Collaboration could improve cyber resilience

A Community of Practice approach in the Rottedam port area

L.B.G.R Duin

Collaboration can improve cyber security

A Community of Practice approach in the Rotterdam port area

By

L.B.G.R. Duin

in partial fulfilment of the requirements for the degree of

Master of Science

in Science Communication

at the Delft University of Technology,

to be defended publicly on May 25th, 2020

Supervisor:	Dr.ir. S. Flipse	TU Delft, TNW - SEC
Thesis committee:	Prof.dr. M.J. de Vries	TU Delft, TNW - SEC
	Dr. É. Kalmar	TU Delft, TNW - SEC
	Dr.ir. Z. Roosenboom-Kwee	TU Delft, TPM - VTI

An electronic version of this thesis is available at http://repository.tudelft.nl/.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

Abbreviation	Full name
CERT	Computer Emergency Response Team
CoP	Community of Practice
CSIRT	Computer Security Incident Response Team
DCMR	DCMR Milieudienst Rijnmond, roughly translated as DCMR environmental service Rijnmond
ENISA	European Union Agency for Cyber security, formally known as European Network and Information Security Agency
FERM	This is not an abbreviation.
ICS	Industrial Control Systems
ISAC	Information Sharing and Analysis Centre
KM	Knowledge Management
NCSC	National Cyber security Centre of the Netherlands
NCTV	Nationaal Coordinator Terrorismebestrijding en Veiligheid, roughly translated as National Coordinator for Safety and Counterterrorism
OM	Openbaar Ministerie, translated as Public Persecutor Service
OT	Operational Technology
PCC	Port Cyber Café
PoR	Port of Rotterdam, the company
PPP	Public Private Partnership
SC	Science Communication
VAR	Veiligheidsalliantie Rotterdam translated as: Safety Alliance Rotterdam
WARP	Warning, Advice and Reporting Points
WEF	World Economic Forum

SUMMARY

Our world is becoming increasingly more digital, but its security has not catched up yet. Therefore, cyber security is becoming ever more important and needs to be improved. This improvement can be made by increasing collaboration and knowledge exchange. A Community of Practice (CoP) is a concept often deemed an appropriate tool to manage knowledge within organizations and between knowledge partners. A better understanding on how to create and implement CoPs for cyber security-related topics could further improve cyber security.

This research aims to achieve two objectives. The first objective is to gain insights in the establishment of Communities of Practice on cyber security in order to contribute the current scientific literature. The second is to use these insights to provide a possible solution to create a Community of Practice on cyber security for the FERM case in the Rotterdam port area. These two objectives were translated to the main research question:

How could a Community of Practice on cyber security be established?

An abductive research approach commenced to answer this question. An analysis phase started in order to understand the context of the FERM case and the CoP concept as well as to gain theoretical and empirical insights on elements that affect a CoP. The context was determined with an initial literature review and an analysis of the FERM case. The theoretical insights were synthesized from scientific literature by a systematic review and meta-ethnography. This resulted in the translation of five goals, fourteen drivers, and eight barriers affecting the establishment of a CoP. These elements were triangulated with the results of the interviews with participants in the Rotterdam port area. However, the interviews also provided empirical insights in new elements and in the prioritization of elements.

By combining all insights, it is concluded that the most important factor is the social dynamics: "*the interaction between the members that binds and holds them together*". Another conclusion is a set of nineteen conditions based on the elements: Culture, Social, Trust, Management, Facilitator & Leadership, Awareness & Urgency, and Direct Relevance.

After that, a design phase began, based on previous conclusions in order to determine a solution on how to establish a Community of Practice. A narrative review provided sub solutions from practice orientated sources, while a brainstorm provided sub solutions from a free-thinking perspective. A morphological chart provided a schematic overview of all sub solutions.

The feedback of the expert and the insights of the researcher made it possible to connect elements and sub solutions. This resulted in a concept solution that answers the main research question. The answer is a strategy consisting of one informal and internal phase: ***Phase 0) Initiation*** and three formal phases **1) *Exploration***, **2) *Dedication***, and **3) *Continuation***. Actions and meeting structures were designed for every phase in order to give the strategy practical and actionable steps to establish a Community of Practice on cyber security.

1. INTRODUCTION

The digitalization of our world is increasing day by day, making the world more interconnected then ever (Dobs, Manyika, & Woetzel, 2016; EY, 2011). However, the protection of this digital world is not guaranteed. Malware has been taken to unprecedented levels of sophistication and impact making it more dangerous for consumers and businesses. Malicious actors are also adopting new strategies to avoid detection and to exploit undefended gaps in the digital security of systems (Cisco, 2018). While the current damage is still mostly confined to the IT space, the further digitization of Operational Technology (OT) and Industrial Control Systems (ICS) could also result in physical damage (Dobs et al., 2016; Schwab & Poujol, 2018). It is therefore essential that cyber security will be an integral part of this digital change (Dobs et al., 2016; Verhagen, 2016; WEF, 2012)[1].

Cyber security is even more important for processes where a disturbance or an outage would lead to severe societal disruption and they are a threat to national safety. In the Netherlands, these processes are deemed to be part of the vital infrastructure (NCTV, 2017). The Rotterdam port area can be classified as such, since it contributes to ship management, the production, processing and storage of (petro-) chemicals, and oil and gas supply. These are examples of the sort of processes and processes existing in the Rotterdam port area. However, this infrastructure is not safe from the cyber threats as was shown in June 2017 with the terminal hack of APM (Bremmer & van Heel, 2017; Noort, 2017; RTV Rijnmond, 2017). Therefore, the Port of Rotterdam (PoR) and other organizations want to gain control on the new digital threats and become resilient to them. They are actively looking and implementing ways to improve their cyber security (Municipality of Rotterdam & 100 Resilient Cities, 2016; PoR, 2017b).

Two important objectives to improve cyber security are increased knowledge and skilled professionals (Dobs et al., 2016; Verhagen, 2016), as well as collaboration and knowledge exchange (ENISA, 2017b; Verhagen, 2016; WEF, 2012, 2016). The first objective is straightforward. The general ICT-competence of workers needs to improve in order to deal with digitalization and its threats, but specialized teams should also be present in case of more complex emergencies (Dobs et al., 2016; Verhagen, 2016). The second objective might be less clear at first sight, but plays a critical role.

The increased interconnectivity caused by the digitalization creates interdependencies that can be exploited, so individual organizations are no longer able to ensure cyber safety on their own. Collaboration is needed to deal with these interdependencies and the exchange of knowledge, and information is needed to improve the cyber security level of the entire set of connected organizations. Organizations are becoming more aware of their interdependencies, and the advantages of information sharing and knowledge exchange. They create all sorts of collaboration concepts solely focused on cyber security such as Public Private Partnerships (WEF, 2016) and CERT (ENISA, 2006b). However, insights from social disciplines have rarely been used to improve the efficiency and effectiveness of these collaboration.

Knowledge Management (KM) is a rising subject in the social science due to its increased relevance for academics and for practitioners in the 21st-century economy as well as its interdisciplinary nature (Fteimi & Lehner, 2018). The concept of a Community of Practice (CoP) is among the most prominent ideas to exchange knowledge, encourage learning and innovate products and processes and has been applied by several global cooperations and organizations (Chu, 2016; Gibson & Meacheam, 2009; Jeon, Kim, & Koh, 2011; Mabery, Gibbs-Scharf, & Bara, 2013; Scarso, Bolisani, & Salvador, 2009). This concept

[1] Appendix A will provide a more detailed overview of the digital trends and developments.

is often deemed an appropriate tool to manage knowledge within organization and between knowledge partners. Many organizations would profit if they knew how to create and implement CoPs for cyber security-related topics.

2. RESEARCH SETUP

This chapter aims to provide an overview of the central thesis of this research. The problem statement, the research objective, the research question with its sub questions, and the research relevance will be discussed. This chapter ends with a small outline of the report that follows.

2.1 PROBLEM STATEMENT

Collaboration and knowledge exchange are essential to improve the cyber security and the concept of a CoP is a promising tool to facilitate this. There is a lack of knowledge both in scientific literature as well as in practice on how this creation can or should be achieved or what contributes to, or limits this establishment.

2.2 RESEARCH OBJECTIVE

The objective of this research is twofold; a scientific objective and a practical objective. The scientific objective is to gain insights in the establishment of Communities of Practice on cyber security in order to contribute the current scientific literature. The practical objective is to use these insights to provide a possible solution to create a Community of Practice on cyber security for a concrete case.

2.3 RESEARCH QUESTIONS

Based on the research objective, a main research question was formulated which is supported by three sub questions. The sub questions provide a structure of intermediate steps for this research to consider and examine. They will be answered using scientific literature and the case study.

The main research question is: ***How could a Community of Practice on cyber security be established?*** This question is supported by the following three sub questions:

1) *Which factors affect the establishment of Community of Practice according to literature?*
2) *Which factors are critical for the establishment of a Community of Practice on cyber security in the case study of the Rotterdam port area according to the key stakeholders?*
3) *How do current cyber security collaboration formats solve the critical factors for the establishment of a Community of Practice on cyber security?*
4) *How could the critical factors for the establishment of a Community of Practice on cyber security be resolved?*

2.4 RESEARCH RELEVANCE

Scientific relevance

The interest in KM is rising and has diversified the past year. It is expected that both these developments will continue and will increase (Fteimi & Lehner, 2018). The concept of CoP has evolved over time and is now part of this field. The current research into CoP in the KM-field is diverse, but rarely focuses on the establishment of CoPs. Furthermore, the current research also does not present an overview of important aspects for CoPs and their establishment.

The scientific relevance of this research originates from its focus on the establishment of CoP as well as the factors that influence CoPs. This focus will provide more insight in both the theoretical as well as the empirical understanding of CoPs. It will add to the research on the theoretical models of CoPs and the factors that influence CoPs. It will also add to the limited research on the design and establishment of CoPs.

Social relevance

The rise of digitalization and with it that of cyber security will continue the coming years and will have great influence on the future outlook of society (Dobs et al., 2016; EY, 2011; Verhagen, 2016). Two important objectives to improve cyber security are increased knowledge and skilled professionals (Dobs et al., 2016; Verhagen, 2016) as well as collaboration and knowledge exchange (ENISA, 2017b; Verhagen, 2016; WEF, 2012, 2016). These two objectives are still a challenge for our current society. This research addresses these two objectives using the CoP concept, thereby contributing to the current societal issue of cyber security.

This issue is quite clear in the FERM case study that is used for this research. FERM[2], a public, private partnership in Rotterdam, has set itself the explicit goal to create a CoP in order to improve the cyber security of the Rotterdam port area (Duin & Zeer, 2015; Verkiel, 2016), a piece of vital infrastructure of the Netherlands (NCTV, 2017). This research proposes a way to establish a CoP in the Rotterdam port area, thus contributing to a current societal challenge. This knowledge can also be applied in other case studies.

Practical relevance

The FERM case study provides for this research the opportunity to propose a practical application for their issue: the establishment of a CoP in the Rotterdam port area. The insights of this research as well as this practical application hold a greater practical relevance, since they can be used in contexts outside of the Rotterdam port area as well. Better understanding of CoP's establishment contributes to the further establishment of CoPs in other places or similar ecosystems.

2.5 Report outline

This report continues with the Methodology. This chapter provides a further explanation on how the research is set up, how the research objective will be reached, and how the research questions will be answered. This chapter also includes an explanation on the methods used. The Methodology section will be followed by chapter 4, containing the results from the first part of this research: the analysis phase. This chapter contains subsections presenting the details of the context, the theoretical insights gained from literature, and the empirical insights gained from interviews. This chapter ends with a comparison of theory and practice in which a critical node and a set of conditions will be defined. Chapter 5 contains the results of the second part of the research: the design phase. It contains subsections that will elaborate on the possible sub solutions, and the final concept of the strategy. This report will end with chapter 6 containing the conclusions and the discussion. The main conclusions will be drawn and reflected on. This chapter will also elaborate on the implications and limitations of this research as well as possibilities for new research.

[2] More about FERM in Chapter 3.2.3.

3. METHODOLOGY

This chapter will clarify all aspects of the methodology and the underlying rationale. A methodology of a research project traditionally consists of several aspects; the research strategy, the research design, and the research methods. The research strategy is the most abstractive overview and concerns itself with the orientation of the research. An important aspect of the research strategy is the approach of the research: deductive, inductive or abductive (Bryman, 2012, p. 35). The research design entails the framework, used for the data collection and data analysis (Bryman, 2012, p. 46). It highlights the stages and different steps that are taken during the research. The research methods focus on the techniques used for the collection and analysis of the data (Bryman, 2012, p. 46), thus operationalizing the research design. These three aspects will be explained in the following sections.

3.1 RESEARCH STRATEGY

The research strategy of this research follows an abductive approach. This approach differs from the more classical approach of deduction and induction as explained by Timmermans & Tavory (2012). Deduction start with a theory or a rule, sets a hypothesis and proceeds to test this using a case demonstrating whether it is true or false (Bryman, 2012, p. 24). On the other hand, induction starts a collection of observations and proceeds by examining their implied results in order to construct a theory or rule (Bryman, 2012, p. 24). Deduction and induction can be seen as each other's counterpart; they move in opposite direction on the line between theory and observation. However, abduction follows neither of these paths. This form of reasoning is such that "we perceive the phenomenon as related to other observations either in the sense that there is a cause and effect hidden from view, or in the sense that the phenomenon is seen as similar to other phenomena already experienced and explained in other situations, or in the sense of creating new general descriptions." (Timmermans & Tavory, 2012, p. 171). This gives rise to the following definition of abduction: "*a creative inferential process aimed at proposing new theory based on empirical research evidence"* (Timmermans & Tavory, 2012).

The abductive approach shows its advantages when observations are done while applying concepts from existing fields of our knowledge as well. (Friedrichs & Kratochwil, 2009, pp. 713–714). Therefore the abductive approach works well in combination with a case study research design (Dubois & Gadde, 2002), since the theory can be fitted to the observations and vice versa.

3.2 RESEARCH DESIGN

The research design is a case study. The case study focuses on the FERM initiative in the Rotterdam port area that wished to establish a CoP on cyber security. The case description is provided in section 3.2.3. The case of this research can be described as a representative or typical case in the typology of Yin (2009, p. 48): "the objective is to capture the circumstances and conditions of an everyday or commonplace situation". This holds true for the FERM case to much extent, because collaboration and knowledge sharing regarding cyber security among parties remains an issue both on a Dutch-national level (Kamp, 2017) as well as on an international level (WEF, 2012, 2016). The FERM case also has local and unique characteristics, such as the interconnectedness of the Rotterdam port area, the sheer (economic) size, and the local mentality and mindset. These unique characteristics are not present in many other cases; however, the researcher still believes that insights in the social processes of this case will provide interesting insights for other parties as well as for the scientific community.

The case study design is also well suited for the abductive approach, because theory and empirical findings are intertwined and constantly evolving, and in-depth insights can be gained in through the case study (Dubois & Gadde, 2002). Furthermore, the case study design aligns well with the research objective to provide a possible solution to the challenge of FERM.

3.2.1 Flowchart of the research design

The steps of the research design are shown in the flowchart of Figure 3-1. Each step contains methods that will be explained in section 3.3. It starts with a combination of practice and theory with the respective case analysis and initial literature review. The insights and information from these two steps are needed to continue with the definition of the research objective, the research questions and the methodology. This step is crucial to ensure the quality of this scientific research. The next steps are done in parallel in order to triangulate results. On the theoretical side, a systematic review is done and examined using meta-ethnography in order to gain a theoretical insight. On the practical side, semi-structured interviews with key stakeholders in the Rotterdam port area are performed and processed to gain practical insights. The insights from these two perspectives were triangulated and made it possible to define a critical node and conditions. At this moment, the design stage of the research can start. Current collaboration concepts and solutions in cyber security are sought in practical literature using a narrative review. Brainstorming is used to think of practical solutions. The results of the narrative review and the brainstorm are combined in a morphological chart. The morphological chart provides an overview of all possible sub solutions. These sub solutions are discussed with an expert. The expert feedback prioritizes several sub solutions. The prioritization of sub solution provides the basis for the concept solution that is created now. This concept solution answers the main research question. Conclusions and recommendations are determined based on the entire research process and the main findings.

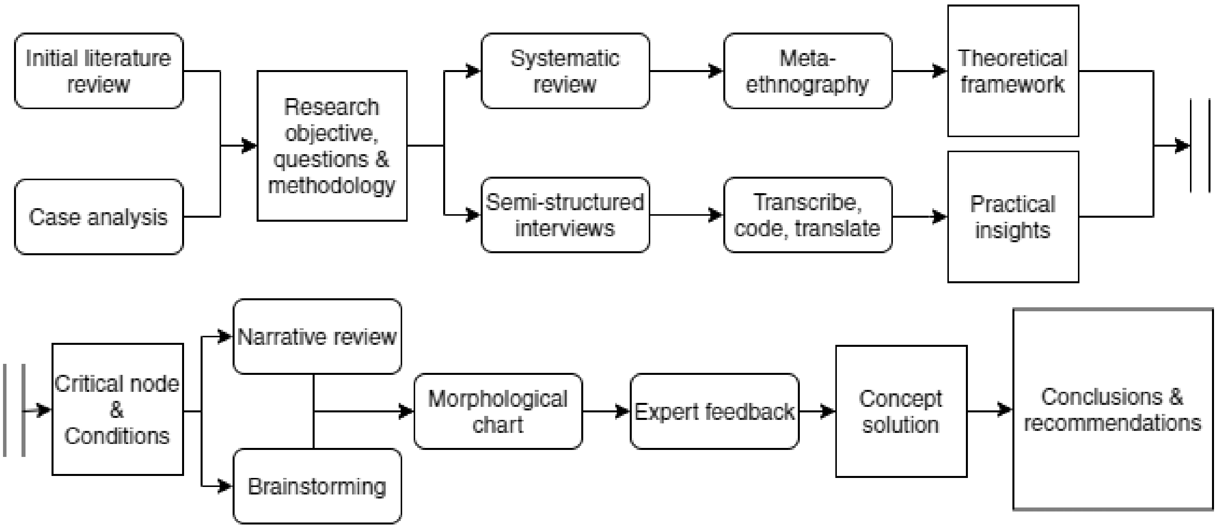
Initial literature review
Case analysis
Research objective, questions & methodology
Systematic review
Meta-ethnography
Theoretical framework
Semi-structured interviews
Transcribe, code, translate
Practical insights
Critical node & Conditions
Narrative review
Brainstorming
Morphological chart
Expert feedback
Concept solution
Conclusions & recommendations

Figure 3-1: Research design in a flowchart

3.2.2 Double diamond model

The abductive research approach shares many similarities with design-based research. This is due to the linking of theoretical and empirical insights. Models used in the design-based research can help to structure the research design.

A model commonly used in the design-based research is the Double Diamond (Design Council, 2019) This model provides structure and overview for complex social, economic and environmental problems. It is a clear, comprehensive and visual description of the design process, shown in Figure 3-2. This process consists of two diamonds with both divergent in order to explore an issue and convergent thinking to take focused action. There is a total of four phases in this process: Discover, Define, Develop and Deliver. These phases are defined as (Design Council, 2019):

- **Discover**. The first diamond helps people understand, rather than simply assume, what the problem is. It involves speaking to and spending time with people who are affected by the issues.
- **Define**. The insight gathered from the discovery phase can help you to define the challenge in a different way.
- **Develop**. The second diamond encourages people to give different answers to the clearly defined problem, seeking inspiration from elsewhere.
- **Deliver**. Delivery involves testing out different solutions at small-scale, rejecting those that will not work and improving the ones that will.

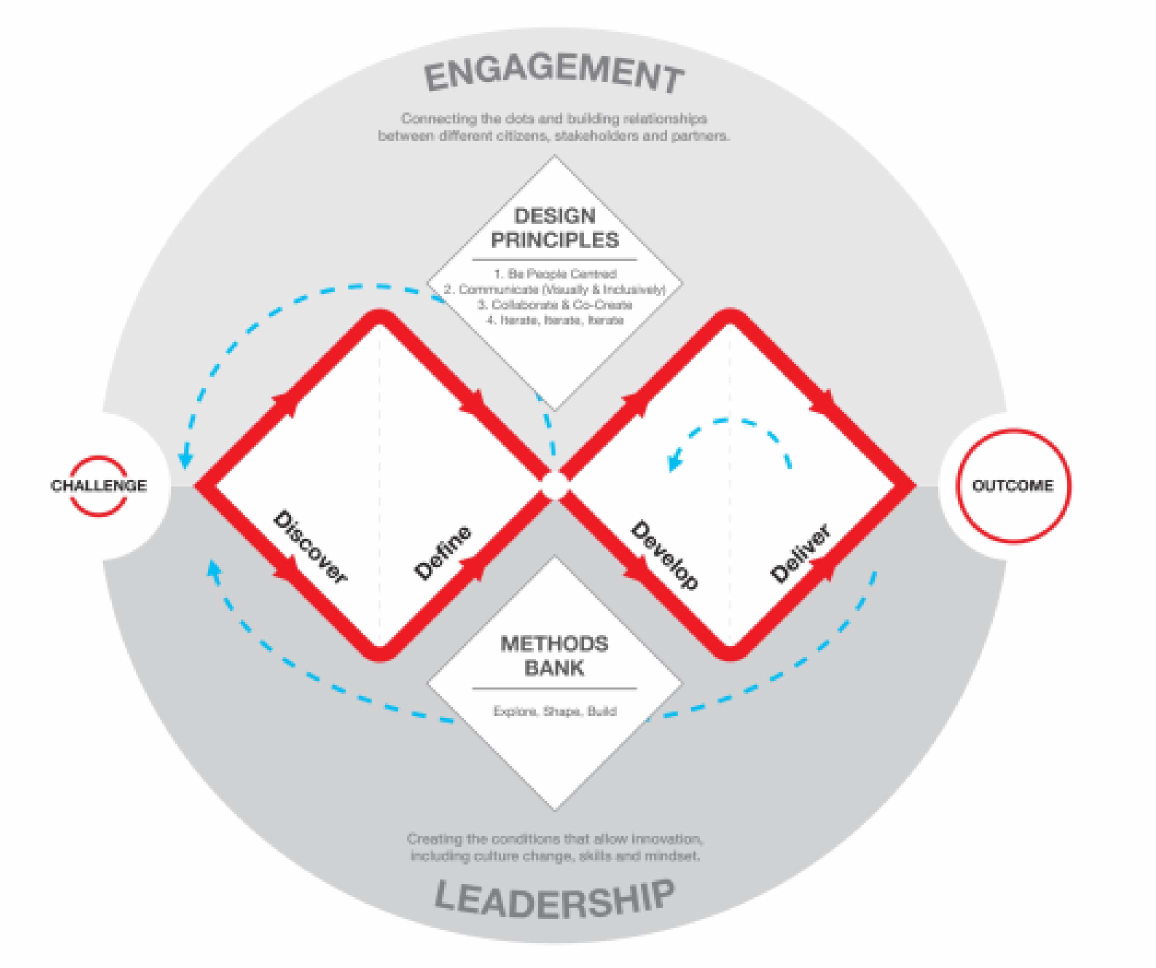
ENGAGEMENT
Connecting the dots and building relationships between different citizens, stakeholders and partners.
DESIGN PRINCIPLES
1. Be People Centred
2. Communicate (Visually & Inclusively)
3. Collaborate & Co-Create
4. Iterate, Iterate, Iterate
CHALLENGE
Discover
Define
Develop
Deliver
OUTCOME
METHODS BANK
Explore, Shape, Build
Creating the conditions that allow innovation, including culture change, skills and mindset.
LEADERSHIP

Figure 3-2: Double Diamond model created by the Design Council

By applying the Double Diamond on the research design shown in Figure 3-1 (Design Council, 2019), some clarity arises. The model starts with a complex and ill-defined challenge. The challenge of this research is combining the main research question: *How could a Community of Practice on cyber security be established?* with the FERM case. The Discover phase is entered for the first time by starting with a case analysis and an initial literature review. These insights make it possible to enter an intuitive Define phase where the research objectives, questions and methodologies can be defined. After that an iteration starts, as indicated by the first blue arrow in Figure 3-2, in order to Discover more about challenge and the case. A systematic review is used to explore scientific literature. Semi-structured interviews are also part of this phase since they gather empirical information. The Define phase starts with the meta-ethnography to determine theoretical insights and with the transcription, coding and translation of the interviews into practical insights. The phase ends by combining these two sets of insights with the case analysis in order to determine a critical node and conditions.

