ECHO EUROPEAN NETWORK OF CYBERSECURITY CENTRES AND COMPETENCE HUB FOR INNOVATION AND OPERATIONS

D3.8 UPDATE – GOVERNANCE NEEDS AND OBJECTIVES

Lead author: Todor Tagarev, IICT

Submission date: 31 January 2022

PUBLIC DOCUMENT

The work described in this document has been conducted within the ECHO project. This project has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830943

Title	European network of Cybersecurity centres and competence Hub for innovation and Operations
Acronym	ECHO
Number	830943
Type of instrument	Research and Innovation Action
Topic	SU-ICT-03-2018
Starting date	01/02/2019
Duration	48
Website	www.echonetwork.eu

D3.8 UPDATE – GOVERNANCE NEEDS AND OBJECTIVES

Work package	WP3 ECHO Governance Model
Lead author	Todor Tagarev (IICT)
Contributors	Yantsislav Yanakiev (BDI), Bríd Davis (NUIM), Antoniya Shalamanova (IICT), Ewa Konieczna (VST), Lina Smovziuk (KhAI), Georgi Penchev (IICT)
Peer reviewers	Sébastien Hespel (VTCB), Tiia Somer (TUT)
Version	V1.0
Due date	31/01/2022
Submission date	31/01/2022

Dissemination level:

X	PU: Public
	CO: Confidential, only for members of the consortium (including the Commission)
	EU-RES. Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)
	EU-CON. Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)
	EU-SEC. Classified Information: SECRET UE (Commission Decision 2005/444/EC)

Version history

Revision	Date	Editor	Comments
0.1	10/03/2021	Todor Tagarev (IICT)	Amended structure of the document
0.2	17/03/2021	Todor Tagarev (IICT), Yantsislav Yanakiev (BDI)	Revised and edited sections on business (3.2) and governance models (5.3) identified in the academic literature
0.3	31/03/2021	Todor Tagarev (IICT), Bríd Davis (NUIM)	Revised and edited sub-sections on findings from existing networks 3.3, 4.4 and 5.2.
0.4	19/11/2021	Todor Tagarev (IICT)	Added section 5.4 on organisational modalities of existing CNOs
0.5	02/12/2021	Tagarev (IICT), Antoniya Shalamanova (IICT), Ewa Konieczna (VST), Lina Smovziuk (KhAI), Georgi Penchev (IICT), Yantsislav Yanakiev (BDI)	Added section 6 on partners' expectations to the governance model
0.6	13/12/2021	Todor Tagarev (IICT)	Updated analysis of normative documents in sub-sections 3.1, 4.1 and 5.1
0.7	27/01/2022	Todor Tagarev (IICT)	Revised version upon the recommendations from the internal review
0.8	29/01/2022	Ewa Konieczna (VST)	Minor formatting updates
1.0	31/01/2022	Matteo Merialdo (RHEA)	Final QA, Document closed

List of contributors

The list of contributors to updated and new sections in this deliverable are presented in the following table:

Section	Author(s)
Updated analysis of normative documents (3.1, 4.1, 5.1)	Todor Tagarev (IICT)
Organisational modalities of existing CNOs	Todor Tagarev (IICT)
Partners' expectations to the governance model	Todor Tagarev (IICT), Antoniya Shalamanova (IICT), Ewa Konieczna (VST), Lina Smovziuk (KhAI), Irena Mladenova (IICT), Georgi Penchev (IICT), Yantsislav Yanakiev (BDI)

Keywords

COLLABORATIVE NETWORKED ORGANIZATION, CNO, NETWORK GOVERNANCE, GOVERNANCE REQUIREMENTS, NETWORK BUSINESS MODEL, GOVERNANCE MODEL, ORGANISATION

Disclaimer

This document contains information which is proprietary to the ECHO consortium. Neither this document nor the information contained herein shall be used, duplicated, or communicated by any means to any third party, in whole or parts, except with the prior written consent of the ECHO consortium.

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

Personal Data collected, used, and stored to produce the content of the deliverable were processed in compliance to requirements from the GDPR, according to ECHO Data Management Plan and ECHO Ethics deliverables.

Executive summary

The overarching objective of Work Package 3 (WP3) "ECHO Governance Model" is to define and establish an appropriate governance model of the ECHO network, as by the completion of this Horizon 2020 funding the ECHO project aims to transition from a Consortium to a networked organisation. The governance model as a whole, or the underlying principles and some of its main components, would potentially be of interest for establishing and operating the European Cybersecurity Competence Centre and the Network of National Coordination Centres.

In these instances, a networked organisation is defined as an organisation incorporating independent entities connected (*networked*) to collaborate in the design, development, and provision of cybersecurity products and services.

Thus, in the effort to determine what factors underlie the establishment of a strong and efficient governance model, Task 3.1 "Governance needs and objectives", under the remit of WP3, pursues three objectives:

1. identifying and clustering existing network business models; analysing clusters vis-a-vis ECHO objectives so as to identify business models of potential utility for ECHO;
2. identifying and prioritising governance needs; and
3. structuring the space of possible governance models of network organisations and providing examples of how existing network governance models fit into that space.

To achieve these objectives, contributing partners devised a common methodological approach, analysed four types of primary sources: norms and regulations relevant to networked organisations in the field of cybersecurity; existing networks; academic sources; and interviews with stakeholders.

The comprehensiveness and the complementarity of the primary sources allowed to treat the subject of governance comprehensively (all aspects of governance referenced in the primary sources were structured in 34 "governance issues"); to identify and describe good practices in the elaboration and implementation of business and governance models of collaborative networked organisations; to cluster examples of business and governance models of existing networks and thus indicate possible alternative models in the follow up studies in WP3; and to prioritise governance needs and objectives.

The results in terms of identified best practice, clusters of business and governance models and the prioritised list of governance needs and objectives served to *inform* and *orient* the development of alternative governance models and their evaluation, and not to predetermine the actions of the ECHO research team in follow-up tasks in WP3.

The current deliverable D3.8 is the first update of *D3.1: "Governance needs and objectives"*, submitted in the beginning of February 2020. In addition to a revision and editing of substantial portions of the text of D3.1, this deliverable includes analysis of Regulation (EU) 2021/887 of 20 May 2021 on establishing the European Cybersecurity Competence Centre and Network, analysis of the organizational forms used in existing CNOs, and results from a study of the ECHO partners' expectations regarding the governance model of the future ECHO network.

The second update (D3.9, due in January 2023 - M48) will be used to reflect on key new developments at EU and cybersecurity community levels and contribute to the delivery of a current and consistent package of documents presenting in detail governance requirements, analysis of practice, and the final (within the project duration) ECHO governance and transition models.

Table of contents

List of figures

List of tables

1. Introduction

1.1 Purpose and scope of the document

The long-term objective for the *European network of Cybersecurity centres and competence Hub for innovation and Operations* (ECHO) project following the completion of Horizon 2020 funding, is to transition from a project-based consortium to an established, stand-alone networked organisation, i.e. an organisation composed of independent companies and other entities with complementary competences which collaborate to provide cybersecurity products and services and contribute as a whole for the improved cyber resilience of the EU and Member States. Towards that purpose, the overarching objective of Work Package 3 (WP3) is to develop a governance model of the future ECHO-base network and a plan to transition (change management plan) from Consortium governance and management to Network governance and management. This governance model—as a whole, or the underlying principles and some of its main components—would potentially be of interest for establishing and operating the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres and Competence Community.

The purpose of Task 3.1 “Governance needs and objectives” under the remit of WP3 centres on identifying and prioritising governance needs and objectives and thus to establish requirements to the governance model of the ECHO network. Further, it aims to establish best practices for governance and management of networked organisations to assist the later elaboration of governance models (subject of Task 3.3). The experience of existing networks and the academic publications serve as main sources for identifying good practice. In accordance with the project programme of work, towards that purpose the project team evaluates existing centres of competence in the area of cybersecurity and elicits the opinion and expectations of stakeholders from two types of organisations – potential major customers and other funding organisations. In addition, the team analysed applicable norms and regulations, some of which were expected to codify good practices in the governance and management of network organisations.

Key decisions with respect to the operation of the ECHO network will also be identified in accordance with the business model developed – with a particular focus on the processes of engagement with potential customers, funding and delivery models. These case studies will highlight which governance frameworks need to be prioritised so that the network can be run in an effective and efficient manner.

Thus, in an effort to determine what factors underlie the establishment of a strong and efficient governance model, Task 3.1 “Governance needs and objectives”, under the remit of WP3, pursues three objectives:

1. identifying and clustering existing network business models; analysing clusters vis-a-vis ECHO objectives so as to identify business models of potential utility for ECHO;
2. identifying and prioritising governance needs; and
3. structuring the space of possible governance models of network organisations and providing examples of how existing network governance models fit into that space.

1.2 Structure of the document

This document details the means by which data derived from various sources—existing networks, academic literature, norms and regulations, and interviews with stakeholders—was compiled, collated, analysed and critiqued in an effort to determine what factors underlie the establishment of a strong and efficient governance model. As such the layout of this document reflects the process by which all relevant information was procured and assimilated culminating in recommendations with respect to governance for the ECHO project (following the cessation of Horizon 2020 funding).

The next section of the report presents the *methodological approach* underlying the Task 3.1 study. It describes the process and the methods used to select and analyse norms and regulations, existing networked organisations, academic sources, and to conduct interviews with stakeholders external to the ECHO consortium.

The following three sections are structured in accordance with the three study objectives of Task 3.1, presented above.

The key questions in the elaboration of a future business model relate to the profit or non-profit orientation of the network, the funding streams, and the level of coordination (or centralisation) both in the provision of services and sales of products and in taking decisions on network development. These questions are addressed in Section 3 which - based on the analysis of the academic literature, existing networks and quantitative analysis of the available data - presents good practices and outlines major options for the future ECHO business model.

Section 4 presents needs, objectives and requirements to the governance of networked organisations. It builds on the analysis of all four types of primary sources and concludes with a prioritised list of governance needs and objectives.

Section 5 presents the findings on the governance models and good practices in the governance of networked organisations. It builds primarily on findings from the analysis of the academic literature and existing networked organisations.

Section 7 concludes the report with a summary of the findings and envisioned future activities leading to the two updates of this report, respectively in M36 and M48.

The report includes five annexes. Annex 1 presents a glossary of key terms, while the remaining four annexes list the primary sources used in the study: Annex 2 – the Norms and Regulations; Annex 3 – the analysed academic sources; Annex 4 – the list of interviews; and Annex 5 – the list of analysed networked organisations.

1.3 Relation to other work in the project

This deliverable is an update of D3.1 “Governance Needs and Objectives”, submitted in the beginning of February 2020 and accepted. It differs from D3.1 in the following:

First, after D3.1 was submitted, the study team invested in the dissemination of the publishable results. Six articles and papers have already been published (see Annex 6). In the process of publication, including rigorous peer review, the texts were revised, amended, and edited. The revisions and the editorial changes facilitated the enhancement of the text and have been introduced in the bulk of this report. New findings were added in the process, e.g. the taxonomy of business models of collaborative networks (see section 3.2.5 and in particular Table 6).

Second, in the work on the ECHO exploitation strategy, launched in the Summer of 2020, it quickly became clear that, looking for most suitable organisation, the exploitation teams structured around the main ECHO assets can benefit from the practical experience of existing collaborative networked organisations. Therefore, it was decided to explore the database of CNOs (Annex 5) and identify the organisational modalities, e.g. profit/non-profit orientation of a CNO and some of its constituent elements. The results of that study are presented in the new section 5.4 of this report and have already been published in publication # 6 (see Annex 6).

Third, the discussions on the organisation of the future ECHO network in early 2021 were hindered by the uncertainty regarding interested partners and their roles. Therefore, we decided to solicit the opinion of each partner regarding their likely involvement in structured post-project collaboration and what benefits, conditions or obstacles they see. The approach and the findings are presented in the newly added section 6 in this report.

Finally, in May 2021 the European Parliament and the Council adopted Regulation (EU) 2021/887 for establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.[1] This is a significant normative change, reflected in the respective texts in this report.

1.4 Applicable and reference documents

The following documents contain requirements applicable to the generation of this document:

Reference	Document Title	Document Reference	Version	Date
[GA]	Grant Agreement 830943 – ECHO	-	1.0	02/04/2019
[PH]	D1.1 Project Handbook	ECHO_D1.1_v1.42	1.42	20/10/2019
[PQP]	D1.3 Project Quality Plan	ECHO_D1.3_v1.4	1.4	23/04/2021
[D3.1]	D3.1 Governance Needs and Objectives	ECHO_D3.1_v1.1	1.1	03/02/2020

Table 1: Applicable documents

[1] Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, https://eur-lex.europa.eu/eli/reg/2021/887/oj.

In addition, Annex 2 lists norms and regulations used to identify governance needs and objectives and identify good practices, while Annex 3 presents a list of 60 books, book chapters, and articles subject of analysis. A small number of additional reference sources are included in footnotes.

1.5 Intellectual Property Rights

Based on the legal framework provided in the ECHO Grant Agreement and the Consortium Agreement, ECHO specific IPR procedures have been established to protect the innovations and knowledge developed within this deliverable.

1.6 List of acronyms

Acronym	Description
AACC	Authority Authorised to Conclude Contracts
ACAP	Absorptive CAPacity
BM	Business Model
BN	Business Network
CA	Consortium Agreement
CAB	Change Advisory Board
CCC	Cybersecurity Competence Centre
CEF	Connecting Europe Facility
CFSP	Common Foreign and Security Policy
CN	Collaborative Network
CNO	Collaborative Networked Organisation
COBIT	Control Objectives for Information and Related Technologies
COINs	Collaborative Innovation Networks
COM	Current Operating Mode
CSDP	Common Security and Defence Policy
DOA	Description of Activity
ECCC	European Cybersecurity Competence Centre
ECHO	European network of Cybersecurity centres and competence Hub for innovation and Operations
ECSO	European Cyber Security Organisation
EDA	European Defence Agency
EE	Extended Enterprise
ENISA	European Cybersecurity Agency (previously “European Network and Information Security Agency”)
GA	Grant Agreement
GaaS	Governance as a Service
GDPR	General Data Protection Regulation
GNE	Governance in Networked Enterprises
GRI	Global Reporting Initiative

Acronym	Description
IBAN	International Board of Auditors
ICT	Information and Communication Technologies
IFIP	International Federation for Information Processing
IPR	Intellectual Property Rights
ISAC	Information Sharing and Analysis Centre
ITIL	Information Technology Infrastructure Library
JRC	Joint Research Centre [of the EU]
KPI	Key Performance Indicator
MSP	Microsoft Project
NDA	Non-Disclosure Agreement
OECD	Organization for Economic Cooperation and Development
POW	Programs of Work
PRINCE II	PRojects IN Controlled Environments (PRINCE II)
PSS	Product-Service System
R&I	Research & Innovation
RACI	Responsible, Accountable, Consulted, and Informed (model)
SBM	Social Business Model
SBN	Strategic Business Network
SMEs	Small- and Medium-sized Enterprises
SN	Supply-chain Network
SOCN	Service-Oriented Collaborative Network
SOVO	Service-Oriented Virtual Organization
TLP	Traffic Light Protocol
VBE	Virtual organisations Breeding Environment
VCC	Virtual Customer Community
VDO	Virtual Development Office
VE	Virtual Enterprise
VEE	Virtual Extended Enterprise
VIBBM	Virtual Industry Broker Business Model
VO	Virtual Organisation
VS	Value System
WP	Work Package

Table 2: List of acronyms, initialisms, and abbreviations

2. Methodological approach

This study was organised in four phases, illustrated in a simplified manner in Figure 1. These are: (1) Preparation; (2) Preliminary analysis; (3) Secondary analysis; and (4) Aggregation.

In the ***Preparation*** phase, based on analysis of the project documents, own experience and desktop research, the task leader prepared the preliminary structure of this deliverable, a list of governance issues and issues related to business and governance models of networked organisations and a list of existing networked organisation of possible interest to this study. All these were presented in a preliminary draft, distributed to ECHO WP3 partners for feedback and amendment. An amended draft list was presented by the task leader and discussed during the WP3 kick-off meeting in Brussels on June 3rd.

A final draft list and a template in Excel format to present the analysis of networked organisations were created as a result of these “crowd sourcing” activities. The template was piloted by six ECHO partner organisations, analysing 12 networks in total by using its online version on the ECHO SharePoint repository. The feedback received from piloting the template and the overall analysis process was used to prepare the final template and to clarify information of administrative nature, e.g. the average effort needed to analyse a network organisation. The template is presented in Table 3 below. It includes also detailed instructions for analysing network organisations.

The list of governance issues in this final template served also to construct the questionnaire for interviews with stakeholders and to orient the selection and analysis of normative documents and academic sources.

In the second phase of ***Preliminary analysis*** partners analysed in parallel three types of sources: existing network organisations, norms and regulations related to the governance of networked organisations in the field of cybersecurity, and academic literature. The fourth source of information came from conducting interviews with stakeholders. The sub-sections below provide detail on methods of selection and analysis.

In the phase of ***Secondary analysis***, a small group of researchers, working individually or in teams of two, analysed the results of the preliminary (or primary) analysis for each type of primary source. In regard to governance needs and objectives, the content analysis was complemented by quantitative analysis – all governance issues were placed in four tiers, depending on the number of times a certain issue was addressed in the respective types of sources. Placement in a higher tier is indicative of a higher interest to that governance issue, and hence it is likely of a higher priority.

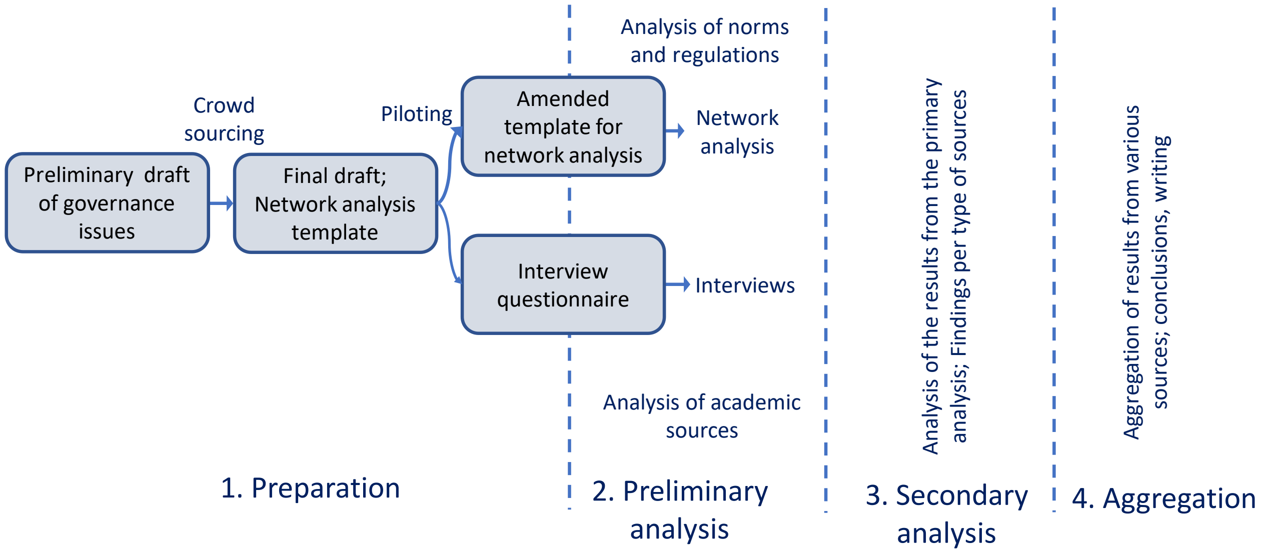
Analysis of norms and regulations
Crowd sourcing
Piloting
Preliminary draft of governance issues
Final draft; Network analysis template
Amended template for network analysis
Network analysis
Interview questionnaire
Interviews
Analysis of academic sources
Analysis of the results from the primary analysis; Findings per type of sources
Aggregation of results from various sources; conclusions, writing
1. Preparation
2. Preliminary analysis
3. Secondary analysis
4. Aggregation

Figure 1: Methodological approach.

The final phase of ***Aggregation*** of results from various sources allowed to highlight the key issues in business and governance models of network organisations and, in particular, to prioritise governance needs, objectives, and requirements.

The methodologies for the new studies conducted during the update are presented in the respective newly added sections 3.2.5 and 5.4, as well as in Chapter 6.

2.1 Existing networks: primary analysis

This phase involved partners collating and analysing data with respect to existing networks. The list of networks included four types of networks:

- Networks dedicated to information/cybersecurity research and services;
- Cybersecurity incubators/ accelerators/ tech parks/ ecosystems;
- Other research-intensive networks;
- Networked organisations providing (among others) information services.

Each contributing partner was assigned a specific set of existing networks to analyse. To ensure that the scope of the analysis was inclusive and robust, networks which operated worldwide were also selected, not just those which originate from European Union countries.

When the publicly available information on a certain network was not sufficient to analyse it properly, the respective partner could either select from networks unassigned at the time (the full list contained more than 100 networks) or suggest to the task leader another network. Such suggestions were approved with the exception of two cases, when the suggested networks consisted of geographically distributed entities, each one with specific competences in the field of cybersecurity, but all part of a larger hierarchical organisation. The reason for rejection was that the governance mechanisms of those networks were defined beyond their boundaries, largely adhering to some more general governance principles and regulations.

A comprehensive template was devised to capture inputs from partners, wherein relevant data was accounted for using the captions outlined in Table 3 which was uploaded to the ECHO SharePoint. A hyperlink to the Excel file was circulated to partners shortly thereafter seeking analyses of assigned Collaborative Networked Organisations (CNO's). Partners were also tasked with uploading key governance/management documentation relating to the respective network into the relevant sub-folder on the T3.1 SharePoint location.

A total of 92 CNO's were assessed during the primary analysis phase. The full list of these networks is included in Annex 5.

Excel Template Captions

Administrative information	
Network Code	
Short name	
Responsible ECHO partner	
Date the analysis is uploaded or amended	
General information	
Network name	
Website	
Year established	
Number of members	
Number of countries represented	
Restricted to EU countries	Y/N
Restricted to EU and Associated countries	
Type of partners (select all applicable types)	
` Public sector (e.g. central or local government body)	
` Defence/military	
` Academia/Research	
` Foundation	
` Company	
` Individuals	
Annual budget	
Main markets/customers	
Main products and services	
Applicable sectors	

Legal status	
Does the network have a legal status?	Y/N
Legal name	
Legal form	
Country of registration	
Duration according to the statute	
Goals according to the statute	
Is the network a for profit organisation?	
How profit is distributed among members?	
Rights of members	
Obligations of members	
Business model	
Income streams/funding model	
Provision of services & sales of products	
Network development/Investment decisions	
Outreach/ Dissemination strategy	
Other features of interest	
Definition of governance needs and objectives	
Please be short and precise in extracting governance requirements, goals, objectives	
Governance model	
Senior decision-making body, e.g. Board of Directors, and powers	
Mechanisms for assuring fair representation on the Board	
General Assembly (or equivalent); powers	
Working Groups/Panels	
Decision making rules (e.g. by consensus, simple or qualified majority; one organisation – one vote or weighted votes; …)	
List the external stakeholders and the modalities of their involvement, e.g. through an “Advisory Board”, Supervisory bodies of representatives from outside/above the network, etc.	
Policy (model) to allow partners to enter or exit the network (to allow partners to enter or exit the network)	
Does the network have a secretariat? If Yes, please describe	
` Personnel size of the secretariat	
` Annual budget of the secretariat	

Governance model	
Other executive functions in the network (e.g. CEO, operations, resources, finances, security, technology, strategy, … Where possible, please provide the "job descriptions")	
Other organizational bodies of interest	
Key governance documents (List with links to key governance (and management, where available) documents, e.g. strategy, policies, organizational structure, manning list, business plan, financial plan, partnership development plan, performance measures/KPIs, risks register, annual reports, financial statements, audit reports, etc.)	
Standards and methodologies adopted (List standards or methodologies on which it is based the day by day governance and management of the Hub, e.g. COBIT 5, SCRUM, etc.)	
Financial management arrangements	
Auditing – internal and external	
Dispute/conflict management	
Confidentiality (Rules, NDAs, …)	
Intellectual Property – IPR rules and provision	
Codes, applicability – Codes, applicability	
Specific ethical issues, e.g. in regard to slavery, labour of minors, etc.	
Gender policies , e.g. equality, representation, etc.	
Other good governance issues, e.g. transparency, integrity policy, etc.	
References	
List the key governance/management documents with links; Number and upload the files in the respective sub-folder on SharePoint	

Table 3: Template for analysis of networked organisations.

2.2 Norms and regulations: primary analysis

With respect to the norms and regulations that can influence networks which are similar in design to the ECHO project in terms of structure, three types of documents were reviewed:

1. EU norms, with focus on the 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. Initial governance models of ECHO and the other three consortia – ECHO grant and consortium agreements, project handbook; DOAs and CAs (if available) of the other three pilot projects;
3. Relevant national regulations.

The ECHO project is concerned with norms which are relevant to networks comprising independent entities, ideally both public and private, profit and non-profit, but NOT to networks of organisations that are in hierarchical relationship or with common ownership.

The list of identified norms and regulations is presented in Table 4. Although EU member states have already identified their national cyber coordination centre (R 887/2021), no national regulations on establishing collaborative cybersecurity networks have been identified so far.

ID	Document	Type	Source
R887, 2021	Regulation of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres	EU Regulation/ Document	https://eur-lex.europa.eu/eli/reg/2021/887/oj
CA, 2019	Cybersecurity Act	EU Regulation/ Document	https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act
Incidents & Crisis	EC Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises	EU Regulation/ Document	http://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-6100-F1-EN-MAIN-PART-1.PDF
RDD, 2017	Joint Communication to the European Parliament and the Council “Resilience, Deterrence and Defence: Building strong cybersecurity for the EU”	EU Regulation/ Document	https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450
NIS, 2016	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, 2016)	EU Regulation/ Document	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC
Pilots	Pilot Projects - Overview analysis	H2020 Contractual document	
Pilots HB	Pilots Handbook	H2020 Contractual document	
ECHO GA	ECHO Grant Agreement	H2020 Contractual document	
ECHO CA	ECHO Consortium Agreement	H2020 Contractual document	
ECHOPH	ECHO Project Handbook	H2020 Contractual document	
Concordia GA	CONCORDIA GA - part B	H2020 Contractual document	
Concordia Proposal	CONCORDIA Proposal	H2020 Contractual document	
Cyber4EU	CYBERSEC4EU RIA - IA Part B	H2020 Contractual document	
Sparta DoA	SPARTA DoA - Part B	H2020 Contractual document	

Table 4: Summary of norms and regulations sources.

Akin to the examination of 'existing networks', an MS Excel matrix was devised to collate and summarize norms and regulations data; Table 5 provides an overview of the captions used to gather relevant information.

Norms and Regulations – Excel Matrix Captions	
1	Document
2	Explicit Requirements
3	Implicit Requirements
4	Expectations to the governance of networks
5	Governance Structure/ Roles and Responsibilities
6	Particular Feature (Differentiator)
7	Points of Strength (with regards to Pilots)
8	Points of Weakness (with regards to Pilots)
9	Processes and procedures

Table 5: Norms and regulations – summary table of captions.

2.3 Academic literature: primary analysis

The following approach was used to identify and select academic publications for the primary analysis. At the first stage, an extensive search was conducted in the SCOPUS database using two key phrases: "networked organizations" and "networked organisations", correspondingly in US and UK spelling of the English language. The search was then specified adding the term "collaborative". The results gave a set of 543 publications. Figure 2 illustrates the dynamics of these publications.

The first review of the search results showed that while publications on networked organisations appear already in the early 1990s, the field is dominated by publications out of the EU-funded ECOLEAD project [2] in the EU Sixth Framework Programme (the peak of the chart below coincides with the end of that project) and follow up publications of key researchers, including in the IFIP PRO-VE series of conferences of virtual enterprises, published by Springer in the series "IFIP Advances in Information and Communication Technology".[3]

At the second stage therefore the research team:

- read the abstracts of the publications to identify those that would be useful from the viewpoint of presenting and discussing governance needs and various aspects of business and governance models of networked organisations;
- looked to add authors beyond the European Union;
- gave preference to open access publications;

[2] The ECOLEAD (European COllaborative networked Organisations LEADership) project involved 27 industry and research organisations from 13 EU Member States, Mexico and Brazil. See, for example, David Romero, Servane Crave, Nathalie Galeano, and Arturo Molina, "Experiences of ECOLEAD Research Project: Working in a Cross-Cultural and Multidisciplinary Professional Virtual Community," *4th International Conference on Intercultural Communication Competence, "Building Bridges across Educational Communities: World Class Practices in Higher Education,"* Monterrey, Mexico, February 2007.

[3] See https://www.springer.com/series/6102.

- searched for books presenting comparative analyses and benchmarking studies of collaborative networked organisations; and
- gave some preference to more recent publications.

As a result, the team selected 60 publications for further analysis, illustrated in Figure 3. While half of the publications in the Scopus generated set were published in the last decade, that percentage is 72 % for the set selected for primary analysis.

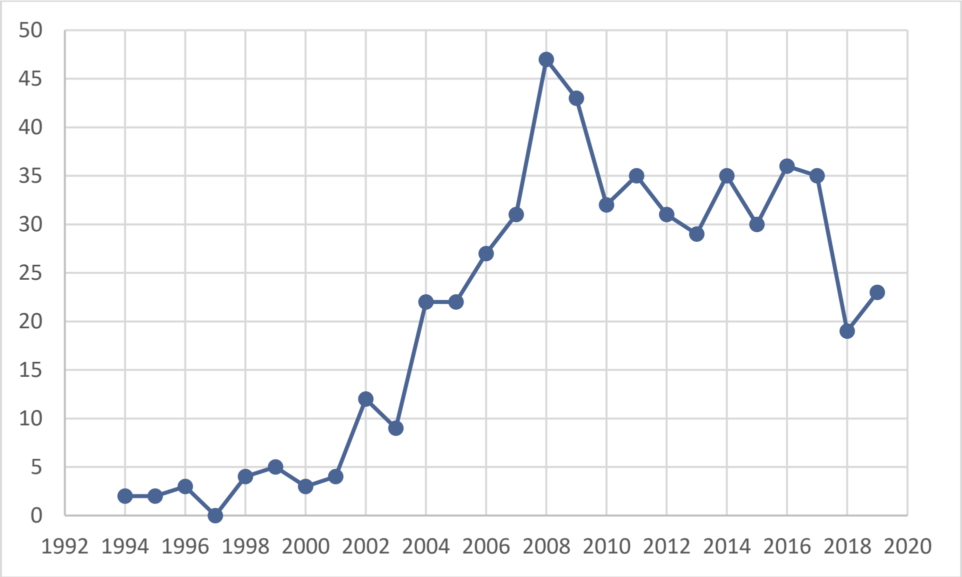

Figure 2: Academic sources in a Scopus search.

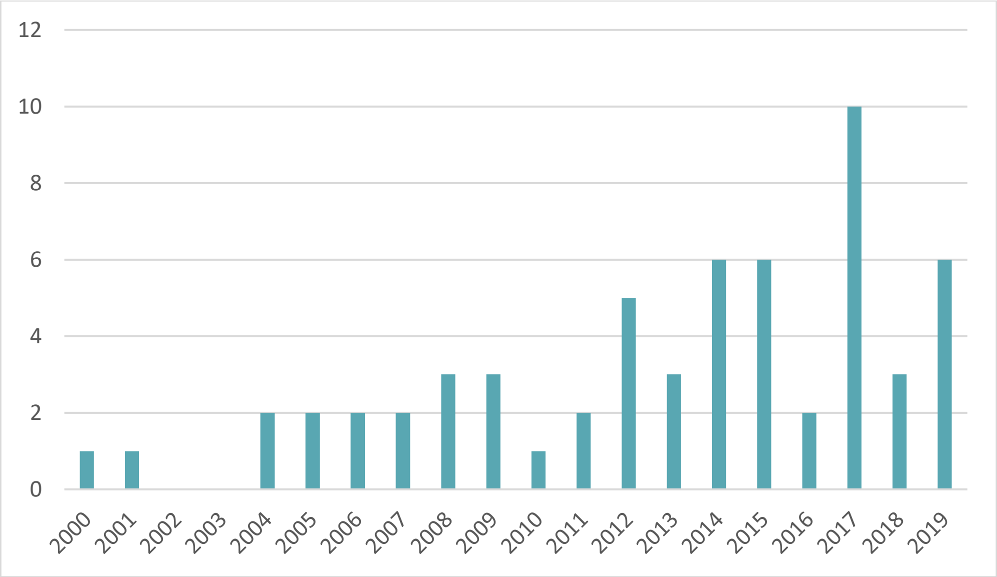

Figure 3: Academic sources selected for primary analysis.

An MS Excel template was created to structure the analysis which contains the following attributes: bibliographic information, short reference, year of publication, ECHO partner responsible for the analysis, countries of origin of the authors, abstract, keywords, focus of the article, business model issues (the type of the business model: centralised vs decentralised, type of funding: public budget vs customer funded, for-profit vs non-for profit organisation); governance model; good practices identified and other statements of potential interest to ECHO. The articles were assigned for analysis to three ECHO partners: BDI, IICT and TME.

2.4 Interviews

The views of major stakeholders are of significant importance for elaborating the governance model of a networked organisation in the field of cybersecurity. ECHO partners were asked to use their institutional and personal connections to approach with a request for an interview with mid- to senior-level representatives of funding organisations and potential major customers who have a tangible impact on decisions to allocate resources.

Nine ECHO partners identified and accepted to approach 12 potential interviewees. By the time of writing this report, eight of these partners had provided transcripts, in English, of nine interviews. Three of the interviewees came with current or recent experience in organisations funding cybersecurity research and technology development, and six came from potential major customers of cybersecurity products and/or services.

A structured questionnaire was used for the interviews. It included questions on the 16 governance issues (Table 3) identified in the *Preparation phase* of the study (as presented earlier in Figure 1) and an open question on additional governance issues of importance. There was a slight variation in the first question depending on whether the interviewee represented a funding organisation or a potential customer. Annex 4 presents the questionnaire for an interview with a representative of a potential major customer.

The team prepared also a privacy statement to assure compliance with GDPR. Every one of the nine interviewees signed this statement prior to giving the interview.

During the follow-on analysis, the research team used both content analysis techniques and a quantitative analysis in order to prioritise governance needs, objectives, and requirements.

3. Business models of network organisations

The governance model of any organisation, including networked organisations, builds on and reflects the specific needs of the selected business model of the organisation. Therefore, the analysis in this report starts with identification of requirements to, good practices and patterns of business models of collaborative networked organisations. The analysis of EU norms and project documents, academic sources, and existing networks allows to shed light on existing or anticipated requirements and business models. The results of the analysis are presented in the three sub-sections below.

3.1 Network business models in normative documents

EU regulations do not address explicitly business models of cybersecurity networks; yet, it is possible to outline main expectations in that regard. Regulation 887 (R 887, 2021) is the main Regulation aiming to establish the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres and Community. The *National Coordination Centres* should be selected by Member States. In addition to the necessary administrative capacity, Centres should either possess or have direct access to cybersecurity technological expertise and should also have the capacity to effectively engage and coordinate with the industry, the public sector, including authorities designated pursuant to the Directive (EU) 2016/1148 of the European Parliament and of the Council (NIS, 2016), and the research community. The *Cybersecurity Competence Community*, which would involve a large, open, and diverse group of actors involved in cybersecurity technology, should include in particular research entities, supply-side industries, demand side industries, and the public sector.

The European Cybersecurity Industrial, Technology and Research Competence Centre, together with the Cybersecurity competence network, will also work towards supporting research to facilitate and accelerate standardisation and certification processes, in particular those related to cybersecurity certification schemes in the meaning of the Cybersecurity Act (CA, 2019). In September 2017, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a Joint Communication on *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU* (RDD, 2017) to further reinforce the Union's resilience, deterrence and response to cyber-attacks.

Other governance regulations can be elicited from the guiding documents of each of the four projects (ECHO, CONCORDIA, SPARTA, CyberSec4EU) and ECSO, which have differing yet complementary approached to shared common goals. They are in fact networks, seen also as the *Competence Centres*.

3.2 Network business models in the academic literature

The term "business model" (BM) is used for a broad range of informal and formal representations of core aspects of a business, including its *purpose*, *target customers*, *strategies*, *offerings*, *business processes*, *organizational structures*, *infrastructure*, *sourcing*, *trading practices*, and *operational processes* and policies in regard to *culture*.

