersecurity:** Especially with cybersecurity, ethical issues play a substantive role. Hence, proposers of a MOOC should address how they handle potential ethical issues due to them teaching offensive capabilities to a wider audience. In this criterion the committee assess to which degree appropriate measures were implemented by the MOOC’s proposers.
- **Ethics & Privacy - Privacy Requirements:** As with all technical offerings the platform providing the MOOC should sufficiently consider students’ privacy, and provide full GDPR compliance.
- **Criteria for Cyberranges:** Cyberranges are a novel concept for teaching active and passive cyber capabilities to students in an applied way. As such, we tested each MOOC in how far practical components of the program might qualify as a cyberrange.

Annex F: Geography of Existing Collaboration Within the EU

Lead-Author	Co-Author	No.
GERMANY	USA	68
UK	USA	35
FRANCE	USA	31
SWITZERLAND	USA	26
NETHERLANDS	USA	16
ITALY	USA	15
FRANCE	SPAIN	15
GERMANY	UK	14
SPAIN	USA	13
BELGIUM	USA	12
FRANCE	UK	11
SWITZERLAND	UK	11
GERMANY	NETHERLANDS	10
GERMANY	SWITZERLAND	10
AUSTRIA	USA	10
FRANCE	GERMANY	9
AUSTRIA	GERMANY	6
GREECE	USA	8
FRANCE	ITALY	6
CHINA	UK	6
SPAIN	UK	5
FINLAND	USA	5
SWEDEN	USA	5

Table 7: Co-Authored papers including at least one EU author (2015-2018)[201]

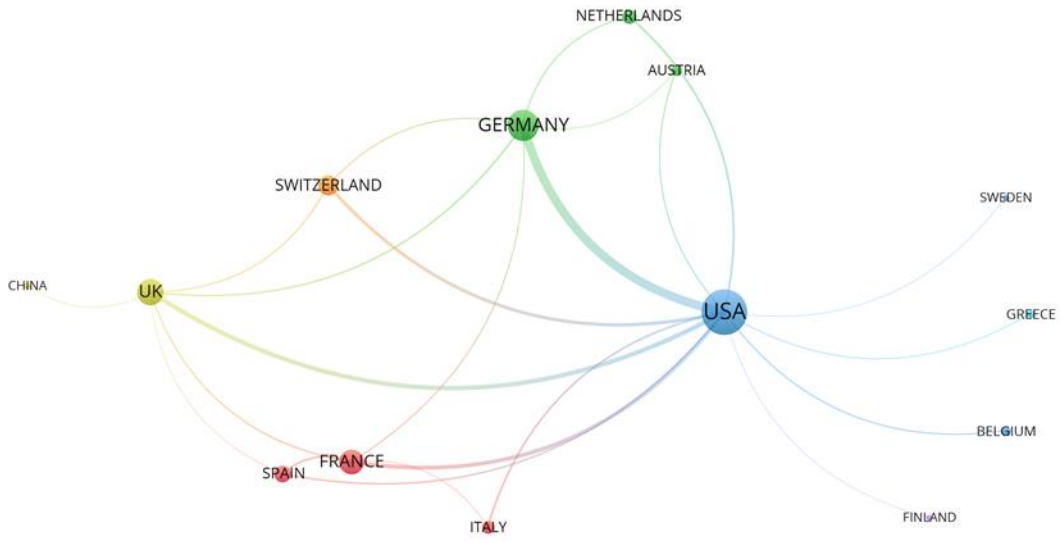

Figure 13: Visualization of Table 7 as a network graph

[201] Data source: Davide Balzarotti, http://s3.eurecom.fr/~balzarot/notes/ [last accessed December 14, 2019].

This page has been intentionally left blank.