The critical node and conditions are the starting point of the next diamond and the Develop phase. A narrative review and brainstorm are used to determine sub solutions for the critical node and the conditions. The Develop phase ends with the morphological chart providing an overview of all possible sub solutions. The Deliver phase starts with the expert feedback in order to prioritize the sub solutions found. This will provide the basis for the concept solution that can be designed now. The concept solution is the outcome of the double diamond and should provide a solution for the challenge. Conclusions can be drawn from these results as well as a discussion on the implications of these findings. A reflection commences at this point as in indicated by the second blue arrow. This reflection considers the entire research and design process, resulting in considerations on the implications and limitations of this research as well as recommendations for future research.

3.2.3 Case description

Port of Rotterdam

The Port of Rotterdam (PoR) is the administrator, exploiter and developer of the Rotterdam port area. Its mission is to create economical and societal value through the realization of sustainable growth in this world-renowned port in collaboration with its clients and stakeholders. This is achieved by focusing on two goals. The first is the development, construction, management and exploitation of the Rotterdam port and industrial area. This goal is pursued by the commercial departments of PoR. The second goal is the improvement of effective, safe, and efficient maritime logistics. This aim is linked to the public obligations PoR has and is carried out by the Division Harbour master (PoR, 2017b, p. 20). One can see a clear division between the private and public aims and this is a result of the history of PoR. It started as a municipality service, but has grown into a state-owned private company.

The Rotterdam port area is considered to be a part of the vital infrastructure (NCTV, 2017). The vital infrastructure supports processes where a disturbance or outage would lead to severe social disruption and are a threat to national safety. These processes can be categorized as rank A and B, where the potential consequences for rank A vital infrastructure are potentially more severe than rank B. Rank A processes in the Rotterdam port area are the production and distribution of gas and the supply of oil. Rank B processes in the Rotterdam port area are regional gas distribution, ship management and large production, processing and storage of (petro)chemicals (NCTV, 2017). These elements influence the PoR, since its mission dictated that the port wants to create economical and societal value for its clients and stakeholders, but the administrator is directly part of these processes.

A trend that has consequences for the vital infrastructure is the accelerating digitalization of the services and process and the cyber security of these services and products (NCTV, 2018; Verhagen, 2016). The same is true for the Rotterdam port area as Cyber security is, or is becoming, a condition for the proper functioning of the nautical and logistic processes and the further development of the Rotterdam port area (PoR, 2017b, p. 91). PoR is well aware of this trend (PoR, 2016, 2017b, 2017a) and intends to increase the cyber resilience in the Rotterdam port area, increase the cyber-awareness, and improve the readiness and risk management of companies in cyber security. The FERM program contributes to make this intent reality.

FERM

FERM is a public-private partnership (PPP) of the municipality of Rotterdam, Deltalinqs, PoR and the Police's Sea Division. This partnership is led by the Harbour master of PoR, René de Vries. It was established in 2016 and its goals are twofold. Firstly, it wants to create awareness at the companies in the port area of Rotterdam in the field of cyber resilience. Secondly, it wants to create a platform for collaboration and knowledge exchange in the field of cyber resilience for the companies in the port area of Rotterdam (FERM, 2019).

The Division Harbour master took the lead in creating a strategy for this collaboration in 2016 and has since then been the main driver of the program. A total of eight building blocks were established to reach before mentioned two aims. These building blocks provide the basic strategic pillars for FERM (Verkiel & Hoitink, 2016).

1) Cyber Co-op
2) Cyber Threat Intelligence Watch
3) Cyber Security Community of Practice
4) Cyber Security & Response Team
5) Cyber Notification Desk
6) the Port Resilience Officer
7) Communication
8) Education

Currently FERM has created more awareness within the Rotterdam port area, thus contributing to its first aim. However, organizations in the Rotterdam port area are not yet collaborating or exchanging knowledge in the field of cyber resilience as is the second aim. The building block CoP is part of the strategy to partially address this. FERM wants to explore how to create a CoP to stimulate collaboration and knowledge exchange, since TNO initially proposed this as a worthwhile concept (TNO, 2015).

3.3 Research methods

3.3.1 Case analysis

Aim of case analysis

The case analysis was aimed to gain more insight in the image, setting, current affairs and history of FERM. This provides a point of reference as well as practical starting point.

Methods used for the case analysis

Five actions were taken to reach this aim: Observations, unstructured interviews, a policy document analysis, an analysis of the FERM event Port Cyber Cafes, and a question added to questionnaire.

Observations

The researcher was able to do observations, since he did part of his research in the PoR headquarters. This provided more insights in the context and mindset of PoR and FERM and provided easy access to multiple people. He could also attend the meetings of the FERM workgroup as well as PCCs. The FERM workgroup meetings provided insight in the current affairs of FERM. The results of the observation were combined with the unstructured interviews to provide a clear context for the case.

Unstructured interviews

Initial unstructured interviews were performed. These interviews had two formal aims as well as several informal aims. The first formal aim was to establish an understanding of how FERM and the theme of cyber security were regarded by people connected to port safety and policy, thus providing insight in the image and setting of FERM. The second formal aim was to get a grasp of the complex network of organizations and people involved with cyber security in the Rotterdam port area. The informal aims were focused on providing a (daily) network for the researcher. Convenience sampling was used for the unstructured interview to decide the participants. Convenience sampling is sampling participants simply on the availability to the researcher by virtue of accessibility (Bryman, 2012, p. 201). 14 participants shown in Table 3-1, since they were available to the researcher and could provide different insights. Notes were made after every interview by the researcher in order to structure thoughts as well as to be able to re-read them. The formal interviews provided further insights on the image of FERM and cyber security in the Rotterdam port area.

Table 3-1: Participants unstructured interviews

Name	Position	Organization	FERM
U1	Medior advisor	PoR – Division Harbour master	No
U2	Trainee	PoR – Data & Information security	No
U3	Senior advisor	PoR – Division Harbour master	No
U4	Intern	PoR - Data & Information security	Partially
U5	Medior advisor	PoR – Division Harbour master	Yes
U6	Peter Duin	Police - Se	Yes
U7	Manager	PoR – Division Harbour master	No
U8	Senior advisor	PoR – Division Harbour master	No
U9	Manager	PoR – Division Harbour master	No
U10	CISO	DCMR	Yes
U11	Manager	PoR – Division Harbour master	No
U12	Advisor	OM	Yes
U13	CISO	PoR - Data & Information security	Partially
U14	Senior advisor	Municipality	Yes

Policy document analysis

A policy document analysis was performed. This analysis aimed to establish the setting and the history of FERM. All documents were sampled with a convenience sample. A part of this analysis focused on internal documents. These documents were provided by the FERM workgroup and its members. Another part focused on external documents. These documents were advised by FERM group members and could be found on the internet. Table 3-2 provides and overview of all documents that were read.

Table 3-2: Policy documents

Type of document	Reference
Internal	(Duin & Zeer, 2015; Erp, 2017; PoR, 2015; TNO, 2015; Verkiel, 2016; Verkiel & Hoitink, 2016)
External	(CBS, 2018; CPB, 2018; Deltalinqs, 2016; Huistra & Krabbendam-Hersman, 2017; Municipality of Rotterdam & 100 Resilient Cities, 2016; Municipality of Rotterdam, 2014, 2015; NCTV, 2017, 2018; PoR, 2017b, 2017a, 2016; Verhagen, 2016; WEF, 2012, 2016, 2018)

Analysis of Port Cyber Cafés

An attendance comparison was done for the Port Cyber Cafés (PCCs) that were organized by FERM. This comparison provided insights in the vibrancy of FERM among its target audience and gave insight in the people and organizations that were directly reached by FERM's PCCs. The data contained which people had noted their attendance and which people actually attended. Excel was used to compare the attendance as well as the individuals.

Questionnaire

A questionnaire was issued by the PoR as part of an exploratory research into cyber security in the Rotterdam port area. This questionnaire was done in collaboration with the Haagse Hogeschool, SmartPort and the Veiligheidsalliantie Rotterdam (VAR, translated as: Safety Alliance Rotterdam). The questionnaire had four aims. The first aim was to gain an overview of the current cyber security landscape in the Rotterdam port area. The second was to find insights in the needs of organizations regarding education and training. The third aim was to strengthen the network by gaining an up-to-date list of contacts. The fourth was to generate results for the graduation thesis project of a student at SmartPort concerning the PDCA-cycle (Plan, Do, Check, and Act Cycle) (Haaften, 2018).

The total set of questions was provided by three parties. It started with a set of 28 questions provided by The Haagse Hogeschool that focused in-depth on the cyber security within organizations. Wouter van Haaften added 19 questions, focusing on the Information systems and information technologies within organizations as well as the cyber security management within organizations. A third set of 12 questions was added by FERM in order to gain insights in the needs of organizations regarding training and education in cyber security. Four questions were added to this questionnaire for this research. These questions aimed to gain some insights in the general acceptance of a CoP by the organizations in the port. All parties reviewed and revised the total set of questions in four meetings until a final set of 47 questions remained. The questionnaire can be found in appendix E.

The questionnaire was spread using several contact lists from PoR. These lists contained a multitude of private organizations in the Rotterdam port area. 93 organizations responded to the questionnaire using the digital questionnaire platform *Typeform* (https://www.typeform.com/).

A matrix with the individual entries could be downloaded from Typeform. This matrix was uploaded in Excel. The data were first cleaned and normalized in Excel, since the raw data contained mostly text-format, and answers to single questions were sometimes shattered over multiple columns. The normalized data could be analysed quite easily with diagrams and tables in Excel. The researcher focused on the questions concerning the company size and type, the importance of cyber security, and the interests of the organizations. This focus was chosen as the researcher wanted to gain a better understanding of the FERM context.

Network analysis

A network analysis was performed on the Rotterdam port area in order to establish an overview of the stakeholders and their interconnections. This presents insights in the network and its workings. First, the stakeholders were established. Second, the basic connections between all stakeholders were determined. Then, the focus shifted to the main interests and resources the actors possessed and how these aligned. These three steps were done using the observations, the unstructured interviews, and logical reasoning.

3.3.2 Initial literature review

Narrative review was done for the initial literature review. The narrative review aims to gain an initial understanding of the topic area and this makes the process more uncertain (Bryman, 2012, p. 110). They have less focus and contain a wider scope compared to more structured approaches. This method suits the initial phase of a research, since it explores the research fields and the status quo of the field.

Aim of the initial literature review

The initial literature review was aimed to gain a first grasp of the scientific literature regarding CoPs and collaborations. This literature review provided a theoretical background and theoretical overview. The theoretical overview was created in order to organize and connect the literature as well as to avoid confusion and loss of knowledge. A second aim of the overview was to locate the gaps in the initial literature search in order to search more specifically in the next stage of the research.

Method used for the initial literature review

The narrative review aims to gain an initial understanding of the topic area and has more of an explorative nature (Bryman, 2012, p. 110). The sampling of literature is therefore less structured, more alike to convenience and snowball sampling.

Convenience sampling is sampling participants simply on the availability to the researcher by virtue of accessibility (Bryman, 2012, p. 201). Snowball sampling is building further on information found in a reviewed source to gain a new source. This is an iterative process. A discussion with the supervisor of this thesis halted the sampling in order to re-examine and summarize all findings.

The initial search words used in this review were: Community of Practice, Collaboration, Alliance, Knowledge Sharing, and Knowledge Management. Google Scholar was used to find relevant literature. The literature was selected based on the impression gained from the summary and the amount of citations. The found literature also provided new articles. Theses from other Science Communication (SC) students were also used to find some literature.

Reviewed literature

A total of 35 articles as well as 3 MSc. theses of SC students were selected and reviewed. Table 3-3 shows the literature that was read for this review. It can be easily seen in this overview that the reviewed literature is not very recent which could suggest that not the latest knowledge or insights were obtained. However, this literature is highly cited and therefore generally accepted by the scientific community.

Table 3-3: Overview of literature reviewed in the initial literature search

Type of document	Reference
Book	Blackmore, 2010 (a collection of 11 articles and 1 added article)
Journal article	Alavi & Leidner, 1999; Bos et al., 2007; Costa e Silva, Bradley, & Sousa, 2012; Dooner et al., 2008; Duguid, 2005; Edwards, 2005; Jeon, Kim, & Koh, 2011; Kelly, Schaan, & Joncas, 2002; H. Lee & Choi, 2003; L. C. Li et al., 2009; Muller, 2006; Parkhe, 1998a, 1998b; Preece, 2004; Roberts, 2006; Sabel, 1993; Sonnenwald, 2003, 2007; Wenger & Snyder, 2000; Wenger, Trayner, & De Laat, 2011
Essay	Wenger, 2000, 2011
Magazine	Wenger, 1998
MSc. Thesis	Beijers, 2018; Kalmár, 2016; Vermeij, 2016

Examination of articles

The examination of the articles was done using NVivo in an iterative fashion as well. NVivo is software designed for qualitative and mixed methods research. Seemingly interesting findings were coded and saved in nodes. The creation of the nodes was completely done in an intuitive manner. The NVivo file with the node structure can be shared upon request.

More structure was added after a discussion between the researcher and a supervisor. All literature was re-examined in order to create a theoretical overview that summarized some of the main findings related to the research question.

The structure of the theoretical overview was based on the goal of the research: to gain insights in the creation of a CoP. Six aspects for the structure were chosen with the supervisor based on common sense: C*haracteristics, Goals, Needs, Drivers, Barriers*, and *Forms & Activities*. These aspects are defined as:

- A *Characteristic* is an attribute that holds true for most or all CoPs and is commonly used to describe a CoP.
- A *Goal* is the objective that is set for the CoP to achieve.
- A *Need* is the cause or limitation that causes people or organizations to start or be part of a CoP.
- A *Driver* is a factor that positively influences the creation, implication or continuation of a CoP.
- A *Barrier* is a factor that negatively influences the creation implementation or continuation of a CoP.
- A *Form* or *Activity* is different structure that a CoP can have and which activities they can pursue in general.

While creating the sub-nodes, the researcher was unable to synthesize individual sub-nodes for the aspect *Needs*. This aspect yielded few results and shows an overlap with other aspects, such as *Characteristics* and *Drivers*. Furthermore, needs are very specific for every case and are hard to determine after the process, because they have become a *Driver* or *Barrier*. Therefore, this aspect is omitted from the theoretical overview.

Synthesis of elements

The approach for the data synthesis holds similarity with phase 5 and 6 of meta-ethnography (Bryman, 2012, p. 107; Noblit & Hare, 1988). The original nodes were re-examined and re-organized according to the different themes giving rise to six nodes for the theoretical overview. Each node was examined again in order to detect grouping or similarities which were grouped again in sub-nodes. Some quotes could not be grouped or were only named once and therefore ignored. For every sub-node, an overarching title was thought off and then defined based on the quotes. The examination of the aspect nodes to sub-nodes was performed in Excel.

3.3.3 Systematic review and meta-ethnography

Systematic review and meta-ethnography are methods that are well suited to gain an overview of the existing literature and to synthesize commonalities. These two methods will be shortly introduced after which their application in this research will be explained. These methods are best used in succession of each other.

A systematic review is "*a replicable, scientific and transparent process (…) that aims to minimize bias through exhaustive literature searchers of published and unpublished studies and by providing an audit trail of the reviewers decisions, procedures and conclusions*." (Tranfield, Denyer, & Smart, 2003, p. 209). This method has three phases: a planning phase, a conducting phase, and a reporting phase (Kitchenham, 2004, p. 3; Tranfield et al., 2003, p. 214). The planning phase focuses on the identification of the need and purpose of the search as well as to create a sound review protocol. The conducting phase contains the actual search, selection of the literature, and data extraction and synthesis. The reporting phase organizes the results of the extraction and synthesis.

Meta-ethnography is a method used to achieve interpretative synthesis of qualitative research and other secondary sources (Bryman, 2012, p. 107; Cahill, Robinson, Pettigrew, Galvin, & Stanley, 2018, p. 130). This method involves induction and interpretation in order to synthesize the findings from several sources (Britten et al., 2002, p. 210). Noblit and Hare (1988) claimed ethnography involves seven steps: getting started, deciding what is relevant to the initial interest, reading the studies, determining how the studies are related, translating the studies into one another, synthesizing translations, and expressing the synthesis.

These two methods were combined in this research, since the steps of the methods overlap. However, each method has its benefits and disadvantages. A combination of the methods allows the benefits of each methods to support the disadvantage of the other method. The systematic review has a stronger planning phase, while the data extraction and synthesis steps are better in the meta-ethnography. The last phase of both methods is a reporting phase where the results are presented in an article or section.

Aim of the systematic review and the meta-ethnography

The systematic review and the meta-ethnography aim to answer the first sub question: *Which factors affect the establishment of Community of Practice according to literature?* This is the start of the planning phase of the systematic review. The focus is on articles that explain or elaborate on factors which contribute to or impede the creation of a CoP. To understand these factors, one must also be aware of the aims or structures that CoPs commonly have. The findings of the theoretical overview were used to determine the aspects. Four of the original six aspects in the theoretical overview are used for this review: *Goals, Drivers, Barriers,* and *Forms*. These four aspects have been defined as follows for transparency and clarity.

- A *Goal* is defined as the objective that is set for the CoP to achieve.
- A *Driver* is defined as a factor that positively influences the creation, implication or continuation of a CoP.

- A *Barrier* is defined as a factor that negatively influences the creation implementation or continuation of a CoP.
- A *Form* is defined as an (organizational) structure that CoP can adopt.

The two aspects that were not copied from the theoretical overview are *Characteristic* and *Need*. The aspect *Characteristic* was not used, since a characteristic provides insights into a concept, but cannot affect something. Therefore, this aspect did not align with the aim of this review. The aspect *Need* are not used here, since the results for this aspect in the theoretical overview were lacking.

During the meta-ethnography, it became clear that the *Form* aspect would not provide meaningful findings. No underlying structures or organizational configuration for CoPs could be found in the literature, making it clear that the CoP itself was the structure. Therefore, this aspect was removed from the final results.

Review protocol

Now that the aim is set, the review protocol secures the reliability and transparency. It contains a detailed procedure of how the articles were found and selected (Bryman, 2012, p. 103). As mentioned before, the final review protocol is a result of an iterative process. The iterative process for this systematic review started with the initial literature review whose findings and experiences contributed to mind maps and discussions with the supervisor that occurred later on.

Scope of the search

The first component of the protocol is to determine the scope, thus limiting the database, the time frame, and the type of documents. The Scopus database was chosen. The time frame was set from 1991 until 2018, since the term CoP was coined in by Wenger and Lave in 1991. There are documents from before 1991 that focus on knowledge management and collaboration; these documents are not considered in this review. The initial literature review showed that knowledge management is a thriving research field, so it can be expected that some the older articles are somewhat outdated or are cited in the more recent literature. This time scope was also chosen in order to make the review manageable for a master thesis. The selected document's types are journal articles, reviews and books. The last addition to the search was done on January 4th, 2019, so it should contain all articles from 2018 as well.

Search terms

A second part of the protocol is the search terms that have been used. The search terms can be divided in two types; topic and keyword. Topic-terms are terms that are present in either the title, the abstract or the keywords of an article. Keyword-terms are terms that are only present in the keywords of the respective article. AND- and OR-statements can be used limit or expand searches. The AND-statement limits the search, since both terms connected by AND need to be present in a document. The OR-statement expands the search, since either term connected by OR need to be present in a document.

The final set of search terms did not include a combination with 'cyber security' for two reasons. The first reason is that the set of literature became very limited with this search term included. It was expected that this would hinder the results of the meta-ethnography. The second reason is that factors that influence CoPs in other settings or fields could also be interesting for the field of cyber security. Therefore, these results based on CoPs in other settings and fields should be reviewed as well, and the search should not be limited to just cyber security.

Table 3-4 contains the final search teams used for this systematic review. The choice for the topic-terms are based on the findings from the initial literature review. The keyword-terms are based on the aspects decided in the search goal using several synonyms.

The final set of search terms did not include a combination with ‘cyber security’ for two reasons. The first reason is that the set of literature became very limited with this search term included. It was expected that this would hinder the results of the meta-ethnography. The second reason is that factors that influence CoPs in other settings or fields could also be interesting for the field of cyber security. Therefore, these results based on CoPs in other settings and fields should be reviewed as well, and the search should not be limited to just cyber security.

Table 3-4: Search terms of the systematic review

Topic	Keywords
communit* of practice	goal OR aim OR purpose OR target OR objective OR intent
	driver OR incentive OR enabler OR “success factor” OR facilitator
	barrier OR “failure factor” OR limit OR challenge
	taxonomy OR form OR type OR typology 11
collaboration OR cooperation OR alliance	“Knowledge management” AND (goal OR aim OR purpose OR target OR objective OR intent)
	“Knowledge management” AND (driver OR incentive OR enabler OR “success factor” OR facilitator)
	“Knowledge management” AND (barrier OR “failure factor” OR limit OR challenge)
	“Knowledge management” AND (taxonomy OR form OR type OR typology)

Selection conditions

The final part of the protocol provides insight in the quality assessment of the literature. Several conditions are set in order to ensure the quality as well as to reduce reading of unrelated articles. These conditions focus on the informational value, the relevance and the validity of the documents (Sanden & Meijman, 2004). The quality assessment was done in two steps. The first condition is a validity benchmark regarding the citations of a document. The rationale of this benchmark is based on peer review, since documents with citations can be considered to contain accepted insights in their field. This condition was based the impact factor of the different journals. The impact factor is a measure of the frequency with which an average article in a journal has been cited in a particular year. The condition for this review is: ***The document needs to be cited five times or more when published before 2016.*** This means that in this review all articles between 2016-2018 were selected and an article between 1991-2016 was selected if it had five citations or more.

The second condition of the quality assessment focused on the relevance and informational value. The abstracts of the remaining articles were examined in order to determine the focus point and the results. The condition for the relevance is described as: ***The focus point of the research needs to be the collaboration or knowledge management for a person, a group, an organization, or between such actors.*** This condition ensured that the articles were relevant with regards to sub question 1. The informational value condition is described as: ***Do the results of the research focus on either of the four aspects that were deemed of interest?*** This condition ensured that the results contain insights to solve the sub question 1.

Selected articles

The search was conducted according to this review protocol. 8 searches were conducted that summed up to 268 articles. This was decreased to 183 items by using the citation condition. This was further limited by reading the abstracts and this left a total of 70 articles. An overview of all these items is presented in Table 3-5. When eliminating the double entries, 60 unique articles are left for complete review using the meta-ethnography. Table 8-13 in Appendix I provides an overview of the articles and the aspects in alphabetic order of the authors.