According to Afuah and Tucci (2001), a business model explains how a business “creates, delivers and captures value” in a relationship with a network of exchange partners.[4] In another level of abstraction Gassmann, Frankenberger and Csik (2014) describe the BM as an archetype of 55 different BM building blocks that can be combined in various ways to accommodate the BM in which the business operates (quoted in Aagaard, 2019).

3.2.1 Traditional vs digital BMs

Traditional BMs are centred on a single company. With the rapid developments of digital infrastructures and the Internet of Things (IoT) ecosystem, firms increasingly collaborate with competitors and across industries, and that makes traditional BMs less adequate. Moreover, to succeed and remain competitive in rapidly changing market environments, companies—particularly those in technology-related industries—must quickly adapt to market challenges.

The analysis of the selected academic literature allowed to identify new ideas for BMs, applicable to networked organisations. In a recent publication, Aagaard (2019) elaborated on the concept of *Digital Business Models* (DBMs) and identified a trend of growing interest in digital transformation. However, the DBMs remain in the early stages of development. Hence, the author addressed the BM concept as the “missing link between business strategy, processes, and information technology” (IT), suggesting three distinct venues of application: a product-oriented, examining business models of IT industries; a process-oriented, focused on the use of IT to enhance BMs; and support-oriented, examining IT as a toolbox in developing and managing business models.

The use of BM frameworks provides advantages in three areas by offering: (a) a “common language” facilitating dialogue; (b) an opportunity to experiment with ideas using scaled-down representations; and (c) representations that help to direct resources and increase legitimacy.

Aagaard further identified six frameworks for business model innovation. Three of them—the *Business Model Canvas*, *Business Model Navigator,* and *Value Design Model*—are considered traditional, and another three—*DNA Model*, *BM Type for IoT*, and *IoT Business Model Framework*—are more recent digitally-focused frameworks adequate for IoT studies.

3.2.2 Ad-hoc, Long-term and Goal-oriented Collaboration

In many of the analysed publications, the authors examine collaborative networked organisations (CNOs) as the answer to the increasingly fluid and competitive global business environment. The Virtual organisations Breeding Environment (VBE) enhances the opportunities to respond swiftly by creating Virtual Organisations (VOs), and a sound VBE management system can automate the process of VO design (Ardakani, Hashemi, and Razzazi, 2019).

The VBE is one type of CNO, aiming to establish long-term strategic collaboration. The interrelations between various types of networked organisations are presented in Figure 4 (adapted from figure 3 on p. 10 of Camarinha-Matos, Afsarmanesh, and Ollus, 2008).

[4] Allan Afuah and Christopher L. Tucci, *Internet Business Models and Strategies* (New York: McGraw-Hill, 2001).

A VBE is defined as "an association of organisations and related supporting institutions adhering to a base long-term cooperation agreement, and adopting common operating principles and infrastructures, with the main goal of increasing both their chances and preparedness towards collaboration in potential Virtual Organisations" (Msanjila and Afsarmanesh, 2007). Further, the authors of the same study define the Virtual Organisation as an association of (legally) independent organisations that combine their resources and skills to exploit an emerging opportunity in a common interest and use the opportunity's specific requirements in terms of competencies, market position, trust, etc., to select suitable VBE members and configure the VO. The creation of the respective VO is supported by a number of VBE management sub-systems, including:

- the *trust management* sub-system assisting a variety of VBE users – the planning team for the new organisation, the administrator of the VBE, member organisations, external stakeholders and others dealing with trust management in the VBE;
- the *decision support* sub-system providing services supporting the monitoring of a number of indicators in the VBE, notifying and warning users for deficiencies in performance, emerging gaps in VBE competencies, or diminishing trust in a member organisation;
- the *information management* sub-system storing in the VBE profile information on created VOs.

In the fluid and complex environment in which current Small and Medium Enterprises (SMEs) are competing, many already opted for establishing collaborative networks with the aim to add necessary capabilities and to benefit from the access to more resources, e.g., knowledge and skills.

Companies see the involvement in CNOs as a way of protection from current and future competitive risks while becoming more attractive and getting access to new markets (Bandinelli, d'Avolio, and Rinaldi, 2014). The framework for collaboration needs to be process-oriented and sufficiently flexible to cover all core business processes of the member organisations.

Most forms of CNOs (see Figure 4) imply specific roles, governance rules, and procedures for their constituents (Camarinha-Matos and Afsarmanesh, 2008). These can be described in a generic reference model, which is then used to facilitate the derivation of specific models for particular cases. The reference model defines a common basis for understanding and explaining—at a high level of abstraction—the various manifestations of the collaboration paradigm, and can be used to facilitate the design of particular models for specific collaborative organisations.

Two main venues are used for creating reference models of virtual enterprises (VE)/virtual organisations:

- *Enterprise-centric*, starting from the extensive past modelling activities at the enterprise level and incrementally extending and adapting such models to the needs of CNOs; and
- *Network-centric*, focusing on the networks and their properties, and not on their distinct organisational components.

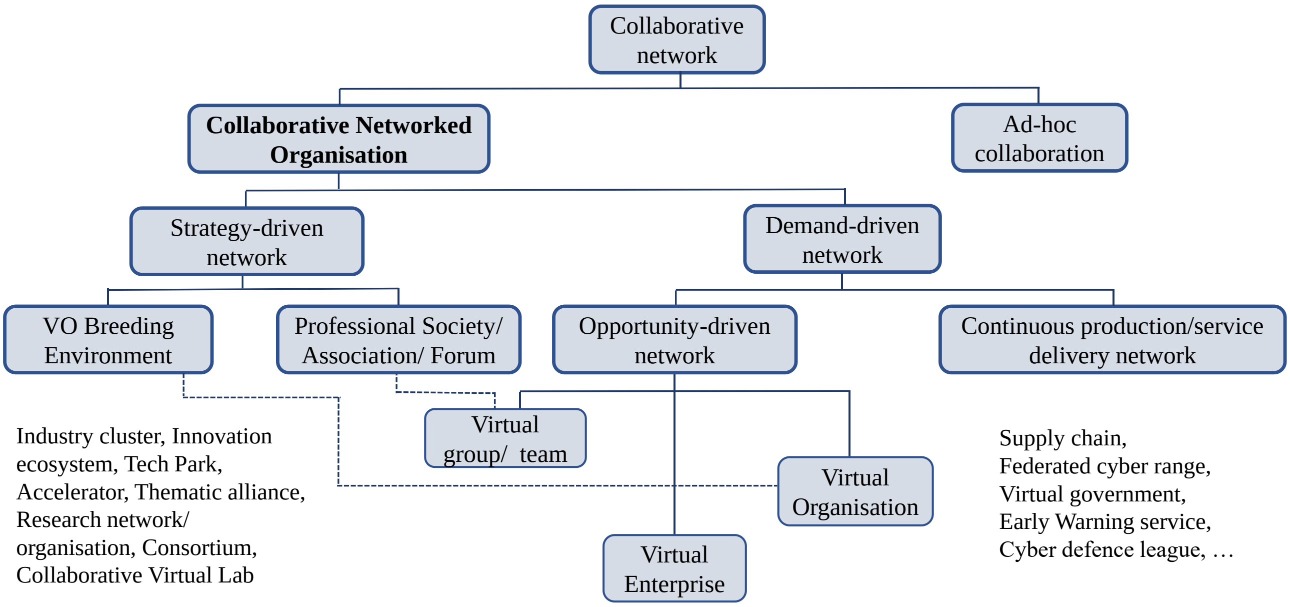
Collaborative network
Collaborative Networked Organisation
Ad-hoc collaboration
Strategy-driven network
Demand-driven network
VO Breeding Environment
Professional Society/ Association/ Forum
Opportunity-driven network
Continuous production/service delivery network
Virtual group/ team
Virtual Organisation
Virtual Enterprise
Industry cluster, Innovation ecosystem, Tech Park, Accelerator, Thematic alliance, Research network/ organisation, Consortium, Collaborative Virtual Lab
Supply chain, Federated cyber range, Virtual government, Early Warning service, Cyber defence league, …

Figure 4: A taxonomy of collaborative networks
(adapted from Camarinha-Matos, Afsarmanesh, and Ollus, 2008).

Also, several studies of virtual organisations emphasise the role of ICT tools and digital infrastructures in supporting collaboration. Camarinha-Matos and Afsarmanesh (2008) provide additional examples of potential interest:

- The *Grid community*, moving towards virtual organisations with the business perspective into account, as demonstrated by the Enterprise Grid Architecture initiative;
- *e-Government* – a broad concept, including the cooperation among many governmental organisations, as exemplified by the US Federal Enterprise Architecture;
- Studies of *social networks* and *virtual communities* utilising for example graph theory to identify basic properties of the networks; and
- *Collaborative networks roadmapping initiatives*.

In the influential definition of Camarinha-Matos et al. (2009), a collaborative network (CN) is an alliance comprising a variety of entities (e.g., organisations and people) that are “largely autonomous, geographically distributed, and heterogeneous in terms of their operating environment, culture, social capital, and goals, but that collaborate to better achieve common or compatible goals, and whose interactions are supported by a computer network.”

Other forms of collaboration, such as in virtual communities or volunteers’ contributions to disaster management, are more spontaneous and have no overarching plan, nor organisation in place. Nevertheless, such *ad-hoc collaboration* processes contribute to resilience and are already codified in international standards.[5] A related example from the cybersecurity domain is the Estonian Defence League’s Cyber

[5] ISO 22319:2017 “Security and resilience – Community resilience – Guidelines for planning the involvement of spontaneous volunteers,” 2017, https://www.iso.org/standard/66951.html.

Defence unit Estonian cyber defence league that brings together volunteers for the purposes of the national cyber defence.[6]

Goal-oriented CNOs are of two complementary types: one group is formed by those seeking intensively to exploit a new opportunity (to the right in Figure 4). In contrast, others try to establish long-term strategic alliances, build knowledge trust, and other conditions for the agile configuration of collaborative networks when opportunities arise (Camarinha-Matos and H. Afsarmanesh, 2008).

3.2.3 Examples of Business Models of Collaborative Networked Organisations

Many case studies in the analysed academic publications present examples of CNOs illustrating the state of applicability of CNO concepts in manufacturing industries. Camarinha-Matos et al. (2009) draw some general conclusions from these cases regarding the main characteristics of Virtual organisations Breeding Environments (VBEs):

1. Small and medium enterprises (SMEs) are often the main entities involved in VBEs, with integrators, brokers, and sub-networks appearing in some cases. Universities, national and regional development agencies, and funding organisations are often part of the VBEs intending to facilitate and enhance the performance of the network.

2. Membership in a VBE could be at different levels. For example, an organisation may become an "accredited member" after it successfully passes an evaluation or accreditation process. If such a process is not mandatory in the VBE, the definition of the actual profile and competencies of a prospective member remains a key issue.

3. Typically, a VBE is not limited to a single industry sector; member organisations usually belong to complementary sectors or a supply chain. VBEs can exhibit both vertical and horizontal chain integration.

4. In many cases, regional collaboration drives the establishment of analysed VBEs seeking enhanced competitiveness of a specific region or industry sector in a geographical area by creating a regional ecosystem. A possible explanation is in the incentives offered by local or regional support institutions to SMEs in a given country or region to sustain its social and economic development.

5. Among the core business processes common to the studied VBEs are:

- Processes supporting the *network creation and enhancement*: partner's profiling, partners' accreditation, training, and education;
- Processes supporting the *creation and management of virtual enterprises/organisations*: marketing and commercialisation tasks, identification and assessment of business opportunities, brokerage, search for new partners, quotation, support in negotiations, project management, and quality assurance, support for export, customer relationship management;
- *Innovation and technology processes*: supporting research and technology development, entrepreneurship programmes, and intellectual property rights services;

[6] K. Kaska, A.-M. Osula, and J. Stinissen, The Cyber Defence Unit of the Estonian Defence League: Legal, Policy and Organisational Analysis. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013. By the time of writing this report, it is a fully established part of Defence League and hence not an example of ad-hoc collaboration.

- *ICT processes*, supporting service delivery through ICT tools and, increasingly, internet-based applications;
- *Complementary processes*, e.g. specialised training, financial support, tools for collaboration, job search, advertising, and public relations.

6. The VBE governance arrangements depend on its statutory documents and the possibilities offered by the applicable legal framework. Commonly, VBEs are established as industrial associations or networks coordinated by a designated company (or companies).

Recent advances in the ICT that support network collaboration have provided opportunities to transition from primarily data-driven environments to cooperative environments driven by information and knowledge. The sharing of knowledge and know-how at the network level, the adoption of common best practices, and web-based applications enhance individual companies and enable the implementation of the CNO concept in the manufacturing industry.

Some publications (e.g. da Silva and de Almeida, 2017) describe the virtual organization's business model as a distributed, geographically dispersed, ongoing, dynamic self-restructuring network of independent win-win partners that extends the internal, enterprise-level organisation by cooperative processes. These processes are driven by market and demand, relationships of trust coordinated and aligned with internal systems, opportunities to share information, knowledge, costs, and risk, and are supported by a common IT infrastructure.

The goal of a virtual organisation is to address mostly short-term business opportunities in fast-changing markets, to spot challenges and realise value by achieving more together, by focusing on distribution, on knowledge development and innovation.

A VO might be led, designed, and cared for by a so-called 'broker,' 'entrepreneur,' or 'promoter,' who is legitimized by his/her focal position within the network, his/her social competence and also by the customer to be served. A VO might involve both cooperation and competition, or 'co-opetition,' among the partners. These customer-centric networks aim to combine intelligently the complementary competencies of partners, professional services, known routines, and resources for the period needed to realise the added value. Thus, a company may overcome the limits of its internal growth generated by regulations and hierarchies.

Six main roles contribute to its strategic positioning by facilitating requirements specification, organising, managing, and overseeing the VO (da Silva and de Almeida, 2017):

1. the *broker* who acts as an entrepreneur and is responsible for the sale of the competences of potential virtual factories and for acquiring new projects for the VO. The broker must be both willing and able to create opportunities actively and to extend existing competences of VO partners beyond their primary business lines through interaction with stakeholders, to discover the value that partners possess, but is not yet exploited;
2. the *competence manager* who engineers the 'value system,' selects the most suitable partners by delivering the engineering knowledge to meet customers' needs. Experience of value systems has revealed that engineering services are independent competences not necessarily linked to manufacturing. They are needed to back the ability to design and to engineer complete customer solutions;

3. the *project manager* who keeps performance within time and budget constraints and can re-engineer processes, e.g., to replace partners. In general, the project manager organises the response to a customer request without actively encouraging or looking for new work;
4. the *in/outsourcing manager* of each network partner that provides a dedicated interface by offering know-how, technology, and resources for the network, representing the interests of his/her company;
5. the *auditor* who provides the business environment with neutral financial solidity, which is crucial, especially when there is no track record for the customised on-demand engineered value system;
6. the role of the *network coach* is not related to a business opportunity. Among his or her tasks is the performance of governance functions in the networked organisation, business rules and routines for cooperation, provision of technological infrastructures, and relationship management.

The VBE is a long-term association, and its members come from among the organisations meeting the criteria, defined by the VBE creators or administrators. The virtual organisation, on the other hand, is a temporary consortium or association of independent entities triggered by a specific collaboration opportunity, and its partners are selected primarily from among the VBE members.

Views on some key aspects of CNO business differ. Some authors question the traditional understanding of the centralization/ decentralization issue as an important factor in constructing an organization (Komanda, 2012). They prefer instead to focus on aspects of network design considered crucial for achieving competitive advantage: specialised and complementary resources, joint control over them, and a common goal. Respectively, the key issues that must be resolved in the process of network design are the allocation of tasks and decision-making powers and a smooth process of communication between members of a network to achieve a synergistic effect, often by using advanced communication technologies in the implementation of the tasks.

Further, a classification of networks is suggested by Komanda (2012) in accordance with:

- High or low level of formalisation of cooperation, e.g., imposing binding rules of operation within a network system (franchising is one example of a high level of formalization);
- The horizon of the existence of the network, which is closely related to its purpose;
- Informal level of cooperation;
- Nature of the entities – complementing resources or competitors, characteristics of organisations, and social groups forming the network.

Among the essential issues are also the roles of formal and informal groups within the organisation, the objectives of these groups, and the quality of issues of leadership (Komanda, 2012).

In multinational research projects of non-profit organisations like ATLAS,[7] analysts have identified a specific—*disaggregated*—organisational form of collaboration. While ATLAS is in some ways a unique knowledge-intensive enterprise, the collaboration model it offers relies on effective exchange of knowledge across non-hierarchical networks (Mabey and Zhao, 2017).

Another view on collaboration is that of business processes and services of Service-Oriented Virtual Organisations (SOVO). SOVO quickly adapt to meet the requirements of the competitive and fluid

[7] ATLAS Network, https://www.atlasnetwork.org.

environment in which they operate. Towards that purpose, a SOVO implements efficient and transparent change management solutions used to facilitate adaptation and transformation (Obidallah, Raahemi, and Alaieri, 2014).

A related concept is that of a Service-Oriented Collaborative Network (SOCN), which supports collaboration among members of a network through their shared business services (Sargolzaei and Afsarmanesh, 2017). Compared to traditional collaborative networks, SOCN promotes the reusability of shared software services. A set of sub-systems is designed and interconnected within a common implementation architecture, supporting the necessary functionalities. Each VO partner is expected to announce their services in a directory of shared services, to be identifiable and accessible for all other partners in the virtual organisation.

Some publications focus on the lifecycle of the Virtual Enterprise (VE), where partners share assets and sensitive information and execute intra- and inter-organisational business processes in a coordinated and secure way (e.g. Rabelo, Costa, and Romero, 2014). VE partners remain independent enterprises and maintain their own business strategies. Therefore, it is necessary to properly govern a VE so that conflicts among partners are minimised, and the risks for achieving the VE goals are reduced.

Some related works on VBE and VE governance assume that a given VE should, as a rule, inherit, at least partially, the governance model of the VBE to which partners belong. This is justified since the VBE already imposes on its members a set of common principles, operating rules and procedures. Keeping the particular VE governance model aligned to that of the VBE allows us to utilise its bylaws and preserve the VBE values (Rabelo, Costa, and Romero, 2014).

Requirements, customer requests, and commercial rules associated with a collaborative business opportunity have a profound impact of many aspects of the VE's business model and the way it is managed, e.g., the applicable legal framework, logistics routes and type of logistics partners, the decision-making roles of partners, and the influence of customers. Therefore, additional and complementary coordination instruments often need to be created. The respective general governance framework can be classified as "buyer-driven, relational value chain and core-ring with a coordinating firm" (Rabelo, Costa, and Romero, 2014).

One important goal in designing business models, and DBMs in particular, is building a community based on a value proposition attractive for societies. This is reflected in the concept of Social Business Models, SBMs (Jabłoński and Jabłoński, 2020). SBM goals need to be socially accepted and are expected to solve problems universally, regardless of cultural factors. Arguably, the concept of Social Business Models is adequate for the needs of the globalised economy. It allows for the achievement of expected financial results while, at the same time, respecting ethical and environmental concerns. SBMs fit in with social expectations through the types of created value. Accordingly, only socially acceptable ideas generating positive results in terms of business ethics could exist in the modern business space. Implementing these ideas, collaborating organisations can deliver a socially attractive value proposition to recipients (Jabłoński and Jabłoński, 2020).

The *Virtual Customer Communities* (VCCs) are a type of networked organisations aiming at value co-creation and co-innovation (Romero and Molina, 2011). Both CNOs and VCCs look at the network structures as a source of joint creation of value and open innovation facilitated by easier access to knowledge, new technologies, skills and markets, and by complementing partners' competencies and sharing risk. Such collaborative endeavours can enhance the adaptability and flexibility of VCCs' value-creation capacity to react to external drivers such as emerging business opportunities, to follow the industry dynamics and the changing needs and preferences of customers. Value co-creation is seen as the new trend in open-business models integrating organisational competencies and involving customers into network and community formation for the purposes of co-creation (Romero and Molina, 2011).

Saetta, Tiacci, and Cagnazzo (2013) consider the experience of the CNO “Gruppo Poligrafico Tiberino,” Italy, as one of the most thought-provoking. This was the first networked organisation in the country that adopted a model with a Virtual Development Office (VDO) – an innovative model with a particular focus on SMEs. Existing forms of collaboration evolve in the direction of extending ‘classical’ collaboration fields of product, service development, and supply chains. However, this is more challenging when collaboration is among SMEs, and a lead company is missing. The VDO model was introduced to overcome this limitation and stimulate innovation in networks of SMEs (Saetta, Tiacci, and Cagnazzo, 2013).

Several organisations may act as a VDO in a decentralised manner. There are several options for such VDO to satisfy a particular business opportunity: selecting the most appropriate companies from the network and thus creating either a virtual enterprise; creating a virtual organisation when public agencies, funding institutions or research centres are required; or creating a Virtual Extended Enterprise (VEE) if the participation of companies external to the network is necessary. In this particular case, the VDO business model is for-profit and includes three firms providing a range of complementary competencies and services, and characterised by a partnership based on a solid personal knowledge of the entrepreneurs, who decided to form a new company and to involve academia (University of Perugia) to drive the company strategy (Saetta, Tiacci, and Cagnazzo, 2013).

3.2.4 Forms of Collaboration, Processes and Roles

Two essential characteristics of collaborative business models are (1) the *multi-value perspective*, taking into account economic and social value and the value of acquired knowledge; and (2) the multi-stakeholder approach combined with transparency on the contribution of each stakeholder to the value created by the network (Romero et al., 2006).

Many of the analysed publications focus on knowledge management and organisational processes in CNOs, arguing, for example, that the success of networked organisations is based on the quality of management of informal processes and activities that are not codified as business practices (Barchetti et al., 2012). The main challenge is to organise knowledge activities and integrate them with business processes; otherwise, the networked organisation faces limits on its growth. Besides, companies face the challenge of preserving social capital through “knowledge workers” (Barchetti et al., 2012). The business model must envision supporting information systems allowing knowledge workers to access and use the right information at the right time and in a suitable format.

Three main types of problems in CNOs have been identified:

1. Collaboration issues, related to the design of rules, procedures, and infrastructure for collaboration among people working towards a specific goal;
2. Problems of coordination, i.e., keeping on record exchanges of data during cooperative activities and avoiding information losses; and
3. Problems of know-how elicitation, i.e., related to the design of recurrent activities and involving the risk of losing information essential for the company.

Many of the analysed publications focus on the collaborative environment supporting the exchange of information and knowledge, and coordination of actions in geographically distributed (decentralised) networked organisations. A strategic view of a network organisation considers it "long term purposeful arrangements among distinct but related for-profit organizations, which allow those firms therein to gain or sustain competitive advantage" (Santoro, Borges and Rezende, 2006). A network organisation functions in a new type of environment, allowing people to organise themselves towards a common or shared objective. To solve complex problems, the environment enables the interactions among people bringing in a multidisciplinary perspective and varieties of experience. Typically, networked organisations provide for interactions of geographically distributed entities and try to foster coherence of purpose of local activities for achieving overall effectiveness (Santoro, Borges and Rezende, 2006).

Whatever is the form of collaboration between networked companies, it provides for organisation of the partners' activities with clear roles of each participant and well-defined rules by which the network operates (e.g. Serrier, Ducq, and Vallespir, 2017). This type of organisation can take several forms:

- strategic alliance;
- integrated logistics management;
- network enterprise; and
- virtual organisations and clusters.

Typically, there is a "pivot company" in each form of CNO.

Three key collaboration processes are of particular interest: (1) collaborative predicting; (2) collaborative planning; and (3) collaboration with suppliers (Tain, 2019).

One recent publication focuses on network-based organisations as adaptive, decentralised systems that create value (profit) through iterative and systematic interactions between agents (Tain, 2019). The supporting architectures enhance knowledge creation in turbulent environments and compel agents to seek solutions outside their functional boundaries. To maximise value creation, it is essential to characterise the role of agents in organisational networks, implementing an entrepreneurial corporate culture where agents, understanding their responsibilities in seeking new opportunities, are properly incentivised to make collaboration effective (Tain, 2019).

Some authors argue that the most significant power of a digital ecosystem is its ability to create added value based on partnerships (Krčo et al., 2019). The benefits of a well-developed ecosystem are numerous. First, it provides easy access to the knowledge and know-how of subject matter experts at a reasonable cost. Second, it reduces the time to market by reuse of multiple components and distributing more evenly the workload among partners. That brings a higher return on investment and better customer experience. Third, these results can be achieved in a shorter timeframe. Finally, customers and stakeholders are more confident that solutions built by a well-developed CNO will receive continuous support and innovation (Krčo et al., 2019).

The application of social network theory allows us to identify and quantify existing or potential hazards in collaboration, for example, at the level of management, communication, or knowledge sharing among partners in a collaborative organisation (Abreu and Calado, 2017). Among the nodes of CNOs identified are people, knowledge, resources, and tasks. To avoid conflict and misunderstanding, it is important to identify and understand potential risks. Abreu and Calado (2017) classify related risks into seven categories:

1. Critical employee risk;

2. Risk pertaining to resource allocation;
3. Communication risk, associated with the structure of authority and communication level within the collaborative ecosystem;
4. Redundancy risk;
5. Task risk;
6. Personnel interaction risk; and
7. Performance risk.

3.2.5 Taxonomy of Business Models of Collaborative Networked Organisations

The analysed academic publications present business models of collaborative networked organisations. A collaborative network is an alliance constituted by a variety of geographically distributed and autonomous entities—heterogeneous in terms of their culture, social capital, and goals, and each operating in a particular environment—which collaborate to share resources and risks in achieving common or compatible objectives, and whose interactions are supported by adequate digital infrastructure. Network-based organisations are adaptive, decentralised systems that create value through recurrent and systematic interactions. A CNO's framework for collaboration is usually process-oriented, aiming to cover all business processes carried out by the companies. The advantage of a collaborative environment is that it supports knowledge sharing and coordination of actions in geographically distributed and decentralised networked organisations.

Contrary to the traditional business models that are designed on a firm-centric basis, the new digital business models are enhanced by ICT and, as a rule, are decentralised. However, the business model concept is still considered a “missing link” between business strategy, processes, and information technology.

Based on the review and the analysis of the selected academic sources, Table 6 presents a taxonomy of possible business models of CNOs along with several main criteria for classification.

This classification, along with the taxonomy of collaborative networked organisations, presented in Table 6, and identified governance needs, objectives, requirements, and models, serve to guide the search for business, governance and management models adequate to the future European cybersecurity industrial, technology and research competence centre and a network of national centres. They can serve as well as a target model in the evolution of the ECHO project consortium into a self-sustained cybersecurity collaborative networked organisation.

Criteria	Types of CNO Business Models
Degree of formalisation	Collaborative Networked Organisation (CNO) Ad-hoc (informal) collaboration
Goal and horizon of collaboration on CNOs	Long-term strategic collaboration (e.g., VBE) Goal-oriented, opportunity-driven network (e.g., a temporary VO to exploit an emerging market opportunity)
Nature of CNO entities	CNOs or organisations with complementary competences CNOs of competitors
Types of partner organisations in the CNO	A CNO may include one or more of the following partner types: SMEs, brokers, integrators, business support organisations, funding

Criteria	Types of CNO Business Models
	institutions, public agencies, research institutes and universities, individual customers and customer communities, etc.
Geographic diversity	Local or regional CNOs/ecosystems CNOs with geographically distributed memberships
Sectoral diversity	CNOs focusing on one type of products and the supply chain CNOs covering complementary business sectors
Degree of centralisation	Fully distributed CNO (e.g., a VO of SMEs) CNO with a Virtual Development Office comprised of selected (core) members CNO with a "pivot company"
Levels of membership	A CNO may allow only accredited members, or use a classification system to distinguish, for example, accredited members, trusted partners, observers, etc.
Process or service orientation	Service-Oriented Collaborative Network (SOCN) Service-Oriented Virtual Organisations (SOVO) Virtual Enterprise (process-oriented)

Table 6: Taxonomy of CNO digital business models

3.2.6 Implications for a Cybersecurity CNO

The main goal of section 3.2. was to identify and analyse best practices of business models of collaborative organisations, described in the academic literature, and to suggest a feasible approach for the development of a business model of a collaborative networked organisation in the area of cybersecurity. Two of the findings presented here may be of particular interest to achieve this goal. First is the concept of a Virtual organisations Breeding Environment (VBE)—a long-term alliance of business companies, research institutes, and relevant support institutions—aiming primarily to increase their chances and preparedness for concrete collaborative projects. With that aim, the VBE establishes a cooperation agreement, adopts common operating principles, develops personal and organisational relationships and the supporting digital infrastructure, and strengthens trust among partners.

The second concept is that of a virtual organisation (VO)—usually a temporary, geographically dispersed network of independent entities established around a particular series of products or services and aiming to capture a market opportunity—and its business model. The VO may be flat or have a pivot company or a virtual development office where several core partners are represented.

Of particular importance in view of the future implementation of Regulation 887 or, for that matter, any other cybersecurity competence network, is the realisation that the cybersecurity CNO does not need to be a single, unified organisation; instead, it can be designed as a VBE and a number of VOs, each one established around a particular cybersecurity product or service.

The presented results were used as main building blocks in the process of identification and selection of business and governance models for the ECHO cybersecurity competence network. The follow-on analysis comprises two steps in order to identify the most appropriate business and governance models.

The first step includes identification of four alternatives of business and governance models of CNOs based on the results of this analysis and identified patterns in both business and governance models of existing networks. Correspondingly, to span the exploration space, each of the four alternatives will be designed around one of the following respective pillars:

1. High degree of centralisation of funding streams AND high degree of centralisation of main business and governance decisions;
2. High degree of centralisation of funding streams AND medium degree of centralisation of main business and governance decisions;
3. Distributed and balanced funding streams (i.e. public funding and commercial sales) AND high degree of centralisation of main business and governance decisions; and
4. Distributed and balanced funding streams AND medium degree of centralisation of main business and governance decisions.

The taxonomy in Table 6 provided further criteria for designing sufficiently distinct alternatives of business and governance models.

At the second step, in ECHO Task 3.3 the research team applied the Analytical Hierarchy Process (AHP) methodology to solicit the opinion of subject matter experts (SMEs) on evaluation criteria and pairwise comparison of the alternatives along each criterion.[8] Through processing the expert opinions, the research team ranked the designed alternatives in terms of SME preferences, thus setting a solid foundation for integrating the ECHO cybersecurity competence network in the evolving EU cybersecurity research, technological, and industrial landscape. These elements were reflected in Deliverable D3.2. and will inform its updates at M36 and M48.

3.3 Business models of existing networks

The models used by existing networked organisations provide additional information of interest. This section will outline how data with regards to existing collaborative networked organisations (CNOs) was critiqued. Secondary analysis of the data contained within the MS Excel matrix was a two-step process. First, key indicators concerning the business models of CNOs were assessed. Two dimensions were evaluated and compared, representing respectively profit orientation and funding streams and degree of coordination of main network activities. Then the dimensions were used to visualise and cluster available information on the business models of existing networks.

[8] Velizar Shalamanov and Georgi Penchev, "Methodology for Organisational Design of Cyber Research Networks," in *Digital Transformation, Cyber Security and Resilience of Modern Societies*, edited by Todor Tagarev, Krassimir Atanassov, Vyacheslav Kharchenko, and Janusz Kasprzyk, Studies in Big Data, vol. 84 (Cham: Springer, 2021), 25-47, https://doi.org/10.1007/978-3-030-65722-2_3.

3.3.1 Dimensions for representing CNO business models

In the preparation phase, including piloting, it was decided that profit orientation of the network (not-for-profit or for-profit status), the funding model/ income streams, the degree of coordination in the provision of services and sales of products, and decisions on network development are the key considerations in deciding on a possible business model of a CNO (see the Business model section in Table 3).

Two dimensions were designed to represent these considerations – **dimension 1**: profit orientation and funding streams and **dimension 2**: degree of coordination. An arbitrary numerical scale was devised in an effort to visualise these characteristics of the business model in two dimensions (outlined in Table 7 and Table 8 respectively).

Profit orientation ***Funding streams***	**Not-for-profit**	**For profit**
Exclusively /entirely/ public funding	5	Not applicable
Primarily public funding	3	1 (unlikely)
Balanced funding streams	1	-1
Primarily commercial funding	- 1 (unlikely)	-3
Exclusively commercial funding	Not applicable	-5

Table 7: Dimension 1. Existing networks: Profit and funding streams, scale from -5 to 5.

'Commercial' in this context implies revenue or funding that is primarily derived from the selling of products and services. The use of the adverbs 'exclusively,' 'primarily,' and 'balanced,' while subjective, nonetheless allow for a useful comparative assessment as they are not regulatory terms, nor do they feature in statutory documentation.

Network development decisions: ***Provision of products & services***	**Single process**	**Coordination on main issues**	**Ad-hoc coordination**	**No coordination**
Single centralised point	5	4	2	1
One POC for each main product/service	4	3	1	-1
Several POCs per product/ service	2	1	-1	-3
Through each CNO member	0	-2	-3	-5

Table 8: Dimension 2. Existing networks: Degree of coordination.

The following section outlines the various values under the remit of Dimension 2. Degree of coordination.

The provision of services and sales of products (including information exchange with customers, contracting, contract management, etc.) can potentially be realised through a spectrum from a single centralised point to fully decentralised arrangements:

- A single centralised point for provision of services and sales of products;
- Designated point of contact (responsible organisation) for each main service/product;
- Several points of contact (lead organisations) for each of the main services/products;
- Each CNO member can contract network products and services.

Network development decisions (including on adding new members, establishing partnerships, investing in R&D or new capabilities, etc.) can be made in a spectrum of potential arrangements, e.g. from a single decision-making process for the CNO to fully independent decisions by each organisation (i.e. without coordination):

- Decisions are made in a single process for the CNO;
- Decisions on main 'issues' (capabilities) are coordinated within the CNO;
- Decisions are coordinated among some CNO member organisations (variable configurations; possibly ad-hoc);
- No coordination, i.e. each CNO member decides independently.

These two sub-dimensions outlined above did not merge well, as the assignment of an arbitrary scale posed an issue in the first instance as it contains duplicate numbers, which therefore cannot be arranged in a continuum, or indeed graphed. However, aspects of the scale (i.e. categorial hierarchy) were utilised to devise a two-dimensional presentation of the business models, wherein an alternative analytical approach with the same underlying principles (i.e. modelling data dimensionally) was adopted.

Notably, in instances wherein data with regards to the two dimensions—profit and funding streams and/or degree of coordination—were not available, the 'not available' criteria (n/a) was applied. All classifications with respect to the CNOs were recorded, but those denoted with this label were not included in the various generated graphical representations.

3.3.2 Findings from the analysis of existing networks

Dimension 1. Profit and funding streams

All of the qualitative data gathered concerning the profit-orientation and funding streams were assessed in line with the categorical labels presented above.

Data relating to the profit orientation and funding streams for 32 CNOs were unavailable and so were excluded from subsequent analysis. Among the sixty CNOs that remained, a total of 53 were determined to be not-for-profit, with seven deemed as for-profit networks.

Most of the *not-for-profit* CNOs worked with "balanced funding streams," which means a mix of commercial and public funding. These made up 41 % (n=22) of the sample. Public funding relates to the national government or EU grant funding; commercial funding also includes business revenue, sponsorship, and donations. Exclusive reliance on public funding comprised the second largest funding model category, accounting for 36 % of the sample (n=19).

Most of the *for-profit* CNOs relied exclusively on commercial revenue accounting for 71 % of the sample (n=5). Nevertheless, there were examples, although few (n=2 at 29 %), of for-profit CNOs, utilising a balanced funding stream with a somewhat equal mix of public and commercial sources.

Dimension 2. Degree of coordination

In this section, the different values under the heading 'Degree of coordination' are outlined. Service provision and product sales activities, which includes within that process the exchange of relevant information, contracting, and the management of contracts, can be imagined as a spectrum ranging from a single centralised point on the one end to more or less completely decentralised systems on the other, as summarised below:

- a single, centralised point for the provision of services and sales of products;
- a designated point of contact (POC; responsible organisation) for each main service or product;
- multiple points of contact (lead organisations) for each of the main services and/or products;
- a decentralised structure whereby each CNO member contracts the delivery of products and services for the network.

All of the qualitative data gathered in relation to the degree of coordination (i.e., in the provision of goods and services) were assessed according to their respective categorical labels. Data relating to the degree of coordination for 45 CNOs were incomplete and were excluded from subsequent analysis. A pie graph (Figure 5) was generated to show how the distribution of product and service provision was inter-connected with network development decisions for the other remaining 47 CNOs.