Table 3-5: Overview of the final set of literature found with the systematic review

Topic	Keywords	Literature
communit* of practice	goal OR aim OR purpose OR target OR objective OR intent 7	Borzillo, 2017; Cheung, Lee, & Lee, 2013; Cornes et al., 2014; Dawson, Persson, Balfors, Mörtberg, & Jarsjö, 2018; Du Plessis, 2008; Fetterman, 2002; Lathlean & Le May, 2002
	driver OR incentive OR enabler OR "success factor" OR facilitator	Alali & Salim, 2016; Chu, 2016; Cochrane, 2011, 2014; Del Giudice, Della Peruta, & Maggioni, 2015; Du Plessis, 2008; Hall & Graham, 2004; Ho & Kuo, 2013; J. Hong, 2017; Y. M. Li & Jhang-Li, 2010; Mabery, Gibbs-Scharf, & Bara, 2013; Nielsen, 2012; Pharo, Davison, McGregor, Warr, & Brown, 2014; Scarso, Bolisani, & Salvador, 2009; Sheffield & Lemétayer, 2013
	barrier OR "failure factor" OR limit OR challenge	Bos et al., 2007; D. Hong, Suh, & Koo, 2011; Kaplan & Thomson Reed, 2007; Lyons, Acsente, & van Waesberghe, 2008; Rooke, Rooke, Koskela, & Tzortzopoulos, 2010
	taxonomy OR form OR type OR typology	Alali & Salim, 2016; Bos et al., 2007; Crowley, McAdam, Cunningham, & Hilliard, 2018; Dahlander & O'Mahony, 2011; Dube, Bourhis, & Jacob, 2006; Ekberg et al., 2010; Faraj, von Krogh, Monteiro, & Lakhani, 2016; Ferlie, Crilly, Jashapara, & Peckham, 2012; Gagnon, 2011; Gibson & Meacheam, 2009; Hara, Shachaf, & Stoerger, 2009; Robards et al., 2018
collaboration OR cooperation OR alliance	"Knowledge management" AND (goal OR aim OR purpose OR target OR objective OR intent)	Borzillo, 2017; Chen, Lin, & Yen, 2014; Cheung et al., 2013; Dawson et al., 2018; Du Plessis, 2008; Hosseini, Akhavan, & Abbasi, 2017; Lathlean & Le May, 2002; Liu, Cheng, Chao, & Tseng, 2012; X. Wang, Wong, & Wang, 2012; Witherspoon, Bergner, Cockrell, & Stone, 2013
	"Knowledge management" AND (driver OR incentive OR enabler OR "success factor" OR facilitator)	Du Plessis, 2008; Galán-Muros, van der Sijde, Groenewegen, & Baaken, 2017; Kruss & Visser, 2017; H. Lee & Choi, 2003; H. S. Lee, 2017; Y. M. Li & Jhang-Li, 2010; Salo, 2001; Tan & Noor, 2013; J. Wang, Wei, Ding, & Li, 2017
	"Knowledge management" AND (barrier OR "failure factor" OR limit OR challenge)	D. Hong et al., 2011; Jaegersberg & Ure, 2011; Pirkkalainen & Pawlowski, 2014; Ramos-Vielba, Sánchez-Barrioluengo, & Woolley, 2016

	"Knowledge management" AND (taxonomy OR form OR type OR typology)	Dube et al., 2006; Hara et al., 2009; Hsiao, Chen, Lin, & Kuo, 2017; Koh, Ryan, & Prybutok, 2005; Machuca & Costa, 2012; Margaryan, Milligan, & Littlejohn, 2011; Swain & Ekionea, 2008; J. Wang et al., 2017

Data extraction and synthesis

As the appropriate studies have now been determined using the review protocol, the data extraction and synthesis can start using phase 4-6 of meta-ethnography (Noblit & Hare, 1988). Since sub question 1 aims to find factors in literature, the synthesis focused on collecting the similar findings and connecting them in independent factors.

First, the selected studies were read in order to identify concepts (Britten et al., 2002, p. 211; Cahill et al., 2018, p. 133) related to the four aspect defined in the search goal: *Goals, Drivers, Barriers,* and *Forms*. The software NVivo was used to code the findings as they appear in the original text, as suggested by Cahill et al. (2018). The coding was initially done using four nodes related to the four aspects. The coding in four nodes helped with the next phase of translating the studies into each other.

The translation of the studies was done by examining the four nodes, and interpreting and connecting the different concepts presented there. The results of the initial literature search helped with this, since several factors for every aspect were defined there as well. However, the results of the initial literature search weren't copied, but they did act as a reference point. Connected concepts in every node were collected in sub-nodes using the original text.

An important result is the impossibility to synthesize elements for the aspect Form. The reviewed literature shows that no distinctions in CoP formats are made, even when descriptions differed greatly. This was noticed while reviewing the literature, so it was decided before the synthesis phase that it would be futile to create elements for the aspect Form.

The last step is to synthesize the translations by comparing the different translations that are connected. Every sub-node was evaluated and the common concept was interpreted from the original text. The research then followed by creating his own definitions resulting in the factors. The results are presented in section 4.2.2

3.3.4 Semi-structured Interviews

Aim of the interviews

The aim of the interviews is related to sub question 2: *Which factors are critical for the establishment of a Community of Practice on cyber security in the Rotterdam port area according to the key stakeholders?* The interviews aim to uncover the factors that the stakeholders in the case study find relevant for the establishment of a CoP. These factors can be triangulated with the factors found in the systematic review and meta-ethnography. Triangulation is the use of several methods or data sources in order to cross-check results (Bryman, 2012, p. 717). The approach of the interviews was chosen to be inductive in order to achieve triangulation. Induction means that information will be gathered after which a theory or concept will the formed (Bryman, 2012, p. 24). This means for the interview that the findings of the interviews will be translated to elements. As a consequence of this approach, the interviews with the stakeholders will not use the results of the systematic review and meta-ethnography. The inductive approach was chosen in order to avoid direct interrelation between the theoretical insights from the systematic review and the meta-ethnography and the practical insights from the interviews. By avoiding direct interrelations, triangulation is possible.

Sampling

The sampling of the interview participants used a combination of sampling techniques based on purposive sampling. Purposive sampling is sampling participants in a strategic manner to that the sample is relevant to the research question (Bryman, 2012, p. 418). This sampling approach was used here, since the Rotterdam port area contains over 600 organizations which are all different and yet certain groups show similarities. Furthermore, some of the contact information was more readily available than others. Therefore, convenience sampling was used as well.

Sample strategy

The main aim of the sampling was to have proper representation of the stakeholders in the Rotterdam port area. The sample was decided with a sampling strategy based on purposive sampling. First, data and insights gained from the case analysis were also used in the sampling. The case analysis provided insight in the different stakeholders and it seemed reasonable to interview at least one person from every stakeholder group. This is done in stratified purposive sampling approach were participants are selected from subgroups of interest part of the entire sample (Bryman, 2012, p. 419). However, the stakeholder Commercial Companies is quite diversified, so multiple different people were chosen from this group.

Second, convenience sampling was used, since the data from the case analysis gave easy access to some of the organizations as well as insight in the size and sector of the commercial organizations.

Thirdly, random sampling was used on all of the subgroups. The sampling size was determined by the principle of saturation (Bryman, 2012, pp. 425–426) during the process of the interviews.

Lastly, the sample was slightly expanded by the interest of FERM, in the insights from other organizations. The opportunity arose to interview two persons working in organizations unrelated to the Rotterdam port area, but very much connected to the establishment and workings of CoPs. These people were added to the sample. This approach can be described as opportunistic sampling (Bryman, 2012, p. 419).

Sampling conditions

A set of conditions was set for the selection of the participants. This set is:

- The person is connected or responsible for the cyber security of his organization or of the Rotterdam port area.
- The person provides a representation of a larger group.
- The person could be involved in a future CoP in a direct manner.

Selected interview participants

The sample strategy and the sample condition resulted in a set of 13 interview participants. These participants represent a mix of perspectives from the Rotterdam port area. Table 3-6 shows the details of the selected participants.

Table 3-6: Details of the interview participant

Name	Position	Size organization	Private/public	Rotterdam Port area
P1	CISO	Medium	Public	No

P2.1	Terminal manager	Small	Private	Yes
P2.2	ISPS manager	Small	Private	Yes
P3	PFSO	Medium	Private	Yes
P4	Security consultant	Small	Private	Yes
P5	CISO	Large	Public	No
P6	Strategic advisor	Large	Public	Yes
P7	CISO	Large	Public-Private	Yes
P8	Researcher	Large	Public	Yes
P9	Policy advisor	Medium	Semi-public	Yes
P10	Board member	Large	Public-private	Yes
P11.1	Asset manager	Medium	Private	Yes
P11.2	Director of Operations	Medium	Private	Yes
P11.3	QHSE	Medium	Private	Yes
P12	Security manager	Large	Private	Yes
P13	QESH manager	Medium	Private	Yes

Interview protocol

The interview protocol uses a semi-structured approach meaning that the researcher prepared an interview protocol with leeway for the interviewee (Bryman, 2012, p. 471). The interview protocol takes the shape of an interview guide containing a list of topics and some possible questions. However, unlike in structured interviews, there is no exact outline for the interview and the interviewer can ask further for more details.

The interviews were done one-on-one with the participant in a peaceful location at the worksite and at a time convenient for the interviewee. The interviewee was asked if the interview could be recorded for further analysis after the interview. It was also commented that the privacy of the interviewee would be ensured.

The interview's aims are focused on the *Goals, Drivers* and *Barriers* for a CoP in the Rotterdam port area. The aspect *Form* is omitted due to the results of the systematic review and meta-ethnography. This focus provides the initial structure for the interview protocol. The interviewer starts with a personal introduction phase. The interviewee is asked to introduce himself and tell more about his current job and position. This is done in order to relax the interviewee. The second phase is focused on the explanation of the research topic and the interview structure. The research question as well as the concept of CoP will be briefly explained here. This phase ends with a short overview of the topics that are aimed to be discussed: G*oals, Drivers* and *Barriers*. The next phase is a discussion of every aspect, but due to the semi-structured approach there is freedom for the discussion to move along with the interviewee. The interviewer is restricted to mostly (open) questions aimed to either gain insights, clarify the thinking behind the insights, or to examine the rationale of the insights. The interviewer cannot imply concepts or ideas. The prepared questions for every aspect are:

- What factors/goals do you believe would help/impede the establishment and working of a CoP?
- What factors/goals do you believe would help/impede the establishment of the CoP on cyber security in the Rotterdam port area? Why?
- What do you believe is the most critical goal/driver/barrier for the establishment of a CoP on cyber security in the Rotterdam port area?

- Which steps do you believe should be taken to reach these factors/goals? By whom?

These questions are not necessarily used directly, but are used as a fallback when needed. Directly after each interview, the interviewer wrote a small reflection in order to record his initial insights for future reference.

The entire interview protocol can be found in Appendix D. The rationale for every question is also clarified in this protocol.

Data extraction and synthesis

Transcription

The recordings of the interviews were first transcribed using the software of https://transcribe.wreally.com/ and https://otranscribe.com/. After completion of each transcript, a small reflection was written for future references. After that the completed transcripts were uploaded to NVivo for data extraction and synthesis using coding and translation.

Coding and translation

The data extraction and synthesis continued with coding and translation. This was done with a similar approach as the literature: by using meta-ethnography. The first step was to read and code the transcripts in the nodes of the three aspects: *Goals, Drivers* and *Barriers*.

The second step was the translation of the concepts. The translation started with an examination of the findings using the elements synthesized from the literature and were placed in their respective sub-node. The remaining nodes were possible new elements. They were re-examined, and connected findings were put in a sub-node as well. The synthesis step could then be taken for the new elements.

Synthesis

The synthesis starts by summarizing the interviews in order to gain an overview of the interview for future reference and to show an initial prioritization of elements by the interviewee. Three sources were used to construct this initial prioritization and summary: the interviewer's reflection written directly after the interview, the reflection written after the transcript completion, and the findings from NVivo. According to these sources, a table was created, prioritizing the elements; a small summary was written to clarify the intent of the interviewee further, and some small notes were added in case of novelties or special circumstances. The summaries of all interviews can be found in Appendix L. The transcripts can be viewed upon request and were omitted from this report due to their sheer size (227 pages in total) and the participant's privacy.

Prioritization

The last step in the analysis of the semi-structured interviews was to translate the prioritization of the synthesis step to a more general setting as a means to compare the elements independent of the participants. An overall score was created for every element by using reverse ranking for every interview and adding these rankings to calculate the score. The process consisted of three steps. The first step was done in the previous step by creating a table that prioritized the elements per aspect based on the insights from the different sources in every summary. This gave a first impression of the most important elements for every individual participant. The second step was the to create a table containing the reverse ranking for every aspect, element, and every participant. With reserve ranking, the rank goes from high to low instead of the classical low to high. This means that a high (numerical) score is given to elements with a higher priority, while a low (numerical) score is given to elements with low priority. The ranking was done as follows:

- A score of ***3*** was given when the element is very important according to the participant, since the participant put a lot of emphasis on this element or often referred to it.
- A score of ***2*** was given when the element is fairly important according to the participant, since the participant put some emphasis on this element or referred to it a few times.
- A score of ***1*** was given when the element is mentioned, but not deemed important according to the participant. The participant has mentioned once or twice, but never emphasized it in any way.

The tables of the summaries, the summaries and the other sources were used to rank every mentioned element for every participant in this table. The last step consisted of adding the rankings of all the participants to create the overall score for every element. The overall score gives insight into both the priority given to the element by the individual participants as well as the sheer number of participants mentioning the element. If the score is high, both the priority given, and the amount of references should be high. Further insights can be gained by comparing the overall scores to the individual rankings and considering the background of the participants.

Privacy of interviewee

It is vital that the privacy of the interviewee is ensured. At the same time, it is in the research's best interest to obtain the data from the interview in context and in pure form. Three actions have been taken to satisfy both objectives. Firstly, the interviewee and his background are anonymized in the transcripts and further documents. Even with this action, an observant reader and connected stakeholder might be able to determine the identity of the interviewee from the transcript. The second action is that the transcript will not be published and will only be shared to fellow researchers when an if they present reasonable arguments such as to deeply analyse the methodology of this research. The last action is translation of the interviewee's words to more general terms and to prevent direct quotes.

3.3.5 Determination of the critical node and the conditions

Aim of the determination of the critical node and the conditions

The determination of the critical node and the conditions uses triangulation by combining and comparing the answers on the first and second research question. The first research question is: *Which factors affect the establishment of Community of Practice according to literature?* The second research question is: *Which factors are critical for the establishment of a Community of Practice on cyber security in the case study of the Rotterdam port area according to the key stakeholders?* The combination of these answers provides the basis for the and fourth research question*:*

3) How do current cyber security collaboration formats solve the critical factors for the establishment of a Community of Practice on cyber security?
4) How could the critical factors for the establishment of a Community of Practice on cyber security be resolved?

In order to establish a community, the most important factors affecting a community, must be resolved. The representation of the factors is done through a critical node and several conditions.

Process of determination

The results of the case analysis, the systematic review and meta-ethnography, and the semi-structured interviews need to be combined in order to gain enter the design phase of this research. No formal method was used for this step. The process encompasses the determination of conclusions for all three parts of the analysis and synthesizing these insights into a critical node and conditions.

A critical node is the most important link in the challenge that connects all issues in the case. Solving the critical node inevitably means solving the challenge. The critical node has therefore the highest priority. The critical node is supported by several conditions. These conditions are practical restrictions or design principles that need to be taken into account for the case. Although these conditions are ancillary to the critical node, they do play a crucial part in a proper solution of the challenge.

3.3.6 Narrative review of practical literature for solutions

A narrative review aims is to gain an initial understanding of the topic area and this makes the process more uncertain (Bryman, 2012, p. 110). They have less focus and contain a wider scope, compared to the systematic review. This method suits the design process starting in chapter 5, aimed to find a solution for the research question and the case.

Aim of the narrative review for solutions

This narrative review was aimed to answer sub question 3: *How do current cyber security collaboration formats solve the critical factors for the establishment of a Community of Practice on cyber security?* The review provides insight in the strategies and structures used in other collaboration formats. The review also provides an overview of sub solutions that resolve the critical node and conditions. This overview can be combined with the results of the brainstorm as explained in section 3.3.7 to answer sub question 4: *How could the critical factors for the establishment of a Community of Practice on cyber security be resolved?*

Search and review process

Since the aim of the narrative review is clearly stated, the scope is set to practically orientated literature. Two purposive sampling approaches were used for this review: opportunistic sampling and snowball sampling. Opportunistic sampling is using opportunities that arise in an empirical context to collect data from individuals. Several actors in the case advised, or referred to documents or articles, so these were examined in this review. Snowball sampling is building further on information found in a reviewed source to gain a new source. This is an iterative process, ceased at the moment of the theoretical saturation. This approach halted the process of searching for this review.

Several organizations that could provide interesting insights were mentioned to the researcher. These organizations are ENISA, NCSC and the WEF. Documents of these organizations will be examined and reviewed if they seem interesting. Furthermore, the book *Cultivating Communities of Practice* by Wenger et al. (2002) is written as a guide to start CoP's, so this book was examined as well. All these documents are practical in nature and are aimed to help organizations set up a form of collaboration.

Scientific literature is not examined for two reasons. The first reason is the more abstract nature of scientific inquiry, rarely offering solutions. The aim is to find elements which can establish a community, and thus a more practical approach is desired. The second reason is that the examined literature from the governmental organization is based on scientific inquiry combined with empirical evidence. Therefore, the researcher would argue that the scientific insights are represented by the examined practical-orientated literature.

Selected articles

A total of seventeen articles were reviewed to look for solutions. Table 3-7 shows the literature that was found. It can be seen that no scientific articles were reviewed, because the focus of the review was practical-orientated.

Table 3-7: Overview of literature for solutions

Type of document	Title	Reference
Management Book	Cultivating Communities of Practice	(Wenger et al., 2002)
National guides	Starting a collective CSIRT	(NCSC, 2018a)
	Starting a regional collaboration	(NCSC, 2018b)
	Starting a Supply chain collaboration	(NCSC, 2018c)
	Starting an ISAC	(NCSC, 2018d)
	CSIRT Maturity Kit: A step-by-step guide towards enhancing CSIRT Maturity	(NCSC, 2015)
	An information sharing vision to improve Internet security	(NISCC, 2002)
	WARPs – the Business case	(NISCC, 2006)
International guides	A step-by-step approach on how to set up a CSIRT	(ENISA, 2006a)
International analysis & best practices	Information Sharing and Analysis Centers (ISACs) – Cooperative models	(ENISA, 2017a)
	Public Private Partnerships (PPPs) – Cooperative models	(ENISA, 2017b)
	Scalable and Accepted Methods for Trust Building in Operational Communities	(ENISA, 2014)
	Strategies for Incident Response and Cyber Crisis Cooperation	(ENISA, 2016)
	CERT cooperation and its further facilitation by relevant stakeholders	(ENISA, 2006b)
	WARP case study – Experience setting up a WARP	(Askwith, 2006)
	The evolution of WARPS	(Hakkaja, 2006)
	CSIRTs and WARPs: Improving security together	(UKERNA, 2006)

Examination of articles

The examination of the articles was done using NVivo in an iterative fashion. Seemingly interesting findings were coded and saved in nodes. The creation of the nodes was completely done in an intuitive manner. More structure was added when the literature was reviewed a second time in order to establish common elements and shared points. A summary of all findings can be found in appendix O. These findings are overall solutions based on existing concepts, recommended strategies and structures, and the other practical tips and recommendations.

3.3.7 Brainstorm

A brainstorm is a well-known design concept aimed to promote free thinking and out-of-the-box thinking. Designers have a wide scope of practical methods for this concept, ranging from individual session to group sessions, with brainstorm tools or without, and so on. The researcher decided to use an individual approach with the morphological chart as a support tool. Section 3.3.8 contains more details on the morphological chart.

Aim of the brainstorm

The brainstorm sessions aimed to partially answer sub question 4: *How could the critical factors for the establishment of a Community of Practice on cyber security be resolved?* Free thinking is used to establish empirical-based solutions for the challenges presented in the case. These solutions can be combined with the results of the narrative review explained in section 3.3.6.

Method used for the brainstorm

The researcher decided to use an individual approach with the morphological chart as a support tool to structure this brainstorm. The morphological chart was set up with the rows containing all the conditions. Three columns were decided on to ensure different perspectives on the empirical side of this research: Experience, Intuition, and Creativity. The Experience column encompasses solutions based on past experiences of the researcher, thus taking into account his time experiencing the context in the Rotterdam port area. The Intuition column encompasses solutions based on links created by the researcher on the found information till this point. Usually these solutions can only be partially explained with research evidence. The Creativity column encompasses solutions, formed through free thinking, and are in general more practically orientated. There is no evidence for these sub solutions.

Three iterations for all three columns were used to find sub solutions. These iterations were done on three separate days in order to provide room for new thoughts and ideas. The iterations were done parallel with the narrative review, so literature may have influenced this process.

3.3.8 Morphological chart

The morphological chart originates from the discipline of engineering design (Dragomir, Banyai, Dragomir, Popescu, & Criste, 2016; Tayal, 2013). It is defined as “a general method for structuring and investigating the total set of relationships contained in multi-dimensional, usually non-quantifiable, problem complexes” (Dragomir et al., 2016, p. 207). Practically, this method results in a chart that shows all possible sub solutions for every sub challenge. The overview of solutions makes it possible to prioritize elements and create a holistic solution. Therefore, it is also suited for social design.

Aim of the morphological chart

The morphological chart aims to provide an overview of the answers found by the narrative review and the brainstorm for sub question 4: *How could the critical factors for the establishment of a Community of Practice on cyber security be resolved?* This chart is the starting point to design a concept solution to answer the main research question.

Method used for the morphological chart

The morphological chart of this research provides an overview of all possible sub solutions established through the brainstorm and the narrative review. The rows of the charts list all the conditions based as mentioned in section 4.4.5. Four columns are defined: Narrative review, Experience, Intuition, Creativity. The Narrative review column contains sub solutions as found in the narrative review. The other three columns present the more empirical side of the research. The definitions of these columns were described in section 3.3.7.

The final application of this method is the creation of basis for a concept solution. The researcher can link sub solutions that suit each other. Choosing the combination of sub solutions is based on the insights and intuition of the researcher as well as the feedback of an expert. The expert feedback is explained in section 3.3.9. The implications of the sub conclusions and the influence of the sub solutions on each other can be taken into account in this manner.

3.3.9 Expert feedback

Aim of the expert feedback

The expert feedback is aimed to prioritize certain elements for the concept solution in order to answer the main research question: *How could a Community of Practice on cyber security be established?* The concept solution follows from this feedback and the previous findings. This method will contribute to the reflection on the results of all the previous methods.

Method used for expert feedback

A semi-structured interview method was used to discuss the elements that should be present in the concept solution with an expert to gain his feedback. The semi-structured approach means that the researcher prepared an interview protocol with leeway for the interviewee (Bryman, 2012, p. 471). The interview protocol takes the shape of an interview guide containing a list of topics and some possible questions. However, unlike with structured interviews, there is no exact outline for the interview and the interviewer can ask more specifically to things said by the interviewee and expand on that if necessary.

This approach was chosen in order to create an open and constructive setting. This improves the interaction between the researcher and the expert. Dialogue can then occur where questions can be asked to improve the quality of the feedback. High quality feedback is needed to make a prioritization on the sub solutions in the morphological chart and to address the interactions between the sub solutions.

The interviews were done one-on-one over the telephone at a time convenient for the interviewee. Notes were made during the interview. A summary was written after the interview. It was commented that the privacy of the interviewee would be ensured.

Sampling

The sampling of the expert feedback used convenience sampling. Convenience sampling is sampling participants simply on the availability to the researcher by virtue of accessibility (Bryman, 2012, p. 201). The sampling technique was used, since the expert is aware of the context of the Rotterdam port area case and discussed it with researcher in early stages of the research.

Only one expert is sampled to provide feedback, thus the sample size is one. This was done due to practical constraints, but has consequences for the external validity of this method. External validity is the degree in which results of a study or method can be generalized beyond the specific research context (Bryman, 2012, p. 47). The external validity of this method is low, since comparison of results from other experts cannot be made.

The expert is a researcher and advisor on cyber security collaboration for a private organization. His work connected him to multiple public and private organizations in the Netherlands that face the challenge of cyber security collaboration. Therefore, he has experience and variety of perspectives on the topic of this research. Furthermore, he has been in contact with FERM and the Rotterdam port area, so he was able to connect with this research’s case too.

Interview protocol

The interviews had a deductive and semi-structured approach. The deductive approach means that information will be gathered in the interviews in order to validate concepts or ideas. As a consequence of this approach, the morphological chart was used as a base and elements were discussed with the expert. The semi-structured approach means that the researcher prepared an interview protocol with leeway for the interviewee (Bryman, 2012, p. 471). The interview protocol takes the shape of an interview guide containing a list of topics and some possible questions. However, unlike in structured interviews, there is no exact outline for the interview and the interviewer can ask further for more details.

The deductive and semi-structured approach was chosen in order to connect the theoretical insights from the narrative review and creative ideas from the brainstorm with practical insights from an expert. A prioritization of elements for the concept solution can be done when using this approach.

The structure of the interview is connected to the results summarized in the morphological chart. The interview started with a small introduction by the researcher. The first topic for discussion and feedback is the general conditions and standard strategies used to establish collaboration in cyber security. After this discussion, the researcher explains that literature suggests multiple strategies and most consist of three phases: a first phase that explores and prepares, a second phase that launches the collaboration, and a third phase that strengthens the collaboration. Every phase is discussed and feedback is gained. The researcher puts extra focus on the use of a facilitator, the involvement of management, and trust building. These elements were mentioned often in literature.

The entire interview protocol can be found in Appendix R. The rationale for every question is clarified in this protocol.

Privacy of interviewee

It is vital that the privacy of the expert is ensured. At the same time, it is in the research's best interest to obtain the data from the interview in context and in pure form. Two actions have been taken to satisfy both objectives. First, the interviewee and his background are anonymized. The second action is translation of the interviewee's words to more general terms in the summary and in the report. No direct quotes were used as well.

4. Analysis phase

This chapter encompasses the results of the analysis performed for this research. These are the results of the Discover and Define phase of the double diamond model as displayed in Figure 4-1. These will answer the first and second sub question:

1) *Which factors affect the establishment of Community of Practice according to literature?*
2) *Which factors are critical for the establishment of a Community of Practice on cyber security in the case study of the Rotterdam port area according to the key stakeholders?*

An answer to the first sub question provides theoretical insights in how to affect CoPs. This will be done with the initial narrative review and the systematic review. These insights from the first sub question can be triangulated and validated by the answer to the second sub question. Practical insights are gained here with the use of the semi-structured interviews and partly with the case analysis. The case analysis and the initial narrative review also provide a theoretical and practical context. Section 3.3 explained all methods in detail.

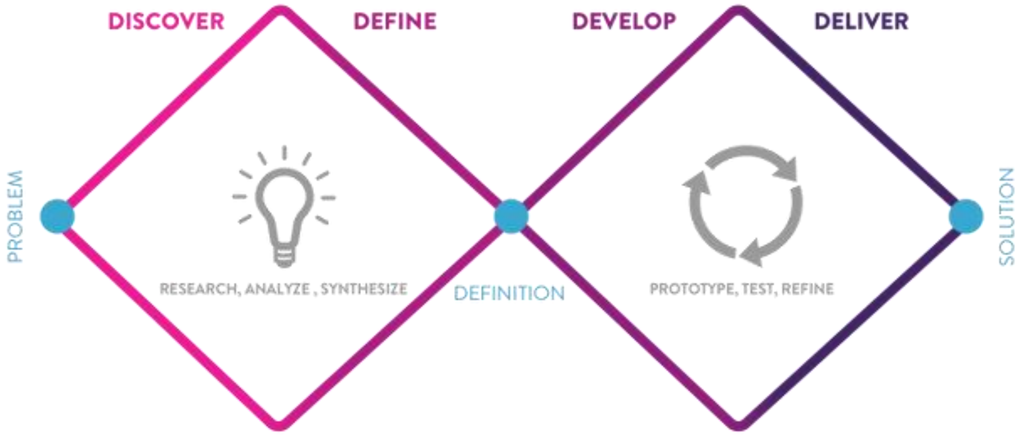

Figure 4-1: Double diamond model

The results of these methods will be shown in section 4.1-4.3. A summary of the results is made in section 4.4. All insights are combined and connected to determine a critical node and conditions in section 4.4.4 and 4.4.5. This will end this chapter and provide the basis for the Design phase presented in chapter 5.

4.1 Case analysis

The case analysis combined with the initial literature review presented in section 4.2.1 helped to shape this research's setup. However, it also provided interesting insights that were essential to remain connected with practice. This section elaborates on the results of the case analysis starting with an insight into the context of FERM. Next, important observations of the researcher will be presented as well as the results of a questionnaire among organizations in the Rotterdam port area. This section ends with a network analysis.

4.1.1 Context of FERM

The context of FERM is strongly connected to the emergence of the need for cyber resilience and security in the Rotterdam port area. Initial ideas and concepts regarding cyber resilience for the Rotterdam port area, can be traced back to 2012 and 2013. This topic became more active in the period between 2012 and 2015 on top management level. The first concrete step for FERM was taken in May 2015 when TNO was asked by Deltalinqs, the Police's Sea Division and the Haven-ISAC[3] to do a TNO-challenge on the cyber resilience of the Rotterdam port area. This challenge aimed to answer the question: *"How can small and larger organizations in the port logistic chain collectively create an overview of their needs and vulnerabilities and what are starting points for them to increase their cyber resilience?"* (translated from: *"Hoe kunnen grote en kleine partijen in een havenlogistieke keten gezamenlijk hun belangen en kwetsbaarheden inzichtelijk maken en wat zijn voor hen aanknopingspunten om hun cyber resilience te vergroten?")* (Duin & Zeer, 2015; TNO, 2015). The results were presented in September 2015 and consisted of six so-called building blocks, sub-concepts to increase the cyber resilience capacity of the port ecosystem (TNO, 2015). The original TNO building blocks are:

1) Cyber Co-op
2) Cyber Threat Intelligence Watch
3) Cyber Security Community of Practice
4) Cyber Security & Response Team
5) Cyber Notification Desk
6) the Port Resilience Officer

These building blocks were used as a tangible start to explore the options of a collaboration, which would later be called FERM.

The Port of Rotterdam took the lead in 2016 in creating a strategy for this collaboration after the PoR Harbour master was asked by Ahmed Aboutaleb, the mayor of Rotterdam to take charge in creating cyber resilience in the Rotterdam port area. The building blocks were expanded to a total of eight in this period:

1) Cyber Co-op
2) Cyber Threat Intelligence Watch
3) Cyber Security Community of Practice
4) Cyber Security & Response Team
5) Cyber Notification Desk
6) the Port Resilience Officer
7) Communication
8) Education

These building blocks provide the basic strategic pillars for FERM. The aim and definition of these building blocks have changed over time. An overview of the building blocks including the different aims and related results are presented in appendix D.

Four workgroups were created that focused on different aspects of strategy (Verkiel & Hoitink, 2016). The first workgroup is *Organization and Communication. Organization* aimed to define the role of the Port Resilience Officer and is led by two people from PoR. They focused on the CoP and the Co-Op, and they wanted to set up the strategy for the entire Cyber Resilient Officer (CRO) program. *Communication* was led by someone from PoR and someone from Deltalinqs. Their task was to create a communication strategy, a corporate identity, and a website. The second workgroup, *Legal framework***,** was led by two people from PoR. Their task was to determine the legal responsibilities and

[3] Haven-ISAC is the Haven Information Sharing and Analysis Center which consists of some of the bigger companies in the Rotterdam port area, the Port of Rotterdam and the NCSC. This is a legally required organ.

obligations of the Harbour master and to provide advice regarding his position. This focused more on PoR. The third workgroup was *Risk Management* led by two people from Police's Sea Division. Their task was to create Cyber Notification Desk, Cyber Threat Intelligence Watch, and Cyber Security & Response Team. The last workgroup was *Education, Training and Awareness* led by someone from Deltalinqs and the Police's Sea Division. Their task was to provide training, training materials and checklists.

The current PPP was officially established in June 2016 during the first Steering Committee meeting and the FERM-trademark is officially announced during the Deltalinqs conference on Security Awareness on November 30th, 2016. The official partners of FERM are PoR, Deltalinqs, the municipality of Rotterdam and the Police's Sea division. They also finance FERM together.

Since its establishment, FERM has focused on tangible and quick results while pursuing its two-fold goal of creating awareness, and creating a platform for collaboration and knowledge exchange. Furthermore, DCMR, NCSC and the Public Persecutor Service (OM) also joined the workgroup as informants. The PCCs and the annual Cyber security exercise belong to the most consistent and tangible activities of FERM. These meetings are aimed to connect organizations in the Rotterdam port area and to engage them with topics concerning cyber security. A more detailed overview of the history and activities of FERM between 2012 and April 2018 can be found in appendix C.

4.1.2 Observations

A total of fourteen informal interviews were conducted in the preliminary phase. Ten of these were with colleagues from PoR of whom seven were part of the Division Harbour master. Four of the interviews were with colleagues from FERM partner organizations. Furthermore, there were conversations with several people from private organizations during the Port Cyber Cafés and during the formal interviews. These conversations helped to constructed an overview of different perspectives on FERM. The notes from these observations are not placed in an appendix due to privacy reasons.

PoR colleagues differed in their views on FERM. Some did not see it as a part of PoR and did not understand why PoR was connected to this initiative. Others believed that FERM served as an extension on the services of PoR. Something most had in common was that they were quite unaware of the current affairs of FERM and its achievements. They knew the brand and name of FERM, but most had a hard time to describe its purpose and its activities.

The FERM partners were more aware of FERM, but noticed that PoR had a big influence on the activities of FERM. They conceded that this was obvious as PoR was the only organization supplying man power to FERM and the other partners gave less mandate for action. This gave some tension in the group. All partners preferred to look at FERM as a network instrument in order to share internal information and knowledge from the different partners. One colleague noted that the connection with industrial partners was still very limited and believed that the need for such interaction was high.

People from the private organizations were positive about FERM and said that it provided them with some direction on the topic of cyber security. They also were more informed about the aim of FERM to raise awareness, however they were less aware of the aim to collaborate. They believed that FERM was a strong communication channel on cyber security in the Rotterdam port area. The interaction between FERM and private organizations seemed like a classic sender-receiver mode where the private organizations consistently took the receiver role.

4.1.3 Questionnaire

The questionnaire was distributed to the private organizations in the Rotterdam port area. 93 organizations responded to questionnaire. All questions can be found in appendix E. This section and its appendix will only focus on the results of the five questions for this research and on the general characteristics. This subsection will only highlight certain results that are most relevant. An overview of all the results with graphs and tables can be found in appendix F.

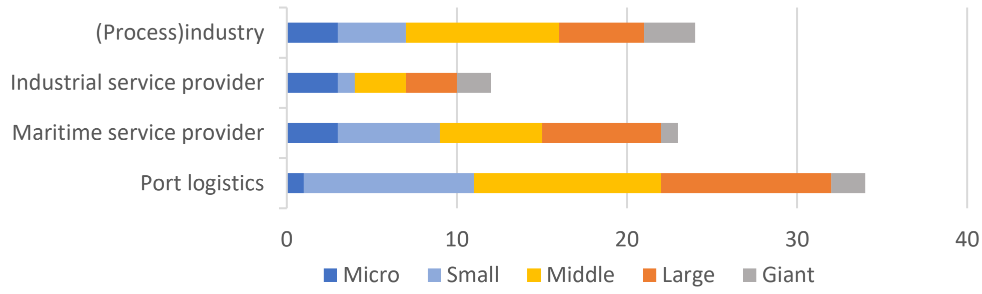

Figure 4-2: Overview of the company type and size

The participants were from a wide variety in size and type as is shown in Figure 4-2. The most representation came from middle and large sized organizations in the port logistics sector. It is unclear whether this composition provides a proper comparison with the Rotterdam port area as a whole, but the port logistic organization are very involved in the digitalization of their services in order to reduce and handle it themselves, since the responses to collective purchase, training and exercises and facilitated knowledge exchange are not deemed useful by at least 60% of the participating companies. costs and increase the effectivity. This may affect the results.

Furthermore, 60% of the participants were familiar with the FERM initiative. The importance of cyber security from an organization's perspective was in comparison deemed higher by organizations of the (process)industry or maritime service provider type. This suggests that organizations in these sectors experience a higher perceived threat. The importance from an employee's perspective is in general lower compared to the organization's perspective.

Figure 4-3 provides insights in the interest that companies have. It shows that more than half of the participating organizations would consider all three modes of interaction. Closer examination from the data shows that a group of maritime service providers does not want any of these three modes as well as that port logistics organizations are more hesitant for collaboration.

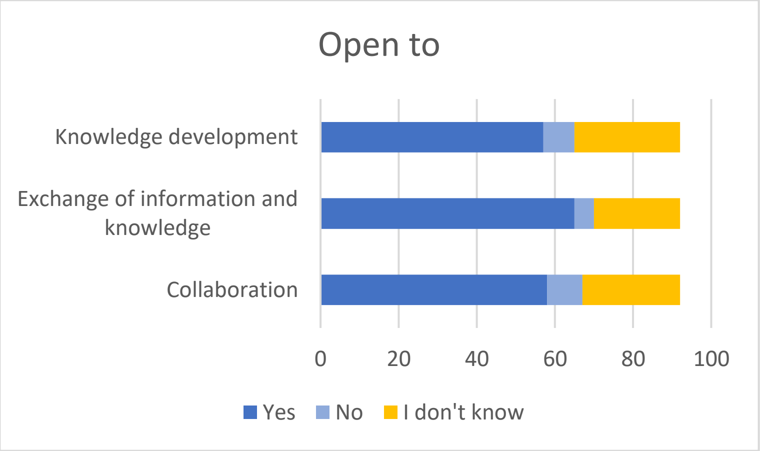

Figure 4-3: Overview of the interests of companies

The feedback from the companies on what activities they considered useful showed that sharing of information and receiving information concerning cyber security and cyber threats are deemed most useful. This can be seen in Figure 4-4. It can also be seen that at least half of the participating companies wishes for some more privacy concerning their cyber security.

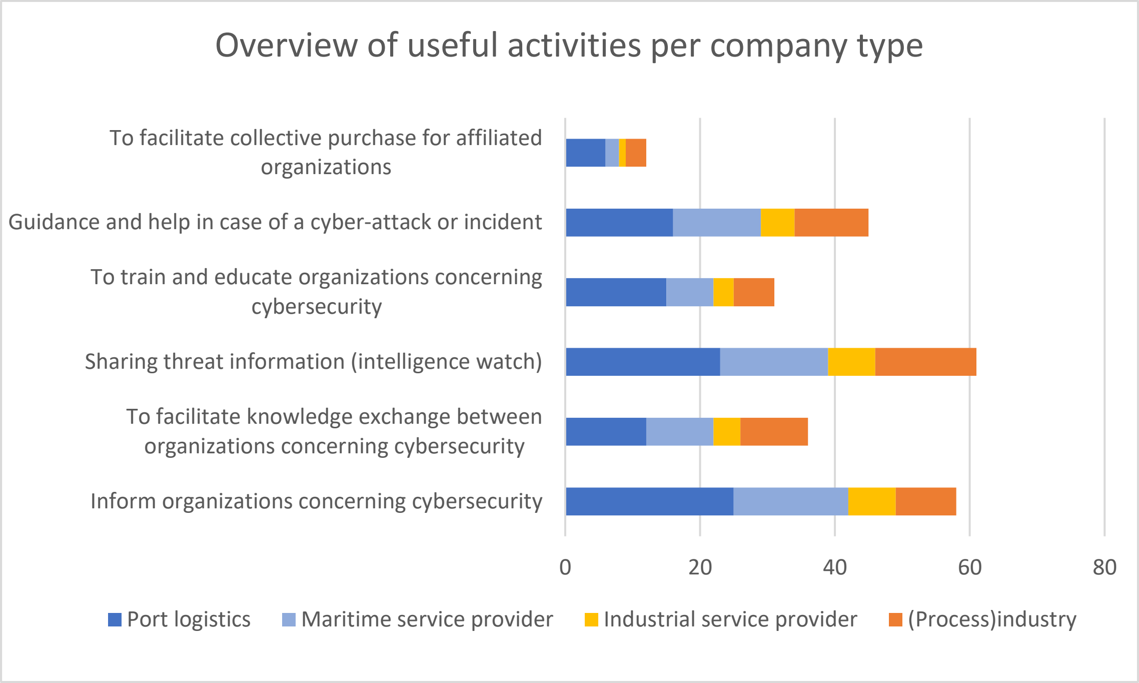

Figure 4-4: Overview of useful activities per company type

4.1.4 Network analysis

This case involves several actors with different aims, and resources that depend on each other to reach their goals thus forming a network. The main actors are PoR, the municipality of Rotterdam, the Police's Sea Division, Deltalinqs, the companies, DCMR, the OM, and NCSC. These organizations are directly involved in FERM usually through one or more people. An overview of these actors is presented in appendix G. This overview provides a description, their main aim and interest, and their resources.

Figure 4-5 provides a schematic overview of the network with the main actors in the Rotterdam port area for this case. Two collaborative vehicles are highlighted with the boxes: FERM and the Haven-ISAC. The Haven Information Sharing and Analysis Center consists of some of the bigger companies in the Rotterdam port area, the Port of Rotterdam and the several public organizations. This is a legally required organ. It currently consists of 32 members from 21 organizations.

The Haven-ISAC gives the impression of a CoP, especially if the initial definition of a CoP is used: a group that coheres through mutual engagement on appropriated enterprise and by creating a common repertoire (Wenger, 1998a). There is mutual engagement within the Haven-ISAC since they share information and hold trust towards each other to do so. Their joint enterprise is cyber security threats and they have a shared repertoire of routines and a shared history. However, there are certain differences between the Haven-ISAC and the current understanding of a CoP.

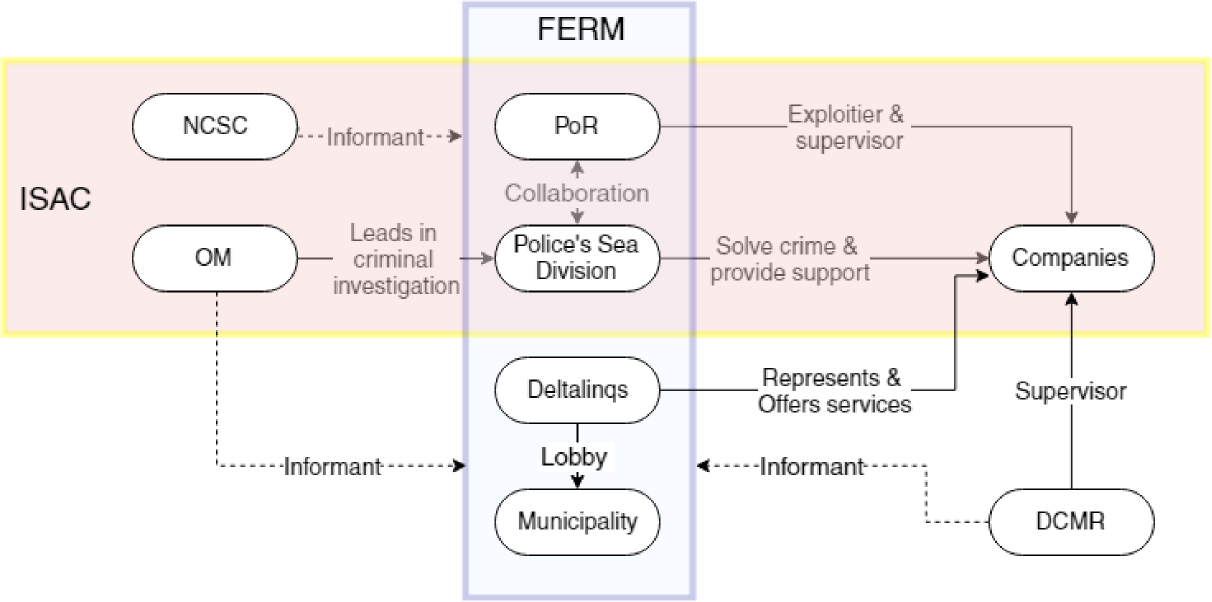

Figure 4-5: Schematic overview of the network

First and foremost, it is a legally required authority for organizations that are part of the vital infrastructure. Therefore, it was started on demand of the NCSC and was organized according to their vision. So, it lacks a self-creation as well as a natural occurrence. A second difference is that the Haven-ISAC focuses on sharing information on threats and incidents for their respective companies. The current understanding of CoP based on Wenger et al. (2002) suggest that a proper CoP should try to further their expertise and knowledge regarding their topic of interest. The Haven-ISAC creates no new knowledge, and learning does not occur, thus making it less aligned with the current view on CoP. The last difference is that no new members can join the Haven-ISAC and only selected organizations take place in the Haven-ISAC. It can be argued that opening a CoP for new members is a choice, but the fact that organizations were selected and no new members can enter, shows the formal nature of this body. These three differences show that the Haven-ISAC is not a CoP when compared with the current scientific view. However, this does not dismiss the importance of this body and the role it plays in the Rotterdam port area.

FERM is the second collaborative body highlighted in Figure 4-5. It consists of four partners and three informants. These actors are either public organizations or have a nature similar to a public organization (such as the Division Harbour master of PoR and Deltalinqs). This body is therefore an excellent platform to exchange information as well as align initiatives and projects. FERM targets the companies, as was explained in section 3.2.3. However, the resources of FERM and of the partners are limited to move and activate companies, for example appendix C shows that the attendance to Port Cyber Cafés is around 20 persons and that number decreases. Deltalinqs could play a connecting role, but this role has remained limited to this point.

However, Deltalinqs is strongly connected with the companies due to the services it offers. Deltalinqs facilitates multiple platforms and meetings for companies to exchange experiences, for example on physical security or environmental affairs. Several of the interviewees acknowledged the value of these meetings. However, there does not seem to be a meeting for cyber security yet, because it is not included in the current services yet.

A last note on the network concerns its complexity. Figure 4-5 might suggest a straightforward connection between actors, but the contrary is true. Firstly, the actor Companies encompasses more than 600 organizations differing in size, sector and way of working. Interaction with this many organizations is difficult and cannot be generalized. Secondly, within every actor there are people establishing this formal network, but they have a more informal network as well, which increases the complexity. Thirdly, because of the professionalization and specialization of certain people they have more knowledge, expertise and competencies making it more difficult to stir them hierarchically (De Bruijn & Heuvelhof, 2008, pp. 2–4).

4.2 SCIENTIFIC LITERATURE

This section will elaborate on the scientific literature that was consulted in the analysis phase. It starts with the results of the initial literature review of which the method was explained in section 3.3.2. The initial literature review combined with the case analysis presented in section 4.1 helped to shape this research's setup The results of the initial literature review are the theoretical background of the CoP concept and a theoretical overview of important factors of CoPs. This review was done simultaneously with the case analysis presented in section 4.1. This section ends with the results of the systematic review and the meta-ethnography of which the methods was explained in section 3.3.3. These methods resulted an overview of elements that affect the establishment of a CoP.

4.2.1 Initial literature review

Theoretical background

The concept Community of Practice (CoP) and its definition have taken several twists and turns since its introduction to our current age. A Community of Practice was introduced as a concept to describe how workers engage in informal group both at work and off the job to share information and to develop solution of job-related problems (Cox, 2005; Lave & Wenger, 1991; L. C. Li et al., 2009). It was believed that CoPs emerged informally. However, nowadays, it is believed that a CoP is *"a group of people who share a concern, a set of problems, or a passion about a topic, and who deepen their knowledge and expertise in this area by interacting on an ongoing basis"*. It has also become generally accepted that CoPs can be created and fostered to enhance the competitiveness of firms ((L. C. Li et al., 2009). A more detailed account on the history of the CoP context can be found in appendix B.

Three main characteristics of CoPs are presented and explained. The first is the domain, the common ground and boundaries that enable members to share and decide if it is worth spending time on. The second is the community, the social structure that facilitates learning through interaction. And the third is practice, the set of shared repertoires of resources. These three characteristics could be shaped and created. The role of leaders and facilitators is also introduced in order to create the CoPs. This book is sometimes seen as an inspirational and practical handbook with little value for research, especially since its contents are not empirically tested (Cox, 2005). However, this book did place the concept of CoP in the KM field.

The ideas on CoP provided by Wenger, McDermott and Snyder (2002) were taken as the basis by many in the KM field and build on by other researchers. The current research on CoPs is diverse and ranges from theoretical models on its functioning (Borzillo, 2017; Du Plessis, 2008; Edwards, 2005; Handley, Sturdy, Finchman, & Clark, 2006; Jeon et al., 2011; Y. M. Li & Jhang-Li, 2010) to empirical descriptions in real world situations such as schools (Chu, 2016), hospitals (Blackmore, 2010, Chapter 9; Cornes et al., 2014; Egan & Jaye, 2009; Lathlean & Le May, 2002; Mabery et al., 2013), and businesses (Machuca

& Costa, 2012). This diverse set of research all pushed the concept of CoP forward and made it accepted as a KM tool for practices in the new knowledge-based economy.

There have been comments and critiques on the concept of CoP (Blackmore, 2010, Chapter 11; Roberts, 2006), especially concerning power and its influence on a CoP, the degree of informality, the tension between the goals of a CoP and an organization, and size and spatial reach. There have also been researchers who believe that the concept of CoP should return to its original field of social learning (Handley et al., 2006). However, none have been able to stop the popularity of this concept in organizational settings as a KM-tool.

However, little can be found on the establishment, creation or design of a CoP; sometimes they are designed, sometimes they just exist, and sometimes they are just named as such. The only reference found is the book of Wenger, McDermott and Snyder (2002) that spurred the interest of many, but as mentioned above, the ideas from this book have not all been empirically tested. New insights are needed on the design and establishment of CoPs.

Theoretical overview

The re-examination of the literature aimed to create a theoretical overview covering five aspects: *Characteristics, Goals, Drivers, Barriers and Forms/Activities*. The elements of the aspects are presented in alphabetical order in Table 4-1. The definitions of every element can be found in appendix H.