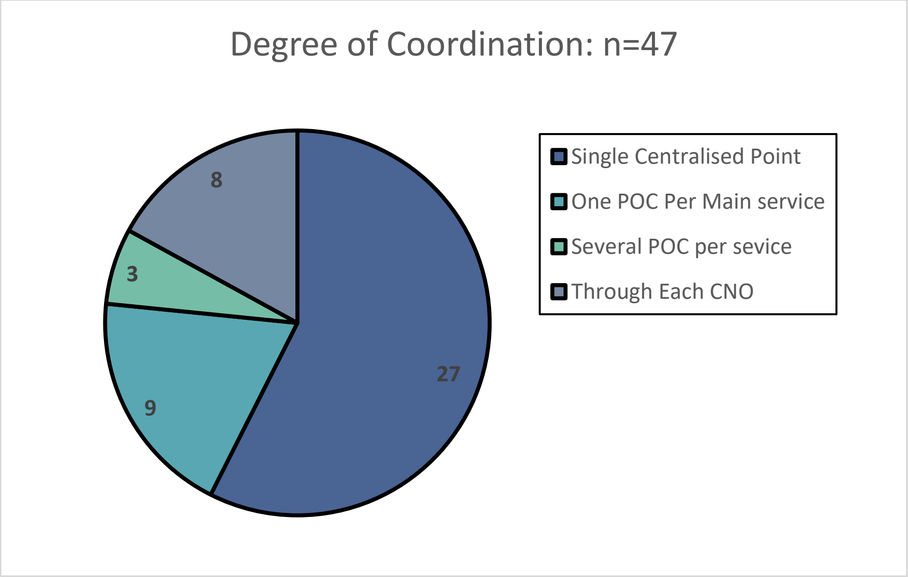

Figure 5: Degree of coordination among CNOs.

Most of the CNOs provide products and services via a single centralised point making up 57 % of the sample (n=27). This indicates that for a majority of the surveyed CNOs, the provision of goods and services was coordinated at the network level rather than through different points of contact or coordinated by various CNO members (who have standalone autonomy).

Also, but not to the same degree, 19 % of the analysed CNOs used one designated point of contact for every main service/product (n=9), while 17 % of the sample positioned each CNO member to contract network products and services (n=8).

The data analysis involved using IBM SPSS™ 25 to carry out a contingency table analysis to examine the link between Dimension 1 and Dimension 2 above. It was determined that regarding the 'degree of coordination' classification, most of the existing networks were not-for-profit, relying solely on public funding (n=11; 23 %), or on a balanced funding stream (n=6; 13 %) operationalised under the constraints of a single process-single centralised point.

The findings show that of the 92 CNOs that were examined, the provision of services and sales of products tends to be coordinated via a single centralised point, regardless of whether this relates to the exchange of information with customers, contracting, or contract management. Furthermore, these organisations depend on either public funding exclusively (i.e., government/EU grants, etc.) or a more or less equal ratio of commercial and public funding. See Figure 6 below for a visual display of these findings.

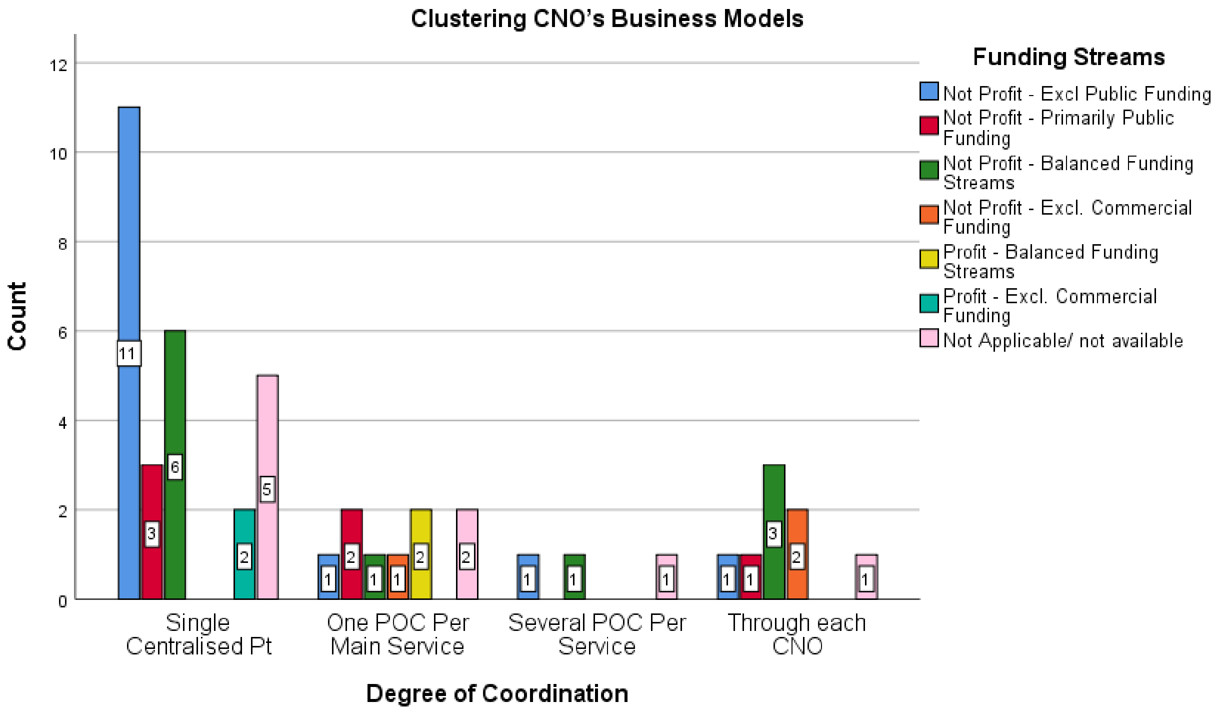

Figure 6: Clustering CNO's business models – Profit and funding stream vs. Degree of coordination.

4. Governance of network organisations: needs, requirements, prioritisation

4.1 Normative requirements to networks' governance

Regulation 2021/887 is the Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

This Regulation establishes the European Cybersecurity Industrial, Technology and Research Competence Centre (the '*Competence Centre*'), as well as the *Network of National Coordination Centres*, and lays down rules for the nomination of National Coordination Centres as well as for the establishment of the *Cybersecurity Competence Community*. The Competence Centre is expected to play an essential role in the implementation of the cybersecurity part of the Digital Europe Programme and to contribute to the implementation of Horizon Europe (Article 1(2)).

According to Article 3 of R 887, the Competence Centre and the Network shall help the Union to:

1. strengthen its leadership and strategic autonomy in the area of cybersecurity;
2. retain and develop the cybersecurity research, academic, technological and industrial capacities necessary to enhance trust in and secure its Digital Single Market;
3. develop its technological capacities, capabilities and skills related to the resilience and reliability of the infrastructure of network and information systems, including critical infrastructures;
4. increase the competitiveness of the Union's cybersecurity industry and turn cybersecurity into competitive advantage of other Union industries;
5. undertake its tasks, where appropriate, in collaboration with the cybersecurity competence community.

Four pilot projects were launched under Horizon2020 as a result of the 2018 call for the topic SU-ICT-03-2018 "*Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap*". The four pilots therefore foresee actions to collaborate with each other and also with similar ongoing projects funded under H2020 and take account of the results and work done in other relevant H2020 projects on cybersecurity/privacy.

Long Name of the Project	Short Name	ID
Cyber security cOmpeteNce fOr Research anD Innovation	CONCORDIA	830927
Cyber Security Network of Competence Centres for Europe	CyberSec4Europe	830929
European network of Cybersecurity centres and competence Hub for innovation and Operations	ECHO	830943
Strategic programs for advanced research and technology in Europe	SPARTA	830892

Table 9: Four SU-ICT-03-2018 projects

This is the reason for which contractual documents of other Pilots have been analysed. These projects will assist EU in defining, testing and establishing the governance model of a European Cybersecurity Competence Network of cybersecurity centres of excellence.

Regulations and norms analysed have been chosen because they are referenced in R 887. In particular:

- In September 2017, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a Joint Communication on *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU* (RDD, 2017) to further reinforce the Union's resilience, deterrence and response to cyber-attacks;
- A National Coordination Centre should also have the capacity to effectively engage and coordinate with the industry, the public sector, including authorities designated pursuant to the *Directive (EU) 2016/1148 of the European Parliament and of the Council* (NIS, 2016);
- *EC Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises* (Incidents & Crisis): a rapid and shared understanding of threats and incidents as they unfold is a prerequisite for deciding whether joint mitigation or response action supported by the EU is needed. Such information exchange requires the involvement of all relevant actors – EU bodies and agencies, as well as Member States – at technical, operational and strategic levels;
- *Cybersecurity Act* (CA, 2019): the growth of the cybersecurity market in the EU – in terms of products, services and processes – is constrained in several ways. A key aspect is the lack of cybersecurity certification schemes recognised across the EU to build higher standards of resilience into products and to underpin EU-wide market confidence. The Commission is therefore putting forward a proposal to set up an EU cybersecurity certification framework. The Framework would lay down the procedure for the creation of EU-wide cybersecurity certification schemes, covering products, services and/or systems, which adapt the level of assurance to the use involved (be it critical infrastructures or consumer devices).

4.1.1 Explicit requirements

Governance requirements need to be in line with the vision of the draft Regulation 887 (R887, 2021). Table 10 summarizes in a high-level approach the different roles and duties in the future to the European, the national centres and the cybersecurity competence community.

For the purpose of this Regulation, the following definitions shall apply (see R 887, Article 2):

- *'cybersecurity'* means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats;
- *'cybersecurity products, services and processes'* means commercial and non-commercial ICT products, services or processes with the specific purpose of protecting network and information systems or ensuring the confidentiality, integrity and availability of data that are processed or stored in network and information systems, as well as the cybersecurity of the users of such systems and other persons affected by cyber threats;
- *'technical assistance'* means assistance by the Competence Centre to the national coordination centres or the Community in the performance of theirs tasks by providing knowledge or facilitating access to expertise in the area of cybersecurity research, technology and industry, facilitating

networking, raising awareness and promoting cooperation, or means assistance by the Competence Centre together with the national coordination centres to stakeholders with respect to the preparation of projects in relation to the mission of the Competence Centre and the Network and the objectives of the Competence Centre.

	Competence Centre (CC)	Network	National Coordination Centres (NCC)	Cybersecurity Competence Community (CCC)
Contractual documents	Provision to guarantee the liability and transparency of the competence centre Contractual public-private partnership on cybersecurity during the duration of Horizon2020, through its Industrial and Scientific Advisory Board Working arrangements for cooperation with Union institutions, bodies, offices and agencies (prior approval of the EU Commission)	Contractual agreement with the CC	The list of NCCCs shall be published by the Commission The relationship between the CC and the NCC shall be based on a contractual agreement signed between them. The agreement shall provide for the rules governing the relationship and division of tasks between the CC and each NCC	Only entities which are established within the Union may be accredited as members of the competence community Assessment made by the NCC of the Member State where the entity is established;
Governing Structure	Industrial and Scientific Advisory Board Governing Board of the Competence Centre, composed of the Member States and the Commission Executive Director	The Network shall be composed of all the National Coordination Centres nominated by the Member States	NCC are selected by Members States	CCC consists of Industry, academic and non-profit research organisations, public entities, entities dealing with technological matters Joint Research Centre of the Commission and ENISA have active part in the CCC Representatives of the Commission may participate in the work of the Community

	Competence Centre (CC)	Network	National Coordination Centres (NCC)	Cybersecurity Competence Community (CCC)
Main Objectives	Disseminate latest cybersecurity solutions Support to operators of critical services	Retain and develop the cybersecurity technological and industrial capacities necessary to secure its Digital Single Market Increase the competitiveness of the Union's cybersecurity industry and turn cybersecurity into competitive advantage of other Union industries	Effective engage and coordinate with the industry, Public sector and research community Access to cyber security technological expertise	Contribute to the mission of the Competence Centre and enhance and disseminate cybersecurity expertise across the Union Provide input and work plan for the Competence Centre
Functions/ Tasks	Coordination the Network Feeding the CCC Allocation of Grants for implementation of Digital Europe and Horizon Programmes Acquiring, upgrading, operating and making available cybersecurity industrial and research infrastructures and related services Facilitating access to the expertise available in the Network and the CCC Development of Cyber security products	Assist the CC in joint procurement actions Assist the CC in the implementation of the mission and vision	Assist the CC in joint procurement actions Coordinating the CCC Addressing sector-specific cyber security industrial challenges Contact point between CC and CCC Implementing specific actions under conditions specified in the concerned grant agreements Disseminating the relevant outcomes at national or regional level Assessing requests by entities for becoming part of the Cybersecurity	Work closely with the CC and the relevant NCC Participate in working groups established by the Governing Board of the CC to carry out specific activities as provided by the CC's work plan Participate in activities promoted by the CC and NCC Promoting specific projects and their relevant outcomes

	Competence Centre (CC)	Network	National Coordination Centres (NCC)	Cybersecurity Competence Community (CCC)
	Development of Cyber security skills Annual agenda for innovation and standardisation of Cyber security in EU Enhance cooperation between Defence and the civil sphere Cooperation with relevant Union institutions, bodies, offices and agencies (Art. 10)		Competence Community Cooperate through the Network to implement aforementioned tasks	
Financial	EU finances half of the costs arising from the establishment, administrative and coordination activities Investment in and use of infrastructures, capabilities, products or solutions		Financial contribution from the general budget of the Union The Commission may terminate, proportionally reduce or suspend the Union's financial contribution to the Competence Centre if the participating Member States do not contribute, contribute only partially or contribute late	Support by NCC
Voting		Only Member States who contribute financially to the administrative and operational costs of the CC should hold voting rights	Direct Union financial support	

	Competence Centre (CC)	Network	National Coordination Centres (NCC)	Cybersecurity Competence Community (CCC)
Decision Making	Rules regarding the prevention and the management of conflict of interest			
Duties	Operational and financial reporting Article 29 Financial rules Article 30 Protection of financial interests Prevention, detection and investigation of irregularities, the recovery of lost, wrongly paid or incorrectly used funds The rules of procedure of the bodies of the Competence Centre should be made publicly available		The participating Member States shall make a total contribution to the operational and administrative costs of the Competence Centre of at least the same amounts as those in Article 21(1) of this Regulation The participating Member States shall report by 31 January each year to the Governing Board on the value of the contributions made in each of the previous financial year	Members of CCC shall demonstrate that they have cybersecurity expertise with regard to at least one of the following domains: (a) research; (b) industrial development; (c) training and education Fulfil the criteria set out in paragraph 3 or it falls under the relevant provisions set out in Article 136 of the new financial regulation

Table 10: Summary of the Normative Requirements.

The Competence Centre and the Network should be at the service of developers and operators in critical sectors (NIS, 2016) such as transport, energy, health, financial, government, telecom, manufacturing, defence, and space to help them solve their cybersecurity challenges.

Among the specific requirements identified in the NIS Directive are:

- understanding own resources and a tool for identifying unknown devices;
- establishing a vulnerability management program;
- advanced systems for threat detection, including detection, identification and reporting capabilities with effective mechanisms for reporting incidents, including systems to record and report incidents within 72 hours of detection to CSIRTs;

- effective incident management, including response and recovery plans.

The organizational requirements include:

- an organisational approach to risk management;
- adequate management policies and processes to govern the approach to security of networks and information systems;
- understanding and managing security risks throughout the production chain;
- adequate staff training and awareness in the field of security of networks and information systems.

A rapid and shared understanding of threats and incidents as they unfold is a prerequisite for deciding whether joint mitigation or response action is needed. Such information exchange requires the involvement of all relevant actors – EU bodies and agencies, as well as Member States – at technical, operational and strategic levels. Furthermore, the important role of third-party security researchers in discovering vulnerabilities in existing products and services needs to be acknowledged and conditions to enable coordinated vulnerability disclosure should be created across Member States, building on best practices and relevant standards. At the same time, specific sectors face specific issues and should be encouraged to develop their own approach. In this way, general cybersecurity strategies would be complemented by sector-specific cybersecurity strategies in areas like financial services, energy, transport and health.

Resilience through rapid emergency response must be grounded on:

- full implementation of the Directive on the Security of Network and Information Systems;
- adoption of the ENISA European Framework for certification;
- a joint Commission/industry initiative to define a “duty of care” principle for reducing product/ software vulnerabilities and promoting “security by design”;
- swift implementation of the blueprint for cross-border major incident response;
- support Member States in identifying areas where common cybersecurity projects could be considered for support by the European Defence Fund;
- an EU-wide *one-stop-shop* to help victims of cyber-attacks, providing information on latest threats and bringing together practical advice and cybersecurity tools;
- action by Member States to mainstream cybersecurity into skills programmes, e-government and awareness campaigns;
- action by industry to step up cybersecurity-related training for their staff and adopt a "security by design" approach for their products, services and processes;
- set up a Network of Cybersecurity competence centres and a European Cybersecurity Research and Competence Centre (R 887, 2021);

Deterrence means putting in place a framework of measures that are both credible and dissuasive for would-be cyber criminals and attackers. Deterrence must be grounded on:

- Commission initiative for cross-border access to electronic evidence;
- swift adoption by the European Parliament and the Council of the proposed Directive on combatting fraud and counterfeiting of non-cash means of payment;

- introduction of requirements on IPv6 in EU procurement, research and project funding; voluntary agreements between Member States and Internet Service Providers to drive up the uptake of IPv6;
- a renewed/expanded focus in Europol on cyber forensics and monitoring the darknet;
- implementation of the framework for a joint EU diplomatic response to malicious cyber activities;
- enhanced financial support to national and transnational projects improving criminal justice in cyberspace;
- a cybersecurity-related education platform to address the current skills gap in cybersecurity and cyber defence.

To strengthen the European cooperation on cybersecurity, key initiatives aim to:

- advance the strategic framework for conflict prevention and stability in cyberspace;
- develop a new Capacity Building Network to support third countries' ability to address cyber threats and EU Cybersecurity Capacity Building Guidelines to better prioritise EU efforts;
- further the cooperation between EU and NATO, including participation in parallel and coordinated exercises and enhanced interoperability of cybersecurity standards.

Among the normative documents, the NIS Directive (NIS, 2016) makes an essential step in promoting a culture of *risk management* by introducing security requirements as legal obligations for the key economic actors, notably operators providing essential services and suppliers of some key digital services. With security requirements seen as essential to safeguard the benefits of the evolving digitalisation of society, and given the rapid proliferation of connected devices, the NIS Directive also puts forward the idea of establishing a framework for security certification for ICT products and services in order to increase trust and security in the digital single market. ICT *cybersecurity certification* becomes particularly relevant in view of the increased use of technologies which require a high level of cybersecurity, such as connected and automated cars, electronic health or industrial automation control systems.

Article 4 of Regulation 887 (R 887, 2021) states that the Competence Centre shall aim to promote research, innovation and deployment in the area of cybersecurity in order to fulfil the mission as set out in Article 3, in pursuit of the following specific objectives:

1. enhancing cybersecurity capacities, capabilities, knowledge and infrastructure for the benefit of industry, in particular SMEs, research communities, the public sector and civil society, as appropriate;
2. promoting cybersecurity *resilience*, the uptake of cybersecurity best practices, the principle of security by design, and the *certification* of the security of digital products and services, in a manner that complements the efforts of other public entities;
3. contributing to a strong European cybersecurity ecosystem which brings together all relevant stakeholders.

4.1.2 Implicit requirements

Each of the four pilot projects (ECHO, CONCORDIA, SPARTA, CyberSec4Europe) has a different but complementary approach to shared common goals. In order to maximize the individual project impact and leverage on the joint communication and dissemination activities, the four projects of the Horizon 2020 cybersecurity call have decided to build a joint web platform. The umbrella website is intended to promote the joint cybersecurity effort of the projects, as well as provide a central platform for advertising joint and individual events. Furthermore, it will be used to publish news from the pilots along with general information regarding the cybersecurity domain. In recognition of the European Commission's communication objectives, ECHO has also undertaken the lead in producing the domain www.cybercompetencenetwork.eu to serve as the common web platform for all four of the Pilot Projects. The joint umbrella website is live since 3rd June 2019.

These are some of the potentially relevant synergies and overlaps about *Governance* identified in the contractual documents of the Projects. ECHO should aim to form a working group to build and deliver a common roadmap. The common tasks are presented in the following table.

Category	CONCORDIA	ECHO	SPARTA	CyberSec4Europe
Community and governance	T3.5: Community Building, Support and Incentive Models Governance models will also be studied in: Task T3.4: Establishing an European Education Ecosystem for Cybersecurity Task T3.2: Piloting a DDoS Clearing House for Europe Objective 2: CONCORDIA addresses this with a governance model that combines the agility of a start-up with the sustainability of a large centre	T3.1: Governance needs and objectives T3.2: Information sharing models' definition T3.3: Governance models definition T3.4: Governance operations T3.5: New partner engagements	T1.1: Drive, continuous improvement and networking for the governance T1.2: Adaptation, synchronization, progress, measurement and improvement for governance of R&D&I activities T1.3: Adaptation, synchronization, progress, measurement and improvement for governance community and exploitation activities T1.4: Governance assessment and recommendations T8.1: Establishment of the SPARTA Joint Competence Centre Infrastructure	T1.1: Drive, continuous improvement and networking for the governance T1.4: Governance assessment and recommendations T2.1 Stakeholders Viewpoints T2.2 Assessing Best Governance Practices T2.3 Governance Structure Design T2.4 Operation and Testing of the Governance Structure T2.5 Preparation for the future Cybersecurity Competence Network T10.1 Clustering and collaboration activities with funded projects from SU-ICT-03

Category	CONCORDIA	ECHO	SPARTA	CyberSec4Europe
			T8.2: Clustering of SPARTA activities at national and EU level T8.3: Clustering of SPARTA project with the other two EU projects of SU-ICT-03 and other calls T8.4: Cooperation of SPARTA consortium with other EU and international bodies	and other EC cybersecurity projects T10.2 Collaboration with existing cybersecurity communities and ecosystems innovation T10.3 Cooperative efforts and interactions with EU bodies
Legal aspects and IPR	T4.2: Legal aspects		T2.1: Identification of CCN relevant ethical, legal and societal aspects T2.5: Internal ethical, legal and societal aspects auditing and supervision T4.5: Legal issues analysis and framework development T10.1: Legal and licensing support	T4.2 Legal and regulatory requirements
Financial aspects	T4.3: Economic perspectives	T3.3: Governance models definition T3.4: Governance operations	T10.2: Sustainable exploitation and commercial deployment strategy definition	T3.10 Impact on Society
Stakeholders	T4.6: Liaison with stakeholders	T3.4: Governance operations	T8.4: Cooperation of SPARTA consortium with other EU and international bodies	T4.1 Vertical stakeholders engagement and consultation T2.1 Stakeholders Viewpoints

Category	CONCORDIA	ECHO	SPARTA	CyberSec4Europe
			T11.2: Liaison with EU and national cybersecurity authorities	T10.2 Collaboration with existing cybersecurity communities and ecosystems innovation T10.3 Cooperative efforts and interactions with EU bodies
Gender balance	T4.5: Women in cybersecurity		T12.4: Closing the gender and diversity gap	

There are also synergies in the *technological* context. A roadmap working group was created with project participants responsible to work on the roadmap from each pilot to further enhance the cooperation and the communication.

Category	CONCORDIA	ECHO	SPARTA	CyberSec4Europe
Technologies	T1.1: Device-centric security T1.2: Network-centric security T1.3: Software system-centric security	T2.3: Transversal cybersecurity challenges and opportunities	T5.3: Risk discovery assessment and management of complex systems T6.1: Securing operating system software T6.2: Hardening Legacy components T6.4: Resilience by-design of II	T3.2 Research and Integration on Cybersecurity Enablers and underlying Technologies T3.3 SDL – Software Development Lifecycle T3.4 Security Intelligence T3.5 Adaptive Security
Technologies	T1.4: Data/Application-centric security	T2.3: Transversal cybersecurity challenges and opportunities	T4.4: Information sharing integration technologies contest	
Technologies	T1.5: User-centric security	T2.3: Transversal cybersecurity challenges and opportunities		T3.6 Usable Security (Human-centred Cybersecurity)

Category	CONCORDIA	ECHO	SPARTA	CyberSec4Europe
Information exchange	T3.1: Building a Threat Intelligence for Europe T3.2: Piloting a DDoS Clearing House for Europe	T2.4: Inter-sector technology challenges and opportunities T3.2: Information sharing models definition T4.1: Detailed analysis of common technical security challenges T5.1: EWS system architecture and reference models T5.2: EWS Research, development and implementation	T4.4: Information sharing integration challenges contest WP7 Program #4 T7.1: Threat modelling for AI systems T7.2: Design defensive and reactive security measures T7.3: Enhance explainability of AI T7.4: Design measures of fairness in AI T7.5: Testing and validation	T3.4: Security Intelligence T3.5: Adaptive security T4.7: Roadmap for industrial challenge 5.4 (Incident Reporting)
Infrastructure	T3.3: Developing the CONCORDIA's Ecosystem: Virtual Lab, Services and Training	T6.1: FCR system architecture and reference models T6.2: FCR Research, development and implementation T6.3: FCR Integration and test	T8.2: Clustering of SPARTA activities at national and EU level	T7.1: Open tools and common portable virtual labs T7.2: Federated infrastructures for cyber range and testing T7.3: Certification-methodologies, tools and infrastructures
Education /training/ awareness	T3.4: Establishing a European Education Ecosystem for Cybersecurity	T2.6: Derivation of ECHO Cyber skills Framework and related trainings T8.2: EWS/FCR Demonstration workshops T8.3: Early prototypes demonstration workshops	T9.2: Academic programs in cybersecurity T9.3: Professional training in cybersecurity T9.4: Raising awareness in cybersecurity	T6.1 University Education T6.2 Professional Training and Workforce Assessment T6.3 Virtual Education T6.4: Cyber Ranges as platform for education, training and exercises

Category	CONCORDIA	ECHO	SPARTA	CyberSec4Europe
Roadmap	T4.4: Cybersecurity Roadmap for Europe	T4.2: Inter-sector roadmap and demonstration cases definition T4.3: Early prototype selection, research and development	T3.1: Initial roadmap design T3.2: Accomplish a general view over different EU and national research and innovation roadmaps T3.3: Identification and selection of strategic challenges T3.4: Taskforce emerging and disruptive topics and technologies	T4.4 Roadmap for industrial challenge 5.1 (e-Commerce) T4.5 Roadmap for industrial challenge 5.2 (Supply Chain) T4.6 Roadmap for industrial challenge 5.3 (Privacy-preserving Identity Management) T4.7 Roadmap for industrial challenge 5.4 (Incident Reporting) T4.8 Roadmap for industrial challenge 5.5 (Maritime Transport) T4.9 Roadmap for industrial challenge 5.6 (Medical Data Exchange) T4.10 Roadmap for industrial challenge 5.7 Smart cities
Standardisation	T5.3: Certification and standardization activities	T2.7: Derivation of ECHO Cybersecurity certification scheme	T11.1: Mapping international and EU cybersecurity certification T11.4: Process oriented certification concepts for complex mainstream commercial software systems	Task 8.1 Maintaining contacts with the (European) SDOs and the relevant cybersecurity committees Task 8.2 Linking the technical work of the project to standards and

Category	CONCORDIA	ECHO	SPARTA	CyberSec4Europe
				standards to the project Task 8.3: Assessing the appropriateness of the existing standardization procedures for the cybersecurity goals
Certification	T5.3: Certification and standardization activities	T2.7: Derivation of ECHO Cybersecurity certification scheme	T11.1: Mapping international and EU cybersecurity certification T11.4: Process oriented certification concepts for complex mainstream commercial software systems	T7.3: Certification-methodologies, tools and infrastructures

Possible synergies related to *communication* are:

Category	CONCORDIA	ECHO	SPARTA	CyberSec4Europe
Communication & Dissemination	T5.1: Exploitation and incubators T5.2: Dissemination and communication activities	T9.1: Marketing and communication T9.2: Dissemination T9.3: Market analysis, Business models and exploitation	T12.1: Dissemination and communication strategy, planning, updates and evaluation T12.2: Communication activities T12.3: Dissemination materials and dissemination events T12.5: Outermost Regions engagement – "Go cyber with SPARTA" campaign	T9.1 Dissemination activities & reporting T9.2 Outreach T9.3 Spreading of excellence T9.4 Raising cybersecurity awareness T9.5 Exploitation & Sustainability T9.6 Policy Recommendations

The following implicit requirements have been identified in projects' documents:

- bring together the research, industry and public sector communities to facilitate research and innovation in cybersecurity;
- address sector specific, as well as inter- and cross-sector challenges and threats;
- provide a distinct position dedicated to administrative matters;
- envision distinct functions in the network for HR development, financial management, Innovation management, and partnership development;
- assure adequate competences on legal and organizational matters;
- introduce accreditation procedures for members of the Cybersecurity Competence Community.

4.2 Interviews with stakeholders

The findings in this sub-section resulted from the secondary analysis of conducted interviews with stakeholders. ECHO partners identified and reached preliminary agreement with 12 interviewees. Full transcripts of nine interviews are available, along with the agreement of the interviewees that the response can be used in the current study.

Three of the interviewees came from funding organisations, while the other six represent potential major customer organisations.

The current sub-section presents the responses along the 16 governance issues included in the questionnaire (Annex 4), analysis of the responses to the open-ended question to list additional governance issues, and concludes by ranking the governance requirements based on the stakeholders' views.

4.2.1 Profit orientation

Interviewees were asked whether they find profit or non-profit arrangements of preference for collaborative networked organisations. All interviewees considered both options possible. Two of them stated their preference for for-profit provisions since that would provide better flexibility of decisions to invest in infrastructure. Another two prefer non-profit arrangements assuming that, in such cases, it would be easier to find an agreement between constituent organisations and to exercise public oversight. One of the interviewees combined the two types of arguments, stating that a non-profit collaborative organisation may be preferable for participation in some funding programmes. At the same time, the provision of sustainability could be easier in the case of for-profit arrangements.

4.2.2 Geographical representation and limitations

Interviewees were asked whether particular geographical representation needs to be guaranteed and constraints imposed on membership from certain countries or regions. One of the interviewees noted that the composition of the network depends on its purpose. All respondents shared this understanding. Two of them focused on national representation, one of them stating that "national arrangements are preferred for strategic sectors [as cybersecurity]."

Most of the interviewees stated that balanced, EU-wide representation of member states is necessary or even imperative. One respondent emphasised the need to achieve cohesion through support to less developed regions, for example, by implementing a strategy of smart specialization. Another interviewee emphasised the importance of attaining EU cohesion to guarantee "European cyber sovereignty." Instead of national, two of the respondents focused on local representation; while not mandatory, one saw it as beneficial, and the other emphasised the advantages local representation provides in the access to local target markets.

One interviewee stated that even though the cybersecurity network can be centred in the European Union, it should have the flexibility to add partners from countries associated with the EU, as well as from other NATO members.

Two of the respondents expressed concern about opening EU-centred cybersecurity networks to partners from "Eastern countries" without specifying the meaning of "Eastern" in this case.

4.2.3 Supply chain security

The question on involving non-EU partners relates to supply chain security concerns and potential measures. The majority of the interviewees shared these concerns.

One interviewee interpreted the question as guaranteed availability of the necessary components of cybersecurity capability and expressed two main concerns: the provision of basic and advanced skills and R&D, in particular academic research and development.

The interviewees' opinions on the appropriate measures to provide supply chain security differ widely, including:

- sufficiency of a legally binding agreement;
- preference for entirely national management of the cybersecurity services;
- provision of transparency and fairness between the parties in the network;
- a requirement for security accreditation of each supplier and, preferably, guarantees from the national level authority;
- the need to put in place relevant policies and control mechanisms and to introduce applicable supply chain standards;
- provision of comprehensive tracking of the supply chain with the aim of reducing the related cybersecurity risks.

4.2.4 Involvement of external stakeholders

There is a general agreement that a collaborative organisation needs to involve and engage external stakeholders. Interviewees identified several possible roles of such stakeholders:

- strengthen the network by enhancing its cybersecurity capacity, e.g., by providing access to knowledge and experience in relevant R&D and innovation; knowledge and capabilities suppliers;
- representatives of universities in order to foster education and training activities;
- piloting (cybersecurity services) by companies or in certain countries;
- expert users to realise some specialization and customization of knowledge;
- opinion-makers for big enterprises or service providers;
- representatives of major funding organisations;
- when applicable, civil society representatives.

Government entities can be among the external stakeholders. The opinions of the interviewees differed in that regard. Two of them supported the involvement of governmental (political) stakeholders. In contrast, another one held the opposite view, stating that “representation of organisations with political or governmental affiliation [on network bodies] should be avoided.”

One interviewee explicitly stated that industry associations of SMEs are not the primary targets (contrary to big companies).

Interviewees pointed to several ways of involving external stakeholders:

- membership on an Advisory Board/Council;
- directly by a permanent robust “secretariat”;
- by regularly informing stakeholders on the network plans and activities.

One interviewee recommended “major funding organisations to be invited on a Steering or even on the Supervisory Board.”

4.2.5 Standards and methodologies

The fifth question was, “What standards and methodologies are or need to be used in the governance and management of the networked organisation?” The interviewees identified the following norms, frameworks, and methodologies:

- The EU Cybersecurity Act for general guidelines;
- COBIT as the key governance/management framework with ITIL for service provision and PRINCE II / MSP for project/programme management;
- GDPR for personal data protection;
- The RACI model as inspiration to keep the size of the governance structure efficient while allowing to exercise its central role, i.e., take and implement fair and knowledge-based decisions.

The need to govern and manage the network based on standards was underlined by one of the interviewees. However, most of the interviewees in their responses did not focus on standards and methodologies, emphasising instead that the importance of flexibility of the decision-making process and the autonomy in implementation. Hence, the governance model should provide for unity of purpose and the “right level” of decision-making autonomy to the chief executive, so that he or she can develop the network’s capacity to adapt to changing technological and market conditions.

One of the respondents elaborated on the need to have standardised rules and procedures for processing sensitive information and, if necessary, of classified information.

4.2.6 Representation on senior governance body/ies

“Fair” representation of network members on the senior governance body or bodies was considered essential by all interviewees who responded to this question. In certain cases, this might be the factor influencing the decisions, whether the services provided by the network will be used or not.

The respondents made several specific points of interest:

- "fair" may be considered in terms of regional representation on the 'Board';
- the representation must provide for collaboration between academia, industry and government;

- for a "European Union network," all member states need to be represented, plus key stakeholders such as ENISA, the EU Military Staff, the European Defence Agency, ECSO (for industry representatives), and the EU Joint Research Centre.

One interviewee noted that smaller partners might have limited human resources to allow for participation in senior governance bodies of a network.

4.2.7 Decision making

Interviewees were asked what in their view are the appropriate decision-making principles and rules, i.e.

1. whether votes of partners need to be of equal value or a weighted in some way, and
2. whether decisions need to be made by consensus or by a majority vote, with a simple or qualified majority.

All interviewees that commented on the first sub-question stated that votes of all partners need to have equal weight.

Interviewees agreed that decision-making by consensus is the desired underlying principle or the “preferred option.” However, they were also in agreement that consensus may be difficult to reach. Nevertheless, some of the decisions, for example, to add a new partner to the network, do require consensus. In other cases, a decision by majority vote may suffice. The opinions of respondents who commented on this issue were split. Some of the interviewees recommended decision-making by a simple majority vote, i.e., adhering to the “one partner – one vote” principle. In contrast, the others suggested that some form of decision-making by a qualified majority would be more relevant.

4.2.8 Auditing

One-third of the interviewees did not respond to the question of the need for internal or external audits of networked organisations. The remaining respondents, however, agreed that regular auditing is necessary. The use of external auditors, i.e., auditors that are not and have not been part of the network operation is preferred. The importance of auditors having a mandate was underlined by one of the respondents. It was suggested that for an EU-centred network, that mandate should be given by a relevant EU organisation.

One interviewee cautions not to overplay the need for auditing, stating that “there has been an increasing tendency to over-audit in public organisations in the past 10-15 years. This is counterproductive and resources intensive, often with doubtful results.” The same interviewee recommends adopting a risk-based approach to auditing, ensuring that audits are proportionate to the pursued objectives of the network.

One interviewee stated that financial audits should be performed by external auditors, while internally conducted audits of results and performance may be more beneficial for the network.

Agreeing with the need for internal and external audits, one interviewee recommends that they are complemented by certification, e.g., ISO 27001 certification, which also increases confidence in the network organisation.

4.2.9 Dispute and conflict management arrangements

Two-thirds of the respondents consider as important having some sort of arbitration in place to resolve disputes or conflicts between network partners, with a strong preference for setting up respective rules and procedures in advance.