Table 4-1: Theoretical overview

Characteristic	Goal	Driver	Barrier	Form/Activity
Community	Financial	Characteristics of a CoP	Characteristics of a CoP	Activities
Identity	Information	Commitment	Communication	Digital infrastructure & tools
Informality	Knowledge management	Communication	Culture	Forms
Knowledge management	Learning	Culture	Finance	Indirect communication
Learning	Network	Identity	Initial phase	Meeting each other
Mutuality	Problem solving	Initial phase	Management	
Network		Management	Operational	
Problem solving		Learning	Technology	
Self-constructing		Relationship management	Trust	
Social		Structure	Uncertainty	
Social capital		Trust		

The aspect *Forms/Activities* were very operation-oriented as well as very diverse. Some sub-nodes could be created on a more abstract level, but no universal definition could capture them. Therefore, the list of *Forms/Activities* remains limited.

The *Driver* and *Barrier* elements share a close relation. There are even some elements that occur in both, such as Characteristics of the CoP, Communication, Culture, Management and Trust. However, even when they are named the same, they have a difference in nature as can be seen in the definition in Appendix H. The difference is mostly that the *Driver* focuses on the positive, while the *Barrier* focuses on the negative. There is a balancing act between these elements which needs to be managed properly. A clear example of the element Characteristic of the CoP is the *Characteristic* Community. This will inevitably create boundaries. These boundaries can drive the CoP as it will strengthen the group feeling and make the CoP grow (Blackmore, 2010, pp. 110–111). On the other hand, it can become a barrier when these boundaries are used to strictly and thus excluded other people or new ideas (Dooner et al., 2008, p. 566; Roberts, 2006, p. 626).

However, it is wrong to assume that every *Driver* is inevitably a *Barrier* or vice versa. Some elements have only positive or only negative influence. The lack of such a *Driver* would not immediately result in a negative effect, while the presence of such a *Barrier* would always result in a negative effect. An example is the *Barrier* Technology. A problem with software compatibility between members of the CoP would negatively influence the CoP, but if the compatibility would be good, it would not result in a positive influence since it is deemed obvious (Kelly et al., 2002, p. 17).

4.2.2 Systematic review and meta-ethnography

The systematic review and meta-ethnography resulted in an overview of elements that could affect the establishment of a CoP. As explained in section 3.3.3, the results focus on three of the five aspects of the theoretical overview: *Goals, Drivers* and *Barriers*. The aspect *Characteristic* was not used, since a characteristic provides insights into a concept, but cannot affect something. Therefore, this aspect did not align with the aim of this review. The *Form* aspect was not used, since it could not provide meaningful findings. No underlying structures or organizational configuration for CoPs could be found in the literature, making it clear that the CoP itself was the structure. Therefore, this aspect was removed from the final results. The results for the three aspects are presented in Table 4-2.

Table 4-2: Elements found with the meta-ethnography

Goals	Drivers	Barriers
Company Improvement	Awareness of knowledge and information	Alignment and focus
Knowledge management	Commitment	Commitment & Participation
Learning	Communication	Communication
Network & Interactions	Culture	Culture
Strategic (company) advantage	Facilitator & Leadership	Management
	Management	Structure
	People	ICT & Tools
	Reward and recognition	Trust and social relations
	Shared and negotiable goals	
	Social	
	Strategy	
	Structure	
	ICT & Tools	
	Trust	

The results of the meta-ethnography show similarities with the elements found in the theoretical overview, described in section 4.2.1. As mentioned in section 3.3.3, the results from the theoretical overview were used as a reference point and were not copied. All elements in Table 4-2 are based on the findings in reviewed literature and even elements, with the same name have different definitions compared to the theoretical overview. The definitions of the elements for every aspect will be described below. The number of unique sources will also be mentioned. Appendix J provides insights in the sources used per element for the synthesis. The specific findings used per source are stored in a NVivo-file which can be shared upon request.

Goals

The aspect *Goals* has a total of 49 initial findings in 17 sources (out of a total of 60). 15 of these initial findings could not be grouped and synthesized. The synthesized elements consist of at least 13 findings that were connected. The definitions for every *Goal* element as well as the number of used sources are presented in Table 4-3.

Table 4-3: Definitions of Goal-elements

Goal	Definition	Sources
Company Improvement	The direct improvements of business processes or employees through the improvement of skills and behaviour of employees and reduction of cycle time of projects due to increased knowledge.	10
Knowledge management	The efficient and effective sharing, exchange, capture and creation of both tacit and explicit knowledge between people within and between organizations.	13
Learning	Participant want to learn and improve in their own practice, abilities and skills.	9
Network and Interactions	The creation of social capital and valuable collaborative networks to sustain and improve relationships.	10
Strategic (company) advantage	The improvement or creation of strategic assets for organizations, such as innovation potential, sustainable growth or competitiveness.	10

An important note on these defined Goals is that the aims are not always perceived or constructed at the start of a CoP. The reviewed literature mostly analysed CoPs and can therefore rationalize these goals. However, it remains vague whether or not a goal for CoP is always set at its start. For example, Scarso et al. (2009) mentioned that *"CoPs have the twofold function of helping the line in their usual activities by acting as ''answer providers'', and preserving the company knowledge base."*. This suggests that a CoP has Knowledge management as a goal, however, it is unclear whether this is a conclusion from their analysis or that it has been predefined.

The *Goal* Knowledge management was most frequently found in literature. This goal contains multiple dimensions: the sharing, the exchange, the capture, and the creation of knowledge. Some sources referred to a limited set of these dimensions, however all sources had in common that they referred to an action to be taken for the sake of knowledge itself. There are, however, practical differences when a CoP has a stronger focus on certain dimensions.

Drivers

The aspect *Driver* has a total of 394 initial findings in 35 sources (out of a total of 60). 114 findings of these initial findings could not be grouped and synthesized. The synthesized elements consist of at least 10 findings that were connected. The definitions for every *Driver* element as well as the number of used sources are presented in Table 4-4.

Table 4-4: Definitions of Driver-elements

Drivers	Definition	Sources
Awareness of knowledge and information	The practitioners' recognition of the importance of knowledge and information as well as their access this knowledge or information.	5
Commitment	The continuing motivation and willingness of members to participate and engage in the CoP and its practice.	16
Communication	The continuous, transparent and free-flowing interaction between the members.	19
Culture	An atmosphere with shared values that enables the working of a CoP, shapes the members by teaching them the social norms, and creates an identity.	31
Facilitator & Leadership	A person whose main task is to improve the functioning of the CoP by showing leadership, monitoring progress and people, supporting members, coordinating process. He/she creates conditions for members to engage in the CoP.	20
Management	The visible support of (higher) management layers to the CoP e.g. by providing resources and time for its members.	24
People	The presence of the "right" people and skillsets, as well as the right combination of people in the CoP.	13
Reward and recognition	The reinforcement of the "right" behavior to increase the motivation and commitment of the CoP members through social rewards or material incentives.	16
Shared & Negotiable Goals	The purpose or desire that connects the members of the CoP and provides direction to the efforts of the members.	17
Social	The personal relationships and connections between members.	30
Strategy	The purpose of the CoP needs to connect to the overall strategy of the organization of which it is part. This improves the acceptance of the COP and its success.	6
Structure	The setup and organization of the operations of the CoP to function.	14
ICT & Tools	The ICT and other tools that support the operations of the CoP, such as social interaction and knowledge exchange.	18
Trust	"A psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another." (Sonnenwald, 2003)	22

Deeper insights into some Drivers

Several *Drivers* need a more detailed account due to their complicity. These *Drivers* are Culture, People and Structure.

The *Driver* Culture has an increased complexity, since it consists of several values that are commonly perceived in successful CoPs. The list of important values includes sharing, collaboration, transparency, informality, trust, learning, flexibility and reciprocity. These values are not deemed as independent elements, since they are only explicitly named by several authors. If these values are named independently, the researcher argues that they all contribute to the overall culture.

The definition of the *Driver* People may appear vague, since no definition is given for 'right' people. No definition is given, since what is right depends on the context. On an intuitive level, this *Driver* makes sense, since most people have been in a situation where a certain person is present who feels perfectly suited for the situation and his position. The people who are important for this *Driver* are the managers of a CoP.

The *Driver* Structure has an inherent complexity due to the balance needed between structure and informality. A CoP needs both, but every CoP needs it in a different balance. On one hand, spontaneity must be cultivated and structured (Roberts, 2006, p. 625). On the other hand, organizational and technological infrastructure has to be created to support the CoP and make it more efficient. An important choice is how the CoP fits in the existing organization and in the organizational structure.

Connected set of Drivers

These *Drivers* influence the establishment of a CoP positively, both directly and indirectly. The direct influence is quite clear; if any of these *Drivers* is taken care of, there is an immediate improvement of the CoP. For example, when there is management support, certain organizational barriers such as time and funding will be lessened and this in turn has a positive effect on the creation of the CoP. The indirect manner may be less evident, since it involves effects the *Drivers* have on each other, therefore creating a form of synergy. Three sets of connections were found in this set of literature.

The first set concerns the *Drivers* Trust, Social, Culture, Commitment, and Shared & Negotiable Goals. A schematic overview of these connections is presented in Figure 4-6. The arrowheads show if the connection between the *Drivers* is unidirectional or reciprocal. The main components of this set are the *Drivers* Trust and Social. They strongly improve each other, e.g. improvements in trust will improve social relations, but more social interactions will establish trust. Trust will motivate people to commit themselves to the CoP, thus linking it to the *Driver* Commitment, but is also an important value that helps to create the proper Culture for the CoP. This Culture will in return provide a discourse for its members that will strengthen Trust. The connection between Social and Culture is similar to the one between Social and Trust; social interactions provide the basis to create a discourse, but a common discourse will make it easier to connect with one another. The connection of Shared & Negotiable Goals with Trust and Social is shaped by the clarity and unification that a common aim provides. The members are connected by the shared aim which makes it easier to interact with each other and build trust.

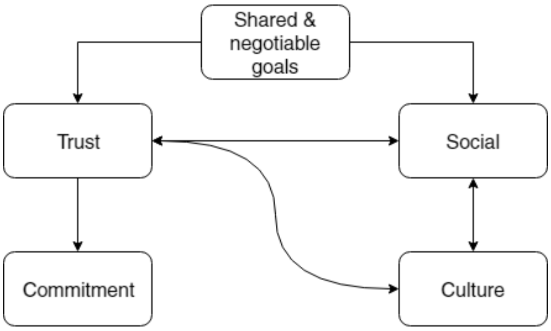

Figure 4-6: Schematic overview of the first set Driver connections

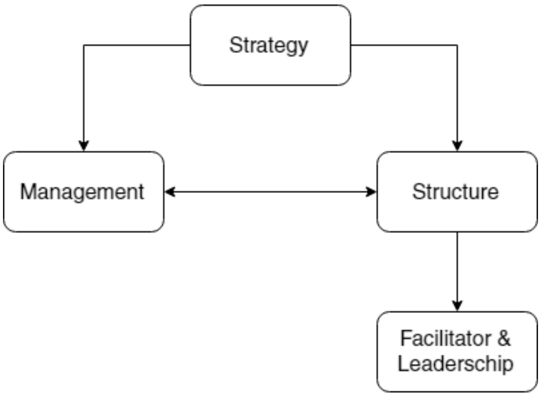

Figure 4-7: Schematic overview of the second set of Driver connections

The second set involves the *Drivers* Management, Structure, Strategy, and Facilitator & Leadership. A schematic overview is presented in Figure 4-7. As before, the arrowheads show if the connection between the *Drivers* is unidirectional or reciprocal. This is involved with the organizational-type of *Drivers*. The Strategy of the CoP provides insights in the aims and way of working of the CoP. This greatly influences how the Management perceives the CoP, and it provides the basis of a Structure. Similarly, the Structure and Management are connected, since the perception of Management is based on the Structure, so it's worthwhile to create a Structure that is approved by Management as well. Lastly, the Structure is connected to the influence of a facilitator or a leader.

The third set involves just two *Drivers*, Communication and ICT & Tools. This connection is quite straightforward, since certain ICT tools, such as Skype and email, encourage quick and easy communication. This connection is unidirectional from ICT & Tools to communication.

Barriers

The aspect *Barrier* has a total of 134 initial findings in 28 sources (out of a total of 60). 52 of these initial findings could not be grouped and synthesized. The synthesized elements consist of at least 9 findings that were connected. The definitions for every *Barrier* element as well as the number of used sources are presented in Table 4-5.

Table 4-5: Definitions of Barrier-elements

Barriers	Definition	Sources
Alignment and Focus	The lack of focus or alignment with the organization can impede a CoP by causing miscommunication or demotivating members.	7
Commitment & Participation	The unwillingness or lack of motivation that prevents (continuous) engagement and participation in the CoP.	11
Communication	Difficulties in the interaction of members.	7
Culture	The overall atmosphere that consists of certain values can impede the CoP or create barriers between the members.	20
Management	The lack of support of higher management layers to the CoPs in different forms.	16
Structure	The over organization and bureaucracy that impedes the CoP.	7
ICT & Tools	Badly engineered tools or the lack of support tools can impede and demotivate the CoP.	12
Trust and Social Relations	The lack the interactions between people as well as the lack of trust between participants of the CoP.	14

Deeper insights into some Barriers

There are some elements occurring in both *Drivers* and *Barriers*: Communication, Culture, Management, Structure, and ICT & Tools. The *Barriers* Communication, Management, and ICT & Tools, are quite literally the opposite of their *Driver*, but this is not the case for the elements Culture and Structure. These two elements are more context-dependent and so the immediate results are slower.

Some of the *Barriers* are a combination or a collection of Drivers: Commitment & Participation, and Trust and Social Relations. *Barriers* that consist of two *Driver* elements were created, since the negative effects of such *Drivers* were mentioned less, or were mentioned together often. The difference for the *Barrier* Commitment & Participation focuses on the lack of participation that contributed to the lack of commitment. The literature was less explicit about participation for the *Driver*. For the *Barrier* Trust and Social relations, it was already seen at the *Drivers* that they share a strong connection. This connection was named more explicitly in the literature for the *Barriers*.

4.3 SEMI-STRUCTURED INTERVIEWS

The semi-structured interviews provided empirical insights that could be triangulated with the theoretical insights of the systematic review and the meta-ethnography of section 4.2.2. Thirteen semi-structured interviews were conducted with the participants presented in section 3.3.4. All the interviews were transcribed, coded, translated and summarized. The summaries of all interviews can be found in Appendix L. The transcripts can be viewed upon request and were omitted from this report due to their sheer size (227 pages in total) and the participant's privacy.

Theoretical elements

The process of transcribing, coding and translating, explained in section 3.3.4 made it possible to determine whether any of the theoretical elements were mentioned by the participants. Appendix M contains overviews for every aspect, showing how many times a theoretical element of a certain aspect is mentioned by a specific participant as well as a sum of how many of the participants mentioned a certain element. These overviews provide some first information on the recognition of the theoretical elements by stakeholders.

An interesting finding is that for every aspect some elements were never or only rarely mentioned by any of the participants. For the *Goal* aspects, this is the case for the element Strategic (company) advantage. For the *Driver* aspect, the following elements were never or only once mentioned: Awareness of knowledge, Communication, People, Reward & Recognition, Strategy, Structure, and ICT & Tools. For the *Barrier* aspect, the following elements were never or only once mentioned: Alignment & Focus, Commitment & Participation, Structure, and ICT & Tools.

Another interesting finding is that there is a difference in the average amount of references per participant for every aspect. It can be seen that, in general, the *Driver* aspects was discussed most, followed by the *Barrier* aspect. The *Goal* aspect is discussed less and most participant only refer to a certain goal once or twice.

4.3.1 New elements

New elements emerged from the interviews that were not covered by the literature using the process described in section 3.3.4. Appendix N contains overviews for every aspect, showing how many times a new element of a certain aspect is mentioned by a specific participant as well as a sum of how many of the participants mentioned a certain element. Table 4-6 shows the definition of every new element. These definitions were synthesized using the interviews.

An interesting finding is that some elements are mentioned by more than half of the participants. This is the case for the *Drivers* Awareness & urgency and Direct relevance and for the *Barrier* Mutual Differences. This suggest that these elements could be important in this case and could be researched more.

Table 4-6: Definitions of the new elements

Aspect	Element	Definition
Goals	Collective cyber unit	A (public-private) partnership that aims to address all cyber-related issues both during crisis (such as assisting and stabilizing) as well as in the preparation (such as training and advising).
	Collective training or exercise	Collaboration in training exercises and drills both developing as in performing them.
Drivers	Awareness and Urgency	The need to be aware of the subject itself as well as understand the need to deal with it immediately.
	Confidentiality	The certainty that certain knowledge or information will remain private or at least not made public knowledge.
	Direct relevance	The topics discussed or the aims of the CoP must connect to current and relatable issues faced by organizations.

	Distinctions	The differences between organizations must be made clear in order to match the level of knowledge and needs.
	Group size	The amount of people at a meeting should remain limited in order to promote interaction and openness.
	Interest in others	Organizations want to compare themselves with others and know what other are doing.
	Pride for Rotterdam	A feeling that companies in the Rotterdam Port area share and that motivates them to make Rotterdam the best port worldwide.
	Time	The passage of time helps a CoP to take shape, to gain substance and to attract members. It will constantly improve in these areas.
Barriers	Group size	Meetings with many participants hinder openness and make the participant more reserved.
	Lack of awareness and knowledge	Participants do not hold enough knowledge on a certain topic and don't realize its importance.
	Limited Sharing	Participants are hesitant to share and restricted the information they share with others.
	Mutual differences	Differences between companies (i.e. size or branch) hinders them to effectively exchange information and knowledge.
	People	Individuals that can hinder the process of a CoP due to their personalities, organizational positions or aims.
	Priority	Participants rank a certain topic relatively lower than others and therefore do take action for this topic.

4.3.2 Prioritization of elements

The process of prioritization of elements explained in section 3.3.4 was used to determine the priorities for the different aspects of every participant. More insights in the participants and their priorities can be found in appendix L, which contains the summaries of all 13 interviews.

Table 4-7, Table 4-8, and Table 4-9 present the prioritization based on reverse ranking of the respective aspects. The first two columns note the element and its origin respectively from theory, from the interviews (New), or from one specific person (Personal). The third column, the #-column, shows how many participants noted this element. The Score-column presents the scoring based on the reverse ranking. If the Score is higher, the element has a higher priority based on all interviews. The P-columns note the ranking for every participant P1-P13.

Goals

The prioritization of the *Goal* aspect is presented in Table 4-7. The *Goal* Knowledge management attains the highest score. Upon closer examination of the individual scoring the *Goal* Knowledge management, it can be seen that only four of the 13 participants give this goal the highest ranking. The *Goal* Knowledge management is recognized by all participants and is perceived as important or very important by nine of the participants. This suggest that Knowledge management is a goal that every participant believes should be part of a CoP.

It is interesting that the *Goal* Company improvement was also awarded the highest ranking by four participants, but is not recognized by most participants to be of interest. Even though the Score of Company improvement and Network & Interaction are the same, it can be easily spotted that the average score of the *Goal* Company improvement is higher. Furthermore, the group of participants that perceived Company improvement as a (very important) goal did not perceive Network & Interaction as a goal. This group also contains four of the six private companies. This suggests a divide between the participants of public and private organizations: the public organization recognize Network & Interaction as a goal, but the importance placed on Company improvement is higher for most of the private organizations.

Table 4-7: Prioritization of the Goal aspect

Goal	Element	#	Score	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13
Theory	Company improvement	5	13		3	1				3				3		3
	Knowledge management	13	26	2	1	2	2	3	3	1	2	3	1	2	3	1
	Learning	3	5		2							1		2		
	Network & Interactions	7	13				1	2	3		3	1	1		2	
	Strategic (company) advantage	1	1		1											
New	Collective cyber unit	2	5	2									3			
	Collective training or exercise	3	8				3			2						3
Personal	Create collective products	2	5	3				2								
	Enabling board-level members	1	2						2							

Drivers

Table 4-8 presents the prioritization of the *Driver* aspect. The Scores suggest that a divide can be made into four segments. *Drivers* with the highest Score (above 15), with an upper middle Score (between 9-15), with a lower middle Score (between 6-9), and with a low Score (lower than 6).

The *Drives* with the highest Score are Social and Trust. These elements also are mentioned by most participants as shown in the #-column. When looking at the individual ranking, both elements are often ranked as important or very important. This suggests that there is an agreement among the participants that these two *Drivers* are very important for a CoP and deserve most attention.

The *Drivers* in the upper middle segment contain five elements of which three are theoretical ones and two are new ones. The theoretical elements are Culture, Facilitator & Leadership, Management. The new elements are Awareness & Urgency and Direct relevance. All these elements are recognized by five or six participants, except for Awareness & Urgency which was recognized by eight participants and whose Score is also the highest of this segment. Upon examination of the individual Scores, it can be seen that these elements are rarely perceived as very important, but mostly as something which should receive some attention.

The *Drivers* in the lower middle segment contain five elements of which two are theoretical ones and three are new ones. The theoretical elements are Commitment and Shared & Negotiable goals. The new elements are Distinctions, Interest in others, and Time. All of these elements are recognized by five or six of the participants, except Interest in others which is perceived as very important by two of the six participants of private organizations. This suggest that Interest in others can be a very important *Driver* for a part of the private organizations. The other elements in this segment are perceived, but are mostly mentioned and often do not hold much importance for the participants. This can be based on their individual Scores. The element Interest in others should be researched more to determine its worth and importance, since this result is not yet conclusive on its importance.

The *Drivers* in the lower segment contain ten elements of which seven theoretical ones and three are new elements. The other four elements are Communication, People, Structure, and Tools & ICT. The new elements are Confidentiality, Group size and Pride for Rotterdam. P9 also holds the *Driver* Enjoyment, which can be defined as making the meetings fun and entertaining, in high regards. When looking at the individual scores, most elements in this segment are only mentioned once and are only recognized by less than a quarter of the participants. This suggests that these elements are either under-appreciated by the participants or hold little importance and should not get attention.

Table 4-8: Prioritization of the Driver aspect

Driver	Element	#	Score	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13
Theory	Awareness of knowledge	0	0													
	Commitment	5	8	2					1	1			3		1	
	Communication	2	2								1		1			
	Culture	6	12						3		1	2	3		2	1
	Facilitator & Leadership	6	10		1				1	3	2	2				1
	Management	5	10					2	1				2		2	3
	People	2	4								2	2				
	Reward & recognition	0	0													
	Shared & negotiable goals	6	6	1		1			1	1			1		1	
	Social	11	21	2	1			1	3	1	3	2	1	2	3	2
	Strategy	0	0													
	Structure	1	1											1		
	Tools & ICT	1	3							3						
	Trust	9	20	3				3	3	2	1	2	1	2	3	
New	Awareness & urgency	8	13	1		2	3		1				1	2	1	2
	Confidentiality	4	5							1		1		1	2	
	Direct relevance	6	11		2			3	1	1		1		3		
	Distinctions	6	7		1	1	2			1		1	1			
	Group size	2	3		2										1	
	Interest in others	2	6		3									3		
	Pride for Rotterdam	4	5										2	1	1	1
	Time	5	7				1	1	2		2	1				
Personal	Enjoyment	1	3									3				

Barriers

Table 4-9 presents the prioritization of the *Barrier* aspect. The scores suggest a division in three segments: a high, a middle, and a lower one. The high segment consists of the two elements Culture and Trust & Social relations, since both have a high score, are mentioned by more than ten participants, and have high individual rankings. This suggest that these two *Barriers* are very important and should have a lot of attention.

Table 4-9: Prioritization of the Barrier aspect

Barrier	Element	#	Score	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13
Theory	Alignment & Focus	0	0													
	Commitment & Participation	4	6	3	1		1		1							
	Communication	6	6		1				1	1		1	1		1	
	Culture	10	24	1	3		3		3		2	3	3	1	3	2
	Management	6	11	2				1	2				2		2	2
	Structure	0	0													
	Tools & ICT	1	1							1						
	Trust & Social relations	11	26	1	3		3	3	3	1	2	2		3	3	2
New	Group size	3	5		3							1			1	
	Lack of awareness and knowledge	4	9	1		3	2			3						
	Limited Sharing	5	11							2		2	1		3	3
	Mutual differences	7	10	1	1	2			2	2	1					1
	People	5	8					1	3		1	1		2		
	Priority	6	13	2		3	2			3			1		2	

The middle segment consists of six elements of which one is theoretical and five are new. The theoretical element is Management. The new elements are Lack of awareness and knowledge, Limited sharing, Mutual differences, and People. There is some variety in how many participants perceive these elements and the individual scoring. The *Barriers* Management and Mutual differences have a relatively good score and the individual rankings suggest that the participant find it important, but not a priority. On the other hand, Limited sharing and Priority have a similar score, but the individual rankings show some participants hold it a higher regard. The *Barrier* Lack of awareness and knowledge is mentioned by few participants, but has a relative high ranking for those who mentioned. In line with the definition of this element, it may be that participants lack awareness and knowledge of this *Barrier*. This should be examined further. Based on these observations, it seems that in this segment the *Barriers* Limited Sharing, Priority and Lack of awareness and knowledge should receive some attention and could be important.

The low segment consists of six elements of which three are never or only once mentioned. The three mentioned elements are Commitment, Communication, and Group size. The *Barrier* Communication is only mentioned by few participants and is held in low regard. The *Barriers* Commitment and Group size both have one high ranking meaning that one participant deemed it very important. The individual rankings of these two *Barriers* suggest that most participant do not notice (the importance of) these *Barriers*, except for one. Therefore, it is not important.

4.4 Summary and conclusions of the analysis phase

This section summarizes and concludes the results presented in sections 4.1-4.3. Every section will be discussed individually in order to gain a clear overview of the gained insights. This section will end by combining all insights from the previous sections to describe critical nodes and conditions for the second part of this research.

4.4.1 Case analysis

The Rotterdam port area is part of the vital infrastructure of the Netherlands. This makes cyber security a high priority. Public organizations in Rotterdam started addressing this theme several years ago and in turn co-founded FERM. FERM is a public private partnership focused on 1) raising awareness on cyber security and 2) becoming a platform for collaboration on cyber security. Companies in the Rotterdam port area admit that FERM has raised awareness on cyber security, although they have not been activated to collaborate. However, companies are interested in collaboration, especially when the focus is on information exchange and gaining insight in each other's security. The nature of FERM's past activities confirm this.

The network of the Rotterdam port area is complex and consists of many formal and informal networks. It is also characterized by low hierarchy and high connectivity. The partners of FERM do not possess the necessary resources to force companies. This makes the network difficult to manage with classical instruments and therefore focus must be put on social network management strategies.

It can be concluded that FERM has succeeded in raising awareness, but the results when it comes to becoming a collaboration platform remain limited. The limited results do not mean that there is no room for development. Companies show interest for collaboration on information exchange and therefore this could be a proper starting point for future collaborations. Network management strategies can support the initiation of these collaboration.

4.4.2 Theory

An examination of the scientific literature provided a set of 5 *Goals*, 13 *Drivers* and 8 *Barriers* for CoPs respectively explained in Table 4-3, Table 4-4 and Table 4-5. This list is not deemed exhaustive, but provides a strong basis due to the structured approach of the systematic review. The most cited *Goal* is Knowledge management: the efficient and effective sharing, exchange, capture and creation of both tacit and explicit knowledge between people within and between organizations. This *Goal* encompasses several dimensions, such as sharing information, learning, increasing knowledge, containing knowledge, or innovating. The literature is less conclusive on these dimensions even though the different dimensions provide other directions for a CoP. It can be concluded that Knowledge management is a common goal for CoP, but that a choice must be made about the dimension of Knowledge management. The dimensions of Knowledge management could also be an interesting point for further research into CoPs.

The three *Drivers* cited most often are: Culture, Management, and Social. The *Driver* Culture is the atmosphere with shared values that enables the working of a CoP, shapes the members by teaching them the social norms, and creates an identity. The *Driver* Management concerns the visible support of (higher) management layers to the CoP, e.g. by providing resources and time for its members. Social refers to the personal relationships and connections between members.

Literature also indicated that several *Drivers* could be connected to each other. Culture, Social, Trust, Shared Goals, and Commitment share connections, and influence each other greatly. The reviewed literature in this research is not conclusive on these connections. It can therefore be a starting point for new research to understand the underlying mechanics of these connections. However, it is clear that these *Drivers* influence each other. It can be concluded that the group and social interactions are essential to create a CoP and require attention. The support of management also needs to be managed properly, but the focus should be the group dynamics.

The most cited *Barriers* are Culture and Management. These *Barriers* are the opposites of two important *Drivers*; however, this does not prove that every *Barrier* is a *Driver* or vice versa. It does show that there is a delicate balance in elements to be positive or negative and that the consequences affect the CoP strongly. It can be concluded that this puts extra emphasis on the social dynamics.

4.4.3 Practice

The participants of the interviews recognize several elements, but some *Drivers* and *Barriers* are barely or never mentioned. This suggest that these are either not recognized as important or are less important. No conclusion regarding this matter can be made based on these interviews as it should be validated with more interviews. Participants also mentioned several new elements: 2 *Goals*, 8 *Drivers*, and 6 *Barriers*. The most mentioned new *Drivers* are Awareness & Urgency, referring to the need to be aware of the subject itself as well as understand the need to deal with it immediately, and Direct relevance, meaning that topics discussed or the aims of the CoP must connect to current and relatable issues faced by organizations. The most mentioned *Barrier* is Mutual differences that highlights that differences between companies (i.e. size or branch) hinders them to effectively exchange information and knowledge. These new elements were not directly found in the current literature review, therefore providing opportunity for new research. A new literature search and/or more empirical methods can be used to validate and research these new elements.

The prioritization shown in Table 4-7, Table 4-8 and Table 4-9 provide insights in the elements participants prioritize when setting up a collaboration. The *Goal* Knowledge management is shared by all and got the highest ranking. Therefore, the conclusion can be that participants believe that the *Goal* Knowledge management is a proper starting point and aim for a CoP with FERM.

The *Drivers* with the highest priority ranking are Social and Trust and are followed by the group Culture, Facilitator & Leadership, Management, Awareness & Urgency, and Direct relevance. This shows that participants believe that the social dynamics between people are most important and that practical manners, such as the organization of events and the support of higher management, should not be neglected. It also suggests that incentives due to awareness or relevance help to promote collaboration in the Rotterdam port area.

The *Barriers* with the highest priority ranking are Culture, Trust & Social relations. These are the counterparts of the highest ranked *Drivers*. This means that the balance between these elements is recognized by the participants. It also puts extra focus on getting the balance right when setting up a collaboration. The social process has the highest priority to drive collaboration and to prevent barriers.

4.4.4 Connecting insights

The insights of the individual results can be connected in order to gain a holistic view. The connection of the results provides a more detailed and more robust view on the case. This will help to determine a critical node and useful conditions.

The *Goal* Knowledge management reoccurs in all three sections in a positive manner. Scientific literature suggests that knowledge management is the most common goal for a CoP. All interview participants note that knowledge management is important. The case analysis showed that FERM and the companies desire knowledge management. This makes knowledge management on cyber security a shared goal for the actors in the Rotterdam port area.

In the theory it is also noted that this *Goal*, knowledge management, has multiple dimensions that provide different directions to a CoP. The case analysis showed and the interviews suggested, that information sharing and insight in each other were preferred directions for companies. This information suggests that it is most beneficial to aim for knowledge management with a focus on information sharing. However, to demand the goal of knowledge management will not likely provide fruitful results due to the complexity of the network. The process becomes the focus in network settings so that decisions are taken through dialogue and negotiation (De Bruijn & Heuvelhof, 2008, p. 4). This puts extra focus on the social dynamics and dictates that the group makes all the decisions.

The scientific literature showed that the *Drivers* Culture, Management, and Social as well as the *Barriers* Culture and Management are important. This was confirmed by participants in interviews that also prioritized the *Drivers* Social, Trust, Culture, Facilitator & Leadership, Management, Awareness & Urgency, and Direct relevance and *Barriers* Culture, Trust & Social relations. These results show that theory and practice align on the importance of these *Drivers* and *Barriers*.

The results regarding the prioritization of the elements can be split in two groups: social dynamics and practical conditions. The group social dynamics encompasses the *Drivers* Culture, Social, Trust and that Barriers Culture, Trust & Social relations. These *Drivers* and *Barriers* all relate to the feelings of the participants and the interaction with each other and in the group. All these elements are difficult to control or direct and are dependent on the participants. The group conditions present the *Drivers* Management Facilitator & Leadership, Awareness & Urgency, and Direct relevance and the *Barrier* Management. These *Drivers* and *Barrier* represent elements that need to be in place for participants to collaborate in a CoP or help to activate them. They range from practical matters to context or perception. This means that some of these matters can be controlled.

The groups have a different degree of control as well as a difference of importance. Social dynamics are hard to control, while there is more control over the conditions. The importance of these groups can be based on the connections of the results. Theory and practice both prioritize the group social dynamics, since these elements are cited most often and prioritized by the interview participants. The case analysis and the interviews also showed that the actors of the Rotterdam port area value personal connections. On the other hand, the group practical conditions are cited less and prioritized lower than the elements in the social dynamics group. This group is also more controllable. It is concluded from these observations and facts that the importance of social dynamics is higher than of the practical conditions, but that both should be taken into account for a strategy.

4.4.5 Critical node and conditions

The insight of previous sections provides the arguments why social dynamics is a critical node of this case. Firstly, the elements of this group reoccur often in scientific literature where they are deemed important. Secondly, the interview participants prioritized the social dynamics elements above the other elements. Thirdly, the case analysis showed the complex nature of the network and the need for decision making through dialogue and negation. This puts emphasis on the social dynamics of the group. Lastly, this group is difficult to control from the outside, since it is created between people.

The formal defection of critical node social dynamics is defined as: "*the interaction between the members that binds and holds them together*". This definition contains the essence of the supporting *Drivers* Culture, Social, and Trust, as well as the *Barriers* Culture and Trust & Social relations. Since these *Drivers* and *Barriers* are each other's counterpart, the elements Culture, Social, and Trust are deemed as supporting element that require the attention of the critical node. Conditions can be defined for these elements.

The practical conditions in the second group are all very suited for conditions, since this group contains elements focused on the facilitation. The underlying *Drivers* of this group are Management, Facilitator & Leadership, Awareness & Urgency, and Direct Relevance. The underlying *Barrier* is Management. These elements are more controllable and thus better set as conditions. The elements are deemed important, but not as much as the social dynamics.

All conditions can be determined based on the elements. Table 4-10 provides an overview of all the conditions. Every condition is named after an element and is enumerated with a corresponding definition.

Table 4-10: List of all conditions

Condition name	**Conditions and definitions**
Culture	C1. Similar ideas, customs and social behavior should be created together and agreed on.
Social	S1. There must be a mix of group meetings and individual meetings.
	S2. Members must be encouraged to meet each other, but individual meetings should also be arranged if deemed necessary by a third party (the facilitator).
Trust	T1. Trust building exercises should be organized.
	T2. Trust and the sense of safety should regularly be discussed in the group.
	T3. Trust building and maintenance is a priority in the CoP.
Management	M1. Management must be activated from the start for every actor.
	M2. Actors must be assisted in convincing their management.
Facilitator & Leadership	FL1. The CoP must have a person that is responsible for the daily needs, a facilitator.
	FL2. The facilitator of the CoP should organize events and keep in touch with the members.
	FL3. The facilitator leads the process, but the participants make the strategic and practical decisions concerning the CoP.
	FL4. There are reoccurring moments for decision making by the participants of the CoP.
Awareness & Urgency	AU1. The facilitator should regularly talk to participants to check the value that is added.
	AU2. Results should be communicated clearly and distinctly to the participants.
	AU3. Information about incidents and prospects in similar groups should be reported to the CoP.
	AU4. Incidents or troubles of participants need to discussed.
Direct relevance	DR1. Topics discussed in the CoP must hold direct value for its members. This must be checked with every event and should be reflected on.
	DR2. The relevance must be measured and reflected on after each event in the form of feedback.
	DR3. Feedback must be documented and used for future events.

5. DESIGN PHASE

This chapter encompasses the results of the design phase of this research. These results are connected to the Develop and Deliver phase of the Double Diamond model as shown in Figure 5-1. The aim of the design phase is to fulfill the research objective and to answer the main research question:

How could a Community of Practice on cyber security be established?

The insights gained from the different analyses in chapter 4 are used to focus the design process. The critical node and the conditions, determined in section 4.4.5, limit the space of solutions and offer concrete challenges to solve. Solutions will be sought through a combination of sub questions 3 and 4:

3) *How do current cyber security collaboration formats solve the critical factors for the establishment of a Community of Practice on cyber security?*
4) *How could the critical factors for the establishment of a Community of Practice on cyber security be resolved?*

The third sub question provides theoretical insights by a narrative review. This method shows existing concepts, sub solutions for the conditions, and promising strategies and structures. A brainstorm is used to add empirical insights. The results of the narrative review and the brainstorm are combined in a morphological chart in order to answer the fourth sub question.

The next step is to make a prioritization of the elements and sub solutions based on the feedback of an expert. By combining these insights with the results of the narrative review and the brainstorm, the researcher is able to design a concept solution. This concept solution answers the main research question.

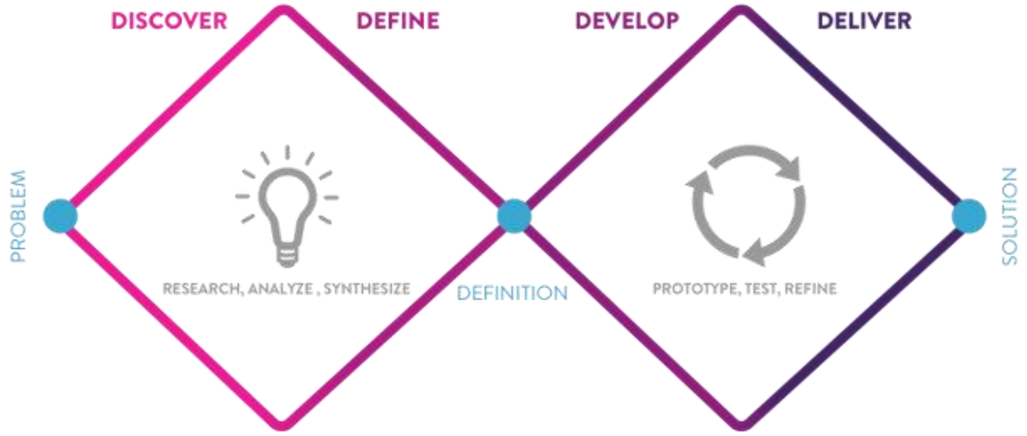

Figure 5-1: Double diamand

Section 5.1 elaborates on the theoretical insights gained from the narrative review. This will be a summarized version of the results. A summary of the narrative review can be found in appendix O. A selection of results of the brainstorm is presented in 5.2. The complete set of sub solutions gained by the narrative review and the brainstorm is presented in appendix P. Section 5.3 provides an overview of the expert feedback. This chapter continues with a reduced version of the morphological chart and a selection of the basic elements for the concept solution in section 5.4. The final section of this chapter presents the concept solution.

5.1 THEORETICAL SOLUTIONS

This section elaborates on the solutions that were found in articles on current cyber security collaboration formats. The set of literature as presented in section 3.3.6 provided several interesting insights that could provide solutions for the challenge of the FERM case. A complete summary of the insights gained from the narrative review can be found in appendix O. These insights can be separated in two sections. Section 5.1.1 mentions all existing concepts found in the available literature. The most relevant concepts will be explained briefly and their relevance will be reflected on. An explanation on all concepts can be found in appendix O.1. Section 5.1.2 is concerned with the sub solutions literature provides. First the most relevant sub solutions for the conditions will be presented. An overview of all sub solutions for the conditions can be found in appendix P.1. These sub solutions are based on possible strategies and structures as well as the practical tips and recommendation found in literature. An overview of possible strategies and structures can be found in appendix O.2. An overview of the practical tips and recommendation can be found in appendix O.3. Next, the strategies for the most relevant existing concepts will be explained. An explanation on all promising strategies and structures can be found in appendix P.2.

5.1.1 Existing Concepts

In the literature, several concepts were found that could be useful for this case. The concepts are:

- the Information Sharing and Analysis Centre, abbreviated as ISAC
- the Computer Emergency Response Team, abbreviated as CERT
- the Computer Security Incident Response Team, abbreviated as CSIRT
- the Warning, Advice and Reporting Points, abbreviated as WARP
- the Abuse Team
- the CoP
- the distributed CoP,
- the community-based knowledge initiative
- the supply chain collaboration
- the regional collaboration
- the Public-Private Partnership, abbreviated as PPP.

These concepts could be used as a solution on their own or as a source of inspiration. A more detailed explanation of all the concepts can be found in appendix O.1.

Several of these concepts provide a better example or greater source of inspiration for this case. These concepts are the WARP and ISAC, the CoP and SCIRT, and the collaboration models of supply chain and a regional ecosystem.

The WARP and ISAC are interesting, since they provide an ideal starting point in the FERM case. Section 4.4.4 showed that knowledge management with a focus on information sharing is the most appropriate goal. These two concepts focus heavily on the sharing of information in order to improve the cyber security of the members. Trust and social connections are a central part of this process. This connects well with the critical node. Furthermore, these concepts can provide the foundation to make a step to more expansive form of collaboration, such as the CoP or a SCIRT.

A CoP and the SCIRT are concepts that encompass more responsibilities and tasks in their final form and find a similar start, compared with a WARP and ISAC. Both a CoP and an ISAC focus on other dimensions of knowledge management such as knowledge exchange or knowledge creation. They can also perform more operational or supportive services and activities. This requires a more complex form of collaboration.

The collaboration models of supply chain or a regional ecosystem are interesting concepts, since they focus on a more strategical level and support organizations. The PoR case holds a multitude of organizations, all active in the same supply chain and in the same region. These collaboration models provide ways to create more strategical connections between organizations. These models can also be supported by other concepts for more operational services, such as the SCIRT or CoP.

5.1.2 Sub solutions found in literature

The literature presents advice to create collaborations. Part of this advice can be directly linked to the conditions to establish sub solutions. However, the literature also provides strategies and structures for collaboration that provide a framework for the collaboration. This section starts with the most relevant sub solutions for every condition. An overview of all sub solutions for every condition is presented in appendix P.1. The section continues with an explanation on the strategies connected to the concepts ISAC and CoP, since these were deemed most relevant in section 5.1.1. An explanation on all promising concepts is presented in appendix P.2. This section ends with an overview of the most interesting structures. An explanation on all structures can be found in appendix P.2 as well.

Most relevant sub solutions for every condition

An overview of the most relevant sub solutions is presented in order of the conditions. The advice for every condition is summarized. An overview of all sub solutions with their reference can be found in appendix P.1. No advices were found for conditions T3 and FL4, so no sub solutions are listed for these two conditions.

C1. Similar ideas, customs and social behavior should be created together and agreed on.

The consensus in literature is that the initial phase is the most important moment to create this. This can be done through discussion and dialogue in order to reach a consensus, while also connecting the members and building trust.

S1. There must be a mix of group meetings and individual meetings.

Some suggestions for a type of meetings are: launching event, community building events, renewal workshop, and fieldtrips. It is advised to make a meeting structure and to have public events with informal moments for networking.

S2. Members must be encouraged to meet each other, but individual meetings should also be arranged if deemed necessary by a third party.

The literature suggest that a facilitator is very useful to fulfill this condition.

T1. Trust building exercises should be organized.

The literature suggests certain legal forms, such as a Code of Conduct (CoC), since they help to build trust.

T2. Trust and the sense of safety should regularly be discussed in the group.

Agreements as a CoC can serve as a conversation starter to discuss trust and safety, but a facilitator is very important.

T3. Trust building and maintenance is a priority in the CoP.

M1. Management must be activated from the start for every actor.
Literature suggest to start convincing and involving (senior) management soon after the initiating phase as it allows for support and recognition.

M2. Actors must be assisted in convincing their management.
The facilitator has a critical role in establishing a clear communication channel for management. Another suggestion is the use of a business plan as a format to convince management.

FL1. The CoP must have a person that is responsible for the daily needs, a facilitator.
Literature supports this condition and suggest to establish this function as soon as possible.

FL2. The facilitator of the CoP should organize events and keep in touch with the members.
Certain tasks for the facilitator are listed in literature: ensuring attendance, connecting core members, and organization events.

FL3. The facilitator leads the process, but the participants make the strategic and practical decisions concerning the CoP.
There should be a validation of ideas within a large group to broaden support. A decision-making structure should be developed as well.

FL4. There are reoccurring moments for decision making by the participants of the CoP.

AU1. The facilitator should regularly talk to participants to check the value that is added.
There should be continuous focus on value as it provides opportunities to further improve the CoP.

AU2. Results should be communicated clearly and distinctly to the participants.
It is suggested to have a process where steps are developed, performed and monitored. Another option is to collect success stories and save these in a knowledge repository.

AU3. Information about incidents and prospects in similar groups should be reported to the CoP.
Information sharing is believed to be a basic capability of an ISAC. This is usually formalized with an agreement.

AU4. Incidents or troubles of participants need to discussed.
Information sharing is believed to be a basic capability of an ISAC. This is usually formalized with an agreement.

DR1. Topics discussed in the CoP must hold direct value for its members. This must be checked with every event and should be reflected on.
Dialogue between members is important to understand of each other what is needed and to evaluate past activities.

DR2. The relevance must be measured and reflected on after each event in the form of feedback.
It is suggested to set goals or to determine steps after which you perform, monitor, and reflect on their value. This is a result that should be produced in order reflect on the activities.

DR3. Feedback must be documented and used for future events.
A focus point is to document steps and processes in order to make them available. This can be done with a knowledge repository.

Most relevant strategies

Section 5.1.1 noted several promising concepts: ISAC, WARP, CSIRT, CoP, supply chain collaboration, and regional collaboration. Obviously, the CoP concept is very relevant, since this is the research aim. The ISAC and CSIRTconcept is also very relevant, since they have become the current international standard for collaboration on cyber security.

The WARP and the collaboration models of supply chain and regional ecosystem are less relevant. The WARP concept is a UK-based format that started around 2000, however there is little recent literature on this concept. The collaboration models of supply chain and regional ecosystem have a more strategic outlook which makes them less relevant for the aim of this research. Appendix P.2 provides insights in the strategies of these three concepts.

CoP

The book of Wenger et al. (2002) determines five stages of community development. Every CoP starts with a *Potential* phase where an existing social network flocks together around a shared subject or need. The primary intent of the community is established and members are connected. This stage is followed by the *Coalescing* stage where the CoP is officially launched and the trust and relations between members are solidified. The CoP is nurtured to grow and gain value in this phase. The third stage is the *Maturing*. The CoP is re-examined and the focus, role and boundaries are aligned. The CoP can now become part of an organization. The next stage is *Stewardship* where momentum needs to be sustained while members can shift. Usually the CoP needs to be rejuvenated in this stage. The final stage is *Transformation* where it either fades away, dies by turning in social club, splits or merges, or becomes institutionalized.

ISAC

Two strategies were mentioned for the creation of an ISAC. The Dutch NCSC recommends to set up an ISAC in three phases: *Explore, Build*, and *Continue* (NCSC, 2018d). The *Explore* phase focuses on finding like-minded parties and trying to reach a consensus about the collaboration. This is followed by the *Build* phase where the ISAC is started officially. The focus shifts to building trust, setting up the governance model, and establishing an effective meeting structure. The final phase *Continue* aims to maintain and expand the level of trust while increasing the value of every meeting. New members can also enter during this phase.

ENISA recommends a formation process centering on the initial phase (ENISA, 2017a). Three parts need to be considered in this phase. The first part is the rationale for creation: why and in which area is the ISAC started? The second part is the driving force of the ISAC. The final part is the consideration of the motivation for possible participants to join. This is directly linked to what value the ISAC provides for its participants.

CSIRT

Two strategies are also recommended for the CSIRT. The Dutch NCSC advises three phases (NCSC, 2018a). The *Explore* phase centers on creating support and seek consensus. Possible partners and an initial workgroup need to be established in this phase. The *Consensus* phase aims to solidify the consensus by defining the mandate, the services and the activities of the CSIRT. The final phase *Grow* is about increasing the capabilities of the CSIRT in order to provide more value to its members.