One interviewee suggests having the Chairperson of a Governance group/ structure as internal Arbiter.

Another interviewee calls for such internal arbitration, stipulated in the network governance documents, in disputes of a business or financial nature, while referring to an *Ethics Code* to resolve ethical disputes, e.g., related to spreading information that can be damaging to a partner or an external stakeholder.

A third interviewee recommends setting up in network governance documents an escalation path to the highest governance body of the network, followed by the respective court authority, depending on registration.

Another interviewee opts for national management guarantees and the principle of territoriality in dispute/ conflict scenario envisioning escalation.

4.2.10 Confidentiality

For a network in the field of cybersecurity, confidentiality was seen as a key consideration by the majority of interviewees. This governance issue covers the protection of personal data, classified or other sensitive information. Among the specific measures, interviewees listed:

- signing mutual non-disclosure agreements (NDAs);
- introducing layered confidentiality agreements;
- adhering to applicable legislation/rules of international or EU organisations, i.e., the guidelines from EU, OECD or UN should serve as a basis to establish a reliable confidentiality framework;
- implementing vetting and levels of classification;
- screening and profiling of people;
- introducing methods for controlled use of shared information, like Chatham House Rules and TLP protocols (for unclassified information);
- establishing mechanisms in place to allow working with sensitive, confidential information; at least some of the partners need to have in place the organisational prerequisites and the technical infrastructure to allow work with classified information, including for example security of collaborative environments and provision of communications security;
- not allowing external partners to work with local classified information;
- continuous verification or rules, procedures, and actual status of confidentiality.

4.2.11 Intellectual Property management arrangements

Most respondents saw arrangements for the management of the intellectual property as important in order to protect valuable knowledge and the competitive advantages of the network while enhancing its capacity through collaboration and sharing of information and experience.

One interviewee emphasises the need to put in place strong fees and penalties for intellectual properties infringements, and to provide regular evidence that the protection of intellectual properties is well managed.

Another interviewee advises to build on the rules set by the European Commission and model grant agreements for the management of intellectual property developed under EU funding by introducing specific arrangements for IPR as a result of implementing customer-funded projects. In any case, it is necessary to seek preservation of intellectual property for the network organisation as a whole, thus providing for replication of knowledge and a larger market share.

4.2.12 Ethics code

Almost half of the respondents considered ethical behaviour as an issue that does not require special treatment since all partners in the network are expected to observe the applicable EU policies. The remaining interviewees, however, believed that a network organisation needs an Ethics Code that is:

- accessible, well documented and well communicated throughout the network and its external stakeholders;
- includes a map of values and is supported by an "action structure" allowing to implement ethical guidelines;
- covers confidentiality and transparency considerations, equal access to services, incentives, non-discrimination of members and partners;
- of specific interest is the regulations for "ethical hacking," as well as the potential collaboration with law enforcement and secret services.

One interviewee emphasises that it is fairly easy to adopt a set of standards that should be respected in delivering services, in organising and managing the network, etc., while enforcement is trickier; yet, "removal from duties / laying off/ stopping ongoing third-party contractors, etc. should be embodied as possibilities/ rules in the 'founding principles' of the network."

4.2.13 Specific ethical issues

With this question, interviewees were asked whether they consider issues such as having a policy in regard to slavery or the use of labour of minors relevant for cybersecurity. Most interviewees consider these issues either not applicable or not in need of discussion. In the words of one of the respondents, "we would never engage ourselves with anything unethical."

Only one interviewee states that it is "mandatory [for a network organisation] to conform on EU regulations on these topics in order to be considered a service supplier for my organization." Yet, the general opinion is that it will be sufficient to implement relevant EU norms and regulations.

4.2.14 'Green' policies

Most interviewees agree that environmental considerations are important, e.g., to reach the 2030 sustainable development targets. Still, they cannot be in the focus of network governance policies and models, and that adherence to "applicable EU policy" is sufficient.

One of the respondents elaborates on the issue, stating that

> Green policies should ensure: preference for green services, products and processes, for economic operators and groups actively engaged in respecting international commitments as far as climate

> change is considered; they (policies) should ensure mandatory clauses in contracts and procurement securing preference for products and services, and in hiring staff who display a green mindset.

4.2.15 Gender policies and representation

More than half of the interviewees elaborated on this governance aspect, and some of them stated clearly that they do not consider this “a fundamental aspect,” and that merit needs to be put ahead of gender equality. Others among the respondents stated that adherence to “applicable EU policy” will be sufficient.

One of the interviewees emphasised the advantages of ensuring diversity of the cybersecurity workforce and gave examples in delivering courses, incl. e-learning courses, aimed at girls to contribute to skills’ objectives, as well as in having women in leadership positions.

Further, one of the interviewees recommends the adoption of an “equal treatment, equal opportunities” framework using the existing corpus of UN, EC, Council of Europe, and OECD policies, and seeking expertise and ready-to-use material from agencies of the European Union, pointing explicitly to the Fundamental Rights Agency and the European Institute for Gender Equality.

4.2.16 Transparency and integrity policies

With this question, the interviewees were invited to express their opinion on the importance of good governance issues, such as transparency, integrity policy, whistle-blowers’ protection, or anti-corruption policy more generally.

The majority of the respondents considered these aspects important, and one called for “maximum transparency and integrity in the governance” of the networked organisation. Yet, the prevailing view is that if the network and each individual member follow the relevant EU legislation, there is no need for special additional requirements. One of the interviewees states that

> There is a robust existing architecture for integrity, anti-corruption, integrity at EU level, and international guidelines and instruments that can be used to design a framework ensuring for such networks the rule of law, legality and ethics in all their dimensions. If the network organization is financed by the EU, the existing framework at EU level can be readily used. If the network is operating internationally, respective frameworks and conventions designed at UN, OECD, OSCE, World Bank etc. could be adopted.

One of the more specific recommendations was to provide special training [for the personnel of the network organisation] for avoiding conflict of interest and anti-fraud training, followed by an online exam and signing of a declaration.

4.2.17 Additional governance issues

Interviewees were asked to list additional governance issues that they consider important but were not included in the list of previous questions.

Some used the opportunity to reemphasise ***transparency***, ***openness*** and ***accountability***, e.g. by introducing requirements for publication of an annual report and financial statement; separation of roles and responsibilities to assure that decision-making bodies abide to transparency; and assuring compliance to the regulatory, legal and operational framework defined in the founding charter of the network.

Respondents also stressed ***ethical considerations***, including:

- adherence to formal and strict rules that ensure the selection of the right staff, whereas such rules are defined during the network's founding and establishment phase and endorsed by the networks' "ultimate stakeholders";
- support the implementation of such HR policy by formal guidance, toolkits, and rewarding mechanisms;
- development of a charter defining funding, selection of the key leaders on governance and management level and their respective accountability;
- remain independent from partisan and political influence.

A related group of governance needs and requirements relate to ***trust*** between the partners and to the network as a whole. Internally, all participants in the network must have a good reputation and share goals and values that are considered fair, honest, and equal. Cultural differences need to be recognised and mutually tolerated, except for illegal or immoral behaviour. Towards that purpose, fair and open communication between the members of the network needs to be maintained. Externally, the trust in the network depends on the extent to which it includes recognised authorities in relevant technical/research fields.

Fairness and trust facilitate the network's ***cohesion***, which may be further strengthened by a common perception of threats in cyberspace, providing opportunities to all network members, supporting the ones that are more active while giving feasible challenges to those who are not highly involved.

One interviewee again emphasised the preference to having one supplier of cybersecurity products and services per country or even to look for solutions envisioning "full nationality" in both the resources used and the potential suppliers. One possible approach here is that the network provides its technology for license to national implementors.

Interviewees referred also to some ***managerial considerations*** such as:

- introduction of results-oriented management, supported by appropriate instruments for performance monitoring and measurement, e-Procurement, and provision of information and targeted training opportunities;
- sharing of knowledge;
- quality control.

A group of statements calls for governance assuring ***openness, adaptiveness*** of the network and ***innovation***, needed to:

- remain open for new opportunities and partners to pursue new initiatives;
- connect the network with other technology-specific EU organisations and EU partnerships so that new multidisciplinary initiatives can be pursued;
- create a rapid, dynamic organisation with short decision-making process which detects opportunities, adapts to the needs of the times and generates innovation;
- use crises to promote change.

Among others, these qualities of the network are expected to make it more ***resilient*** and ***sustainable***.

In the final group of needs and requirements, interviewees underline the role of ***strategic communication and engagement*** aiming to:

- develop the network's capacity to work with media, stakeholders, and the wider public;
- create opportunities to share knowledge and awareness about the network;
- formal use of collaborative platforms and social media to stimulate/encourage citizen feedback, participation and continuous input;
- engage in an open culture favouring open interaction with the civil society, encouraging co-creation, social innovation and an open participatory network.

4.2.18 Ranking governance requirements

Figure 7 summarises the results of the analysis of interviews, allowing to suggest three categories of governance needs and requirements:

1. Those that need to be in the focus of attention in developing and evaluating network governance models (addressed by more than 75 percent of the interviews). In this tier are the ***geographic representation***, the involvement of ***external stakeholders***, the ***decision-making arrangements***, and the need to provide for ***confidentiality***;
2. "Important" may be considered governance needs addressed by 50 to 75 percent of the interviewees. ***Supply chain security***, ***representation*** on the senior governance bodies, ***auditing***, ***dispute*** and ***IPR*** management, having an ***ethics code***, ***gender policy***, ***transparency***, ***accountability*** and ***integrity***.
3. The remaining governance issues were found of interest by less than 50 percent of the respondents. Hence, it is possible that a reference to some more general norms, e.g. EU norms, might be sufficient to address these governance issues. They can be further subdivided in two tiers – referenced by 25 to 50 percent of the respondents (***profit orientation*** of the network and the implemented ***standards and methodologies***), and those found to be of interest by less than a quarter of the interviewees (the use of ***slave labour*** or ***labour of minors***, and ***'green' policies***).
4. Several additional governance issues were identified by interviewees: ***innovation***, ***adaptiveness***, network ***cohesion***, ***trust*** between the partners, as well as to the network as a whole, ***sustainability***, ***resilience***, ***communication and engagement***, and ***knowledge sharing***. Some of the respondents referred also to some managerial considerations aimed at making the network more effective, efficient and, as a result, more ***competitive*.**

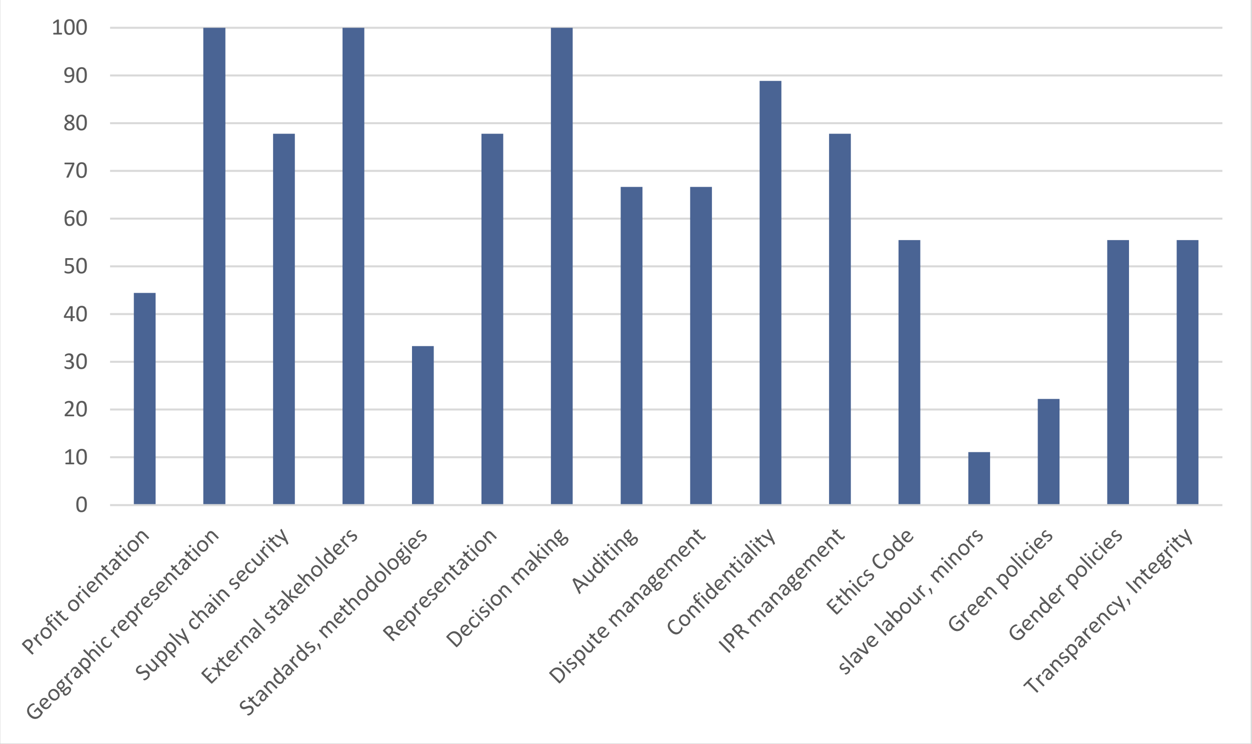

Figure 7: Interviews-based ranking of governance requirements.

The interviews allowed to elicit expectations of representatives of funding organisations and potential major customers to the governance of networked cybersecurity organisations. No substantial distinctions in these expectations among the two groups of stakeholders were identified.

4.3 The academic literature on network governance requirements

4.3.1 Reflection of governance requirements included in the interviews' and network analysis template

The governance issues listed in the template for interviews with stakeholders and analysis of networked organisations do not feature prominently in the academic sources. None of the sources addresses explicitly ***supply chain security*** concerns and measures, ways of involving ***external stakeholders*** (other than the general recommendations for communication); the ***representation*** of member organisation on the senior governance body; ***specific ethical issues*** such as the use of labour of minors or slave labour; and ***gender*** policies and representation. Only one source refers respectively to ***auditing*** and the need for ***anti-corruption policy***, while ***accountability*** and the need for an ***ethics code*** are addressed by two sources each.

The ***management of disputes*** and ***IPR*** issues are referenced in four academic sources, i.e. in discussing escalation patterns (Barchetti et al., 2012) and risks of Intellectual Property Rights infringement (Su, Biennier, and Ouedraogo, 2012).

Five publications treat ***confidentiality and security*** issues, e.g. the collaborative security requirements and protection of knowledge (Aagaard, 2019). These are newer publications, dealing with the importance of the digital infrastructure for collaboration or the advantages novel technologies, such as blockchain (Schaffers, 2018). Another five sources address ***green policies***, e.g. the need to respect ecological aspects, to take account of environmental challenges, promote biodiversity and apply the concepts of cyclic economy and the “Green Virtual Enterprise Breeding Environment”.

Geographical representation is addressed in seven publications primarily from the point of view of regional collaboration with positive economic and social impact on local communities (e.g. Bandinelli, d’Avolio, and Rinaldi, 2014), but also accounting for the need to access new markets and go beyond traditional geographic boundaries (Arrais-Castro et al., 2018).

The authors of nine academic publications address ***decision making*** aspects of governance, e.g. that member organisations want to maintain a “fair level of autonomy in their decision-making and negotiation processes” (Rossignoli, Mola, and Zardini, 2007) and to provide for “similarity regarding authority and rank” within their organisations to assure “decision making within rank homogenous” groups (Ulbrich et al., 2011).

Most salient among the ‘original’ governance requirements, i.e. those included in the interview questionnaires and the template for analysis of networked organisations, is ***transparency***. Authors of 15 of the analysed publications discuss the needs of greater visibility and open access to information, in particular in:

- understanding how the network creates value (Romero and Molina, 2011), how different variables of the collaboration fit together as a system to help creating value for each participant (Tapia, 2009), and assuring that the ‘value system’ that is relevant to all network stakeholders (Harrington and Srai, 2016);
- assessing partner competences (Durugbo and Riedel, 2013);
- network delivery assessment (Durugbo and Riedel, 2013);
- revenue streams and cost structures between collaborators (Romero and Molina, 2011); and
- enabling traceability of changes in collaborative processes and organisation (Obidallah, Raahemi, and Alaieri, 2014).

The ranking of these governance needs according to the number of academic sources that refer to them is visualised in Figure 8.

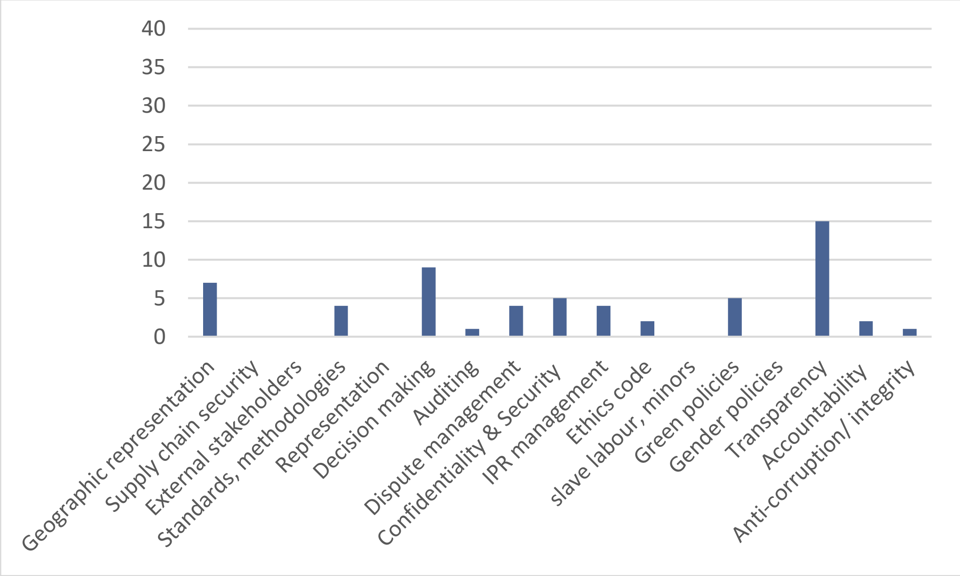

Figure 8: Ranking of ‘original’ governance requirements in the academic literature.

The following subsections present findings on governance issues already identified by interviewees (innovation, adaptiveness, cohesion, trust, sustainability, and resilience), as well as new ones referenced in the analysed academic sources – communication and engagement, knowledge management, long-term perspective on collaboration, interoperability, leadership, organisational culture, competences, risk management, evidence-based decision-making, and competitiveness. The next subsection highlights briefly the interplay among a number of the presented governance issues, and the final one summarises the findings of the analysis of academic sources.

4.3.2 Innovation

The need for and the opportunities for innovation provided by collaboration are addressed in 24 of the analysed academic sources. The references span from the importance of innovation to capture new business opportunities through the need to develop capacity and readiness to innovate and the application of the Open Innovation paradigm arguing for the need to establish new models, where much of the knowledge comes from outside the boundaries of the company (Mortati, 2013) to the call for establishing Collaborative Innovation Networks, or COINs—"self-organizing emergent social systems”—as “primary building blocks of innovation” (Grippa et al., 2018).

The ECHO consortium will deal with this governance aspect in more detail in Task 9.4 “Innovation Management”.

4.3.3 Adaptiveness

Based on the analysis of the academic literature, ***adaptiveness*** emerged as the most salient governance issue, along with the consideration of *competitiveness*. It is addressed by 35, or nearly 60 percent, of the analysed sources. Authors emphasise that “systems that want to live long must co-evolve with their environment” (Kandjani and Bernus, 2012) and highlight various aspects of adaptiveness, including:

- CNOs' adaptability to changing environment (markets, technologies), the need to cope with external change through an adequate rate of adaptation, and evolutionary development, aiming at continuous improvement;
- flexibility and the need to swiftly adjust to market challenges and adapt to turbulent contexts;
- change management; redesign, reengineering, renewal and restructuring; process reengineering and having flexible business processes;
- agility and the capabilities "to sense and respond to predictable and unpredictable events (Hovorka and Larsen, 2006);
- the capacity to self-organise, self-adapt, and exhibit emergent behaviour (Bilal, Daclin, and Chapurlat, 2014);
- achieving "strategic flexibility" (Crawford et al., 2009), e.g. through adaptive policy-making (Jackson and Cardoni, 2017).

4.3.4 Cohesion

Sixteen academic sources underline the importance of achieving ***cohesion***. Network cohesion builds on shared understanding and attitudes, negotiation and agreement on rules of cooperation, planning and prediction process shaped by negotiation, good level of alignment among the value systems of the various members of the network, and other intangible elements, such as reputation, friendship, interdependence, and trust.

When there is harmonization among CNO partners and cohesion of the network one witnesses sense of identity, high levels of solidarity, shared passion and motivation, and better opportunities for:

- balancing interests;
- complementarity and subdivision of successes and risks;
- developing social capital;
- alignment and integration across an increasingly complex network of multiple partners and collaborators; and
- exploiting creative synergies.

4.3.5 Trust

Twenty-seven of the analysed academic sources refer to ***trust***. Twenty-six of them look into *trust among partners*, i.e. trust building and confidence among participants, while five reference trust into the collaborative networked organisation by external stakeholders, users, and society, including criticality of relationships and knowledge, image and reputation of the CNO and customer confidence. Four of the sources address both internal and external aspects of trust.

4.3.6 Sustainability

Seven of the academic sources reference aspects of ***sustainability***, including sustenance under uncertain and rapidly changing conditions (Durugbo, 2016), that would provide for more predictable organisational behaviour and less turbulence (Noran, 2004), stability and robustness.

4.3.7 Resilience

Resilience of networked organisations is referenced in six sources. A resilient organisation preserves its key functionalities under negative impact and has a capacity to recover from disruptive and even catastrophic events by securing access to critical resources and information in an effective and timely manner (Jung, 2017).

4.3.8 Communication and engagement

Eighteen of the studied academic sources address the issue of ***communication*** is several aspects. First, communication among partners in the networked organisation, in particular that related to knowledge sharing, is seen as an indicator of the level of maturity of the network (Durugbo, 2016). Second is the communication with external stakeholders, more specifically the interaction with customers and customer communities, e.g. to receive feedback from users. Third, open and transparent communication and engagement of users and wider society may be of strategic nature, leading to co-creation (Krčo et al., 2019) and co-innovation, or "open innovation" (Romero and Molina, 2011). It needs to include rewarding mechanisms for involved customers and will thus reinforce the network's social influence and support knowledge transfer.

4.3.9 Knowledge management

Fifty percent of the studied academic sources (the third highest percentage) emphasise the importance of ***knowledge management***, including:

- knowledge acquisition and the organisation's capacity to transform information gathered from a vast array of diverse sources into useful knowledge;
- knowledge exchange or knowledge sharing;
- knowledge enrichment and the creation of transdisciplinary knowledge;
- knowledge representation;
- the use of knowledge (enterprise knowledge resources), e.g. for making effective decisions;
- knowledge retention or minimising knowledge loss in changes of the networked organisation.

The analysis of the literature allows also to highlight also some more specific issues of interest, such as:

- managing tacit knowledge (Crawford et al., 2009; Barchetti et al., 2012);
- the importance of aligning knowledge management with structured business processes (Barchetti et al., 2012);
- the need for systematic efforts to increase the *absorptive capacity* of the networked organisation, i.e. its "ability to acquire, assimilate, transform and exploit new knowledge" (Hovorka and Larsen, 2005);
- the conditions of performance, creativity and collaboration of *knowledge workers*, seen as central to an organisation's success (Barchetti et al., 2012);
- information and knowledge brokering and the roles a knowledge broker may play in a networked organisation (Rostek, 2015); and
- the use of active knowledge models (Pawlak and Jørgensen, 2015).

4.3.10 Long-term perspective on collaboration

Fourteen sources, or nearly a quarter of the ones under study, refer to the need for ***longer-term view on collaboration***. Some of the authors emphasise prerequisites, such as having a common purpose, or coherence of the purposes of collaborating partners, and shared goals. Among the tools for achieving such long-term perspective as the collaborative predicting and planning (Serrier, Ducq, and Vallespir, 2017) and setting reasonable expectation of success (Ulbrich et al., 2011). Of particular importance is the 'strategic approach' to collaboration by establishing a long-term "network vision" (Cardoni, Saetta, and Tiacci, 2010; Saetta, Tiacci and Cagnazzo, 2013) to define the strategic mission and strategic options. In that respect some authors call for strategy-based governance and management and focusing efforts by aligning proactive strategies (Andres, Poler, and Sanchis, 2015).

4.3.11 Interoperability

The issue of ***interoperability*** is subject of discussion in seven academic sources. Some of them examine technical aspects, such as requirements to the technical infrastructure supporting the collaboration, including to information systems (e.g. Bilal, Daclin, and Chapurlat, 2014) and architecture frameworks that can be used to facilitate interoperability, while others refer to norms, procedures and allocation of decision-making roles to allow for smooth interoperation among network partners. Importantly, interoperability is included among key issues examined in assessing the readiness of collaborative networked organisations to effectively deliver their products and services (Durugbo and Riedel, 2013).

4.3.12 Leadership

Six of the examined sources refer to the ***leadership*** in collaborative organisations, including commitment, motivating and empowering members of the networks, e.g. through enhancement of their capacities, readiness of executives able to allocate resources when needed, and adhering to the principle of neutrality in network management. Some of the authors emphasise even less tangible aspects of leadership, such as fairness and capacity to effectively manage complexity, as well as the understanding and utilisation of informal leadership in the network.

4.3.13 Organisational culture

Ten sources refer to ***cultural issues*** in collaborative networked organisations. Bilal, Daclin, and Chapurlat (2014) examine diversity as a "crucial characteristic" of a system of systems (the "engineering twin" of a CNO). Others see differences in organisational cultures as a significant deterrent to effective collaboration (Durugbo, 2016). Yet others argue that adequate culture, in their case study—through professional peer pressure—is more conducive to shaping ideas, motivating and energising the workforce, than is the strict compliance to rules and regulations (Mabey, Wong and Hsieh, 2014). In any case, CNO leaders are advised to promote mutual respect, spirit and ethic of collaboration, culture of openness and sharing ideas, and to invest in advancing cultural competence and mutual understanding (Song et al., 2019) and "communicative culture" (Enquist, Nilsson and Magnusson, 2004).

4.3.14 Competences

Forty percent of the analysed sources address CNO ***competences*** and ***learning***. That includes:

- understanding of and developing the CNO expertise potential, seeking to build the network mass and also multidisciplinary competences;
- building CNO competences by sharing knowledge and exchanging skills (Mortati, 2013);
- developing individual and organisational capabilities for intuitive thinking, complex data analysis and communication (Crawford et al., 2009).

The issue of network competences (along with the access to new markets) is of particular importance in the process of identification, assessment and selection of new partners (Arrais-Castro et al., 2018), as well as retaining existing partners. The purpose is to develop and maintain the requisite collaborative capability (Ulbrich et al., 2011).

Individual and organisational learning is another venue to develop the network competences. The academic literature addresses a number of learning issues, including the learning process, self-learning, agile learning, learning mechanisms for transformation, incremental learning, and the adoption of common best practices for organisational learning.

4.3.15 Risk management

The role of ***risk*** is referenced in 14 academic sources, covering respectively the need for:

- Identifying and quantifying existing or potential hazards, for example at the level of communication, management and sharing of knowledge (Abreu and Calado, 2017);
- major concerns related to the use of shared assets and risks of intellectual property infringement (Su, Biennier, and Ouedraogo, 2012);
- reducing uncertainty (Komanda, 2012);
- risk mitigation (Durugbo, 2016); and
- sharing risks among network partners (Romero and Molina, 2011).

4.3.16 Evidence-based decision-making

The importance of ***data- and evidence-based decision-making*** is referenced in nine sources. The implementation of this core principle of quality management according to the international standards (including the ISO 9000 series) requires putting in place organisational processes for systematic data collection (e.g. Pierce, Ricciardi and Zardini, 2017) and maintaining a repository of network assets (Tapia, 2009), including data, information and knowledge.

4.3.17 Competitiveness

Aspects of ***competitiveness*** are addressed in the highest number of the analysed academic sources – 39 sources or nearly 70 percent. This can be expected, since value, generated benefits and, for the profit-oriented organisations, market share, return on investments, etc. are the lead drivers for establishing collaborative networked organisations in the first place. This governance objective was not among those studied in the interviews and the analysis of existing networked organisations, with the assumption that a collaborative networked organisation coming out of the ECHO consortium would have the technical capacity and organisational performance to be among the top most competitive suppliers of cybersecurity services; hence the focus there was on other governance issues.

The academic literature addresses, at times very comprehensively, aspects of competitiveness like:

- effectiveness;
- involving the most suitable partners with complementary competencies and providing access to new markets;
- customer-focus;
- reduced time to market;
- lower costs;
- delivery of higher quality services and products;
- larger service and product portfolio;
- enhanced enterprise assets value;
- faster delivery;
- reliability;
- efficiency; etc.

Among the tools to achieve a differentiated competitive advantage, the academic literature suggests performance management, collaborative process management, business process alignment, effective and timely resource coordination, quality control, etc.

4.3.18 Interplay of governance issues

The academic literature reveals numerous interdependencies between two and more governance issues. The review of these interdependencies is not within the scope of the current studies. The following four examples serve only for illustration purposes.

Durugbo (2016) points out that the collaborative culture is "instrumental to openness, commitment, leadership, trust-building, self-learning, continuous training, long-term and global vision, effective communication, knowledge sharing and innovation".

Li, Biennier, and Amghar (2012) concur underlining that a culture of openness and sharing ideas is conducive to "enhancing flexibility in business processes and innate ability to embrace innovation".

According to Hovorka and Larsen (2006) there is sufficient data suggesting that "network organization characteristics and communication processes that reinforced social influence and supported knowledge transfer positively influenced adoption agility".

Finally, there are also links between self-organisation, innovation and resilience: Grippa and co-authors (2018) claim that "Collaborative Innovation Networks build resilience by forming, spontaneously and without intervention on the part of the management, to creatively respond to new risks and external threats".

4.3.19 Ranking governance requirements

Figure 9 summarises the results on governance requirements, identified in the interviews and the academic literature, presenting the number of times a governance issue has been referenced in the 60 academic publications analysed here. It shows that three of these—***competitiveness***, ***adaptiveness*** and ***knowledge management***—are tier one requirements. Another four requirements—***innovation***, ***trust***, ***competences*** and ***risk management***— correspond to tier 2. Tier 3 includes ***cohesion***, ***communication***, ***long-term perspective***,

culture and ***evidence-based decision-making***, as well as ***decision-making*** and ***transparency*** from the original list of governance issues. All remaining governance issues are in tier 4.

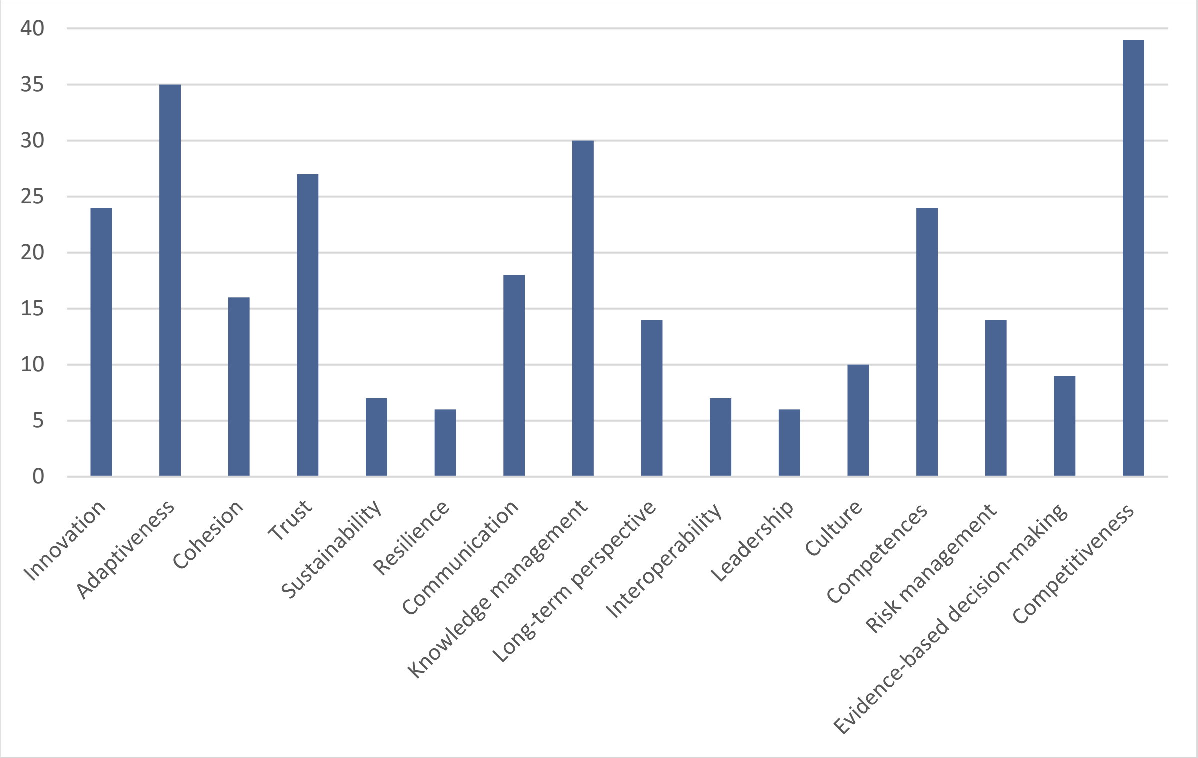

Figure 9: Ranking of additionally identified governance requirements in the academic literature.

4.4 Governance requirements in existing networks

All key information sourced from the primary analysis of the existing networks (n=92) in the MS Excel matrix was collated and summarised; this data is presented in the following section.

A qualitative approach was adopted wherein predominant governance needs and requirements were identified and detailed for the majority of existing networks.

First, the findings for profit-oriented CNOs are presented, followed by the findings for non-profit collaborative organisations and for CNOs, for which the profit status was not available.

4.4.1 Findings for profit-oriented networked organisations

Total number of for-profit CNOs = 7.

Geographical representation or exclusion

- Geographical representation = EU member states, all of the Asia-Pacific region; Australia; USA.
- Predominant geographical exclusion zones = Middle East (aside from Israel); Africa; South America; Russia.

Ways of involving external stakeholders

- Involvement in advisory boards or steering committees;

- Option for University research integration by commercial companies;
- Establishment of a training, education and skills platform;
- Seeking expertise from industry to strengthen cybersecurity capabilities.

Representation on the senior governance body

- Case study 1 – detailed the adoption of a steering committee which oversees the CNO's activity and reports back to European Commission. The Steering committee also has power to appoint the CEO and deputy.
- Case study 2 – establishment of a council.
- Case study 3 – the governance body consists of a Board Chair, 2 Board Members and a Board Advisor.
- Case study 4 – the governance body consists of 2 Co-Chairs, 26 commissioners and a Secretariat.
- Case study 4 – the governance body consists of a Project Management Board (PMB).

Decision making principles

- Steering boards typically have the authority with regards to decision making for the CNO in most cases. Examples include the following:
    - The Steering Committee is the CNO's key decision-making body, which regularly reviews training and education activities, approves the annual academic plan, selects and prioritises the training and education activities; decides on opening specific training activities and education, adopts the curricula for all CNO's training and education activities, etc.
- The Steering Board is the decision-making body of the Agency. The Steering Board acts within the framework of the guidelines and guidance of the Council.
- For one case study, the supreme authority of the CNO ("The Society") was vested in General Meetings and subject to that authority of The Society which was governed by The Council. The quorum for a Council Meeting shall be half the total number of Council Members. Decisions of any Council Meeting shall be arrived at by a majority vote by a show of hands, unless secret ballot shall be demanded by a majority of members of The Council present. In the case of an equality of votes, the chairman of the Council Meeting shall have a casting vote.
- Qualified majority in Project Management Board meetings.

Internal and/or external audits

- An audit of accounts is conducted annually. The necessary auditing services may be outsourced. The audit reports shall be made available to the Steering Committee together with the detailed report.

- The Agency shall have an internal audit function which shall be performed in compliance with the relevant international standards. The internal auditor may neither be the Authorising Officer nor the accounting officer. The internal auditors shall advise the Agency on dealing with risks, by issuing independent opinions on the quality of management and control systems and by issuing recommendations for improving the conditions of implementation of operations and promoting sound financial management. The internal auditor shall draw up an annual audit plan and submit it to the Chief Executive. The internal auditor shall report to the Chief Executive on his or her findings and recommendations.

- The Chief Executive shall ensure the regular monitoring of the implementation of audit recommendations. Each year the Chief Executive shall send to the Steering Board a report containing a summary of the number and type of internal audits carried out, the recommendations made and the action taken on those recommendations.

- The Steering Board shall examine the information and whether the recommendations have been implemented fully and in a timely manner. The reports and findings of the internal auditor shall be accessible to the public only after validation by the internal auditor of the action taken for their implementation.

- The Steering Board shall appoint a College of Auditors to perform the external audit function of the administrative and operational budgets, financial accounts and financial statements. The audit shall be conducted in conformity with accepted international standards on auditing and, subject to approval by the Steering Board, in accordance with additional terms of reference.

- A Voting Member of the Society or a member of the public shall be appointed at the General Meeting to audit the accounts of The Society as soon as the close of each financial year as possible. They will examine all books and accounts of The Society and shall certify as to their correctness or otherwise.

Dispute/conflict management arrangements

- Where a conflict of interest is found to exist, the person in question shall cease all activities in the matter. The Chief Executive, or the Head of the Agency in the event that the conflict of interest concerns the Chief Executive, shall take any further appropriate action. Before recruiting a member of temporary staff, the authority authorised to conclude contracts (AACC) shall examine whether the candidate has any personal interest such as to impair his independence or any other conflict of interest. To that end, the candidate shall inform the AACC, using a specific form, of any actual or potential conflict of interest. In such cases, the AACC shall take this into account in a duly reasoned opinion.

- Members of temporary staff intending to engage in an occupational activity, whether gainful or not, within two years of leaving the service shall inform the Agency thereof using a specific form. If that activity is related to the work carried out by the member of temporary staff during the last three years of service and could lead to a conflict with the legitimate interests of the Agency, the AACC may, having regard to the interests of the service, either forbid him from undertaking it or give its approval subject to any conditions it thinks fit. The AACC shall, after consulting the Staff Committee, notify its decision within 30 working days of being so informed.

Confidentiality

- Compliance with EU security policy regulations (i.e. Decision 2013/488/EU).

Intellectual Property management arrangements

- Users may download or print one copy of any and all materials on the site for personal, non-commercial use, provided that they do not modify or alter the materials in any way, nor delete or change any copyright or trademark notice. None of the information on this site may be copied, distributed or transmitted in any way for commercial use without the express written consent of the organisation. For any materials downloaded from this site source and references must be acknowledged. The organisation reserves full ownership and intellectual property rights of any materials downloaded from this site.

Ethics code and its enforcement

- Devising a transparent declaration.
    - For example: The CNO endeavours to operate in a clear and open manner and is mindful of its duty of transparency towards EU citizens (see Code of good administrative behaviour and cooperation with the European Ombudsman). The CNO also strives to ensure that its staff and management do not have any interests that could affect their impartiality and has put in place specific policies to deal with any potential conflicts of interests.

- Publication information (annually) on its duty to prohibit senior members of temporary staff, during the 12 months after leaving the service, from engaging in lobbying or advocacy vis-à-vis staff of their former institution for their business, clients or employers on matters for which they were responsible during the last three years in the service.

- Notice of use of a product (e.g. CNO website). Users declare that the site will not be used for any purpose that is unlawful or prohibited by these preconceived terms, conditions, and notices. You may not use the site in any manner which could damage, disable, overburden, or impair the CNO's website or interfere with any other party's use of the site.

Specific ethical issues, e.g. policy in regard to slavery, use of labour of minors

- Not explicitly specified.

'Green' policies

- Not explicitly specified.

Gender policies and representation

- Establishment of a "Ladies in Cybersecurity" charter: aimed at promoting development, advancement, and inclusion of women in the cybersecurity field.

- Devising initiatives at a grassroots level and also in senior levels of industry.

- Each geographical chapter is responsible for fair representation/ diversity with respect to governance.

- Establishment of a female led Advisory Board.

Transparency

- Not explicitly specified.

Anti-corruption/ integrity policy (e.g. whistle-blowers protection)

- Not explicitly specified.

4.4.2 Findings for non-profit networked organisations

Total number of not-for-profit CNOs = 73.

Geographical representation or exclusion

- Geographical representation = many not-for-profit CNOs have Worldwide coverage. The majority of CNOs are based in the EU, USA and Asia.

- Predominant geographical exclusion zones = worldwide coverage indicates that no countries are excluded.

Ways of involving external stakeholders

- Establishment of coordination/ strategic/ management/ steering/ industry expertise committees.

- Establishing collaborative partnerships with private industry and policy makers (to share expertise which would benefit the CNO's members and industry partners).

- Provision of a funding scheme for cybersecurity projects.

- Coordinating networks of practitioners and researchers.

- Facilitating sessions with EU and national level funding authorities.

- Hosting cyber-security conferences and networking events.

- Provision of (cyber) training sessions specific to various external stakeholders needs (i.e. governments, academics, etc.).

- Provision of different membership classifications.

- Provision of professional certification either in conjunction with an academic institution or accredited by a professional body.

Standards or methodologies used

- Control Objectives for Information and Related Technologies (COBIT).
- Information Technology Infrastructure Library (ITIL).
- PRojects IN Controlled Environments (PRINCE II).

Representation on the senior governance body

- Case study 5 – The Association's governance is ensured by the following bodies: General Assembly; Board of Directors.
- Case study 6 – a policy body was established to carry out the mission of the organisation as well as exercise unified governance (members not specified).
- Case study 7 – senior governance body representatives include: Board of Directors (and board members), Executive Director, Committees of the Corporation (1. Audit Committee, 2. Business Practices Committee, 3. Professional Conduct (Ethics) Committee).
- Case study 8 – senior governance body representatives include: 1. Founder, 2. Chair of the Board, 3. Treasurer, and various other ordinary board members including: Senior Fellow (research orientated); Director of associated graduate school; Senior Manager of Information Security; Diversity, Inclusion & Engagement Manager; Vice-President of a Corporation, Security Director from Private Industry, a Chief Scientist from an Associated University, and an Emeritus Executive Director.
- Case study 9 – senior governance bodies include: General Assembly, Auditor, President, 2 Vice Presidents, General Secretariat, 20 Directors, 29 Secretaries, 9 Advisers and specialised Committees.
- Case study 10 – senior governance body representatives include: President, 1st Vice President, 2nd Vice President, Honorary Secretary, Assistant Honorary Secretary, Honorary Treasurer, Assistant Honorary Treasurer and up to 7 Ordinary Management Committee Members.
- Case study 11 – senior governance body representatives include: Members of Board: chairman; chief vice chairman; auditor; executive vice chairman and vice chairman.
- Case study 12 – senior governance body representatives include: 1) a Governing Board composed of high-level members experienced in higher education, research, innovation and business. It is assisted by an Executive Committee, which consists of the Governing Board Chairperson and three members

of the Governing Board; 2) a Director, appointed by the Governing Board, who is responsible to the Governing Board for the administrative and financial management of the CNO and is the legal representative of the organisation; 3) an Internal Auditing Function which advises the Governing Board and the Director on financial and administrative management and control structures within the organization, on the organization of financial links with KICs and on any other subject requested by the Governing Board.

- Majority of CNOs host the following directing officers: a President, a Secretary and a Treasurer, each of whom is elected by the Board of Directors. A Chair of the Board, one or more Vice Chairpersons, one or more Vice Presidents, and such other officers and assistant officers and agents as may be deemed necessary may be elected or appointed by the Board of Directors from time to time.

- The business and affairs of the network are typically managed by or under the direction of the Board of Directors.

Decision making principles

- The Annual General Assembly and the Extraordinary General Assembly strive to adopt its resolutions by unanimous consensus of the present Members. If a unanimous consensus has not been reached and a vote proves necessary, the resolution shall be adopted if it receives a: Quorum: one third (1/3) of Members present or represented or Majority: simple majority (more than 50%) of votes of Members present or represented by proxy.

- All decisions are managed by the following (depending on the organisation): steering committee, a management board, a supervisory board, or general assembly by qualified majority (i.e. of two thirds of its members).

- Quorum and Voting: A majority, including one officer, of all Directors then in office shall constitute a quorum at all meetings. When a quorum is present, voting at any meeting shall be by majority vote except as required by law, the Articles of Organization, or these Bylaws. The number of Directors necessary to establish a quorum shall be adjusted as necessary to follow conflict of interest procedures and policies.

- Decisions are passed by qualified majority.

- At any meeting of the Directors, a majority of the Directors then in office shall constitute a quorum of the Board. At any meeting of the Directors at which a quorum is present, the action of the Directors on any matter brought before the meeting shall be decided by vote of a majority of those present, unless a different vote is required by law.

- A majority of the number of Directors shall constitute a quorum for the transaction of business at any meeting of the Board of Directors. If less than such majority is present at a meeting, a majority of the Directors present may adjourn the meeting from time to time without further notice. All decisions will be made by majority vote of those present at a meeting at which a quorum is present. If a Board of Directors vote results in a split decision, the Chairman of the Board, if present at the meeting, can decide the issue.

Internal and/or external audits

- Auditing is conducted in the following manner: 1) Roadmap Implementation Monitoring: The Association will liaise with granted projects to evaluate to which extent these projects contribute to the roadmap and what aspects of the roadmap need further commitment. 2) Metric Reports: Reports evaluating the achievements against the KPIs and monitoring industry commitments and leverage.

- According to its Charter, the International Board of Auditors (IBAN) shall audit the financial statements of the CNO. The IBAN may carry out performance audits that shall ascertain that the operations of the CNO have been implemented in compliance with efficiency, effectiveness and economy. IBAN shall have access to any information necessary to conduct its financial and performance audits.

- Internal Audit Committee – this committee is composed of the Treasurer and at least two other Members who are not Officers of the Board.

- External Audit: The network shall have an annual financial audit by a licensed Certified Public Accountant. The Board, based upon recommendation by the Audit Committee, shall appoint the auditor. The audit report shall be presented to the Audit Committee. A summary of the audit report shall be available to any Member upon written request.

- Two voting members, not being members of the Management Committee, will be elected as Honorary Auditors at each new term of the Management Committee's Annual General Meeting, and will hold office for three years only and may not be re-elected. They will be required to audit each year's accounts and present a report upon them to the Annual General Meeting. They may be required by the President to audit the Association accounts for any period within their tenure of office at any date and make a report to the Committee.

- The Commission may appoint observers to take part in the meetings of the Governing Board.

- The Board of Directors shall appoint an Audit Committee to receive the report of the independent certified public accounting firm which has conducted the annual audit of the Association. The Chair of the Audit Committee shall report to the Chairman in writing on the results of the annual audit. The Committee is also responsible for selecting an independent certified public accounting firm to conduct the annual audit of the Association. The Committee may perform such other duties in connection with the audit of the Association as requested by the Chairman. The accounts shall be audited at least once a year by a certified public accounting firm that is independent of affiliation. Within sixty days following the end of each annual audit, the Treasurer shall furnish the Board of Directors a financial report for the year just completed. The accounts of the Chapter shall be audited annually by the Audit Committee consisting of two Chapter members, who are not current officers, as appointed by the Board of Directors.

Dispute/conflict management arrangements

- All questions not covered by Statutes or by any regulations made for their application shall be settled in accordance with law in the country wherein the CNO is based. These Statutes shall be governed by and construed in all respects in accordance with the laws of the country wherein the CNO is based. Any dispute or difference arising out of or in connection with these Statutes shall be referred to the exclusive jurisdiction of the courts.

- Arbitration tribunal.

- Quorum (board of directors) and action led by consensus.

- Written reprimand; 1-year probation; Expulsion from membership.

- In the event of a dispute arising between members, the members concerned will use all means to endeavour to solve the dispute by internal conciliation with the help of other members. If conciliation is unsuccessful, any legal dispute arising during the life of CNO or during its dissolution shall be dealt with under the law wherein the country is based unless the parties concerned agree otherwise.

Confidentiality

- In principle, no confidential information will be exchanged. If it is deemed necessary, the European Cyber Security Organisation (ECSO) will follow section 14 Confidentiality and exchange of information of the ECSO Bylaws.

- Establishment of a declaration: for example – ensure that appropriate structures exist to manage all aspects of this information and knowledge throughout their life cycle, and to ensure their identification and preservation. In the conduct of its mission, the CNO implements approved Information assurance policies, which ensure that classified and commercial information shared under the auspices of various associated agencies are duly protected in accordance with an appropriate and approved Information Management Policy. In the conduct of its mission, the CNO would also implement policies regarding the disclosure of information to non-governmental representatives to ensure compliance with the competition legislation.

- Additional example of a declaration:
  Confidentiality Obligations: An Interested Person must protect the integrity of Confidential Information at all times and must not use or disclose Confidential Information in an inappropriate or unauthorized manner to unauthorized persons inside or outside the organisation. When a legitimate need for the information exists and proper authorization is obtained, the information may be disclosed. It is critical to review all policies and procedures relative to disclosure prior to releasing such information. In order to protect Confidential Information, Interested Persons should take

reasonable steps to prevent intentional or inadvertent disclosure to unauthorized persons inside or outside the organisation. These steps may include keeping Confidential Information in a secure location, safeguarding electronic-based Confidential Information and not discussing Confidential Information with co-workers in public areas such as elevators and restrooms. The obligation not to disclose Confidential Information continues after termination of service of an Interested Person to the organisation. An Interested Person who is not sure about whether certain information is Confidential Information, should contact the organisation management before releasing the information.

- Maintain appropriate confidentiality of proprietary or otherwise sensitive information encountered in the course of professional activities.

- Members (individuals, academics, corporate, etc.) are required to adhere to a code of conduct (if this is breached, there is a disciplinary process).

- Establishment of binding confidentiality policies/statutes and continual updating of said policies across the lifespan of the organisation. Example of such policy includes: Confidentiality, Transparency and Publicity; each Party shall: treat all Confidential Information it receives as confidential, safeguard it accordingly and not disclose it to any other person without the prior written permission of the disclosing Party; and not use or exploit the disclosing Party's Confidential Information in any way except for the purposes anticipated under the Agreement.

- Example of a Statute: non-disclosure of communications received to third parties, unless this is necessary to fulfil a request of the party that initiated the communication or a legal obligation – using best efforts to minimise the amount and scope of any disclosure.

- Compliance with the General Data Protection Regulation (GDPR).

Intellectual Property management arrangements

- Establishing legally binding Intellectual property rights (IPR).

- Intellectual property rights, including patent rights, copyrights, proprietary technical information and other sensitive commercial or industrial matters pertaining to the CNO are handled according to CNO's Policies and Directives.

- The Secretary General shall not on behalf of the Association, except with the prior written consent of two-thirds (2/3) majority of the Board of Directors, grant any rights (by licence or otherwise) in or over any intellectual property owned or used by the Association.

- On occasions wherein the CNO relies exclusively on volunteer arrangements and Task Group members (except for the Chairs) are not paid; as a rule, IPR remain with authors of the 'product' (usually a report) while it is distributed under open access license.

Ethics code and its enforcement

- Devising a binding statute.
  For example: Each Member of the Association is committed to integrity and to respect the confidentiality of the Associations' internal documents marked as confidential. Each Member shall maintain and enforce its adherence to lawful business practice and shall act in good faith and transparently with respect to other Members. The Association and its Members shall operate in full compliance with European Competition and Antitrust Law. Compliance with these rules is mandatory for everybody who participates in the Association's activities and finally serves as protection for the Association and its Members. The Members shall respect all ethics rules demanded by the European Union when a Member obtains a grant from the European Commission or one of its executive agencies.

- Ensuring an ethics committee is in place.

- Transparency with regards to the Ethics Complaint Process.

- Ensure new members sign and adhere to a code of conduct upon joining the organisation.
  For example: A member shall:
  - perform professional duties in accordance with the law and the highest moral principles, be faithful and diligent in discharging professional responsibilities;
  - promote the implementation of and promote compliance with standards, procedures, controls for application security;
  - maintain appropriate confidentiality of proprietary or otherwise sensitive information encountered in the course of professional activities;
  - discharge professional responsibilities with diligence and honesty;
  - communicate openly and honestly;
  - refrain from any activities which might constitute a conflict of interest or otherwise damage the reputation of employers, the information security profession, or the Association;
  - maintain and affirm our objectivity and independence;
  - reject inappropriate pressure from industry or others;
  - not intentionally injure or impugn the professional reputation of practice of colleagues, clients, or employers;
  - treat everyone with respect and dignity.

Specific ethical issues, e.g. policy in regard to slavery, use of labour of minors

- Not explicitly specified.

‘Green’ policies

- Not explicitly specified.

Gender policies and representation

- Not explicitly specified.

Transparency

- Not explicitly specified.

Anti-corruption/ integrity policy (e.g. whistle-blowers protection)

- Not explicitly specified.

Additional governance matters

- Industry commitment – KPIs are monitored and, with the help of key stakeholders, regularly reviewed and, if necessary, revised to maximize the outcome of the CNO's research and innovation activities.

- Currently discussions were opened up to other stakeholders such as private sector, academia, policy making organisations.

- Transparency with regards to outputs.

4.4.3 Findings for CNOs for which information on profit status is not available

Not for profit status

Total number of CNO’s for which the information on profit status is not available = 12

Geographical representation or exclusion

- Geographical representation = 2 CNOs have worldwide remit, wherein the majority have coverage for EU member states or the USA.
- Predominant geographical exclusion zones = worldwide coverage indicates that no countries are excluded.

Ways of involving external stakeholders

- Academic collaboration

Standards or methodologies used

- Not specified

Representation on the senior governance body

- Case study 13 is governed by executive management, and scientific, steering and advisory committees. The chief executives of the organisation are: the Director; the Deputy-director; the Chairman of the Scientific Committee; the Head of Research Strategy; the Head of Industry Research Cooperation; the Executive Director.

Decision making principles

- The decisions of the Steering Committee are accepted by a majority vote and are summarized in writing.
- Most often, collective bodies make decisions by simple majority. Qualified majority decisions are made only by exception, when required by law.

Internal and/or external audits

- Not specified

Dispute/conflict management arrangements

- According to the CNO's Code of Ethics, conflicts of ethical nature are resolved: 1. at the organizational level which is one degree higher than the level at which they arose; 2. with the participation of all parties to the conflict, while maintaining the maximum possible confidentiality; 3. the decision is made available to all parties concerned, including measures to restore justice.

Confidentiality

- Obligation to keep data confidential at all the circumstances, known in the procedure for registration, protection and use of the intellectual product (secret agreement), which is effective up to 3 years after termination of the contract. In the event of non-fulfilment of the obligation of confidentiality, the directors shall take measures for realization of disciplinary and property liability for the damage caused. Upon termination of the contracts, the intellectual property objects created in the course of their execution shall remain the property of the CNO.

Intellectual Property management arrangements

- Not specified

Ethics code and its enforcement

- Establishing an Ethics Code – a framework of principles for good behaviour in science and support for high moral standards in academic research.

Specific ethical issues, e.g. policy in regard to slavery, use of labour of minors

- Not explicitly specified.

'Green' policies

- Not explicitly specified.

Gender policies and representation

- Not explicitly specified.

Transparency

- Not explicitly specified.

Anti-corruption/ integrity policy (e.g. whistle-blowers protection)

- Not explicitly specified.

4.4.4 Summary of findings: analysis of governance requirements in existing networks

The following section will summarise the findings from the secondary analysis of the existing networks with respect to governance requirements.

While financial accounts for the various networks were not specifically recorded or indeed sought, profit status was noted. Findings from the analysis indicated that the majority of the CNO's surveyed operationalised as not-for-profit organisations (n=73).

Geographical representation or exclusion zone were also noted, as the remit of a cyber-CNO is a crucial parameter towards which to measure the reach of the network with respect to provision of services and products. Crucially, the jurisdictions which networks endeavour to operate within and thus can have implications on how effectively a CNO performs across country borders (and also the confines of larger governing territories – i.e. EU, USA, Asia-Pacific, etc.). A majority of networks have scope within the EU, USA and, to a slightly less extent, Asian Pacific countries; this is particularly evident when CNOs are based in these jurisdictions. Notably, however, a vast majority of networks aim to represent members on a worldwide level and are not just limited by geographic location. This is especially notable for CNOs which represent a specific profession in the cyber-security industry (i.e. auditors, researchers, finance personnel, etc.), which endeavour to provide a base from which professionals can network and upskill (internationally). Typically, the major, better established organisations, had the largest quantity of members, especially when compared to grassroot organisations. Findings from this analysis, however, did highlight that while the coverage of many organisations was at an international level, continental Africa, Russia and Middle Eastern countries were majorly underrepresented, with few or no organisations in place.

One of the key ways of progressing a CNO centres on the ***involvement of external stakeholders***; hence this parameter was also recorded in the primary analysis. The principal ways in which external stakeholders connected with CNO's included the following:

- Involvement in advisory boards or coordination/ strategic/ management/ steering/ industry expertise committees;

- Academic collaboration; engagement with training, education and skills – either as a means of upskilling, provision of professional accreditation or a host;
- Provision of a funding scheme for cybersecurity projects, or facilitating sessions with EU and national level funding authorities;
- Coordinating networks of practitioners and researchers;
- Hosting cybersecurity conferences and networking events; provision of different membership classifications.

The reviewed CNOs are highly heterogenous given that they are scattered across the globe, have a diverse range of objectives and represent a myriad of professional, industries, researchers and individuals. It was therefore crucial to record the various ***standards or methodologies*** utilised in the operation of these networks. Findings from the qualitative analysis highlighted that the most commonly used standards were Control Objectives for Information and Related Technologies (COBIT) and Information Technology Infrastructure Library (ITIL), and to a lesser extent project management tools such as Microsoft Project and PRINCE II.

With respect to the ***representation on senior governance bodies***, the majority of CNOs host the following directing officers: a President, a Secretary and a Treasurer, each of whom are elected by the Board of Directors. A Chair of the Board, Vice Chairs and/or Vice Presidents, and such other officers and assistant officers and agents as may be deemed necessary may also be elected or appointed by the Board of Directors from time to time. Likewise, the business and affairs of the CNOs were typically managed by or under the direction of the Board of Directors. The number of personnel assigned to the board depended on the size of the CNO (i.e. what types and how many members are represented and what products/ services are offered), the funding stream of the CNO, renumeration status (voluntary or salaried positions), the geographical scope of the CNO and the coverage of the CNO.

While various officers can oversee the management of the CNO, the ***decision-making*** principles on which the CNO relies upon are indispensable in the successful operation of the network. In a majority of cases, steering committees or steering boards typically have the authority with regards to decision making for the CNO. Steering committees typically act within the framework of the guidelines and guidance of the Council. Consensus, when a board has reached quorum – individually determined depending on the size of the panel and the number of senior officers present, a qualified majority vote—2/3rds of the panel or above—were the most common frameworks on which motions were passed. In some instances, senior representatives may be required to be present in order for a motion to be voted on in the first instance; a board also has the power to adjourn a vote until such a condition is met.

Regular ***internal and/or external auditing*** ensures the effective operation of a CNO. A majority of the reviewed CNOs had procedures in place with respect to auditing practice. A majority of the CNOs ensured that internal audits were conducted by an independent party (outsourced) to ensure no bias and transparency. Steering boards or board of directors usually appoint the auditor (either an individual or a corporation), wherein the outcome of the audit (report) and recommendations for the future are usually made available to steering committee officers and/ or senior officers on the board (i.e. Chief Executive). It is therefore the responsibility of the respective officer(s) to ensure the regular monitoring of the implementation of audit recommendations. An annual report containing a summary of the number and type of internal audits carried out, the recommendations made and the action taken on those recommendations is compiled and forwarded to senior executives and/or committee members (where relevant). The respective parties then examine the information and assess whether the recommendations have been implemented fully and in a timely manner. The reports and findings of the internal auditor shall be accessible by the public only after validation by the internal auditor of the action taken for their implementation.

To a lesser extent, internal audits were found to be conducted by voting members of the CNO (not board executives) or an Internal Audit Committee—composed of the Treasurer and at least two other Members who are not Officers of the Board—was devised. While this practice was less common, it can confound findings. However, this measure may have been due to financial necessity (as the CNO may have limited funds to support the recruitment of an outside party).

Primary analysis of the CNOs indicated that many networks had arrangements in place with regards to ***dispute/ conflict management***. Members are required to be transparent in the first instance if they were in a position to improperly gain from the products/ services under the auspices of the CNO.

Typical procedure for when a conflict of interest is discovered first involves the respective party ceasing all activities in the matter. Senior executive personnel then determine if appropriate actions need to be taken, wherein a board of directors meets quorum and a decision is led by consensus. The following processes could then be actioned depending on the outcome: 1) Written reprimand, 2) a one-year probation or 3) expulsion from membership. Many CNOs allow for an arbitration tribunal to ensure due process.

Confidentiality practices across the CNOs vary; however, all CNOs based in the EU were General Data Protection Regulation (GDPR) compliant. Indeed, a majority of CNOs had a declaration of confidentiality in place – detailing how data was managed, processed and stored. This information was readily available to stakeholders, members and consumers alike. Binding confidentiality policies and statutes were continually updated across the lifespan of the organisation. Some CNOs were compliant with additional EU security policy regulations (i.e. Decision 2013/488/EU) depending on their remit. The CNOs which were surveyed stated in principle that no confidential information would be exchanged, and that the appropriate confidentiality of proprietary or otherwise sensitive information encountered in the course of professional activities would be maintained. Moreover, members (individuals, academics, corporate, etc.) are required to adhere to a code of conduct with respect to confidentiality practice; if this is breached, a disciplinary process is initiated.

Maintenance of ***intellectual property*** (IP) is integral to the effective operation of an organisation. It is therefore understandable that many CNOs have considerations in place with respect to how their IP is managed (legally binding Intellectual property rights). A majority of networks have clauses in place which state that materials are solely for personal, non-commercial use, parties should not modify or alter the materials in any way, nor delete or change any copyright or trademark notice. Likewise, materials may not be copied, distributed or transmitted in any way for commercial use without the express written consent of the organisation. All references to materials also must be acknowledged and the organisation reserves full ownership and intellectual property rights of these materials. Additionally, Intellectual property rights, including patent rights, copyrights, proprietary technical information and other sensitive commercial or industrial matters pertaining to the CNO is handled according to CNO's Policies and Directives.

While CNOs most likely are ethically run, establishing and enforcing an ***ethics code*** promotes transparency, can be a positive step for retaining members, gaining future members and, overall, ensure the successful management of a network in long term. The most common ways in which ethical codes and standards were prescribed in the surveyed CNOs were as follows:

- Devising a transparent declaration;
- Devising a binding statute with respect to code of conduct/ ethics code/ framework of principles;
- Ensuring an ethics committee is in place;
- Transparency with regards to the Ethics Complaint Process;
- Prohibit personnel, during the 12 months after leaving the service, from engaging in lobbying or advocacy vis-à-vis staff of their former institution for their business, clients or employers on matters for which they were responsible during service.

Specific ethical issues (e.g. policy in regard to ***slavery***, use of ***labour of minors***), ***'Green' policies***, ***Transparency*** and ***anti-corruption/ integrity policy*** (e.g. whistle-blowers protection) across all networks were not noted during the primary phase of analysis. This outcome could indicate that such issues were not specifically highlighted by CNOs in the first instance (i.e. not explicitly outlined on organisations' website, social media streams or governance documentation).

Some CNOs made positive steps towards ensuring gender balance (as noted under the ***Gender policies and representation*** heading) by establishing initiatives and charters to encourage and retain female personnel in the cyber-security domain. However, the primary analysis phase of these CNOs highlighted that the vast majority of networks did not make any significant contributions towards addressing gender balance.

Supplementary ***favourable governance matters*** derived from the primary analysis were limited, however the following were noted. One CNO made a commitment to industry by monitoring key-performance indicators (KPIs) and with the help of key stakeholders regularly reviewed and, when necessary, revised to maximise the outcome of the CNO's research and innovation activities. Another CNO regularly hosted discussions with other stakeholders from the private sector, academia, policy making organisations to inform operations. And lastly, one CNO placed great emphasis on being transparent with members, partners, stakeholders, and to some extent, the public, with regards to outputs and performance.

The results of the primary analysis were also processed quantitatively. Each of the governance issues identified in the analysis of norms, interviews with stakeholders and academic sources is addressed by statutory documents of at least one of the analysed networked organisations. The number of networked organisations that address a specific governance issue in their bylaws or other statutory documents is given on Figure 10 (for the governance issues included in the analysis template) and Figure 11 for the additionally identified governance issues.

Using the same approach applied in the analysis of the other three types of primary sources, the governance issues were split into four tiers.

- The ***representation*** on senior governance bodies and ***knowledge management*** have the highest score of 34. The ***long-term perspective*** on collaboration also fits in Tier 1.
- Tier 2 includes ***geographic representation***, ***accountability***, ***innovation***, ***adaptiveness***, ***cohesion***, trust, and ***leadership***.

- *Confidentiality and security*, *IPR management*, *ethics code*, *gender policies*, *transparency*, *sustainability*, *communication and engagement*, *organisational culture*, and *risk management* fit into Tier 3.

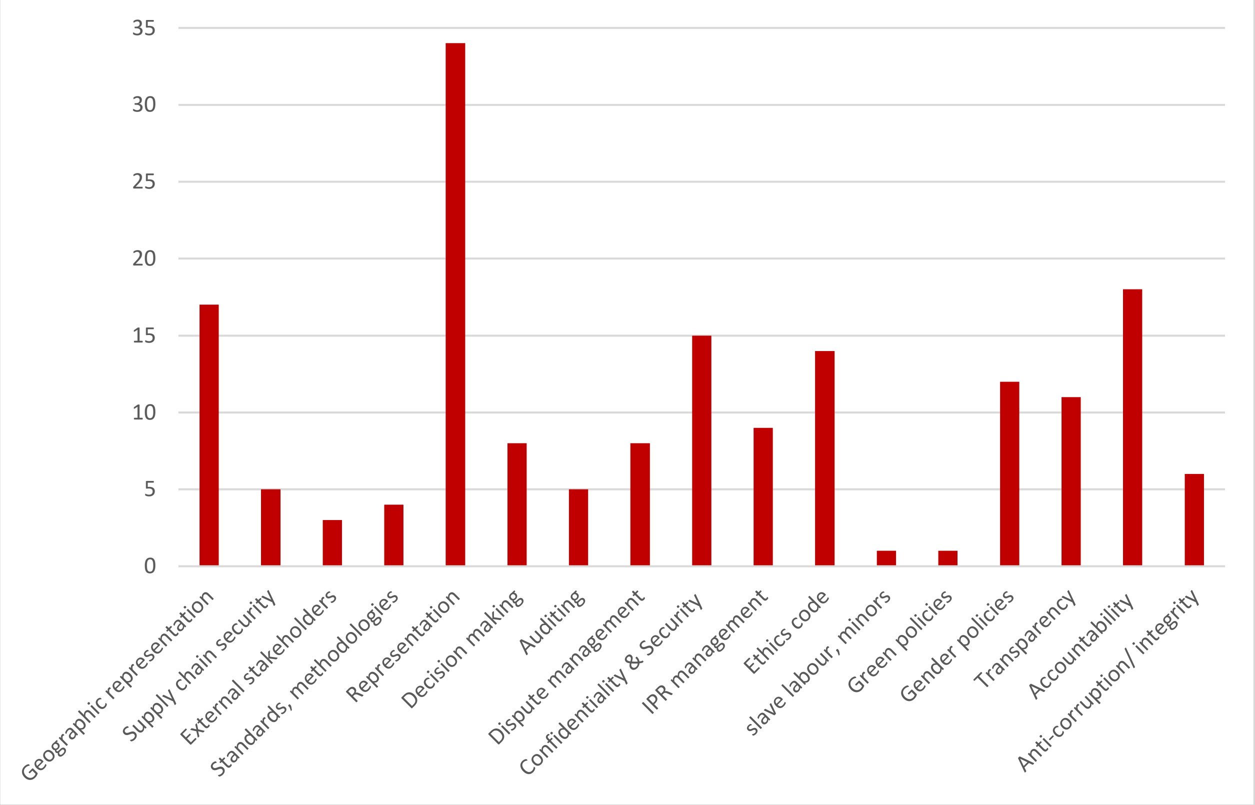

Figure 10: Ranking of initial governance issues based on the analysis of existing networks.

- The remaining governance issues have a score that is less than 25 percent of the maximum and, respectively, are placed in Tier 4.

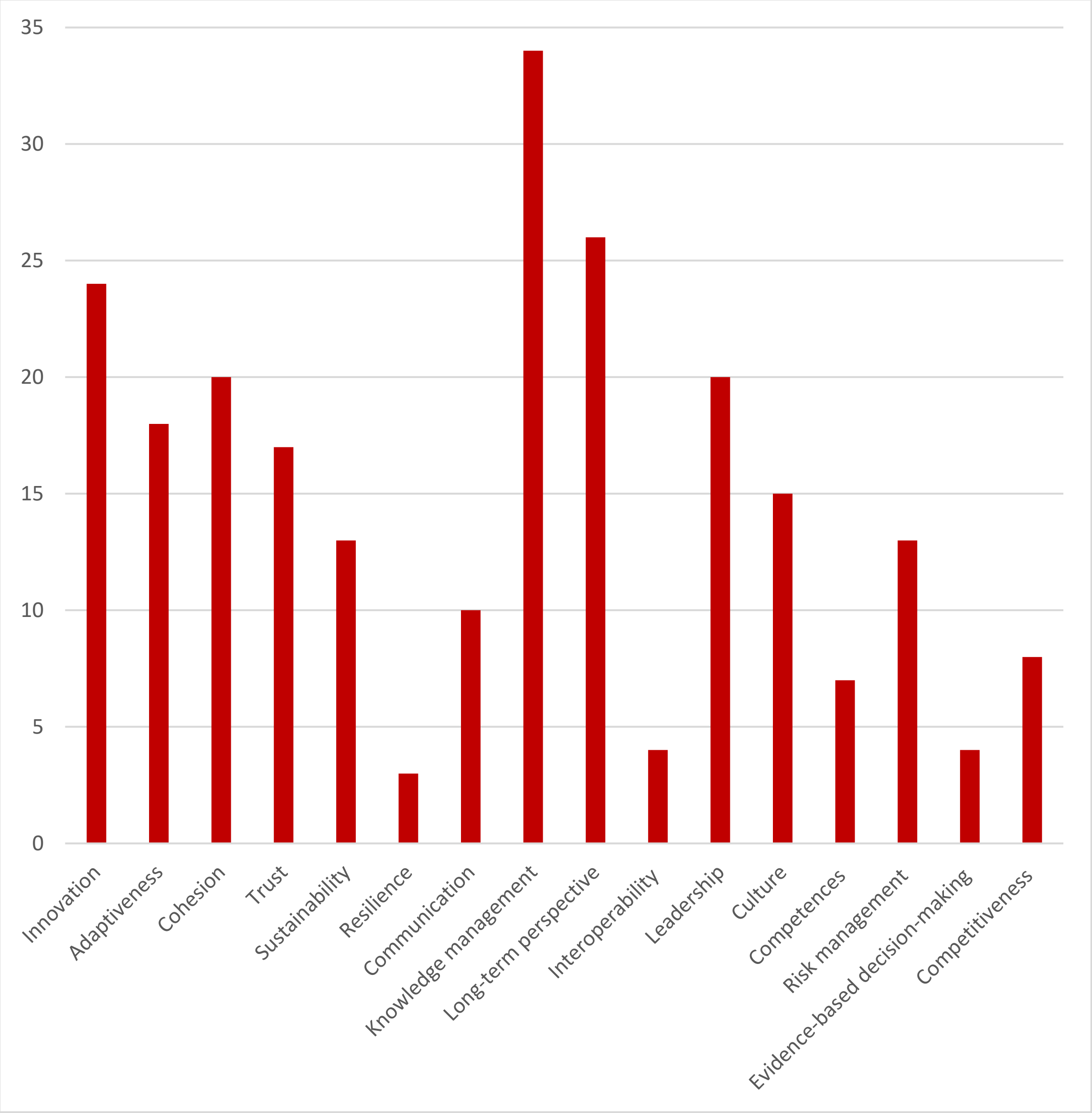

Figure 11: Ranking of additionally identified governance issues based on the analysis of existing networks.

4.5 Summary on governance requirements

Table 11 presents the prioritised list of governance needs, objectives and requirements. It was constructed adhering to the following method.

First, all governance issues were split into two groups:

- Those that can be designated as "objectives" which can be achieved by devising and effectively implementing sets of normative, organisational, procedural, technical and training measures (included in the second column of Table 11); and
- Those that depend on various intangibles and the interplay of numerous factors and contexts, and can be addressed only partially by norms, procedures, training and technical measures. These governance issues are designated as "features of CNOs" and included in the third column of Table 11.