ENISA presents a different approach (ENISA, 2006a). The first step is to determine the type of CSIRT. They provide a list of nine types. The most promising types for this case are the *Commercial CSIRT* and the *Critical Infrastructure Protection CSIRT* (CIP-CSIRT). The following step is selecting the services within four categories: reactive, proactive, artifact handling, and security quality management. An overview of possible services is presented in this document as well. The third step is to define the CSIRT with a business plan containing organizational structure, a financial model, and a sharing policy. This step is followed by the creation of a business case that can be used to convince organizations. The final step is training the members of the CSIRT in order to make it operational.

Most relevant structures

Several sources in the narrative review complemented each other on a specific topic. This could easily be connected and made into a structured overview of options. These structures can be helpful for the case as they address important aspects of a collaboration. The found structures are: dimensions of a CoP, the business case, building trust, funding mechanisms, and governance model.

The most relevant structures are the business case, building trust and the funding mechanisms. The business case is strongly connected to the condition on Management. The Building trust structure is connected to the critical node. The funding mechanism is deemed relevant, since it was a reoccurring item in the found literature. The structures dimensions of the CoP and the governance model are explained in appendix P.2.

The business case

A business case can be used to reach and convince higher management. Therefore, the business case can help to fulfill the conditions concerning Management. The British NISCC and the Dutch NCSC provide advice for the content of a business case. NISCC advises five stages in making a WARP business case (NISCC, 2006). First, the community needs to be identified. Second, the benefits of a WARP for this community needs to be identified. Third, the resources and costs of the WARP need to be determined. Fourth, the funding for these resources and costs needs to be identified. When all these components are clear, the last stage of writing the business case can commence.

The NCSC advises to incorporate three parts in the business case. The first part is fitting the initiative in the current organizational strategy. The second is determining the possible stakeholders of this initiative. The last part is addressing the issues combined with an initial impression of a possible solution.

Building trust

Section 4.4 is clear on the role trust plays in setting up a collaboration. Several models to build trust are presented in literature. A first mode is the use of bilateral and multilateral agreements (ENISA, 2006b) or a NDA (ENISA, 2014). A second mode is through a monetary contribution (ENISA, 2014) or sponsorship (ENISA, 2006b, 2014). A third mode is the use of trusted introduce (ENISA, 2006b, 2014). This mode involves current members to recommend, and guide new members in order to increase the members of the collaboration. A fourth mode is the creation of a Code of Conduct to ensure a baseline for the interaction between members (ENISA, 2006b).

Funding mechanisms

Funding is a reoccurring theme in the literature of the narrative review. Several options are listed for the funding of a collaboration:

- Commercially funded through a mandatory fee or membership subscription (based on size and involvement) (ENISA, 2017a; NISCC, 2002, 2006)
- A voluntary contribution (ENISA, 2017a)

- Government subsidies or sponsorship (rare option, private sector is usually responsible) (ENISA, 2017a; NISCC, 2006)
- Corporate funding as an internal project (NISCC, 2002, 2006)
- Customer service provided by large organizations to its existing customers. (NISCC, 2002)
- Public-private (partnership) (NISCC, 2002, 2006)
- Cooperative funded by all members paying a subscription which pays the WARP's activities and services (NISCC, 2002, 2006).

5.2 Brainstorm for solutions

The most relevant results of three rounds of brainstorm are presented in this section. The results are based on the three perspectives of the brainstorm *Experience, Intuition*, and *Creativity* as explained in section 3.3.7. The results are summarized for every condition.

C1. Similar ideas, customs and social behavior should be created together and agreed on.

The focus should be on individual meetings with limited participants. This usually makes it easier to reach a consensus and to build trust and connection. A twist can be given to these meetings by organizing speed dating between (potential) partners in order to connect them more and to break traditional structures.

S1. There must be a mix of group meetings and individual meetings.

A meeting organizer can support this mix and monitor it. He can organize meetings that combine team building activities and individual meetings. It could be interesting or refreshing to use a game format, such as the Virtues Cards (Deugdenkaarten) by Linda Kavelin Popov, or the 'Ontdekkaarten', by Hanneke Middelburg, for the first individual meetings to break the ice.

S2. Members must be encouraged to meet each other, but individual meetings should also be arranged if deemed necessary by a third party (the facilitator).

Dedicating moments in collective meetings to individual contact can work encouraging based on intuition. It could help to set simple ground rules for the meetings in order to help create interaction.

T1. Trust building exercises should be organized.

These exercises should be un-conventional for optimal bonding.

T2. Trust and the sense of safety should regularly be discussed in the group.

This should be a reoccurring agenda item for every meeting. A creative idea is to dedicate moments for every member's feelings.

T3. Trust building and maintenance is a priority in the CoP.

Someone should have a dedicated role to guard the discussion regarding trust.

M1. Management must be activated from the start for every actor.

There is some general information that every management team should know, so this should be collective in a designed package.

M2. Actors must be assisted in convincing their management.

An intuitive believe is that practice makes perfect, therefore a practical workshop should be organized to train members.

FL1. The CoP must have a person that is responsible for the daily needs, a facilitator.
A third party can provide a sense of neutrality and objectivity.

FL2. The facilitator of the CoP should organize events and keep in touch with the members.
It can be hard for one person to organize the events and to keep a personal connection with all members. The facilitator should have at least someone supporting him, preferably one or more members.

FL3. The facilitator leads the process, but the participants make the strategic and practical decisions concerning the CoP.

FL4. There are reoccurring moments for decision making by the participants of the CoP.
There should be dedicated moments for decision making.

AU1. The facilitator should regularly talk to participants to check the value that is added.
A standardized format can help to check it consistently. Added value should also be one of the main results measured by the members.

AU2. Results should be communicated clearly and distinctly to the participants.
A bullet-list provides a strong overview of the simple results.

AU3. Information about incidents and prospects in similar groups should be reported to the CoP.
The facilitator can play a central role in addressing incidents, but could also act as a central connector with all groups. He can consider the relevance of certain information before sharing it.

AU4. Incidents or troubles of participants need to discussed.
Legal documents are often used to secure confidentiality.

DR1. Topics discussed in the CoP must hold direct value for its members. This must be checked with every event and should be reflected on.
The facilitator can play a central role in finding information and knowledge. This can be done using the combination of a questionnaire with follow-up phone calls.

DR2. The relevance must be measured and reflected on after each event in the form of feedback.
The SMART-format is commonly used to make, measure and reflect on goals.

DR3. Feedback must be documented and used for future events.
Experience shows that short documents in a fixed format provide an excellent guideline to document consistently.

5.3 Expert feedback

This section presents an overview of the most important feedback from the expert. This overview of feedback prioritized elements for the concept solution. A complete summary of the interview can be found in appendix S.

5.3.1 Most important general feedback

The expert noted that the ISAC and PPPs models are currently often used. These collaborations between organizations usually arise when the organizations face the same challenges due to similar systems, similar processes and similar company profiles. He believes that only then collaboration could help organization evolve. It is noted that there is no consensus on how communities for cyber security should be started. Sometimes, it happens voluntary, but sometimes it is demanded by a third party.

An important success factor is a catalytic facilitator. The expert believes that this person leads the group, is the point of contact, and performs the administrative tasks. These tasks should be divided in a later stage over several people.

The expert believes that trust is crucial, but remains unclear on how to build it. It is mentioned that trust is a process that requires time, and thus several phases. The NCTV's advice is, to make agreements regarding information sharing, finding, and capturing, to have small groups, and to keep participants equal, is referred to.

5.3.2 Most important feedback on Phase 1

The expert noted that the start of the collaboration should always be an open dialogue between all involved parties in order to search for a shared challenge. This dialogue contributes to the trust and connection between parties. The facilitator leads the process and should stimulate networking and building the group during this phase.

5.3.3 Most important feedback on Phase 2

The expert believes that the members should make their participation official and become more involved in the facilitation. The most important task of the facilitator shifts to gathering interesting discussion subjects as well as performing researching and writing services.

The expert stresses involvement of higher management in this phase. The added value needs to become clear to higher management. The facilitator can help in the communication to higher management by making reports that can be shared.

The experts noted that by the end of this phase the participants take full responsibility. They need to create their own financing model and action plan for the future.

5.3.4 Most important feedback on Phase 3

During the interview, it is assumed that the members want to continue with the CoP. The expert believes that a large organization should take a leading position. He also notes that a new and common challenge is attracting new members, however in most cases the groups become too big. The expert notes that groups with more than 30 members usually interact less and do not function as a community any longer.

5.4 MORPHOLOGICAL CHART

5.4.1 Overview of relevant sub solutions

The morphological chart provides an overview of all sub solutions from the narrative review and the brainstorm. The complete morphological chart is omitted here due to the sheer size of the chart (a table of 13 A4 pages), yet is presented in appendix Q. A reduced version of the morphological chart is presented in Table 5-1. The elements of this table are the most relevant elements as presented in section 5.1.2 and 5.2. The table consists of three columns. The first column shows the challenges that need to be solved, which are for this research the strategies, structures and the conditions. The second column contains the solutions gained from the brainstorm. The third column contain the solutions gained from the narrative review. The expert feedback and the intuition and creativity of the researcher are used to choose and connect sub solutions in order to establish the basis of the concept solution.

Table 5-1: Reduced version of morphological chart

Challenge	Brainstorm	Narrative review
Strategies		- ISAC - CoP - SCIRT
Structures		- business case - funding mechanism - building trust
C1. Similar ideas, customs and social behavior should be created together and agreed on.	- meetings with limited participants - speed dating event	- establish in initial phase - use discussion and dialogue
S1. There must be a mix of group meetings and individual meetings.	- meeting organizer is key to organize and monitor this - use a game format	- have meeting structure - public events with informal networking
S2. Members must be encouraged to meet each other, but individual meetings should also be arranged if deemed necessary by a third party (the facilitator).	- dedicated moments for individual contact - set ground rules	Have a facilitator
T1. Trust building exercises should be organized.	be un-conventional	certain legal forms. e.g. CoC
T2. Trust and the sense of safety should regularly be discussed in the group.	- reoccurring agenda item - dedicated moments for every member's feelings.	- use CoC as a conversation starter - have a facilitator
T3. Trust building and maintenance is a priority in the CoP.	facilitator guards the discussion regarding trust.	
M1. Management must be activated from the start for every actor.	collective information package	start with management soon after initiation
M2. Actors must be assisted in convincing their management.	train members in a workshop	- the facilitator establishes a clear communication channel for management. - use of a business plan
FL1. The CoP must have a person that is responsible for the daily needs, a facilitator.	have third party do it	- as soon as possible
FL2. The facilitator of the CoP should organize events and keep in touch with the members.	have people support the facilitator	possible tasks: ensuring attendance, connecting core members, and organization events.
FL3. The facilitator leads the process, but the participants make the strategic and practical decisions concerning the CoP.		- validation of ideas within a large group - have a decision-making structure
FL4. There are reoccurring moments for decision making by the participants of the CoP.	dedicated moments for decision making.	

AU1. The facilitator should regularly talk to participants to check the value that is added.	- have a standardized measuring format - make it a main result	continuous focus on value
AU2. Results should be communicated clearly and distinctly to the participants.	use a bullet-list	- use a process where steps are developed, performed and monitored. - collect success stories
AU3. Information about incidents and prospects in similar groups should be reported to the CoP.	facilitator can address incidents and connect it to members	formalize information sharing with an agreement
AU4. Incidents or troubles of participants need to discussed.	use legal documents to secure confidentiality	formalize information sharing with an agreement
DR1. Topics discussed in the CoP must hold direct value for its members. This must be checked with every event and should be reflected on.	- use the facilitator - use questionnaires and follow-up phone calls to gather insights	have dialogue between members
DR2. The relevance must be measured and reflected on after each event in the form of feedback.	use the SMART-format	set goals or steps and perform, monitor, and reflect on their value.
DR3. Feedback must be documented and used for future events.	use short documents in a fixed format	- focus on documenting steps and processes - store it in a knowledge repository.

5.4.2 Basic elements for the concept solution

The concept solution has the form of a strategy for establishing a CoP on cyber security. The strategy will be based on the strategies of the ISAC, CSIRT and CoP. It will contain three phases: a first phase that explores and prepares, a second phase that launches the collaboration, and a third phase that strengthens the collaboration. The critical node presented in section 4.4.5 are combined with the aims and focus points presented in the strategies for the ISAC, CSIRT and CoP in order to establish the aims and focus point of each phase.

The facilitator plays a crucial role, since it is involved as a solution for conditions S2, T2, T3, M2, AU3 and DR1. The conditions FL1-Fl4 also suggest so this is an important task. This suggest that a facilitator should be chosen prior to the start of the first phase.

The critical node is represented by conditions C1-T3. They will remain important for the entire strategy, but should be established firmly early on as suggested by literature for condition C1. Therefore, the focus point of the first phase is the critical node social dynamics and the sub solutions presented for C1-T3 can be used here.

Sub solutions for S2, T2 and T3 suggest dedicated reoccurring moments to discuss feelings and trust. These sub solutions can be combined for a single moment during every meeting, since they all aim to connect members on a personal level.

The sub solutions for S2, T1, AU1-4, DR1-3 and the structure Building trust suggest the use of some form of formalized agreements. Agreements can create clarity that in turn can build trust, create goals to achieve, and set concrete points for reflection and discussion. An agreement can be made about the topics and focus points of the group as suggest in AU1-4 and DR1. Another agreement can also a

CoC that formalizes the actions and rules for interaction between the members as suggested by S2, T2, and AU3-4. Both agreements can be used to monitor and reflect the value of the CoP and to establish results of the CoP as suggested by AU2 and DR2-3. These agreements should therefore be formatted in a manner that allows this, such as the SMART format.

The sub solutions of conditions M1-2 should be implemented from the second phase onwards. The sub solutions shown are all focused on communication and how this should be done. These should be implemented.

5.5 Concept solution

The results of section 5.1-5.3 were used to create the concept solution that will be presented in this section. The concept solution provides an answer to the main research question:

How could a Community of Practice on cyber security be established?

The context for this concept solution is based on the context of the FERM as explained in section 3.2.3 and appendix C, and the overall cyber security context as explained in chapter 1 and appendix A. This context is that the overall challenge of organizations has to become more cyber resilient. The sharing of information and exchange of knowledge is considered a vital part to achieve cyber resilience. The establishment of CoPs or other collaborative concepts are the practical consequence to achieve this sharing and exchange. The concept solution has the form of a strategy for establishing a CoP on cyber security.

This section starts with an overview of the strategy. The phases of the strategy will be explained by elaborating on the aim and focus point of each phase. Next, a more detailed account of each phase is presented. Individual actions are presented along with their underlying reasoning and considerations.

5.5.1 Overview of the strategy

The central aim of the strategy is to establish a CoP where information, experience and knowledge can be shared in order to increase the cyber resilience of the members. The focus points of this strategy are set by the critical node and the conditions described in section 4.4.5. The highest priority is given to the critical node social dynamics: *the interaction between the members that binds and holds them together*. This priority was given not only because of the conclusions from the analyses, but also as a result of the solutions found in the narrative review as well as the feedback of the expert.

The strategy consists of one informal and internal phase named ***Phase 0 Initiation*** and three formal phases **1) *Exploration***, **2) *Dedication***, and **3) *Continuation***.

Initiation has the purpose of preparation for the start of the strategy. It is noted as phase 0, since it is not officially part of the strategy to establish a CoP, yet it is important for the overall strategy. The aim of this phase is to acquire the basic requirements to start the strategy. These requirements are basically an initiating organization, a facilitator, and an initial analysis. An organization has to stand up and initiate the establishment of the CoP. It has to commit some resources as well set some requirements and wishes. A leading facilitator needs to be picked. The facilitator is responsible for the first and second phase of creating the CoP. The facilitator is a critical component of this strategy as is stressed by the expert as well as in literature.

Exploration is the starting phase of the strategy where potential members are brought together to explore a course of action. The central aim of this phase is to attract, connect and maintain members through social connections and direct relevance. The focus of this phase is thus on the social dynamics of the group. This aim and focus are based on the initial phases of the ISAC, CoP and SCIRT (NCSC, 2018d, 2018a; Wenger et al., 2002). At the end of this phase, the concrete results are a prototype consensus, an overview of needs and interests of all potential members, and a fixed and committed group.

Dedication is a solidifying and maturing phase. The aim of this phase is to formalize agreements and then acting according to these agreements. The main focus point shifts to producing results and having direct relevance while strengthening the social dynamics. A secondary focus point is the involvement of higher management. The concrete results at the end of this phase are a signed consensus, a signed Code of Conduct, an information package for management, and a document package of activities containing a summary, the presentation, and action items.

Continuation is the phase where the group decides whether it wants to renew or end the CoP. It follows that the aim is to make a well-considered decision and to celebrate the successes of the previous phase. The focus point is showing the results of the current CoP and the advantages that it brings. Irrelevant of the outcome of the decision, the specific result of this phase is an overview of the results of this CoP. When it will be decided to continue the CoP, two results are added: a renewed consensus and a renewed Code of Conduct.

5.5.2 Details of the strategy

This section will present the details of the strategy. The aim and focus points of every phase will be linked to actions and meetings that should be performed during that phase.

Phase 0 Initiation

The aim of phase 0 is to acquire the basic requirements to start the strategy. These requirements are the initiating organization, the facilitator, and the initial analysis. The requirement of an initiating organization is impossible to plan, since there needs to be one person within an organization who believes that a CoP is necessary to improve the cyber resilience of its organizations and the organizations around them. An initiating organization for the Rotterdam port area could be FERM, PoR, Deltalinqs or NCSC. These organizations are aware of the CoP concept and its benefits for the port area. Furthermore, the organization have to provide services that improve the overall performance of the Rotterdam port area, and not just their own organization.

When an initiating organization presents itself, it will decide on a facilitator. It will be beneficial to choose a facilitator who has experience in leading groups, has strong social skills, and has knowledge about cyber security. The facilitator and the initiating organization should then perform a few actions.

A0.1 Decide on requirements and boundaries for this strategy

The facilitator and the initiating organization discuss and decide on three topics. First, they need to decide on the kind of group that they will start a CoP for. Second, a general timeline for the first and second phase needs to be discussed and agreed on. Third, they need to discuss the initial funding. The time of the facilitator and the activities need to be funded, so a budget needs to be discussed. This will also influence the timeline. The funding types, as presented in the morphological chart, that could be interesting at this point are: a (governmental) subsidy or sponsorship, or corporate funding as an internal project. Therefore, these three topics should be discussed in parallel.

A0.2 Analysis of the network

The facilitator analyses the network in order to localize potential members. He localizes these members, based on the decision in A0.1 about the kind of group, and on his own insights. The analysis of the network provides the facilitator with an overview of potential members for the CoP.

A0.3 Contacting the potential members

The facilitator connects with a potential member in order to build a bond between the potential member and the facilitator. It is recommended to do this by telephone, because this is usually perceived as more personal. The facilitator can inquire whether the potential member is interested in collaboration on cyber security.

Phase 1 Exploration

Phase 1 focuses on attracting, connecting and maintaining members through social connections and direct relevance. This is achieved through several actions by the facilitator and in two meetings focusing on connecting the potential members, both personal as well as in their needs.

A1.1 Invite potential members for an initial meeting.

The facilitator invites the potential members for a meeting to discuss cyber security and connect with congenial other potential members. Since the potential members have yet to meet each other, the facilitator needs to convince them by focusing on the importance of cyber security for their organization.

M1.1 The initial meeting aimed to connect members and build trust.

The meeting starts with a presentation by the facilitator about cyber risks. The facilitator explains that collaboration is very important in order to learn from each other and to tighten the interlinks between potential parties. The next step is a formal introduction of all participants. This is the first interactive element of the meeting aimed to loosen up the potential members. The third step is a speed dating event between potential members. The speed dating is a fun and unconventional event and provides room for the potential members to talk about personal matters instead of business. This interaction can be stimulated by the use of a game such as cards containing personal questions.

The meeting ends with a check-out exercise aimed to build trust by sharing personal impressions and feelings. The group stands in a circle and every person has one-minute to answer the following questions: How are you feeling now? and How did you experience this meeting? After this, the date for the second meeting can be shortly discussed and set.

A1.2 A follow up email with a small summary of the last meeting.

The facilitator sends a follow up mail to all participants of the first meeting with a small summary of meeting M1.1. The summary should note that the aim of the meeting was to connect members and build trust. It should elaborate that this was achieved through the combination of formal introduction and the speed dating. This is a representation of results. The presentation can be shared as well. The date for the second meeting should also be confirmed in this mail. This action aims to remind the potential members of the meeting and to keep them invested.

A1.3 Determining the needs and interests of the potential members.

Since an initial connection has been made in meeting M1.1, this action aims to leverage that connection to determine the needs and interests of the potential members. The facilitator contacts the potential members in order to link two potential members so they can question each other about their needs and interests for a collaboration on cyber security. The couples email the facilitator with the results of their discussion.

Another possibility to determine the needs and interests is to use a questionnaire. The facilitator can design this questionnaire with a combination of open and multiple-choice questions in order to gain a quick overview. A disadvantage of the questionnaire is that it doesn't leverage the social network. It can be used after the pairing in order to validate the overall results of the pairings.

A1.4 Analysis of the needs and interests

The facilitator collects the needs and interests of all potential members. He can analyse these results to determine common needs and interests. The results of this analysis are made into a presentation.

M1.2 A meeting aimed to create a prototype consensus

The start of the meeting is a check-in aimed to reconnect the personal connection between the potential members. Everybody stands in a circle and individually all make a small remark about how they are currently feeling. Next, the potential members take a seat and the facilitator presents the overall results. The presentation ends with a proposal of topics concerning the interests and needs that could be discussed in order to gain a consensus. Now, the group splits up into small groups of 3-4 to discuss the presentation and the proposed topics. They provide feedback per group in a collective setting. The facilitator asks questions and leads the collective setting supported by a secretary who makes notes of the feedback.

A formal break commences where the potential members can network and talk freely, while the facilitator and the secretary discuss the feedback. They try to make a brief summary and try to form a proposal for a consensus. The break ends, when the facilitator has a summary and feels ready to present this result. The proposal for the consensus is presented by summarizing the main points of feedback. The group of potential members can respond with remarks and additional feedback. The meeting ends with a check-out aimed to end the meeting on a personal touch. The groups stand in a circle and every person has one-minute to answer the following questions: What are the general thoughts on the current proposal? and Who wants to remain involved for future collaboration according to the consensus?

A1.5 Fine tuning the proposed consensus

The facilitator examines the second proposal and the last-minute comments and remarks. The fine tuning can start now by writing the prototype consensus. The protocol consensus notes the focus point of the group: information sharing, knowledge exchange, experience discussion, or something else. Some main topics are noted with a general explanation. It ends with a schedule to execute every topic. The schedule is based on the SMART protocol. This makes it possible to monitor and reflect on the activities of the CoP.

A1.6 A follow up mail with a summary and the prototype consensus

The summary of meeting M1.2 and the protype consensus are send to the attendants of meeting M1.2.

Phase 2 Dedication

Phase 2 aims to formalize agreements and to act according to these agreements. There are two agreements the members need to agree on. The first is the consensus stating the aims and topics the group will pursue. The second is a Code of Conduct. This is a set of engagement rules to formalize some important social interactions. These two agreements will help to build trust and will provide directions for the group. Senior management will also be involved during this phase.

A2.1 Define the group's members

The facilitator selects the definite group members based on the response during meeting M1.2. Potential members who noted they were not interested to continue, should be excluded from the group and thanked for their cooperation until point. The group's members are contacted to announce the selection.

A2.2 Adjustments to the prototype consensus

The facilitator uses three rounds of digital feedback to improve on the prototype consensus. The prototype consensus is adjusted after every round by the facilitator. The final consensus is the version after the rounds of feedback.

A2.3 Invitation to formal kick-off meeting

The facilitator invites the members to a formal kick off meeting. This meeting aims to officially start the collaboration by signing the consensus. The facilitator also announces that the meeting will focus on the Code of Conduct.

M2.1 Kick-off meeting

The start of the meeting is a check-in aimed to reconnect the potential members personally. Everybody stands in a circle and individually they make a small remark about how they are currently feeling. Next, the kick-off is done by signing the consensus. This is a special moment, since it officially creates the CoP. The first discussion topic of this meeting surrounds the Code of Conduct. The facilitator starts off by explaining the concept of a CoC. Members can ask questions about the concept before splitting up in small groups. The members discuss in the group how they expect the group and its members to act and treat each other. Every group should present the results of their discussion to the group. The facilitator collects these results.