In the secondary analysis, all these governance issues were classified in tiers depending on the number of times they have been treated in primary sources (with Tier 1 including issues of highest interest, hence possibly of highest priority; followed by Tier 2, etc.).

In Table 11 each governance issue is placed in the highest tier it appears in the secondary analysis, i.e. even if it appears only once in tier 1, e.g. engaging *external stakeholders* in the interviews, *adaptiveness* in the academic literature, and *trust* in norms and regulations, it is included in Tier 1 of the summary table below.

This approach was adopted to reflect on the *complementarity of the primary sources*. For example, so far the academic literature practically does not treat networked organisations in the field of cybersecurity (which are still emerging) and hence the respective secondary analysis places *confidentiality & security* in Tier 4. When, however, cybersecurity is in the focus (e.g. in the interviews with stakeholders and in the analysed norms and regulations) it is placed in Tier 1.

Tier	Governance objectives	Features of CNOs
1	Geographical representation or exclusion Involving external stakeholders Representation on the senior governance body Decision making Auditing Confidentiality & Security Knowledge management Standards or methodologies Long-term perspective on collaboration Competences Risk management Evidence-based decision-making	Adaptiveness Cohesion Trust Competitiveness
2	Supply chain security Dispute/conflict management arrangements Intellectual Property management Ethics code Gender policies and representation Transparency Accountability Integrity/anti-corruption policy	Innovation Leadership
3	Communication and engagement	Organisational culture Sustainability
4	‘Green’ policies Slave labour, labour of minors Interoperability	Resilience

Table 11: Prioritisation of governance needs, objectives, and requirements.

This prioritisation is expected to *orient* the development of alternative governance models and their evaluation, and not to predetermine the actions of the ECHO research team in follow-up tasks in WP3.

5. Governance models of network organisations

5.1 Norms and regulations on network governance models

The Regulation 887 (R 887, 2021) aims to allow the Union to be, through the Competence Centre, the Network and the Community, *flexible* enough to *adapt quickly and continuously* the fast-changing nature of cyber threats and cybersecurity. The Competence Centre should stimulate and support the *long-term strategic cooperation and coordination* of the activities of the Community, which would *involve a large, open, interdisciplinary and diverse* group of European stakeholders involved in cybersecurity technology. The Competence Centre is tasked to provide cybersecurity knowledge and technical assistance to industries, including ICT products, processes and services and all other technological products and processes in which cybersecurity is to be embedded. "Security by design" is the principle underlying the process of developing, maintaining, operating and updating infrastructures, products and services, adequate security testing and security audits, and making available updates remedying known vulnerabilities or threats without delay and, where possible, by enabling third parties to create and provide updates beyond the respective end-of-service of products.

The objective of the NIS Directive is to drive different companies to use IT security solutions and establish practices to protect IT networks and the data, both their own and of third parties. The European Commission therefore wants to stem the phenomenon of cybercrime, which has become prominent in recent years: more and more companies are being violated (e.g. by data theft). The consequences of a successful attack are often very heavy both in terms of economic and reputational losses. Each Member State should have a *national strategy on the security of network and information systems defining the strategic objectives and concrete policy actions to be implemented* (NIS, 2016). The Commission, through the Connecting Europe Facility (CEF) cybersecurity Digital Service Infrastructure, is developing a Core Service Platform cooperation mechanism, known as MeliCERTes, between participating Member States CSIRTs to improve their levels of preparedness, cooperation and response to emerging cyber threats and incidents. The Commission, through competitive calls for proposals for grant awards under CEF is co-funding CSIRTs in the Member States with a view to improving their operational capacities at national level.

5.1.1 Governance structure/ Roles and responsibilities

Regulation 887 (R 887, 2021) establishes:

- a Network of National Coordination Centres;
- a Cybersecurity Competence Community;
- a European Cybersecurity Industrial, Technology and Research Competence Centre.

The members of the Competence Centre shall be the Union, represented by the Commission, and the Member States. The structure of the Competence Centre shall comprise:

- *Governing Board* (representatives of member states, tasks set out in Article 13);
- *Strategic Advisory Group* (consisting of no more than 20 members; tasks set out in Article 13);
- *Executive Director* (tasks set out in Article 17)

In order to effectively disseminate and exploit the main products and services of ECHO, a kind of specific governance models should be proposed. Consortium Members, according their expertise and level of involvement, will contribute to the draft of specific governance models for ECHO products/services.

The ECHO Current Operating Mode (COM) is governed by WP1 and includes:

1. Grant and Consortium Agreements;
2. EC PO, General Assembly;
3. Project Board and supporting Committees;
4. Project Handbook and other similar type of documents;

The current governance model of the ECHO Project consists of WP1 Project Management at the Hub, and the various technological work packages as spokes, with work package 3 providing auditing, recommendations and the necessary governance model for implementing the transition from ECHO project to the future ECHO network.

5.1.2 Processes and Procedures

Governance processes and procedures need to be set up following a number of requirements identified through analysis of norms.

Regulation 887 (R 887, 2021) defines the need for:

- Competence Centre's work plan and multiannual strategic plan reflecting the priorities in achieving the objectives and tasks of the Competence Centre;
- Security rules;
- Financial contribution;
- Members assessing and accrediting;
- Conflict of interest;
- Protection of personal data;
- Document sharing procedures;
- Measures to prevent fraud and irregularities.

The pilot projects handbook (Pilots HB) elaborates:

- IRP;
- Document exchange methods;
- Decision making procedures;
- Licensing;
- New partners engagement;
- Eligibility and admissibility conditions;
- Quality assurance;
- Risk management;
- Ethical rules and standards;

- EUCI secure management.

The ECHO Project Handbook defines:

- Decision process;
- Project communication and communication rules;
- Periodic meetings;
- Data Management Plan;
- KPI definition and measurement;
- Contractual management;
- Administrative and financial reporting;
- Periodic EU reports;
- Periodic internal reports and internal financial reports;
- Configuration management;
- Change control procedures;
- Quality assurance;
- Risk management.

The Grant Agreement of the CONCORDIA project (CONCORDIA GA) addresses:

- Management of research;
- Quality and impact management;
- Management of legal aspects;
- Management of IT infrastructures/labs/education/ training;
- Management of internal and external communication;
- Management of finance, controlling and risk;
- Management of personnel;
- Management of compliance;
- Management of knowledge;
- Decision making process;
- Conflict resolution, consensus building and corrective action.

Table 12 summarises the needed processes and procedures.

Name process/procedure	Scope
Security and Privacy policies	Security and Privacy
Data Management Plan	Security and Privacy
Ethical rules and standards	Security and Privacy
EUCI secure management	Security and Privacy
Risk management	Security and Privacy
Annual Plan: objectives and projects	Governance and Management
Management of legal aspects	Governance and Management

Name process/procedure	Scope
Management of it infrastructures/ labs/ education/ training	Governance and Management
Management of personnel	Governance and Management
Internal audit	Governance and Management
Assessment and accreditation of members	Members and stakeholder
Eligibility and admissibility conditions	Members and stakeholder
New partners engagement	Members and stakeholder
Decision making procedures and management of conflict of interest	Members and stakeholder
Contractual management	Members and stakeholder
Document sharing procedures and methods	Members and stakeholder
IRP	Members and stakeholder
Licensing	Members and stakeholder
Communication rules	Internal Communication
Periodic meetings	Internal Communication
KPI definition and measurement	Monitoring
Measures to prevent fraud and irregularities	Monitoring
Administrative and financial reporting	Monitoring
Periodic EU reports	Monitoring
Configuration management	Monitoring
Change control procedures	Monitoring

Table 12: Processes and procedures needed for network governance.

5.1.3 Possible differentiators

By finding a position for ECHO in the future envisioned Competence Centre and Network, possible differentiators for the proposed governance model can be:

- help companies, especially Start-ups and SMEs, to become more competitive by improving their business/ production processes as well as products and services through smart innovation enabled by digital technology;
- sharing knowledge of real-life sectorial needs with the Network and the Centre to feed the reflection on the research and innovation agenda responding to industrial requirements;contribute to reducing skills gaps in the Union related to cybersecurity by supporting further development of cybersecurity skills, where appropriate together with relevant EU agencies and bodies including ENISA;
- aim at balanced gender representation;
- contribute to create a single digital market for ICT products, services and processes;
- provide strategic direction and guidance in consultation with ENISA and ECSO;
- business model improvement with an organisational and personnel development;

- strategic investments (possibly by combination of customer rates provided investment and central EC funding);
- engagement of partners from different regions and experience;
- assist the implementation of agile approach to management;
- create and support working groups on specific topics;
- maintain communication channels from low level (to individual entities – stakeholders of cybersecurity) to high level (EU Competence Centre);
- enable Member States and EU institutions (where appropriate. involving private sector organisations) to systematically respond to cybersecurity incidents at national and European level, including political responses where appropriate.

5.1.4 Points of strengths

The following points of strength in terms of governance can also be inferred from the analysis of norms and regulations:

- Include a representative from any part of groups of interest in each Member State, so the representation and the opinion/requirements from most of the stakeholders is ensured;
- Identify how best to exploit the activities of existing EU-wide cybersecurity units within existing crisis management mechanisms;
- Facilitate the cooperation between Member States in responding to cybersecurity incidents;
- Establish synergies between public and private sectors;
- Strengthen business, governance and information sharing models;
- Identify research objectives and investigate promising research ideas (CONCORDIA addresses this with a governance model that combines the agility of a start-up with the sustainability of a large centre);
- Address the pillars of research and technology; for example, CONCORDIA identifies five pillars and the issues that play a role within these five pillars are not orthogonal: certain underlying concepts and technologies (such as crypto, blockchain, botnets and data analysis) are applicable to, and will be addressed in, multiple pillars (cross-pillar);
- Build Roadmaps for industrial challenges;
- Set an External Ethics Adviser, external and independent from the project;
- Set an Internal Ethics Committee. Beyond high-level activities, the Ethics Committee sets up and maintains appropriate procedures, criteria, templates, information sheets, potential opinions and approvals from relevant entities, explanations, and relevant compliance documentation as well as descriptions of technical and organizational risk-mitigation strategies and measures (including security ones) implemented to comply to the ethics requirement.

5.1.5 Points of weakness

In developing a governance model, points of weakness should be considered in advance in order to overcome the foreseen difficulties and maintain a timely and efficient transition from a consortium to a network, such as:

- rigid hierarchical structure, which slows down decision-making;
- voting procedures;
- effort required for coordination of many partners/members;
- fragmentation of research and innovation;
- data protection limitations;
- cloud-based shared environments;
- new regulatory requirements;
- interoperability and standardisation of interfaces;
- quality of services guarantees by industry domains;
- unforeseen disruptions to user acceptance;
- internal dependencies of inputs-output for the achieving of a goal/service/product;
- critical risks for the successful implementation of the project;
- internal communication;
- external communication.

With respect to the last point, an area where the NIS Directive will need to be supplemented is information flow. For example, the Directive only covers key strategic sectors. A similar approach by all stakeholders hit by cyberattacks would be necessary to provide for systematic assessment of vulnerabilities and entry points for cyber attackers. In addition, cooperation and information sharing between the public and private sectors faces a number of obstacles:

1. governments and public authorities are reluctant to share cybersecurity-relevant related information for fear of compromising national security or competitiveness;
2. private undertakings enterprises are reluctant to share information on their cyber vulnerabilities and resulting losses for fear of compromising sensitive business information, risking their reputation or risking breaching data protection rules.

Trust needs to be strengthened for public-private partnerships to underpin wider cooperation and sharing of information across a greater number of sectors. The role of Information Sharing and Analysis Centres (ISACs) is particularly important in creating the necessary trust for sharing information between the private and the public sector. Some first steps have been taken in respect of specific critical sectors, such as aviation through the creation of the European centre for cybersecurity in aviation, and energy by developing Information Sharing and Analysis Centres. The Commission aims to facilitate this approach with support from ENISA, with an acceleration needed in particular with regard to sectors providing essential services as identified in the NIS Directive (NIS, 2016).

5.2 Findings of governance models from the analysis of networks

5.2.1 Dimensions and scales for representing CNO governance models

This section will outline how data with regards to existing collaborative networked organisations (CNOs) was critiqued. Secondary analysis of the data contained within the MS Excel matrix was a two-step process. First, key indicators concerning the Governance models of network organisations of CNOs were assessed. Two dimensions were evaluated and compared – **dimension 1**: Representation on the senior governance body/ bodies vs **dimension 2**: Decision making principles.

A scale was devised in an effort to classify the two dimensions. Step two involved plotting this data and identifying prevailing models.

Dimension 1. Representation on the senior governance body/ bodies

1. only few core members are represented;
2. selective representation, e.g. of founding members or members above a certain 'size' or with certain roles (an example here would be a Horizon 2020 "Project Management Team");
3. broad representation, e.g. a representative of any organisation may be elected through a vote open to all CNO member organisations;
4. all CNO member organisations are represented (e.g. a General Assembly of a Horizon 2020 Consortium).

Dimension 2. Decision making principles (of CNO bodies)

Decision are taken:

1. by simple majority, i.e. over 1/2 of the weighted votes of CNO members;
2. by qualified majority (e.g. over 2/3), of the weighted votes of CNO members;
3. by simple majority (i.e. over 1/2 of the votes), with equal weight of the vote of each CNO member;
4. by qualified majority (e.g. 2/3 of the votes), with equal weight of the vote of each CNO member;
5. by consensus.

Note: votes can be weighted for example depending on the 'size' (e.g. annual turnover or personnel size) of CNO members or their financial contribution to some of the CNO expenditures.

5.2.2 Classifying governance models of existing networks

Akin to the approach adopted for the analyses of the business models and the governance requirements, CNOs were categorized in terms of profit orientation in the first instance. The total number of for-profit CNOs equated to 7 and the total number of not-for-profit CNOs = 73; information on profit orientation was not available for 12 CNOs. The following sub-sections will detail the governance models with regards to the for-profit and the not-for-profit CNOs.

Governance Models: for-profit orientated networked organisations

A crosstabulation analysis (as shown in Table 13) was conducted in IBM SPSS 25 to evaluate the spread of the CNOs across the various categories for each dimension as outlined the Excel matrix.

This analysis showed that the principal models for the 7 surveyed for-profit CNOs were: (1) selective representation of senior governance bodies with simple majority, i.e. over 1/2 weighted CNO member votes (n = 2; 29 %) and (2) complete representation of all CNO members with simple majority voting, i.e. decisions are taken with over 1/2 of the weighted CNO member votes (n = 2; 29 %). These findings are also illustrated in Figure 12.

Governance Models: not-for-profit orientated networked organisations

The majority of CNO's surveyed had a not-for-profit orientation (n=73; 79%).
Complete data with regards to governance parameters was not available for 20 CNOs; these networks were excluded from further analysis. Akin to the approach previously utilised towards critiquing the for-profit CNOs, a crosstabulation analysis (findings shown in Table 14) was conducted in IBM SPSS 25 to examine governance models for the remaining not-for-profit CNOs (n=53).

Representation on the Senior Governance Bodies vs Decision-making principles					
		Decision-making principles			
		Simple majority – over 1/2 of the weighted votes	Qualified majority – over 2/3 of the weighted votes	Simple majority – over 1/2 of the votes, with equal vote for each CNO member	**Total:**
Representation on the Senior Governance Bodies	Selective representation	2	0	1	**3**
	Broad representation	0	1	1	**2**
	All CNO member organisations represented	2	0	0	**2**
	Total:	**4**	**1**	**2**	**7**

Table 13: Crosstabulation analysis for classifying governance models of existing for-profit networks.

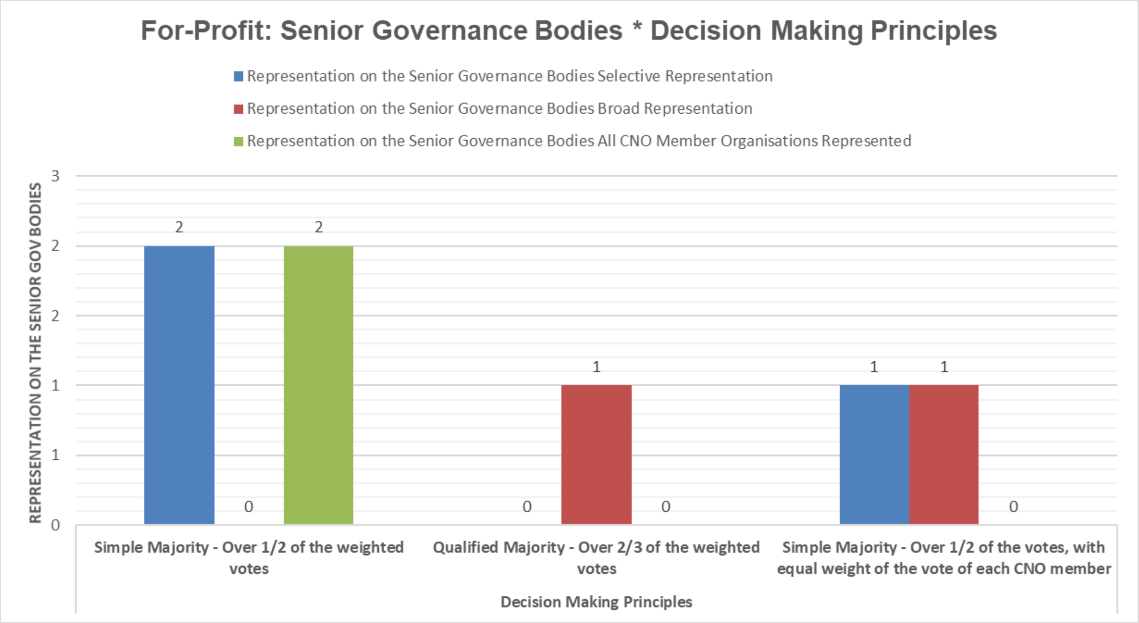

Figure 12: Bar chart demonstrating the distribution of decision-making principles vs representation on the senior governance bodies; for-profit orientation CNOs.

This analysis showed that the most common governance model adopted by not-for-profit CNOs was one which had a complete CNO representation, wherein simple majority equal-weighted decision-making principles were operationalised, i.e. taking decisions with over 1/2 of the votes. This subset accounted for 17 % of the sample (n=9). These findings are also shown in Figure 13.

Representation on the Senior Governance Bodies vs Decision-making principles							
		Decision-making principles					
		Simple majority – over 1/2 of the weighted votes	Qualified majority – over 2/3 of weighted votes	Simple majority – over 1/2 of the votes, with equal vote for each CNO member	Simple majority – over 1/2 of the votes, with equal vote for each CNO member	Consensus	**Total:**
Representation on the Senior Governance Bodies	Only few core members represented	4	1	0	0	0	5
	Selective representation	1	0	2	0	2	5
	Broad representation	5	4	5	2	3	19
	All CNO member organisations represented	3	3	**9**	3	6	24
	Total:	13	8	16	5	11	53

Table 14: Crosstabulation analysis for classifying governance models of existing not-for-profit networks.

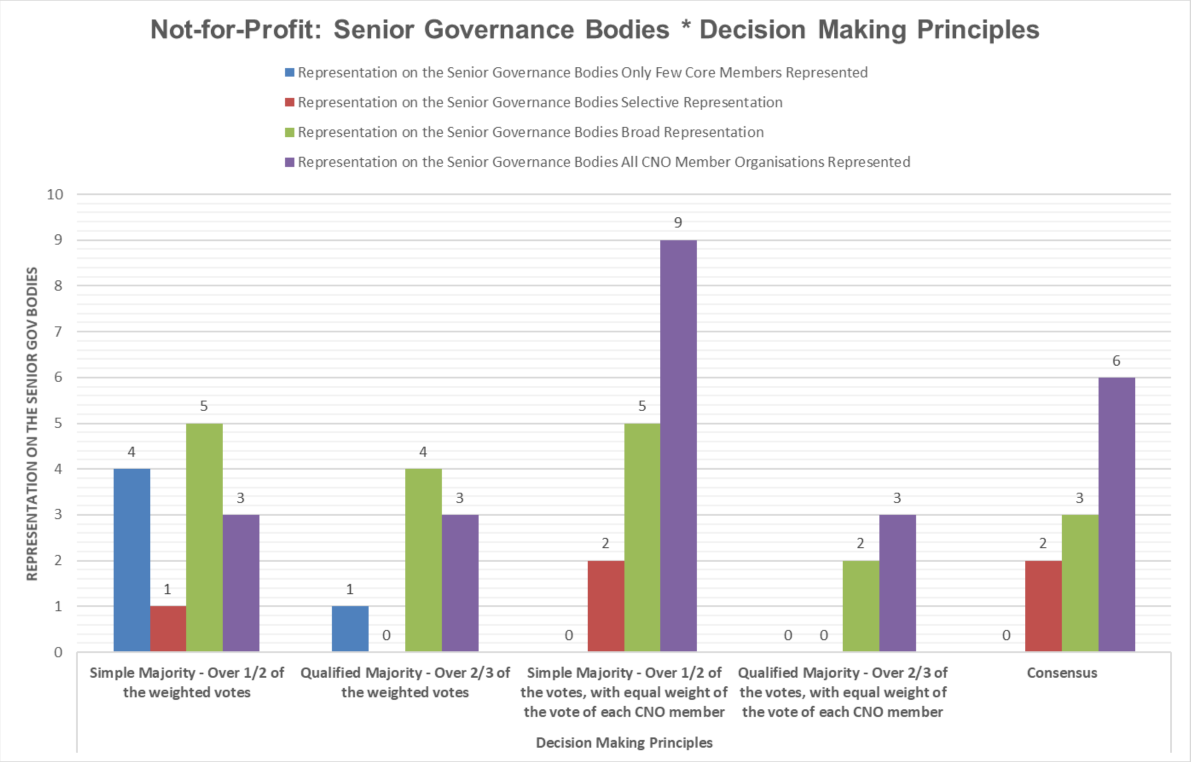

Figure 13: Bar chart demonstrating the distribution of decision-making principles vs representation on the senior governance bodies; not-for-profit orientation CNOs.

Governance Models: existing networked organisations (irrespective of profit orientation)

Combining and critiquing the findings for both types of profit orientation indicates that representation of all CNO members appears to be the most common form of representation on senior governance bodies, accounting for 43 % of the sample (n = 26). Likewise, the most predominant means of making decisions which were adopted—irrespective of profit orientation—was the simple majority (decision-making with over 1/2 of the votes), whereby votes from each CNO member carried equal weight (as highlighted in Table 15 and illustrated visually in Figure 14).

Representation on the Senior Governance Bodies vs Decision-making principles							
		Decision-making principles					
		Simple majority – over 1/2 of the weighted votes	Qualified majority – over 2/3 of weighted votes	Simple majority – over 1/2 of the votes, with equal vote for each CNO member	Simple majority – over 1/2 of the votes, with equal vote for each CNO member	Consensus	Total:
Representation on the Senior Governance Bodies	Only few core members represented	4	1	0	0	0	5
	Selective representation	3	0	3	0	2	8
	Broad representation	5	5	6	2	3	21
	All CNO member organisations represented	5	3	**9**	3	6	**26**
	Total:	17	9	**18**	5	11	60

Table 15: Crosstabulation analysis for classifying governance models of existing networks (irrespective of profit orientation).

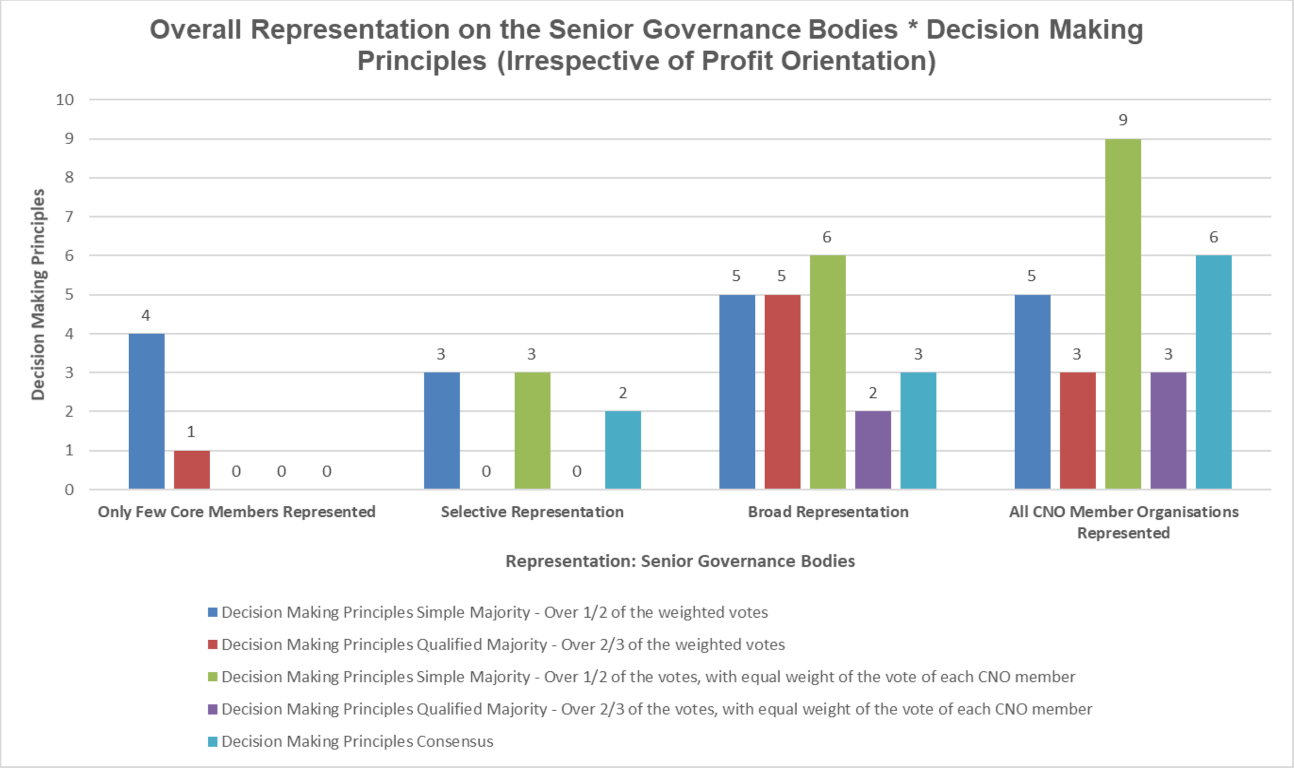

Figure 14: Bar chart demonstrating the distribution of representation on the senior governance bodies vs decision-making principles (irrespective of profit orientation).

5.3 Findings on governance models from the academic literature

5.3.1 Approaches to creating and maintaining a CNO

The creation of collaborative networks has been the subject of several studies. According to a recent publication by Arrais-Castro et al. (2018), a network may be configured as (1) VBE with a broker company; (2) Virtual Enterprise (VE) with a broker company; (3) VE without a broker company; or (4) Collaborative supply chain network. Next, partner roles are revisited, and the CNO role assignments are defined. This may include defining the companies that may assume the broker role, and which companies may coordinate outsourcing initiatives, among other options.

More than a simple hierarchical network, a VBE is characterised by numerous repeated connections between companies that constantly shift and expand. A VBE is, in fact, a type of CNO, representing an association of organisations adhering to a long-term agreement and adoption of common infrastructures and operating principles (Camarinha-Matos et al., 2013). Typically, a VBE includes *a single Broker* that assumes the responsibility of acquiring and processing business opportunities. As a response to new business opportunities, a new VE may be dynamically created in the VBE. Those VEs may be terminated after the corresponding orders have been fulfilled.

5.3.2 Identified Governance Models of CNOs

Camarinha-Matos, Afsarmanesh, and Ollus (2008) present a *VBE Governance Model*. They argue that Collaborative Networked Organisations represent one of the most relevant organisational paradigms in industry and services. *VBE ethical values* represent a guide to stakeholders to consider whether decisions are right or wrong when facing situations that pose a dilemma in action courses. Having an ethical code will help VBE stakeholders to regulate their behaviour and promote fairness in value exchanges among them.

Collaboration needs to be governed to provide for *fairness between individuals, groups, and/or organisations in collaborative endeavours and value exchange to avoid opportunistic behaviours*. Governance models aim to define collective actions where several actors negotiate and collaborate to achieve common and compatible goals. Governance models intend to provide a set of guidelines to adapt, coordinate and safeguard autonomous actions collectively while working in a joint plan where risk, resources, responsibilities, and rewards are shared among actors to achieve a mutual goal.

Three main elements are defined when describing the governance model of a CNO, as follows:

- *Principles* are the values that govern an individual's or an organisation's behaviour. There are some important principles to be followed to assure value creation, maintenance, and development;
- *Bylaws* are generally understood as the document adopted by an organisation to regulate its affairs; they may be formally referred to as the *rules of operation*. When bylaws, or rules and regulations, are adopted by a corporation for its internal governance, they usually contain provisions relating to shareholders, managers, officers and general corporate business;
- *Rules* refer (formally or informally) to various types of guidelines (i.e. direction, standard, method, operation) or standard (i.e. definition, fact, law, code, truth, etc.). Rules are often divided into two groups related to (a) *Behavioural Rules* as rules for good acting and conducting, including ethical behaviour (e.g. ethical code) and culture, and (b) *Functional Rules* that support both operational and administrative procedures along the *VBE lifecycle stages* – creation, operation, evolution, metamorphosis, and dissolution.

Camarinha-Matos et al. (2008) offer a template of an ethical code of virtual breeding environments (VBEs) that covers responsibilities of VBE actors to partners, clients and society and declares certain values, including:

- Collaboration;
- Sharing Attitude;
- Fairness;
- Quality and Reliability;
- Competence;
- Innovation; etc.

In the chapter on VBE value systems, business models, and governance rules, the same publication (p. 87, figure 14 "VBE Governance Model") offers sets of:

- *Principles*, including Collaboration, Honesty, Trust & Integrity, Openness, Performance Orientation, Responsibility & Accountability, Mutual Respect, Commitment to the VBE;
- *Bylaws*: Rights & Duties policies; Membership policies; Incentives; Sanctions; Security issues; ICT Use Guidelines; Conflict Resolution Policy; Financial policies; amendments to bylaws; IPR policies; and
- *Rules*: VBE behaviour (VBE culture, VBE Ethical Code) and VBE function (VBE lifecycle functions; VBE internal/administration functions; Opportunity-based /emergent/ functions).

Cardoni, Saetta, and Tiacci (2010) consider three different forms of CNOs: the *Virtual organisations Breeding Environment* (VBE), the *Virtual Development Office* (VDO), and the *T-Holding.* Their publication presents a comparative study of three model-based approaches to creating and maintaining a CNO, namely:

1) *VBE (Virtual organisations Breeding Environment) model*. VBE is an ampler concept than that of an industry cluster, industry district, business echosystem, virtual laboratories, and crisis management that operates only to the regional level; VBEs are essentially focused on a type of product or service;

2) *VDO (Virtual Development Office) model*. The model provides a *central entity*, namely the Virtual Development Office (VDO), which is tasked to create, coordinate and manage the network of enterprises, supplying some interface with the market and guaranteeing the consolidation of relations of confidence between the actors of the community in a strategic alliance for a long time. The VDO acts as a unique interlocutor toward the ecosystem of businesses; it favours both the wish of cooperation and the collaboration every time that a collaboration opportunity appears. If one compares a VDO with a VBE, a higher degree of coordination can be observed in the former due to the presence of the VDO entity. The VDO is proactive by promoting research, innovation, and marketing within the network, particularly due to its nature of a for-profit company, and the collaboration needs to reach a profitable dynamic.

3) *T-Holding model*. The model was created towards applications to Small and Medium Enterprises (SMEs) that are facing a financial and economic *crisis*. However, the model can also be utilised to aggregate companies that do not necessarily face a crisis, as the model offers a stronger degree of integration compared to the other two models, the VBE and the VDO. The T-holding model implements the following mechanism: the entrepreneur transfers the ownership of his or her firm (both tangible and intangible assets) to the T-Holding and becomes a shareholder of this new company, acquiring several shares (or stocks) based on the value of the asset that is brought to the new company. The entrepreneur can also assume an operative role

of partner-entrepreneur who is responsible, for example, for the production function of the plant. In other cases, the entrepreneur could just participate as a financial partner, without executive responsibilities. The strategic and operative governance is assigned to an "industrial manager," who is responsible for the industrial strategy and the general management, while a "financial manager" is responsible for the financial and economic planning.

The concept of Governance in Networked Enterprises (GNE) is treated by Rabelo, Costa, and Romero (2014). The authors define governance as the "specification of rules, criteria for decision-making, responsibilities, and boundaries of actions and autonomy for the involved actors". A GNE is created by the set of constituent organisations to regulate the networked enterprise. The fundamental role of governance is not managing, but to delimitate/ guide the management instead.

Networked enterprise governance has to consider two complementary dimensions: one related to the coordination of the economic activities, and the other one to the network structure. The essential rationale is that the market and power directly influence the way a network should execute and manage its processes and all related information, and hence on how it should be internally organized to correctly and efficiently respond to market pressures (Rabelo, Costa, and Romero, 2014).

From a scientific perspective, the main contribution of the GNE model refers to the *integration of the economics governance dimension* and that the model is very concrete, more formally expressed, and indicates how its elements can be instantiated.

The *governance model with a Virtual Development Office (VDO)* is addressed also by Saetta, Tiacci, and Cagnazzo (2013). The network analysed by the authors is constituted by 21 companies belonging to the paper converting, packaging, and logistics sectors. The authors define the VDO model as a "strategic association/ alliance of organizations and the related supporting institutions, adhering to a long-term cooperation agreement and adoption of common operating principles and infrastructures, with the primary goal to create innovative business organisations.

The *network enterprise* (or *collaborative enterprise*) structure is presented by Serrier, Ducq, and Vallespir (2017). This is a network of legally independent companies linked to each other by the production cycle (of one or several products or a range of products). They are thus mutually dependent on a network of selected partners that revolves around a central core or a pivot company. Despite this central core, the authors speak of "de-hierarchization" in the sense that the purchaser/ supplier relationship shifts from a traditionally hierarchical relationship to collaboration.

Not all companies in the network have the same importance. The "*pivot company*," which is usually a large manufacturer, does not collaborate in the same way with all the companies of the network. At least three different levels can be identified. One then speaks of the shift from capacity subcontracting (linked to the market) to specialty subcontracting (hierarchical) and eventually to intelligence subcontracting (network): "First of all, one finds capacity subcontracting whereby the subcontractors meticulously comply to the specifications given by the contractor, […] then there is the specialty subcontractor who participates, to some degree, to the definition of the specifications of the ordered product […] and at a third level one finds the subcontractor of 'intelligence' who systematically attempts to design and develop the product best suited to meet the needs expressed by the contractor" (Serrier, Ducq, and Vallespir, 2017).

The article by Su, Biennier, and Ouedraogo (2012) suggests examining *business governance* as an *extension of the Service Oriented Architecture (SOA) governance*. The development of a collaborative business process relies mostly on software services spanning multiple organisations. Uncertainty related to the shared assets and the risks of infringement of intellectual property is of major concern and may hamper the development of inter-enterprise collaboration. This article puts forward a governance framework to enhance trust and assurance in such a collaborative context and to cope with the impacts of cloud infrastructure. First, based on a collaborative security requirements analysis of assets sharing relations in the business process, authors identify risks and uncertainties and, thus, elicit security requirements of partners and their profiles. Secondly, a 'due usage' aware policy model is used to support negotiations between the asset providers' requirements and consumer profiles. The mechanism for enforcement adapts to dynamic business processes and cloud infrastructures to provide end-to-end protection on shared assets. The foundation of the framework suggested in the publication includes *collaboration-oriented security requirements' engineering method* and a domain knowledge base to define partners' security policies and profiles. The application of the method is coupled with a negotiation strategy between the policies and profiles, as well as enforcement of decisions to achieve end-to-end protection for assets.

According to Li, Biennier, and Amghar (2012), governance is still *one of the most important challenges for collaborative enterprises*. Some studies of collaborative networks focus entirely on *technological aspects and often neglect other business-related issues*. Business process management, performance management, and business process alignment are of vital importance in order to increase the synergy of the collaborative organisation. The authors suggest a flexible, efficient collaborative governance framework: Governance as a Service framework (GaaS), supporting dashboard mashups, and the implementation of an autonomous strategy to govern the collaborative environment globally.

They further argue that various barriers (decentralised organisation, uncertainty, dispersed IT infrastructure, etc.) obstruct the development of collaborative governance. To meet the demands of *geographically distributed collaborative enterprises*, the suggested Governance as a Service framework deploys local key performance indicators to govern the performance of each participant organisation and activates local action engines to reduce wastes and errors. They further suggest using cross-platform virtual resources repository to share governance information and make full use of existing resources to establish mashup-based dashboards and improve the efficiency of display governance reports. Even if each component can be geographically distributed according to users' needs, they all closely collaborate to monitor the performance of the collaborative environment comprehensively.

5.3.3 Arrangements for collaboration in CNOs

Truptil et al. (2015) present a *framework of CNO Governance* divided into three main layers to support all previously identified functionalities and thus reach the aim to "instantaneously transform information gathered from a vast array of diverse sources into useful knowledge for making effective decisions." The layers are:

- Agility layer, including model comparison, detection, and collaborative process design;
- Simulation layer; and
- Updating layer, including Trust Management; Information function; Model Adaptation; Compare to process deduction; Process state; Information added by the user; and Semantics reconciliation.

The idea of establishing HUBS—*actors with high centrality or influence*—is addressed also by Durugbo (2016). Such hubs are important in CNOs due to their abilities to act as gatekeepers to link partners. Besides, the beneficiaries of network outcomes and intermediaries who mediate between participants as brokers or supporters are also presented on the hub, as well as stakeholders (e.g. from government, community and industry sectors).

Collaboration arrangements may correspond to one of three main *topologies*:

- A *star topology* in which the hub (the leading partner) dictates or dominates interactions between individuals and groups;
- A *tree topology* where specific problems are solved through mutual work with other collaborators, and hubs are also present but act as connectors to other parts of the collaborative network; and
- A *torus topology* in which uni-, inter- or multi-disciplinary goals are achieved through working exclusively and negotiating with other partners for advice/ updates. Durugbo (2016) explains the torus configuration as "project-oriented federated network".

Collaborative network typologies and interfaces may also be *horizontal*, with a *focus on complementary competencies* of partners, or *vertical*, where the *concentration is on close competence fields* that increase capacities or negotiation powers.

An idea of interest in the distribution of the processes in CNOs, geographically, and culturally, is presented by Enquist, Nilsson, and Magnusson (2004), who focus on creating a *good communicative culture*. This communicative culture is functionalistic, which is highlighted by the communication, often focusing exclusively on the product of the network.

With the main objective for the network management of the Supply-chain Network (SN) being cost reduction through optimisation of joint processes, the usage of goals, checkpoints, forecasting, and follow-ups are essential instruments. Since the Business Network (BN) hub-company acts as an initiating partner and thereby attracts other partners on the notion that their participation will lead to success, the overall responsibility for the outcome is directly attributed to the hub-company.

The importance of the (potential) role of a "*network coordinator*" for the governance of CNOs is addressed by Obidallah, Raahemi, and Alaieri (2014). The authors suggest a structure to govern change, where each VO business partner has a representative in the *Change Advisory Board* (CAB) – a governance body that oversees several processes through change-related management interfaces: Process management; Performance management; Knowledge management; Problem management; Release management; and configuration management: VOs need to evolve to meet the market and customer demands by changing their business processes and services.

The authors focus on the *technical aspect of change management*, which is "a process whereby changes to service are formally introduced, approved before deployment into the next testing or production stage" (Obidallah, Raahemi, and Alaieri, 2014). They focus on changes to service through its whole lifecycle to ensure efficient handling of all changes through the use of standardised methods and procedures based on industry best practices. The goal is to support the process of change, enable the traceability of changes, minimise the impact of change, and gradually improve the day to day operations.

Six layers of change processes are identified, covering respectively: change initiation; identification and assessment; communication and collaboration; planning and authorisation; coordination and implementation; and evaluation and closure.

The process of *change management in CNOs* is also in the focus of the publication by Andres, Poler, and Sanchis (2015), who emphasise the need for flexibility in the process of recovering from disruptions.

According to the authors, to be successful, CNOs have to: (1) restructure their internal operations; (2) make information systems interoperable; (3) coordinate their production processes and align their strategies; (4) share goals; (5) achieve suitable levels of trust; (6) reach agreements on practices; (7) align values, and (8) be more agile and resilient.

An interesting view on *Collaborative Networked Organisations* as a *System of Systems* (SoS) is presented by Bilal, Daclin, and Chapurlat (2014). The authors postulate that there is a parallel between CNOs and SoS. In this regard, and as demonstrated by the literature in the system engineering domain, *interoperability* can be fully understood and considered as a decisive factor when organisations set up a CNO.

In most cases, SoS is seen as a group of existing entities assembled to interact for a period of time to produce some kind of capabilities, products or services, and to achieve a common goal that a system or organisation alone cannot achieve. From the SoS point of view, there are seven crucial characteristics for the SoS: *operational independence*, *managerial independence*, *evolutionary development*, *emergent behaviour*, *geographic distribution*, *connectivity*, and *diversity*.

A lack of *interoperability* among two or more CNO entities can impact the CNO's analysis perspectives:

- *Stability*: the CNO's ability to maintain its viability and to adapt to any change in its environment. A CNO shows both homeostasis and adaptive behaviour, as it can constructively respond to disturbances or novel environmental conditions. Therefore, enhancing the interoperability contributes to ensuring and increasing the CNO stability over its lifetime even if none of the existing architectural styles of self-adaptation for SoS guarantees the SoS' stability;
- *Integrity*: the CNO's ability to adapt to changes in its environment and remain viable, e.g., by modifying or removing some of the existing CNO entities;
- *Performance* is the perspective that reflects the CNO's ability to reach its performance objectives. The goal here is to meet a sufficient level of performance promptly and not necessarily to guarantee a maximum level of performance.

The challenge of operating across professional, cultural, regional and linguistic boundaries in the context of a CNO, where ways of sharing knowledge differ markedly, is discussed by Mabey and Zhao (2017).

Some authors, e.g., Ardakani, Hashemi, and Razzazi (2019), focus on possible *technological solutions to build and sustain CNOs*, for example, the transition from the traditional methods of creating and operating inter-organisational collaborations towards cloud-based solutions. The authors of the cited article present an adaptation of the Scrum methodology to enhance its usability with the specific characteristics of *cloud-oriented collaborations*. In the article, they present a reference architecture for a system deployed on a cloud provider offering the *creation* phase of CNOs' life cycle as a service. The goal is to show that the Cloud is a potentially reliable, scalable, and cost-effective IT solution for the exploitation of external knowledge resources, skills, and production facilities in the CNO domain.

5.3.4 The collaborative and absorptive capacity of networked organisations

The publication by Ulbrich et al. (2011) discusses the *collaborative capability of teams in networked organisations*. The authors present a comparative study on CNOs in Austria and Switzerland. They maintain that, so far, the collaborative capability has mostly been conceptualised on an organisational or individual level as a set of attributes that actors employ to collaborate successfully. They argue that this view of collaborative capability needs to be enlarged. The collaborative capability of teams is characterised by at least two components: (1) an attribute-based perspective that focuses on capabilities of single actors or organisations, and (2) a perspective on group dynamics that describes how teams successfully develop collaborative capability. Also, *neutrality and confidentiality of network management* have been underlined as essential factors for successful collaboration in all three studied networked organisations.

The topic of the *absorptive capacity of CNOs* is discussed by Hovorka and Larsen (2005). Absorptive capacity (ACAP) is defined as a set *of organisational abilities to manage and use new knowledge.* It has four distinct dimensions: (1) acquisition; (2) assimilation; (3) transformation; and (4) exploitation of knowledge. ACAP relies on external connections as well as internal social networks that link the dimensions within and between organisations, thus facilitating the distribution and exploitation of knowledge.

The four dimensions of the *absorptive capacity* are defined as follows:

- *The acquisition* is the ability to recognize, value and obtain external knowledge;
- *Assimilation* is the incorporation of external knowledge and combination with existing capabilities to increase internal knowledge;
- *Transformation* is the ability to adapt and integrate new knowledge with current business practices; and
- *Exploitation* is the ability to utilise new knowledge for commercial purposes.

The time and resources devoted to acquiring and distributing information are also critical components in achieving increased ACAP.

Additionally, Hovorka and Larsen (2005) outline the *key characteristics of a networked organisation*:

- flexibility, decentralised planning and control, multiple connections between CNO entities, and the high degree of integration of various types of socially important relations across formal boundaries;
- they consist of autonomous organisations that come together to reach goals that none of them can reach separately;
- CNOs are particularly suitable for circumstances in which there is a need for efficient, reliable information;
- most useful is not the information flowing down the command chain, but the information obtained from someone with whom one has had prior dealings and experience of reliable performance.

The respective communications network includes both central ties, e.g., from local departments to the lead department or from SMEs to the pivot company or broker, and lateral ties between members of the network. Research has demonstrated that direct connections between organisations are most effective in the transmission of knowledge, particularly if the knowledge is not codified as a set of formal documents.

5.3.5 Organizational resilience of CNOs and value systems alignment

Important findings on *organisational resilience*, *self-organized collaborative networks,* and *sustainable communities* are presented by Jung (2017). The publication provides evidence for the general argument that *organisations centrally positioned between two other actors perceive a higher level of organisational resilience*, thus supporting the bridging hypothesis. The finding implies that organisations with a bridging strategy can increase their capacity to recover from a catastrophic event by their guaranteed access to critical resources and information in an effective and timely manner. Besides, the current trend towards flattening organisational hierarchies can be described by maximising the regulatory abilities of personnel and organisations, using better education and empowerment, management, and technical support.

Macedo and Camarinha-Matos (2017) present *assessment of value systems alignment*. The authors maintain that it can play an essential role in the formation and evolution of collaborative networks, contributing to the reduction of potential risks of collaboration. Towards this purpose, they propose an assessment tool as part of a collaborative network's information system that supports the formation and evolution of both long-term strategic alliances and goal-oriented networks.

5.3.6 Trust relationships and trustworthiness in CNOs

The topic of the necessity for the pre-existence of Virtual organisations Breeding Environments (VBEs) to support the fluid creation of dynamic opportunity-based Virtual Organisations (VOs) is addressed by Msanjila and Afsarmanesh (2007). While collaboration among organisations provides the promise of better success, a big remaining challenge and risk are related to the choice of trustworthy partners to be pulled closer and included in VOs in order to address a market/society opportunity.

To assess and manage trust in VBEs, trust and trust relationships must be properly characterised and modelled. The authors address the modelling of trust relationships in VBEs, seen as very important for industry-based but also other VBEs.

For the specific case of VBEs, trust is essential on three main counts:

- *Trust among members*. The main aim of establishing trust relationships among VBE members is to enhance the efficiency and success both of their cooperation within the VBE and their potential collaboration in VOs that will be configured within the VBE;
- *Trust between the member and the VBE administration*. Trust of VBE members to the VBE administration enhances the chance of members remaining loyal to the VBE, increases their willingness for active involvement in VBE, and encourages VBE members to invite and bring other valuable organisations into VBE;
- *Trust between the customer and the VBE*: VBEs must be trusted by their customers. Customers that create opportunities in the market (to which VBE can respond by creating VOs) must recognise and trust the VBE to accept its proposed bid. Consumers (end users) must trust the VBE to decide positively on purchasing VBE's products and services.

Actors, trust perspectives, and time are the important elements that must be included in models of trust relationships among members in VBEs.

Actors: trustor and trustee. The two parties of the trust relationship are essential for defining, modelling and establishing trust relationships. Generally, a variety of factors might be required by different trustors for assessing the trust level of the same trustee, even with the same 'trust objective.' Therefore, both trustor and trustee must be represented in the trust relationship model distinctively.

Trust perspectives for trust relationships among organisations. Trust perspectives preferred by the trustor guide the process of collecting and deciding on the kind of information that a trustor or trust expert can use to assess the trust level of a trustee. Each pair of Trust-Need is characterised in different trust perspectives. For trust relationships among member organisations, the following trust perspectives were identified:

organisational perspective; social perspective; financial/ economic perspective; technological perspective; behavioural/ managerial perspective.

Time: Trust relationship (and its intensity) between two organisations is a time-dependent issue, which may differ considering yesterday, today, and tomorrow. In other words, the trust level of trustees is not static and may vary depending on changes in the factors as well as the specific assessment approaches. Thus, time is an essential factor and must be addressed in modelling trust relationships in VBEs.

5.3.7 Key performance indicators of CNOs

The idea of *CNOs key performance indicators (KPIs)* is presented by Rodríguez-Rodríguez, Alfaro-Saiz, and Verdecho (2015). The authors identified the following KPIs:

1. Number of knowledge strategies' changes;

2. Improvement of the degree of contextualisation of multi-disciplinary knowledge;

3. Improvement of the service level;

4. Improvement of the customer involvement level;

5. Improvement of the customer fidelity degree;

6. Improvement of the delivery time;

7. Decrement of the life cycle time-to-market;

8. Improvement of the customer satisfaction degree;

9. Improvement level of the GRI (Global Reporting Initiative) indicators related to sustainable production;

10. Number of collaborative product designs;

11. Improvement of the number of additional business services offered;

12. Improvement of the degree of collaborative innovation;

13. Improvement of the degree of perceived quality;

14. Improvement in of sales achieved (% turnover);

15. New business opportunities discovered.

5.3.8 New directions for CN studies

An area of research that could offer new directions for CN studies involves the *analysis of longitudinal relationships within the context of CN logic* (Durugbo, 2016). The notion of longitudinal relationships in CNs extends the horizontal and vertical interfaces that have been examined by researchers by considering the time factors and nature of dynamism for interactions between actors. This has an impact on the configurations of partners which are often overseen by different policy or problem domains. In effect, longitudinal relationship analysis is a network design issue that evokes transitions between network structures, structural change over time (especially due to changing reputations) and efficiency-exploitation trade-offs (see Durugbo, 2016 and the references therein). Further work is also recommended to improve understanding of how novel processes such as outsourcing or transitional relationships are factored into longitudinal relationships. Inevitably, ownership and stewardship are factors that impact how longitudinal relationships are managed in line with the overall CN goal and future work can help explain these factors in CN settings. The role of networking in facilitating such relationships can also be examined. In this regard, researchers may look beyond the social networking that influences promotion of other forms such as 'technological networking' that may take place at trade shows, or 'economic networking' for contracts, takeovers, and memoranda of understanding between partners.

The CN logic is reflected in *structures and behaviours that enable learning, networking and sharing* in collaborative networked environments. It was also highlighted that design methodologies for this logic need to reflect complex factors that contribute to aspects such as the information search capacity, creativity, and productivity of actors – as opposed to entities. CN arrangements require a blend of configurations that are organic in terms of the competencies that provide favourable network positions against the competition. Exchanges within CNs are determined by the mutual trust as partners develop durable and pervasive relationships. From a management perspective, the review, through an exposition of management strategies and mechanisms, emphasised the imperative for maximising advantages on collaboration and minimising collaborative inertia. Against this backdrop are potential constraints on operational autonomy and amplified dependence on partners.

5.3.9 Implications for Building the Governance Model of a Cybersecurity Network

The analysis of academic literature on governance models of CNOs, presented in this section, aimed to identify best practices that can be replicated in the development of the governance model of a cybersecurity network like the future ECHO-base network. Several of the findings discussed in this section may be of particular interest to achieve this goal.

First, the most important characteristics of the CNOs that make them viable and guide the design of the governance model of a cybersecurity network are:

- *flexibility*, decentralised planning and control, and lateral ties with a high degree of integration of multiple types of socially important relations across formal boundaries;
- *autonomous organisations* that come together to reach goals that none of them can achieve separately;
- they are particularly suitable for circumstances in which *reliable information* is needed;
- *they provide easy-going information exchange*: the most useful information does not flow down the command chain; preferably, it is obtained from someone in the network with whom one has had prior dealings and has found to be reliable.

Second, several arrangements of collaboration in a CNO are possible in terms of network topology: 1) *star topologies* in which hubs, or leading partners and points of contact for other collaborators (termed 'spokes') dictate or dominate interactions between individuals and groups, 2) *tree topologies* where specific problems are solved through mutual work, and 3) *torus topologies*.

Third, two philosophies of building and maintaining CNOs will be considered when the governance model of the ECHO network is designed. First is *the concept of a Virtual organisations Breeding Environment*—a long-term alliance of business companies, research institutes, and relevant support institutions—aiming primarily to increase their chances and preparedness for concrete collaborative projects. With that aim, the VBE establishes a cooperation agreement, adopts common operating principles, develops personal and organisational relationships and the supporting digital infrastructure, and strengthens trust among partners.

Second is the concept of a virtual organisation (VO)—usually a temporary, geographically dispersed network of independent entities established around a particular series of products or services and aiming to capture a market opportunity—and its business model. The VO may be flat or have a pivot company or a virtual development office where several core partners are represented. Of specific importance given the future implementation of Regulation 887 or, for that matter, any other cybersecurity competence network is the realisation that the cybersecurity CNO does not need to be a single, unified organisation; instead, it can be designed as a VBE and several VOs, each one established around a particular cybersecurity product or service. From this perspective, the ECHO CNO can be considered a System of Systems or a group of, in most cases, existing entities assembled to collaborate to produce particular capabilities, products, or services and to achieve a global mission that an organisation cannot fulfil on its own.

Fourth, the importance of focusing on VBE ethical values, fairness between individuals, groups, and organisations in collaborative endeavours and value exchanges is a finding that can be instrumental for the development of the governance model of the ECHO network. As well, *trust relationships* are a fundamental issue for VBEs: trust among members, trust between the member and the VBE administration, and trust between the customer and the VBE.

5.4 Organisational Modalities of Collaborative Networked Organisations

The analysis of existing collaborative networks allowed the exploration of more complex organisational modalities, where the CNO involves one or more types of legal entities of a different type.

In nearly 80 percent of the cases, the analysed networks are registered as not-for-profit legal entities – alliance, association, group, 'partnership,' 'institute,' etc. (Figure 15). Other eight percent are registered as corporations, private limited liability companies, or private institutes, while nearly half of that percentage is formed by 'accelerators' providing seed funding for start-ups or investment funding for existing companies.

Another 12 percent are not registered as legal entities. They are formed as a 'programme' or an initiative of an existing organisation or function on the basis of an agreement, often an international agreement, designating an organisation serving as the legal entity representing the network. An example for the latter is provided by the 12 CapTechs (Capability Technology Areas) moderated by the European Defence Agency (an intergovernmental agency of the Council of the European Union [9]) and bringing together experts from government, industry, small and medium enter-prises (SME), and academia to focus on particular technologies related to different military domains.

[9] European Defence Agency (n.d.) Who We Are, https://www.eda.europa.eu/Aboutus/who-we-are. Accessed 19 October 2020.

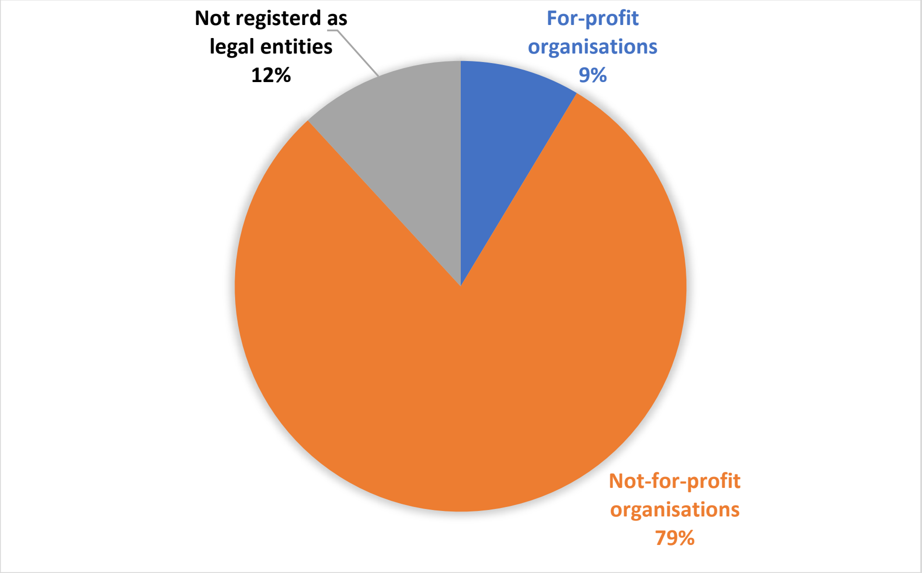

Figure 15: Registration forms of CNOs

Of higher interest for the future evolution of the ECHO network, and the European network of cybersecurity competence centres more generally, are existing organisational collaborations where the CNO includes or is related to one or more types of constituent legal entities. In total, 47 of the explored networks have such units (see Figure 16):

- 27 % of the CNOs have thematic units;
- 17 % have regional units; and
- 9 % have associated virtual organisations,

while five of the CNOs have both thematic and regional units, and one has both regional units and an associated virtual organisation.

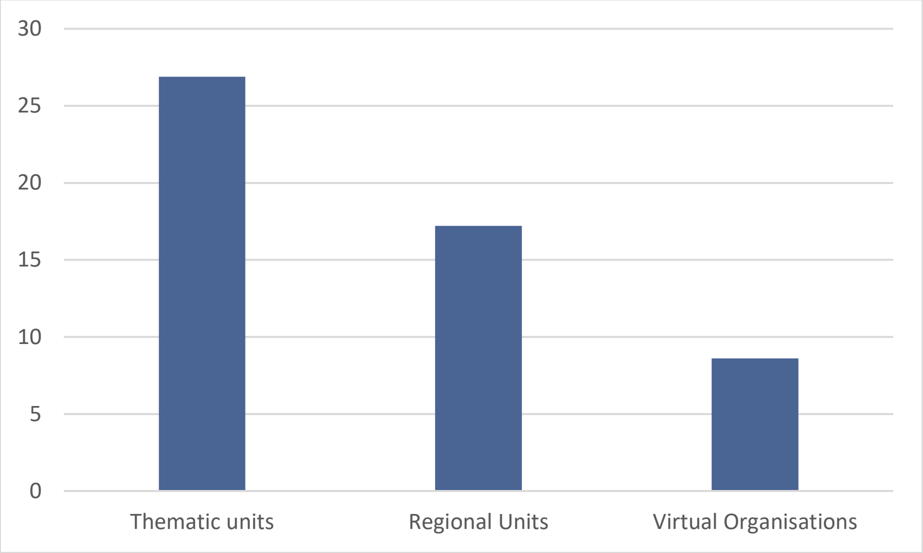

Figure 16: Percentage of the explored CNOs that have thematic units, regional units, or associated virtual organisations.

Twenty-five of the explored networked organisations have distinct, thematically oriented units. The overwhelming majority of these—special interest groups, committees, innovation communities, working groups, engagement areas, 'podlings,' working streams, etc.—are not legal entities. Only in two cases of networks of research and technology organisations—the Bulgarian Academy of Sciences and the Italian Consortium – Telecommunications (CNIT)—the institutes and laboratories specialized in areas of research are registered as legal entities, each one with its representatives on the governance bodies of the network.

The situation with the national or regional units is the opposite. Of the 16 networks with such units, in 14, the regional associations or chapters are registered as legal entities, and only in two the regional associations and groups are not distinct legal entities. In both cases, the relations between the umbrella CNO and its regional units are governed by the CNO's bylaws.

On many occasions, successful cooperation leads to the creation of new organizations in the form of alliances or joint ventures.[10] One can assume that many of the explored collaborations have served that purpose on an ad-hoc basis. Yet, of highest interest in creating a new collaborative networked organisation in the field of cybersecurity is when the CNO serves as a Virtual organisation Breeding Environment (VBE) and CNO governance bodies decide to create a new Virtual Organisation (VO). This decision establishes rights and responsibilities for the use of intellectual property rights and other resources of the network, funding, income distribution from the activity of the VO, etc.

The VOs are of two main types:[11]

[10] Christiane Prange and Ulrike Mayrhofer, "Alliances and Joint Ventures," *International Management* 6 (2015), https://doi.org/10.1002/9781118785317.weom060007.

[11] Hamideh Afsarmanesh and Luis M. Camarinha-Matos, "On the classification and management of Virtual organisation Breeding Environments," *International Journal of Information Technology and Management* 8, no. 3 (2009): 234-259.

- opportunity-driven VOs aiming to exploit an emerging market demand;
- virtual networked organisation for continuous delivery of a product or service, e.g., a federated cyber range or a supply chain.

Eight of the explored CNOs have associated virtual organisations of one of the two types, born out of the CNO. The study provided examples for three of the four possible combinations between a CNO, serving as a 'breeding environment,' and the virtual organisation in terms of their profit orientation (Figure 17).

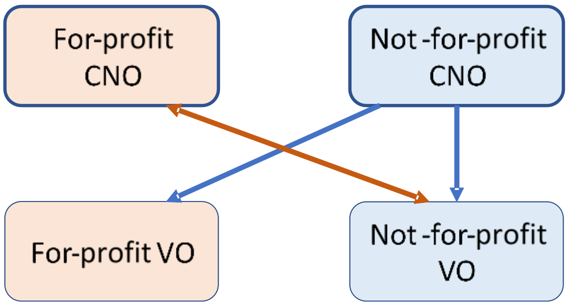

Figure 17: Combinations between CNOs and VOs in terms of profit arrangements.

In the prevailing pattern, with five of the identified cases, the CNO is of a not-for-profit nature, while the virtual organisation, created by the CNO, is business-oriented and serves to exploit a particular product or service developed within the CNO through commercial sales.

In two cases, both the CNO and the VO do not aim to generate profit but find suit-able arrangements for exploiting a particular service. An example here is the Educational Foundation of AFCEA International.[12]

Of particular interest is the case with HITRUST, originating as the Health Information Trust (HITRUST) Alliance, a not-for-profit organisation. The HITRUST Alliance delivered the HITRUST Common Security Framework (CSF). Currently, HITRUST is a private company, including a for-profit division (HITRUST Services Corp.) and a not-for-profit division (HITRUST Alliance).[13]

Any of the combinations outlined in this section is of interest for designing a collaborative networked organisation in the field of cybersecurity.

[12] AFCEA Educational Foundation, https://www.afcea.org/site/educational-foundation, accessed 20 October 2020.

[13] HITRUST Wikipedia page, https://en.wikipedia.org/wiki/HITRUST. Accessed 8 October 2020.

6. Partners expectations regarding the governance of the future ECHO network

6.1 Rationale and methodology of the study

In the Spring of 2021, during the deliberations on the Governance Model of the future (post-project) ECHO Network, it became evident that the lack of clarity the future engagement of consortium members in structured collaboration creates obstacles to effective discussions and decision-making. Therefore, the ECHO leadership decided that it is necessary to understand better the readiness of partners to be part of the ECHO Network and make explicit the considerations they have in that regard.

In order to assess the readiness of ECHO partners to commit to the future ECHO network that will be established after the end of the project, the study team designed a simple template (Table 16) allowing the partners to inform the consortium on their current position (i.e. to select one of the four categories A, B, C or D) and explain their respective considerations in a free text form. The template was disseminated in advance to the ECHO General Assembly meeting on July 15, 2021. Each partner was expected to share their views during the GA meeting and provide a written response as well. It was made clear that the partners' stated position at this time will not equate with commitment to follow a future course in regard to the ECHO Network.

Willingness to be part of the future "ECHO network"
Remark: "ECHO network" here may mean "ECHO Hub", a national chapter, one or more of the functional service groups.
A. My organisation XXXX will be a founding member of the "ECHO Network" and expects the following benefits: 1. 2. 3.
B. My organisation YYYY will be among the founding members of the "ECHO network" under the following conditions: 1. 2. 3.
C. My organisation ZZZZ hesitates to join the "ECHO network" because: 1. 2. 3.
D. My organisation VVVV will not join the "ECHO network" for the following reason(s): 1. 2. 3.

Table 16: ECHO partner's position on joining the future ECHO Network – a template.

As indicated in Table 16, there were four categories of involvement that partners had to choose from and list their arguments behind the decision. The categories are described below, as follows:

- *Category A*, which relates to partners who have expressed their commitment to be founding members of the ECHO network due to expected benefits;
- *Category B* for partners who are willing to be founding members of ECHO but under some conditions;
- *Category C* characterized partners who hesitate to join the future ECHO network due to particular reasons; and
- in *Category D* partners had the opportunity to state their reasons for not willing to be part of the future network.

In a qualitative approach, we used content analysis [14] to group the considerations of partners. Then we applied a simple qualitative analysis to identity issues of primary importance for the partners' attitudes towards the future network.

6.2 Study results

The ECHO Consortium currently includes 30 partners and 90 % of them responded by filling the form or verbally stating their interest in becoming part of the future ECHO network during the General Assembly discussion. Figure 18 presents the distribution of partners by the chosen category.

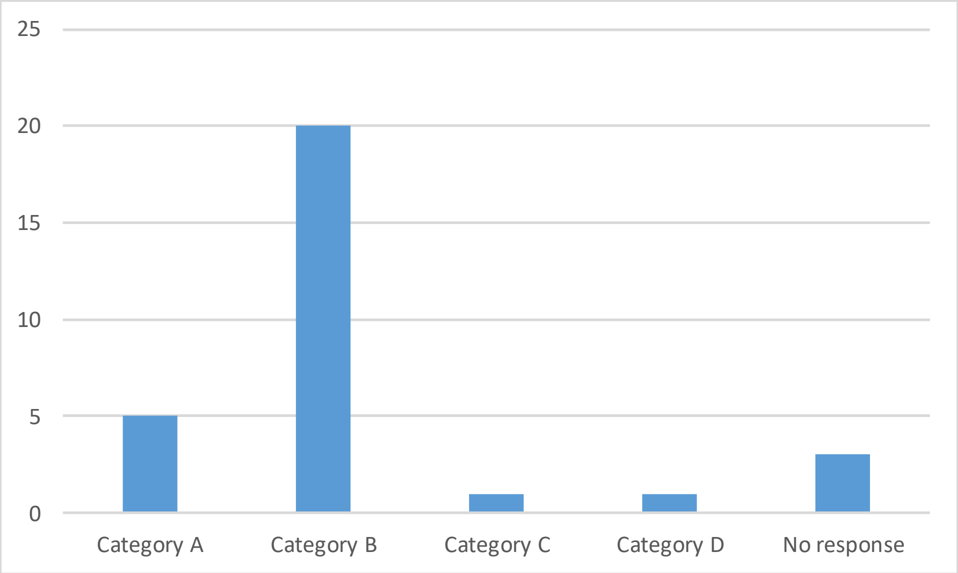

Figure 18: Number of partners per category of commitment to the future ECHO Network.

As seen in the figure, the majority of partners have stated their interest in becoming part of the future ECHO network, as 84 % of the respondents have considered themselves in either Category A or B. Five of them are Category A, i.e. clearly committed to be founding members of the post-project ECHO network. Another 20

[14] Alan Brymann, *Social Research Methods*, 4th ed. (Oxford, UK: Oxford University Press, 2012).

organisations have chosen Category B due to the fact that, as the project is still ongoing, some organisational and business model issues have not yet been resolved.

Further, the content analysis demonstrated that the arguments of partners selecting Category B and Category C are very similar. Therefore, it was decided to merge the considerations for these two categories.

Also, when filling the template, some of the partners decided to list as many arguments as they have and independent of the category they have selected. These arguments were also processed, thus enriching the overall understanding of the expectations to the governance model and the priority assigned to various considerations.

Partners that selected Category A saw as main benefits the prospects for:

- Exploitation of new business opportunities;
- Development of new skills and knowledge base;
- Pan-European partnerships in the field of cybersecurity.

As seen in Figure 19, partners willing to be founding members of the ECHO Network expect that they will be part of pan-European cybersecurity network and thus have a better access to new skills and knowledge, new and wider business opportunities.

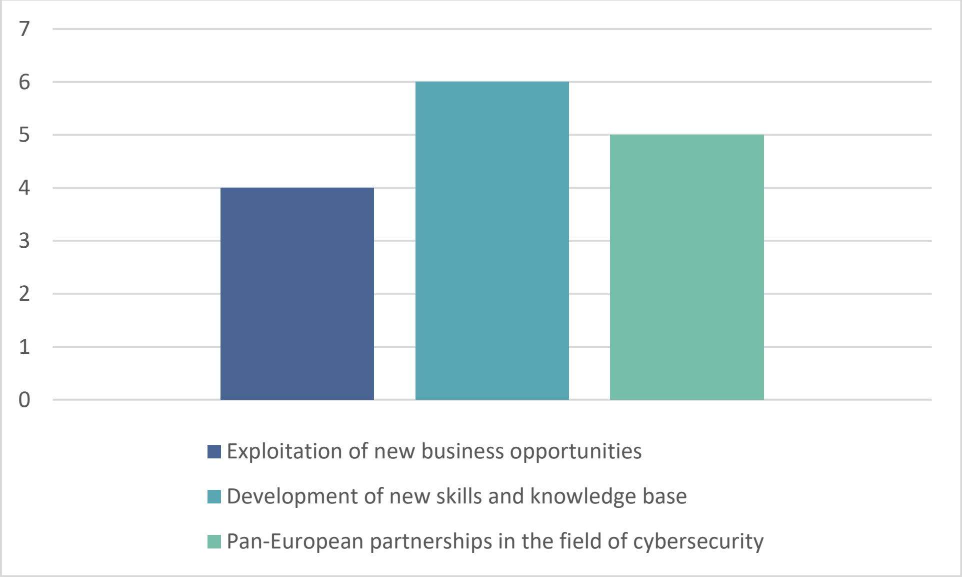

Figure 19: Anticipated benefits for founding members of the ECHO Network.

The conditions for joining the future ECHO network and the reasons for hesitation to do that relate to the need for:

- Clearly defined vision, organisational form, rules, roles and responsibilities;
- Business model (membership fees, “break even” horizon, expected return) and business plan;
- Retaining influence over decision-making, shaping and implementing the vision for the future ECHO network.

Figure 20 demonstrates that the majority of partners are interested to join the future network, with some expressing hesitation, but need to know more about its business model, the organisational form and governance rules and, to a lesser extent, want to make sure that their voice will continue to be important when decisions on the evolution of the network are made.

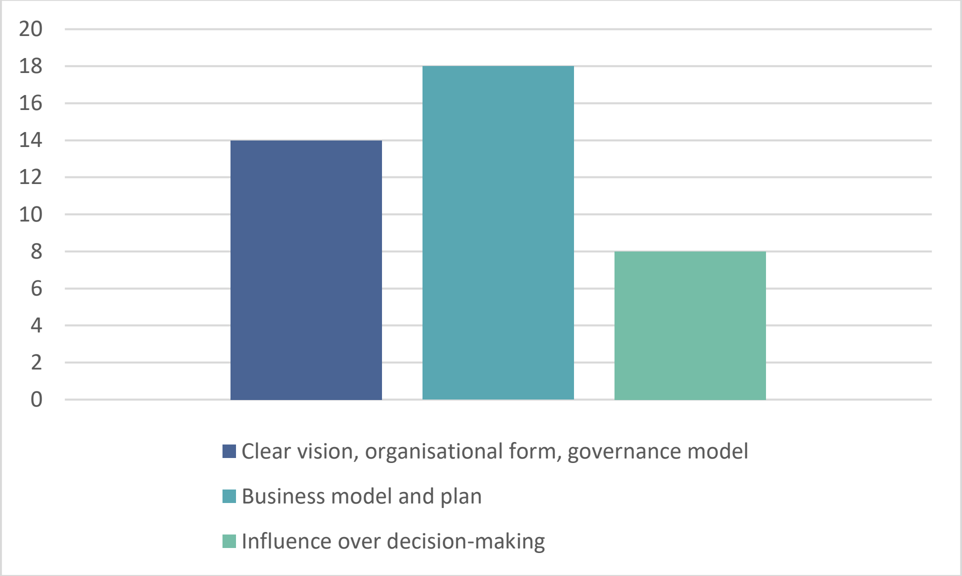

Figure 20: Conditions for joining the ECHO Network and reasons for hesitation.

Out of the 27 organisations that have stated their interest, only one noted that they will not be willing to participate in the future network. The reason they have listed behind their decision is that they plan to explore other spheres of business operations and the products and services that are part of the current ECHO portfolio will be out of their scope.

Since the project is still ongoing and the business model and plans are under development, the findings presented here are preliminary and may change over time with the project development. It is clear, nevertheless, that before partners commit, they want to make sure that the business and governance models of the future ECHO Network will correspond to their needs and will not conflict their interest.

Hence, in the further elaboration of the governance arrangements for the future ECHO Network, the WP3 team needs to take into account the expectations of the partners, presented here, preferably by involving them in the design of and the discussions on the business and governance models.

7. Conclusions and way ahead

This report presented the results of a comprehensive study of governance needs, objectives and requirements to collaborative networked organisations and their business and governance models. It was based on four types of primary sources: norms and regulations relevant to networked organisations in the field of cybersecurity; existing networks; academic sources; and interviews with stakeholders.

The comprehensiveness and the complementarity of the primary sources allowed to:

- Treat the subject of governance comprehensively – all aspects of governance referenced in the primary sources were structured in 34 "governance issues";
- Identify and describe good practices in the elaboration and implementation of business and governance models of collaborative networked organisations, as well as organisational modalities;
- Cluster examples of business and governance models of existing networks and thus indicate possible alternative models in the follow-up studies in WP3 "ECHO Governance Model";
- Prioritise governance needs and objectives;
- Elicit the expectations and requirements of ECHO member organisations towards the business and governance models of the future ECHO network.

In terms of CNO business models, the analysis of existing networks identified two prevailing patterns, respectively relying on *balanced funding streams* or *primarily on public funding*, while in both patterns CNOs are not-for-profit and both operational and network development decisions are taken in a single process or through a central decision point.

The respective picture of the governance models is more diverse. The model where all CNO member organisations are represented on senior governance bodies and decisions are taken with a simple majority, i.e. over 1/2 of the votes, with equal weight of the vote of each CNO member, has some prevalence, but other models are also of use, as illustrated in the analysis of existing networks.

Identified best practices, clusters of business and governance models and the prioritised list of governance needs and objectives are expected to *inform* and *orient* the development of alternative governance models and their evaluation, and not to predetermine the actions of the ECHO research team in follow-up tasks in WP3.

The current deliverable D3.8: "Update - Governance needs and objectives" will be updated once more during the lifetime of the project, in D3.9 due at the end of the project in January 2023 (M48).

This last update is needed to reflect on the evolving cyber threat landscape and the anticipated proliferation of models, including networked models, of developing solutions and organising for cybersecurity, and more general economic and societal developments (and perceptions and attitudes more specifically) that will have an impact on the governance needs and requirements, as well as the evolving understanding of ECHO partners in the process of implementation of the developed ECHO governance model.

Some of these requirements will likely reflect new EU or national legislative acts, as well as the development of Cybersecurity Atlas by the EU Joint Research Centre, ECSO and the collaboration among the four pilot projects and with ECCC and the national coordination centres.

The accumulated experience will be subject of academic scrutiny that may lead to identification of new trends and best practice models.

The study of these developments and the definition of new requirements and priorities will allow to enhance and adapt the ECHO governance model accordingly.

Finally, the forthcoming update will allow us to deliver a current and consistent package of documents presenting in detail governance requirements, analysis of practice, and the final (within the project duration) ECHO governance model.

Annexes

Annex 1 – Glossary of main terms

Term	Definition
Collaborative Network (CN)	A network consisting of a variety of entities (e.g. organisations and people) that are *largely autonomous*, *geographically distributed*, and *heterogeneous* in terms of their operating environment, culture, social capital and goals, but that collaborate to better achieve common or compatible goals, thus jointly generating value, and whose interactions are supported by computer network (Camarinha-Matos et al., 2009)
Collaborative Networked Organisation (CNO)	Network of profit-and-loss responsible organizational units, or of independent organisations, connected by IT, that work together to jointly accomplish tasks, reach common goals and serve customers over a period of time (Tapia, 2009) The second type—of independent organisation—is of primary interest in this report.
Governance	Specification of rules, criteria for decision-making, responsibilities, and boundaries of actions and autonomy for the actors involved in the CNO (based on Rabelo, Costa, and Romero, 2014)
Homophily	Organisational similarity; the tendency for organisations to engage in direct contact with other organisations they view as similar (Hovorka and Larsen, 2005 & 2006).
Value System (VS)	A voluntary cooperation that creates value through the flexible reconfiguration of the resources and competences of its participants (da Silva and de Almeida, 2017)
Virtual Development Office (VDO)	A new for-profit company operating as a permanent network management/ coordination entity for a strategic association/ alliance of organisations and the related supporting institutions, adhering to a base long-term cooperation agreement and adoption of common operating principles and infrastructures, with the main goal to create innovative business organisations (based on Saetta, Tiacci and Cagnazzo, 2013).
Virtual Enterprise (VE)	A temporary alliance between companies for managing business opportunities (Camarinha-Matos and Afsarmanesh, 2004). A relatively temporary network of formally independent companies or individuals uniting their means, skills or resources in order to achieve together a project that could have exceeded the capacities of each involved entity if considered alone (Serrier, Ducq, and Vallespir, 2017).
Virtual Organisation (VO)	An association of legally independent organisations that come together (often temporary, for a certain period of time) to share resources and skills to achieve a common goal such as acquiring and executing a collaboration opportunity. VOs are configured constituting suitable VBE members that are selected based on requirements of the opportunity, such as competence, trust level, etc. (based on Msanjila and Afsarmanesh, 2007).
Virtual organisations Breeding Environment (VBE)	The Virtual organisation Breeding Environment (VBE) is defined as an association of organisations and related supporting institutions adhering to a base long-term cooperation agreement, and adopting common operating principles and infrastructures, with the main goal of increasing both their chances and preparedness towards collaboration in potential Virtual Organisations (Msanjila and Afsarmanesh, 2007).

Annex 2 – List of norms and regulations

EU regulations

- 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 (R 887, 2021);
- Cybersecurity Act (CA, 2019);
- EC Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises
- Joint Communication to the European Parliament and the Council "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" (RDD, 2017);
- 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, 2016).

Pilot projects' regulations

- ECHO: Grant Agreement, Consortium Agreement, Project Handbook
- CONCORDIA: Proposal; Grant Agreement Part B
- CYBERSEC4EU RIA - IA Part B
- SPARTA Description of Activity - Part B

Annex 3 – List of analysed academic sources

Short reference	Full bibliographic information
Aagaard, 2019	Annabeth Aagaard, "The Concept and Frameworks of Digital Business Models," in *Digital Business Models: Driving Transformation and Innovation*, edited by Annabeth Aagaard (Cham, Switzerland: Palgrave MacMillan, 2019), 1-26, https://doi.org/10.1007/978-3-319-96902-2_1.
Abreu and Calado, 2017	Antonio Abreu and João M.F. Calado, "Risk Model to Support the Governance of Collaborative Ecosystems," *IFAC-PapersOnLine* 50, no. 1 (2017): 10544-10549, https://doi.org/10.1016/j.ifacol.2017.08.1313.
Andres, Poler, and Sanchis, 2015	Beatriz Andres, Raul Poler, and Raquel Sanchis, "Collaborative Strategies Alignment to Enhance the Collaborative Network Agility and Resilience," in *Risks and Resilience of Collaborative Networks*, edited by Luis M. Camarinha-Matos, Frédérick Bénaben, and Willy Picard, PRO-VE 2015. IFIP Advances in Information and Communication Technology, vol. 463 (Cham: Springer, 2015), 88-99.
Ardakani, Hashemi, and Razzazi, 2019	Mohammad Reza Mollahoseini Ardakani, Seyyed Mohsen Hashemi, and Mohammadreza Razzazi, "A Cloud-based Solution/Reference Architecture for Establishing Collaborative Networked Organizations," *Journal of Intelligent Manufacturing* 30, no. 5 (2019): 2273-2289, https://doi.org/10.1007/s10845-017-1387-2.
Arrais-Castro et al., 2018	António Arrais-Castro, Maria Leonilde R. Varela, Goran D. Putnik, Rita A. Ribeiro, José Machado, and Luís Ferreira, "Collaborative Framework for Virtual Organization Synthesis Based on a Dynamic Multi-criteria Decision Model," *International Journal of Computer Integrated Manufacturing* 31, no. 9 (2018): 857-868, https://doi.org/10.1080/0951192X.2018.1447146.
Bandinelli, d'Avolio, and Rinaldi, 2014	Romeo Bandinelli, Elisa d'Avolio, and Rinaldo Rinaldi, "Assessing the Maturity of Collaborative Networks: A Case Study Analysis in the Italian Fashion SMEs," 2014 International Conference on Engineering, Technology and Innovation: Engineering Responsible Innovation in Products and Services, ICE 2014, https://doi.org/10.1109/ICE.2014.6871588.
Barchetti et al., 2012	Ugo Barchetti, Antonio Capodieci, Anna Lisa Guido, and Luca Mainetti, "Collaborative Process Management for the Networked Enterprise: A Case Study," Proceedings of the 26th IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA 2012, 1343-1348, https://doi.org/10.1109/WAINA.2012.57.
Bilal, Daclin, and Chapurlat, 2014	Mustapha Bilal, Nicolas Daclin, and Vincent Chapurlat, "Collaborative Networked Organizations as System of Systems: A Model-Based Engineering Approach," in *Collaborative Systems for Smart Networked Environments*, edited by Luis M. Camarinha-Matos and Hamideh Afsarmanesh, PRO-VE 2014. IFIP Advances in Information and Communication Technology, vol. 434 (Berlin, Heidelberg: Springer, 2014), pp. 227-234.
Camarinha-Matos and Afsarmanesh, 2008	Luis M. Camarinha-Matos and Hamideh Afsarmanesh, "On reference models for collaborative networked organizations," *International Journal of Production Research* 46, no. 9 (2008): 2453–2469, https://doi.org/10.1080/00207540701737666.

Short reference	Full bibliographic information
Camarinha-Matos et al., 2009	Luis M. Camarinha-Matos, Hamideh Afsarmanesh, Nathalie Galeano, and Arturo Molina, "Collaborative Networked Organizations – Concepts and Practice in Manufacturing Enterprises," *Computers & Industrial Engineering* 57, no. 1 (2009): 46-60, https://doi.org/10.1016/j.cie.2008.11.024.
Camarinha-Matos, Afsarmanesh, and Ollus, 2008	Luis M. Camarinha-Matos, Hamideh Afsarmanesh, and Martin Ollus, eds., *Methods and Tools for Collaborative Networked Organizations* (New York: Springer Science+Business Media, 2008).
Cardoni, Saetta, and Tiacci, 2010	Andrea Cardoni, Stefano Saetta, and Lorenzo Tiacci, "Evaluating How Potential Pool of Partners Can Join Together in Different Types of Long Term Collaborative Networked Organizations," in *Collaborative Networks for a Sustainable World*, edited by Luis M. Camarinha-Matos, Xavier Boucher, and Hamideh Afsarmanesh, PRO-VE 2010, IFIP Advances in Information and Communication Technology, vol. 336 (Berlin, Heidelberg: Springer, 2010), pp. 312-321.
Crawford et al., 2009	Karyn Crawford, Helen M. Hasan, Leoni Warne, and Henry Linger, "From Traditional Knowledge Management in Hierarchical Organizations to a Network Centric Paradigm for a Changing World," *Emergence: Complexity & Organization* 11, no. 1 (2009): 1-8.
da Silva and de Almeida, 2017	João M. Vilas-Boas da Silva and Isabel Duarte de Almeida, "Collaborative Networks as Incubators of Dynamic Virtual Organisations: A Case Study of the Emerging MAP Sector," *International Journal of Manufacturing Technology and Management* 31, nos. 1/2/3 (2017): 192-216.
Durugbo and Riedel, 2013	Christopher Durugbo and Johann C.K.H. Riedel, "Readiness Assessment of Collaborative Networked Organisations for Integrated Product and Service Delivery," *International Journal of Production Research* 51, no. 2 (2013): 598-613, https://doi.org/10.1080/00207543.2012.658529.
Durugbo, 2016	Christopher Durugbo, "Collaborative Networks: A Systematic Review and Multi-level Framework," *International Journal of Production Research* 54, no. 12 (2016): 3749-3776, https://doi.org/10.1080/00207543.2015.1122249.
Enquist, Nilsson, and Magnusson, 2004	Håkan Enquist, Andreas Nilsson, and Johan Magnusson, "Change Management Implications for Network Organizations," Proceedings of the 37th Annual Hawaii International Conference on System Sciences, Big Island, HI, USA, 5-8 January 2004, https://doi.org/10.1109/HICSS.2004.1265088.
Fulk, 2001	Janet Fulk, "Global Network Organizations: Emergence and Future Prospects," *Human Relations* 54, no. 1 (2001): 91–99, https://doi.org/10.1177/0018726701541012.
Grippa et al., 2018	Francesca Grippa, João Leitão, Julia Gluesing, Ken Riopelle, and Peter Gloor, eds., Collaborative Innovation Networks: Building Adaptive and Resilient Organizations (Cham, Switzerland: Springer, 2018). https://doi.org/10.1007/978-3-319-74295-3
Harrington and Srai, 2016	Tomás Seosamh Harrington and Jagjit Singh Srai, "Designing a 'Concept of Operations' Architecture for Next-Generation Multi-organisational Service Networks," *AI & Society* (2016), https://doi.org/10.1007/s00146-016-0664-5.
Hovorka and Larsen, 2005	Dirk S. Hovorka and Kai R. Larsen, "Increasing Absorptive Capacity through Strategic use of Network Organizations," 11th Americas Conference on Information Systems AMCIS 2005, Omaha, Nebraska, USA, August 11-14, 2005, 270. http://aisel.aisnet.org/amcis2005/270.

Short reference	Full bibliographic information
Hovorka and Larsen, 2006	Dirk S. Hovorka and Kai R. Larsen, “Enabling Agile Adoption Practices through Network Organizations,” *European Journal of Information Systems* 15, no. 2 (2006): 159–168.
Jabłoński and Jabłoński, 2020	Adam Jabłoński and Marek Jabłoński, eds., *Social Business Models in the Digital Economy* (Cham, Switzerland: Palgrave MacMillan, 2020), https://doi.org/10.1007/978-3-030-29732-9.
Jackson and Cardoni, 2017	Paul Jackson and Andrea Cardoni, “Organizational Design and Collaborative Networked Organizations in a Data-Rich World: A Cybernetics Perspective,” in *Collaboration in a Data-Rich World*, edited by Luis M. Camarinha-Matos, Hamideh Afsarmanesh, and Rosanna Fornasiero, PRO-VE 2017: IFIP Advances in Information and Communication Technology, vol. 506 (Cham: Springer, 2017), pp. 185-193, https://doi.org/10.1007/978-3-319-65151-4_18.
Jiménez et al., 2005	Guillermo Jiménez, Nathalie Galeano, Teresa Nájera, José Manuel Aguirre, Ciprian Rodríguez, and Arturo Molina “Methodology for Business Model Definition of Collaborative Networked Organizations,” in *Collaborative Networks and Their Breeding Environments*, edited by Luis M. Camarinha-Matos, Hamideh Afsarmanesh, and Angel Ortiz, PRO-VE 2005, IFIP Advances in Information and Communication Technology, vol. 186 (Boston, MA: Springer, 2005), pp. 347-354.
Jorgensen and Krogstie, 2000	Havard D. Jorgensen and John Krogstie, “Active Models for Dynamic Networked Organisations,” Telecom, Sintef (2000).
Jung, 2017	Kyujin Jung, “Sources of Organizational Resilience for Sustainable Communities: An Institutional Collective Action Perspective,” *Sustainability* 9, no. 7 (2017), 1141; https://doi.org/10.3390/su9071141.
Kandjani and Bernus, 2012	Hadi Kandjani and Peter Bernus, “Towards a Cybernetic Theory and Reference Model of Self-designing Complex Collaborative Networks,” in *Collaborative Networks in the Internet of Services*, edited by Luis M. Camarinha-Matos, Lai Xu, and Hamideh Afsarmanesh (Heidelberg: Springer, 2012), 485-493.
Komanda, 2012	Marcin Komanda, “Foundations of Network Organizations Ontology,” *International Journal of Business and Management Studies* 1, no. 1 (2012): 565–569.
Krčo et al., 2019	Srdjan Krčo, Rob van Kranenburg, Miloš Lončar, Xenia Ziouvelou, and Frank McGroarty, “Digitization of Value Chains and Ecosystems,” in *Digital Business Models: Driving Transformation and Innovation*, edited by Annabeth Aagaard (Cham, Switzerland: Palgrave MacMillan, 2019), 81-116, https://doi.org/10.1007/978-3-319-96902-2_4.
Lavertu, 2017	Jasper Lavertu, “A Journey toward a More Networked Organisation and Improved Management of Knowledge,” in Proceedings of the 18th European Conference on Knowledge Management, ECKM 2017, edited by Frederic Marimon, Marta Mas-Machuca, Jasmina Berbegal-Mirabent, and Ramon Bastida, Barcelona, 7-8 September 2017, pp.1263-1267.
Li, Biennier, and Amghar, 2012	Juan Li, Frédérique Biennier, and Youssef Amghar, “Governance as a Service for Collaborative Environment,” in *Collaborative Networks in the Internet of Services*, edited by Luis M. Camarinha-Matos, Lai Xu, and Hamideh Afsarmanesh (Heidelberg: Springer, 2012), 687-694.
Mabey and Zhao, 2017	Christopher Mabey and Shasha Zhao, Managing Five Paradoxes of Knowledge Exchange in Networked Organizations New Priorities for HRM,” *Human Resource*

Short reference	Full bibliographic information
	Management Journal 27, no. 1 (2017): 39–57, https://doi.org/10.1111/1748-8583.12106.
Mabey, Wong, and Hsieh, 2014	Chris Mabey, Amy L.Y. Wong, and Linda Hsieh, "Knowledge Exchange in Networked Organizations: Does Place Matter?" *R&D Management* 45, no. 5 (2014): 487-500, https://doi.org/10.1111/radm.12099.
Macedo and Camarinha-Matos, 2017	Patricia Macedo and Luis Camarinha-Matos, "Value Systems Alignment Analysis in Collaborative Networked Organizations Management," *Applied Sciences* 7, no. 12 (2017): 1231; https://doi.org/10.3390/app7121231.
Mortati, 2013	Marzia Mortati, *Systemic Aspects of Innovation and Design: The Perspective of Collaborative Networks* (Cham, Switzerland: Springer, 2013).
Msanjila and Afsarmanesh, 2007	Simon Samwel Msanjila and Hamideh Afsarmanesh, "Modelling Trust Relationships in Collaborative Networked Organisations," *International Journal of Technology Transfer and Commercialisation* 6, no. 1 (2007): 40-55, https://doi.org/10.1504/IJTTC.2007.014541.
Noran, 2004	Ovidiu Noran, "Towards a Meta-Methodology for Collaborative Networked Organisations," in *Virtual Enterprises and Collaborative Networks*, edited by Luis M. Camarinha-Matos, PRO-VE 2004. IFIP International Federation for Information Processing, vol. 149 (Boston, MA: Springer, 2004), pp. 71-78.
Obidallah, Raahemi, and Alaieri, 2014	Waeal J. Obidallah, Bijan Raahemi, and Fahad Saleh Alaieri, "Change Processes and Procedures in Service Oriented Virtual Organizations and Collaborative Network," Proceedings of the 6th International Conference on Management of Emergent Digital EcoSystems, MEDES 2014, September 15-17, 2014, Buraidah Al Qassim, Saudi Arabia, 50-55, https://doi.org/10.1145/2668260.2668263.
Pawlak and Jørgensen, 2015	Adam Pawlak and Håvard D. Jørgensen, "Holistic Design of Collaborative Networks of Design Engineering Organizations," in *Risks and Resilience of Collaborative Networks*, edited by Luis M. Camarinha-Matos, Frédérick Bénaben, and Willy Picard, PRO-VE 2015. IFIP Advances in Information and Communication Technology, vol. 463 (Cham: Springer, 2015), 612-621.
Peters, Withalm and Wölfel, 2008	Mike Peters, Josef Withalm and Walter Wölfel, "Capability Maturity Models for SMEs and Collaborative Networked Organisations in Tourism," in *Information and Communication Technologies in Tourism*, edited by Peter O'Connor, Wolfram Höpken, and Ulrike Gretzel (Vienna: Springer, 2008), 568-579, https://doi.org/10.1007/978-3-211-77280-5_50.
Pierce, Ricciardi and Zardini, 2017	Paul Pierce, Francesca Ricciardi and Alessandro Zardini, "Smart Cities as Organizational Fields: A Framework for Mapping Sustainability-Enabling Configurations," *Sustainability* 9, no. 9 (2017): 1506; https://doi.org/10.3390/su9091506.
Rabelo, Costa, and Romero, 2014	Ricardo J. Rabelo, Scheila N. Costa, and David Romero, "A Governance Reference Model for Virtual Enterprises," in *Collaborative Systems for Smart Networked Environments*, edited by Luis M. Camarinha-Matos and Hamideh Afsarmanesh, PRO-VE 2014. IFIP Advances in Information and Communication Technology, vol. 434 (Berlin, Heidelberg: Springer, 2014), pp. 60-70.
Ricciardi, Cardoni, and Tiacci, 2014	Antonio Ricciardi, Andrea Cardoni, and Lorenzo Tiacci, "Strategic Context, Organizational Features and Network Performances: A Survey on Collaborative Networked Organizations of Italian SMEs," in *Collaborative Systems for Smart Networked Environments*, edited by Luis M. Camarinha-Matos and Hamideh

Short reference	Full bibliographic information
	Afsarmanesh, PRO-VE 2014. IFIP Advances in Information and Communication Technology, vol 434 (Berlin, Heidelberg: Springer, 2014), pp. 534-545.
Rodríguez-Rodríguez, Alfaro-Saiz, and Verdecho, 2015	Raúl Rodríguez-Rodríguez, Juan-José Alfaro-Saiz, and María-José Verdecho, "A Performance-Based Scenario Methodology to Assess Collaborative Networks Business Model Dynamicity," in *Risks and Resilience of Collaborative Networks*, edited by Luis M. Camarinha-Matos, Frédérick Bénaben, and Willy Picard, PRO-VE 2015. IFIP Advances in Information and Communication Technology, vol. 463 (Cham: Springer, 2015), 511-517.
Romero and Molina, 2011	David Romero and Arturo Molina, "Collaborative Networked Organisations and Customer Communities: Value Co-Creation and Co-Innovation in the Networking Era," *Journal of Production Planning & Control* 22, no. 4 (2011): 447-472, https://doi.org/10.1080/09537287.2010.536619.
Rossignoli, Mola, and Zardini, 2007	Cecilia Rossignoli, Lapo Mola, and Alessandro Zardini, "Virtual Network Organizations and e-Procurement: A New Outsourcing Perspective," First Information Systems Workshop on Global Sourcing: Services, Knowledge and Innovation Val d'Isère, France 13-15 March 2007, JIT 182.
Rostek, 2015	Katarzyna Rostek, *Benchmarking Collaborative Networks: A Key to SME Competitiveness* (Cham, Switzerland: Springer, 2015). – 182 pp.
Saetta, Tiacci, and Cagnazzo, 2013	Stefano Saetta, Lorenzo Tiacci, and Luca Cagnazzo, "The Innovative Model of the Virtual Development Office for Collaborative Networked Enterprises: The GPT Network Case Study," *International Journal of Computer Integrated Manufacturing* 26, no. 1-2 (2013): 41-54, https://doi.org/10.1080/0951192X.2012.681909.
Santoro, Borges, and Rezende, 2006	Flávia Maria Santoro, Marcos R.S. Borges, and Erick A. Rezende, "Collaboration and Knowledge Sharing in Network Organizations," *Expert Systems with Applications* 31, no. 4 (2006): 715–727, https://doi.org/10.1016/j.eswa.2006.01.002.
Sargolzaei and Afsarmanesh, 2017	Mahdi Sargolzaei and Hamideh Afsarmanesh, "Service Oriented Collaborative Network Architecture," in *Collaboration in a Data-Rich World*, PRO-VE 2017, edited by Luis M. Camarinha-Matos, Hamideh Afsarmanesh, and Rosanna Fornasiero, IFIP Advances in Information and Communication Technology vol. 506 (Cham: Springer, 2017), 381-394, https://doi.org/10.1007/978-3-319-65151-4_35.
Schaffers,2018	Hans Schaffers, "The Relevance of Blockchain for Collaborative Networked Organizations," in *Collaborative Networks of Cognitive Systems*, edited by Luis M. Camarinha-Matos, Hamideh Afsarmanesh, and Yacine Rezgui, PRO-VE 2018. IFIP Advances in Information and Communication Technology, vol 534. (Cham: Springer, 2018), 3-17.]
Serrier, Ducq, and Vallespir, 2017	Séverine Blanc Serrier, Yves Ducq, and Bruno Vallespir, "Networked Companies and a Typology of Collaborations," Enterprise Interoperability: INTEROP-PGSO Vision (2017), 19-42, https://doi.org/10.1002/9781119407928.ch2.
Song et al., 2019	Yang Song, Francesca Grippa, Peter A. Gloor, and João Leitão, eds., *Collaborative Innovation Networks: Latest Insights from Social Innovation, Education, and Emerging Technologies Research* (Cham, Switzerland: Springer, 2019).
Su, Biennier, and Ouedraogo, 2012	Ziyi Su, Frédérique Biennier, and Wendpanga Francis Ouedraogo, "A Governance Framework for Mitigating Risks and Uncertainty in Collaborative Business

Short reference	Full bibliographic information
	Processes," in *Collaborative Networks in the Internet of Services*, edited by Luis M. Camarinha-Matos, Lai Xu, and Hamideh Afsarmanesh (Heidelberg: Springer, 2012), 667-674.
Tain, 2019	David Tain, "Capitalizing on Complexity in Modern Business Environments: A Network-Based Perspective for Projects and Organization," *PM World Journal* 3, no. 2 (2019), available at https://pmworldlibrary.net/wp-content/uploads/2019/02/pmwj79-Feb2019-Tain-capitalizing-on-complexity-in-modern-business-featured-paper.pdf.
Tapia, 2009	Roberto Santana Tapia, "Converging on Business-IT Alignment Best Practices: Lessons Learned from a Dutch Cross-Governmental Partnership," *2009 IEEE International Technology Management Conference (ICE)*, Leiden, Netherlands, 22-24 June 2009, https://doi.org/10.1109/ITMC.2009.7461398.
Treurniet and Van Buul, 2015	Willem Treurniet and Kim Van Buul, "Four Archetypal Networked Organisations," in Proceedings of the ISCRAM 2015 Conference, Kristiansand, Norway, May 24-27, 2015, http://idl.iscram.org/files/willemtreurniet/2015/1178_WillemTreurniet+KimvanBuul2015.pdf.
Truptil et al., 2015	Sébastien Truptil, Anne-Marie Barthe-Delanoë, Tiexin Wang, and Frédérick Bénaben, "Towards a Collaborative Networks Governance Framework," in *Risks and Resilience of Collaborative Networks*, edited by Luis M. Camarinha-Matos, Frédérick Bénaben, and Willy Picard, PRO-VE 2015. IFIP Advances in Information and Communication Technology, vol. 463 (Cham: Springer, 2015), 379-387.
Ulbrich et al., 2011	Sebastian Ulbrich, Heide Troitzsch, Fred van den Anker, Adrian Plüss, and Charles Huber, "How Teams in Networked Organisations Develop Collaborative Capability: Processes, Critical Incidents and Success Factors," *Production Planning & Control: The Management of Operations* 22, no. 5-6 (2011): 488-500, https://doi.org/10.1080/09537287.2010.536621.

Annex 4 – List of interviews and a questionnaire

Representatives of two types of organisations were approached – funding organisations and potential major customers, located in Estonia, Finland, Greece, Hungary, Italy, and Spain, including CEDEFOP – European Centre for the Development of Vocational Training and NATO's Cooperative Cyber Defence Centre of Excellence.

Funding organisations

- Cyber Coordinator of Hungary, Ministry of Interior
- National cybersecurity coordinator, Bulgaria
- Centro Nacional de Excelencia para las Fuerzas y Cuerpos de Seguridad del Estado, Ministerio del Interior, Spain

Potential major customer organisations

- Mektory Estonia (Modern Estonian Knowledge Transfer Organisation For You)
- CEDEFOP – European Centre for the Development of Vocational Training
- CyberIreland
- Balasys IT
- Distretto Tecnologico Aerospaziale (Brindisi)
- NATO Communications and Information Agency

Questionnaire for an interview with a representative of potential major customer

NAME	
SURNAME	
ORGANIZATION	
ROLE	

Major customer

1. According to you, what are the governance requirements a network organization needs to meet with respect to the following topics to be considered as **a supplier of services to you**?

1.1 Profit or non-profit arrangements
1.2 Certain geographical representation or exclusion
1.3 Ways of involving external stakeholders
1.4 Certain standards or methodologies used
1.5 Supply chain security concerns
1.6 'Fair' representation on the senior governance body
1.7 Decision making by consensus or qualified majority, with equal weight of the vote of each partner in the network

1.8 Regular and rigorous internal and/or external audits
1.9 Dispute/conflict management arrangements
1.10 Confidentiality
1.11 Intellectual Property management arrangements
1.12 Ethics code and its effective enforcement
1.13 Specific ethical issues, e.g. policy in regard to slavery, use of labour of minors
1.14 'Green' policies
1.15 Gender policies and representation
1.16 Other good governance issues, e.g. transparency, integrity policy, whistleblowers protection (or anti-corruption policy more generally)

2. Do you have more governance issues you consider important not yet taken into account?

Annex 5 – List of analysed network organisations

Four types of exiting network organisations were analysed:

- Networks dedicated to information/cybersecurity research and services
- Cybersecurity incubators/ accelerators/ tech parks/ ecosystems
- Other research-intensive networks
- Networked organisations providing (among others) information services

The respective lists are presented below.

Networks dedicated to information/cybersecurity research and services

1. European Cyber Security Organization (ECSO)
2. STO Information Systems Technology panel (IST)
3. Singapore Cybersecurity Consortium (SGSC)
4. Distributed Network of Battle Labs (DNBL)
5. Cooperative Cyber Defence Centre of Excellence (CCDCoE)
6. Cyberwatching
7. NSW Network for Cyber Security and Engagement
8. Cloud Security Alliance (CSA)
9. International Information System Security Certification Consortium (ISC2)
10. Women in CyberSecurity (WyCyS)
11. SANS Institute
12. Information Systems Security Association (ISSA)
13. Forum of Incident Response and Security Teams (FIRST
14. Center for Internet Security
15. Anti-Phishing Working Group
16. Cyber Defense Labs
17. Cyber, Space, & Intelligence Association
18. Information Security and Forensics Society (ISFS)
19. Executive Women's Forum (EWF)
20. International Association of Security Awareness Professionals (IASAP)
21. Australian Information Security Association (AISA)
22. Association of Information Security Professionals (AISP)
23. Information Security Research Association (ISRA)
24. The Credit Union Information Security Professionals Association (CIUSPA)
25. The Association for Executives in Healthcare Information Security (AEHIS)
26. Federal Information Systems Security Educators' Association (FISSEA)
27. National Cyber Security Alliance (NCSA)
28. ISACA (previously Information Systems Audit and Control Association)
29. Internet Security Alliance (ISAlliance)
30. National Association of ISACs (NA-ISACs)

31. International Association for Cryptologic Research (IACR)
32. CSIRTs network (the network of European CERTs)
33. ETSI Technical Committee Cyber
34. Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC)
35. Cyber Ireland
36. UN GGE - United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications
37. European Network for Cyber Security (ENCS)
38. Australian Cyber Security Growth Network (AUSTCyber)
39. Japan Network Security Association (JNSA)
40. Association for Information Security (ISECA)
41. Asian Professional Security Association (APSA)
42. Korea Information Security Industry Association (KISIA)
43. International Cyber Security Protection Alliance (ICSPA)

Cybersecurity incubators/ accelerators/ tech parks/ ecosystems

44. Blavatnik Interdisciplinary Cyber Research Center (ICRC)
45. Ben-Gurion Advanced Technologies Park (ATP)
46. CyRise Cyber Security Accelerator
47. European Institute of Innovation and Technology (EIT)
48. EIT Digital
49. CyLon Limited
50. Innovation Cybersecurity Ecosystem at Block71 (ICE71), Singapore
51. Cyber NYC
52. CyberNorth
53. Mektory, Estonia
54. Startup Estonia

Other research-intensive networks

55. GÉANT ‘community’ of National Research and Educational Networks (NRENs)
56. Crisis Management Innovation Network Europe (CMINE)
57. Community of Users in Secure, Safe and Resilient Societies (CoU)
58. Partnership for Peace Consortium (PfP-C)
59. European Security and Defence College (ESDC)
60. European Natural Hazard Scientific Partnership
61. Network of European Hubs for Civil Protection and Crisis Management (CivPro-Hubs)
62. Programme for peer reviews in the framework of EU cooperation on civil protection and disaster risk management (CivPro-peers)
63. Bulgarian Academy of Sciences (BAS)
64. Identity Management Institute (IMI)
65. Shmoo Group
66. African Information Security Association (AISA)

67. Security Analysis & Risk Management Association (SARMA)
68. The Institute of Internal Auditors (IIA)
69. International Association of Privacy Professionals (IAPP)
70. AFCEA (Armed Forces Communications and Electronics Association)
71. Publishers International Linking Association (PILA)
72. Object Management Group (OMG)
73. European Digital SME Alliance
74. AeroSpace and Defence Industries Association of Europe (ASD)
75. Cyberpsychology network (CyPsy)
76. Serenity – Irish Security Research Network
77. EDA CapTechs
78. Atlassian Corporation
79. National Inter-University Consortium for Telecommunication (CNIT)
80. Consorzio INteruniversitario pEr il Calcolo Automatico (CINECA)
81. Associazione Italiana per la Sicurezza Informatica (CLUSIT)
82. The Apache Software Foundation
83. The Guild of European Research-Intensive Universities
84. League of European Research Universities (LERU)
85. Supercomputing Expertise for Small & Medium Enterprise Network (SESAME)
86. European Institute of Innovation and Technology – Health (EIT-Health)
87. Global Digital Health Partnership (GDHP)
88. International Forum to Advance First Responder Innovation (IFAFRI)

Information service providers

This is a list of analysed networked organisations that provide *inter alia* information services.

89. International Cybersecurity Dialogue
90. The Global Commission on the Stability of Cyberspace (GCSC)
91. Open Web Application Security Project (OWASP)
92. Information Security Forum (ISF)

Annex 6 – Publications

The following articles and papers based on the research presented here have already been published or are under publication.

1. Todor Tagarev and Yantsislav Yanakiev, "Business Models of Collaborative Networked Organisations: Implications for Cybersecurity Collaboration," *Proceedings 2020 11th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT 2020,* Kyiv, Ukraine, May 14-18, 2020, pp. 431-438, https://doi.org/10.1109/dessert50317.2020.9125011
2. Todor Tagarev and Bríd Á. Davis, "Towards the Design of a Cybersecurity Competence Network: Findings from the Analysis of Existing Network Organisations," in *Multimedia Communications, Services and Security*, MCSS 2020, edited by Andrzej Dziech, Wim Mees, Andrzej Czyżewski, Communications in Computer and Information Science, vol. 1284 (Cham, Switzerland: Springer, 2020), 37-50, https://doi.org/10.1007/978-3-030-59000-0_4.
3. Todor Tagarev, "Towards the Design of a Collaborative Cybersecurity Networked Organisation: Identification and Prioritisation of Governance Needs and Objectives," *Future Internet* 12, no 4 (2020), 62, https://doi.org/10.3390/fi12040062.
4. Todor Tagarev, "Governance of Collaborative Networked Organisations: Stakeholder Requirements," *Proceedings 2020 11th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT 2020*, Kyiv, Ukraine, May 14-18, 2020, pp. 439-445, https://doi.org/10.1109/dessert50317.2020.9125029.
5. Yantsislav Yanakiev and Todor Tagarev, "Governance Model of a Cybersecurity Network: Best Practices in the Academic Literature," *21st International Conference on Computer Systems and Technologies (CompSysTech'20)*, Russe, Bulgaria, 19-20 June 2020, edited by Tzvetomir Vassilev and Roumen Trifonov (New York, NY: Association for Computing Machinery, 2020), pp. 27-34. https://doi.org/10.1145/3407982.3407992.
6. Todor Tagarev, Brid A. Davis, and Michael Cooke, "Business, Organisational and Governance Modalities of Collaborative Cybersecurity Networks," *Multimedia Tools and Applications* 80 (2021), https://doi.org/10.1007/s11042-021-11109-2.
7. Todor Tagarev, Irena Mladenova, Antoniya Shalamanova, Ewa Konieczna, Lina Smovziuk, Georgi Penchev, and Yantsislav Yanakiev, "A Study on the Readiness of Partners in an EU-funded Cybersecurity Project for Structured Post-project Collaboration," presented at the *Third International Scientific Conference "Digital Transformation, Cyber Security and Resilience" (DIGILIENCE 2021)*, Veliko Tarnovo, Bulgaria, 29 September – 1 October 2021, to be submitted for publication in the post-conference volume in the Springer series "Communications in Computer and Information Science."