A formal break commences where members can discuss freely and network. The facilitator uses this break to summarize the presentation before the break. A small analysis should result in a prototype CoC. This prototype can be presented after the break. The group can discuss this concept collectively and give feedback. The facilitator leads this discussion. The meeting ends with a check-out aimed to end the meeting on a personal note.

A2.4 A follow up mail with signed consensus and prototype CoC

The facilitator sends a follow up mail to all the participants of the kick-off meeting with a small summary of meeting M2.1. The signed consensus is shared as well as the prototype CoC. The facilitator explains that the prototype CoC will be improved in two rounds of digital feedback.

A2.5 Improve the prototype CoC through two rounds of emailing

The facilitator leads the process of digital feedback on the prototype CoC. He updates and improves the CoC based on the feedback. Members are contacted by phone when they are not providing feedback.

M2.2 A meeting aimed to sign the CoC and to hold a discussion about informing senior management

The start of the meeting is a check-in aimed to reconnect the personal connection between the potential members. The CoC is signed by the members after the check-in. The facilitator starts a discussion on how to involve senior management on the results and value of this CoP. The members are split up in groups to discuss their challenges in convincing senior management and how to solve these challenges. All groups present their findings and comment on each other. Now, the facilitator starts a discussion about the information that should be shared with senior management. At the end of the discussion, the facilitator summarizes the most important points of the discussion and comments that he will prepare an information package. The meeting ends with a check-out.

A2.7 Create a concept information package for management and follow up mail with the signed CoC

The facilitator makes a concept for the information package that could be send to management. The business case format is used to structure this information package. The consensus and the CoC are used to provide content and goals of the CoP. This concept is sent to all members together with the summary of meeting M2.2 and the signed CoC.

A2.8 Optimizing the information package

Members can comment on the concept information package, so the facilitator can improve it.

A2.9 Preparation of the first technical presentation and the workshop for management

The consensus provided technical topics that interests the members. The facilitator chooses a subject that is deemed very important and prepares a technical presentation. The format of the presentation is discussed for the CoC. A workshop is also prepared that aims to simulate interaction with management and improve on that. The facilitator could possibly ask help from actors or other professional to prepare and hold this workshop.

M2.3 A meeting with the first technical presentation and a management workshop

The start of the meeting is a check-in aimed to intensify the personal connection between the potential members. The facilitator starts with the first technical presentation according to the preparation. After the presentation, the members can collectively give feedback on the presentation. The facilitator collects this feedback. The second part of the meeting is the workshop on how to interact with management. The meeting ends with a check-out.

A2.10 Follow up mail with the signed CoC and a summary of the technical presentation

The summary of meeting M2.3 is sent to the members combined with materials of the technical presentation. A short document is added for management that presents the aim of the workshop and the main results.

A2.11-X Preparation of the technical presentation

Subjects from the consensus are transformed to a technical presentation in the format of the discussed topics in the CoC. The facilitator leads this preparation, but always involves one of the members to assist him. This is done in order to make the members aware of the actions of the facilitator. The members will also feel more in charge of the activities of the group.

M2.4-X Technical presentations

The next meetings address topics decided on in the consensus in the way described by the CoC. Feedback of every meeting is written down and used to improve upon the practice.

The structure of these meetings will be similar. They start with a check-in in order to personally connect the members. The technical presentation can now commence. The presentation always ends with a round of feedback on the presentation. Members collectively discuss how to improve the meetings to satisfy their needs. The check-in will be the last item of the meeting.

A2.12-X Follow up mail with a summary of the technical presentation/meeting

The summary of meeting M2.X is sent to the members combined with the materials of the technical presentation. A short document is added for management that presents the aim of the workshop and the main results

Phase 3 Continuation

Phase 3 aims to make a well-considered decision and to celebrate the successes of the previous phases. This decision is made during a meeting and all actions prior to this meeting are aimed to provide information in order to make a well-considered decision.

A3.1 Announcement to discuss the future of the group.

The facilitator announces a meeting to discuss the future of the group and to possibly re-new the consensus and CoC. It is important to note in this announcement that the funding of the initiating organization is running to an end, so this needs to be considered as well.

A3.2 Questionnaire aimed to measure the current and future value of this group.

The facilitator sends a questionnaire to the members. This questionnaire contains three parts. The first part focuses on collecting the opinion and view on the current group, the past activities, and the current results. This is followed by a section to gain feedback for improvement. It ends with an inquiry on new needs and interesting new topics.

A3.3 Analysis of questionnaire

The facilitator analyses the activities of the group in phase 2 and the questionnaire. This analysis aims to determine the results and the value the group has brought its members. This is collected in a presentation.

M3.1 A meeting aimed to decide if the group wants to continue and if so, in which manner.

The start of the meeting is a check-in aimed to re-establish the personal connection between the potential members. Everybody stands in a circle and individually they make a small remark about how they are currently feeling. The check-in is followed by a presentation by the facilitator on the results and value determined in the analysis of action A3.3. The facilitator leads a collective discussion on whether to continue or not. This can result in two scenarios.

If the group wants to continue:

The meeting continues with discussion about four topics. The first is the leadership and facilitation of the group. This has currently been done by the facilitator, but the initiating organization will no longer have him available without some funding. The second topic is on new capacities that could be added. Possible capacities are: knowledge exchange, threat analysis, research, or technical support. A third topic is new topics or activities in order to set up a new consensus. The last topic is funding. The group needs to decide on how to fund the activities of the group. Possible funding mechanisms are: mandatory fees or a membership subscription, a voluntary contribution, sponsorship of an individual organization, or a Public Private Partnership (PPP). The meeting ends with the usual check-out.

A3.4 Creating a proposal for the renewed consensus and CoC

The new facilitator or several members use the insights of meeting M3.1 to create a proposal for the renewed consensus and a renewed CoC. The renewed consensus contains an overview of the new aims of the group, the decision regarding the funding, the governance model and an overview of interesting topics.

A3.5 A follow up mail with a presentation of the facilitator, a summary and a proposal for a renewed consensus and CoC.

A3.6 Continuation with inspiration from action A2.2

The new leaders take charge of the group. The organizational changes to the group concerning the funding needs to be dealt with by every individual member. The continuation of the group should start with formalizing the proposal of the renewed consensus and CoC. This can be done in a similar manner as phase 2.

If the group does not want to continue:

The meeting is directed to an informal ending where the members can reminiscence about the group and celebrate the results. The meeting ends with the usual check-out

A3.4 Announcement about the termination of this group.

The last follow up mail is sent by the facilitator. This mail is an announcement that this mail is the end of the group. The presentation of the facilitator and a small summary of the discussion is added.

6. Conclusions and discussion

6.1 Conclusions and main results

This research aimed to accomplish two objectives. The first objective was to gain insights in the establishment of Communities of Practice on cyber security in order to contribute the current scientific literature. The second was to use these insights to provide a possible solution to create a Community of Practice on cyber security for the FERM case in the Rotterdam port area. These two objectives were translated to a main research question and three sub questions that structured an abductive research strategy.

The research started with the first sub question: *Which factors affect the establishment of Community of Practice according to literature?* This sub question provides theoretical insights in how to influence a CoP. A systematic review combined with a meta-ethnography on 60 scientific articles resulted in the translation of five goals, fourteen drivers, and eight barriers that affect the establishment of a CoP. It can be concluded that this set of 27 elements affects the establishment of a CoP according to the current literature.

The second sub question is: *Which factors are critical for the establishment of a Community of Practice on cyber security in the case study of the Rotterdam port area according to the key stakeholders?*
This sub question provides empirical insights that can be triangulated with the theoretical insights. Thirteen semi-structured interviews provided two findings. The first finding is a set of two new goals, eight new drivers, and six new barriers. These new elements are interesting for the scientific community, since they were not mentioned in the articles reviewed in the systematic review. It can be concluded that these 16 elements could also affect the establishment of a CoP.
The second finding is prioritization of the elements based on the response of the participants. This prioritization shows which elements stakeholders find critical for the establishment of a CoP. The highest prioritized goal is Knowledge management. The highest prioritized drivers are Social and Trust followed by the group of drivers Culture, Facilitator & Leadership, Management, Awareness & Urgency, and Direct relevance. The highest prioritized barriers are Culture, and Trust & Social relations. These are the counterparts of the highest ranked *Drivers*. This means that the balance between these elements is recognized by the participants. It can be concluded from this finding that eight elements are deemed most critical for the establishment of a CoP by the stakeholders.

Triangulation of the findings of the first and second sub question was used to determine a critical node and a set of conditions. The critical node and conditions represent the most important link and condition of this case. The critical node is social dynamics which is defined as: "*the interaction between the members that binds and holds them together*". This definition contains the essence of the supporting *Drivers* Culture, Social, and Trust, as well as the *Barriers* Culture and Trust & Social relations. The set of conditions are based on the elements: Culture, Social, Trust, Management, Facilitator & Leadership, Awareness & Urgency, and Direct Relevance. Each has several conditions that result in a total set of nineteen conditions.

The critical node and conditions provide the basis to answer the third and fourth sub question:

3) *How do current cyber security collaboration formats solve the critical factors for the establishment of a Community of Practice on cyber security?*

4) *How could the critical factors for the establishment of a Community of Practice on cyber security be resolved?*

A narrative review on seventeen practically orientated articles was performed in order to answer the third sub question. This provided insight in the strategies and structures used in eleven cyber security collaboration formats. It also provided sub solutions inspired by these formats for the conditions. The conclusion is that the strategies, structures and sub solutions for the conditions are how current cyber security collaboration formats solve the critical factors for the establishment of a CoP on cyber security.

The set of sub solutions is expended by a brainstorm. This brainstorm was used to find sub solutions for the critical node and the conditions. The brainstorm solutions, and solutions found in the narrative are combined in a morphological chart as presented in appendix Q. The morphological chart answers the fourth sub question as it provides an overview of sub solutions for the critical factors for the establishment of a Community of Practice on cyber security.

All these findings can be combined to answer the main research questions: ***How could a Community of Practice on cyber security be established?*** Feedback by one expert and the creativity of the researcher are used to connect elements in the morphological chart and create a strategy to establish a CoP on cyber security. The strategy consists of one informal and internal phase named ***Phase 0 Initiation*** and three formal phases **1)** ***Exploration***, **2)** ***Dedication***, and **3)** ***Continuation***. Every phase has a set of actions that are elaborated in section 5.5.2. The conclusion is that a Community of Practice on cyber security can be established by following these phases and performing the assigned actions.

6.2 Discussion

The conclusions and findings, as presented in section 6.1, and the methods used in this research have some implications, they also indicate some limitations of this research and recommendation for future research. This section will discuss these three aspects of the research for several points split up in science-related items and practice-related items.

6.2.1 Theory

A great addition to the current scientific literature is the overview of elements presented in section 4.2.2. These elements were scattered over articles and had not been combined before. However, the combination of the methods of the systematic review and the meta-ethnography provides a reliable and valid overview of elements enriching the current knowledge on CoPs. The explicit process of these methods improves the thoroughness of the review and reflects on the bias, values and assumptions of the researcher conducting the review (Bryman, 2012, p. 102; Tranfield et al., 2003, p. 208). It provides better insights for other researchers into the validity, relevance and informational value of examined literature (Kitchenham, 2004, p. 2; Sanden & Meijman, 2004, p. 274). A limitation is that the researcher performed this method alone when the validity would increase if it was performed by a group of researchers. This was not possible, since this is a Master's thesis. This limitation can easily be solved by verifying the results with a group of researchers or by repeating this process with a different review protocol. The overview of this review can then be further validated and supported.

These elements were further enriched with the semi-structured interviews, as the participants mentioned a set of sixteen new elements that were not found in the systematic review and the meta-ethnography. This finding implies that there are more elements that affect the establishment of a CoP than the ones currently found in the literature. The validity of these sixteen elements remains somewhat low due to the limited set of participants, however the mix of participants does provide a

good indication. Therefore, this finding provides a starting point for future research. These elements can be validated by performing a larger set of interviews or focus group. Another possibility is conducting a questionnaire about all elements among a large group of professionals as it validates the elements found in the systematic review and meta-ethnography as well.
An interesting finding of this research is that the elements mentioned in the semi-structured interviews could be structured according to their importance. This implies that certain elements hold a greater importance than others. This was not directly found in literature, where elements were only referred to and explained. This prioritization was done through the process described in section 3.3.4 and is mainly based on the interpretation of the researcher. Even though the process is well described and the intermediate steps can be reviewed, the use of a single examiner for this method limits the validity. Validity could be increased by reviewing the interview with multiple researchers or by asking the interview participants specifically to rate elements on importance.

A strong element of this research design is the triangulation of the theoretical findings and the empirical findings. This design brought science and practice together so they could strengthen each other. The semi-structured interview validated several elements found in the systematic review and meta-ethnography. This supports the theoretical findings and connects them to practice.

Another clear result of the triangulation is critical node and set of condition. This result is based on the interpretation of the conclusions from the analysis phase presented in section 4.4. This interpretation has a distinct case-specific relevance, but have a more general implication as well. These originate from the combination of the prioritization of elements found in the interviews with the elements found in literature.

The critical node and conditions are case specific, since the case analysis and the prioritization of elements by the interview participants greatly influenced them. However, the critical node and the conditions should also be true for other cases, since this case is typical and representative for other cases as explained in section 3.2. This implies that the focus for the establishment of all CoPs in cyber security should be on the social dynamics of the participants and should satisfies the conditions for the elements: Culture, Social, Trust, Management, Facilitator & Leadership, Awareness & Urgency, and Direct Relevance. Future research can examine this critical node and conditions using two main direction. The first direction of research is to focus on other cases and examining and comparing the results gained through interviews or focus groups. The other direction is to use experts to validate this finding. This could be done with a focused systematic review, structured interviews, or a questionnaire.

6.2.2 Practice

An important implication of this research is that the concept solution provides a strategy with practical and clear actions to establish a CoP on cyber security from scratch. Organizations can use this strategy to establish CoPs on cyber security as well as support their use of this strategy, since this strategy has a strong scientific and empirical base. This strong foundation is due to an analysis phase that established the critical node and the condition as well as due to the narrative review and brainstorm that provided different perspectives on sub solutions. The expert feedback further validated the choices made in the concept solution. However, only one expert was interviewed due to practical constraints as explained in section 3.3.9. This decreases the validity of the concept solution. Future research could interview more experts in order to have a more validated result. However, the current strategy can already be used by FERM and other organization that want to establish a CoP. By applying the concept solution, it can be tested and improved through practice and experience. Future research can evaluate the use of this concept solution in different cases and determine the effectiveness of the actions and the strategy structure based on the evaluation.

The semi-structured interviews, the narrative review and the expert feedback all mentioned that the total amount of participants should remain limited for a CoP or any other active collaboration format. This was also adopted in the concept solution. This implies for the case that the CoP created with the concept solution will never encompass all the organization in the Rotterdam port area. However, one of FERM’s aims is to exchange knowledge between most organizations. Wenger et al. (2002) recognize this challenge and believe it can be solved with a constellation of multiple CoPs that collaborate with each other. This can be done for the FERM casus using the concept solution. The strategy presented in the concept solution aims to create CoPs based on the needs and wishes of the participants, thus it can work for a multitude of groups in the Rotterdam port area. All these CoPs share the need for improved cyber resilience and security of their systems. This shared need can connect them and make them collaborate. Future research can determine how these CoPs can best collaborate and how these collaboration between CoPs should be established.

7. References

Alali, H., & Salim, J. (2016). Virtual health communities of practice success factors: towards taxonomy and a framework. *International Journal of Web Based Communities*, *12*(2), 180. https://doi.org/10.1504/IJWBC.2016.077256

Alavi, M., & Leidner, D. E. (1999). Knowledge management systems: issues, challenges, and benefits. *Communications of the AIS*, *1*, 1–37. https://doi.org/10.1002/jhrm.20064

Askwith, B. (2006). *WARP Case Study - Experience setting up a WARP*.

Beijers, R. E. (2018). *Development of a Knowledge sharing game to design collaboration in a hierarchical organisation*. Delft University of Technology.

Blackmore, C. (Ed.). (2010). *Social Learning Systems and Communities of Practice*. London: Springer London. https://doi.org/10.1007/978-1-84996-133-2

Borzillo, S. (2017). Balancing control and autonomy in communities of practice: governance patterns and knowledge in nine multinationals. *Journal of Business Strategy*, *38*(3), 10–20. https://doi.org/10.1108/JBS-03-2016-0031

Bos, N., Zimmerman, A., Olson, J., Yew, J., Yerkie, J., Dahl, E., & Olson, G. (2007). From shared databases to communities of practice: A taxonomy of collaboratories. *Journal of Computer-Mediated Communication*, *12*(2), 652–672. https://doi.org/10.1111/j.1083-6101.2007.00343.x

Bremmer, D., & van Heel, L. (2017). Wereldwijde hack legt bedrijven en Rotterdamse terminal plat. *Algemeen Dagblad*. Retrieved from https://www.ad.nl/rotterdam/wereldwijde-hack-legt-bedrijven-en-rotterdamse-terminal-plat~a60dd307/

Britten, N., Campbell, R., Pope, C., Donovan, J., Morgan, M., & Pill, R. (2002). Using meta ethnography to synthesis qualitative research. *Journal of Health Services Research and Policy*, *7*(4), 209–215.

Brown, J. S., & Duguid, P. (1991). Organizational learning and Communities of Practice: Toward a unified view of working, learning and innovation. *Organization Science*, *2*(1), 40–58.

Bryman, A. (2012). *Social Research Methods* (4th editio). Oxford University Press.

Cahill, M., Robinson, K., Pettigrew, J., Galvin, R., & Stanley, M. (2018). Qualitative synthesis: A guide to conducting a meta-ethnography. *British Journal of Occupational Therapy*, *81*(3), 129–137. https://doi.org/10.1177/0308022617745016

CBS. (2018). *Cybersecuritymonitor*.

Chen, Y. H., Lin, T. P., & Yen, D. C. (2014). How to facilitate inter-organizational knowledge sharing: The impact of trust. *Information and Management*, *51*(5), 568–578. https://doi.org/10.1016/j.im.2014.03.007

Cheung, C. M. K., Lee, M. K. O., & Lee, Z. W. Y. (2013). Understanding the continuance intention of knowledge sharing in online communities of practice through the post-knowledge-sharing evaluation processes. *Journal of the American Society for Information Science and Technology*, *64*(7), 1357–1374. https://doi.org/10.1002/asi.22854

Chu, K. W. (2016). Leading knowledge management in a secondary school. *Journal of Knowledge Management*, *20*(5), 1104–1147. https://doi.org/10.1108/JKM-10-2015-0390

Cisco. (2018). *Cisco 2018 Annual Cybersecurity Report*.

Cochrane, T. D. (2011). Reflections on 4 Years of Learning Implementation (2007-2010). *International Journal of Mobile and Blended Learning*, *3*(3), 1–22. https://doi.org/10.4018/jmbl.2011070101

Cochrane, T. D. (2014). Critical success factors for transforming pedagogy with mobile Web 2.0. *British Journal of Educational Technology*, *45*(1), 65–82. https://doi.org/10.1111/j.1467-8535.2012.01384.x

Cornes, M., Manthorpe, J., Hennessy, C., Anderson, S., Clark, M., & Scanlon, C. (2014). Not just a talking shop: Practitioner perspectives on how communities of practice work to improve outcomes for people experiencing multiple exclusion homelessness. *Journal of Interprofessional Care*, *28*(6), 541–546. https://doi.org/10.3109/13561820.2014.917406

Costa e Silva, S., Bradley, F., & Sousa, C. M. P. (2012). Empirical test of the trust-performance link in an international alliances context. *International Business Review*. https://doi.org/10.1016/j.ibusrev.2011.03.006

Cox, A. (2005). What are communities of practice? A comparative review of four seminal works. *Journal of Information Science*, *31*(6), 527–540.

CPB. (2018). *Risicorapportage Cyberveiligheid Economie 2018*.

Crowley, C., McAdam, M., Cunningham, J. A., & Hilliard, R. (2018). Community of Practice: A flexible construct for understanding SME networking roles in the Irish artisan cheese sector. *Journal of Rural Studies*, *64*(October), 50–62. https://doi.org/10.1016/j.jrurstud.2018.08.014

Daft, R. L., & Weick, K. E. (1984). Toward a Model of Organizations as Interpretation Systems1. *The Academy of Management Review*, *9*(2), 284–295.

Dahlander, L., & O'Mahony, S. (2011). Progressing to the Center: Coordinating Project Work. *Organization Science*, *22*(4), 961–979. https://doi.org/10.1287/orsc.1100.0571

Dawson, L., Persson, K., Balfors, B., Mörtberg, U., & Jarsjö, J. (2018). Impacts of the water framework directive on learning and knowledge practices in a Swedish catchment. *Journal of Environmental Management*, *223*(July), 731–742. https://doi.org/10.1016/j.jenvman.2018.06.054

DCMR. (2019). No Title. Retrieved June 18, 2019, from https://www.dcmr.nl/

De Bruijn, H., & Heuvelhof, E. (2008). *Management in Networks*. Routledge.

Del Giudice, M., Della Peruta, M. R., & Maggioni, V. (2015). A model for the diffusion of knowledge sharing technologies inside private transport companies. *Journal of Knowledge Management*, *19*(3), 611–625. https://doi.org/10.1108/JKM-02-2015-0047

Deltalinqs. (2016). *Sterke ondernemingen, Krachtige mainport - Strategische agenda 2016-2019*.

Design Council. (2019). What is the framework for innovation? Design Council's evolved Double Diamond. Retrieved November 18, 2019, from https://www.designcouncil.org.uk/news-opinion/what-framework-innovation-design-councils-evolved-double-diamond

Dobs, R., Manyika, J., & Woetzel, J. (2016). *Digital Globalization: The new era of global flows*.

Dooner, A. M., Mandzuk, D., & Clifton, R. A. (2008). Stages of collaboration and the realities of professional learning communities. *Teaching and Teacher Education*, *24*(3), 564–574. https://doi.org/10.1016/j.tate.2007.09.009

Dragomir, M., Banyai, D., Dragomir, D., Popescu, F., & Criste, A. (2016). Efficiency and resilience in product design by using morphological charts. *Energy Procedia*, *85*(November 2015), 206–210. https://doi.org/10.1016/j.egypro.2015.12.218

Du Plessis, M. (2008). The strategic drivers and objectives of communities of practice as vehicles for knowledge management in small and medium enterprises. *International Journal of Information Management*, *28*(1), 61–67. https://doi.org/10.1016/j.ijinfomgt.2007.05.002

Dube, L., Bourhis, A., & Jacob, R. (2006). Towards a Typology of Virtual Communities of Practice. *Interdisciplinary Journal of Information, Knowledge and Management*, *1*. https://doi.org/10.1145/2441776.2441845

Dubois, A., & Gadde, L.-E. (2002). “Systematic Combining”: An approach to case research. *Journal of Business Research*, *55*(7), 553–560. https://doi.org/10.1080/21639159.2017.1360145

Duguid, P. (2005). The Information Society: An International Journal “The Art of Knowing”: Social and Tacit Dimensions of Knowledge and the Limits of the Community of Practice “ The Art of Knowing ”: Social and Tacit Dimensions of Knowledge and the Limits of the Communit. *The Information Society*, *21*(2), 109–118. https://doi.org/10.1080/01972240590925311

Duin, P., & Zeer, M. (2015). Notitie - Strategie Cyber Resilience.

Edwards, A. (2005). Let’s get beyond community and practice: the many meanings of learning by participating. *Curriculum Journal*, *16*(1), 49–65. https://doi.org/10.1080/0958517042000336809

Egan, T., & Jaye, C. (2009). Communities of clinical practice: the social organization of clinical learning. *Health: An Interdisciplinary Journal for the Social Study of Health, Illness and Medicine*, *13*(1), 107–125. https://doi.org/10.1177/1363459308097363

Ekberg, J., Ericson, L., Timpka, T., Eriksson, H., Nordfeldt, S., Hanberger, L., & Ludvigsson, J. (2010). Web 2.0 systems supporting childhood chronic disease management: Design guidelines based on information behaviour and social learning theories. *Journal of Medical Systems*, *34*(2), 107–117. https://doi.org/10.1007/s10916-008-9222-0

ENISA. (2006a). *A step-by-step approach on how to set up a CSIRT*.

ENISA. (2006b). *CERT cooperation and its further facilitation by relevant stakeholders*.

ENISA. (2014). *Scalable and Accepted Methods for Trust Building in Operational Communities*. https://doi.org/10.2824/320219

ENISA. (2016). *Strategies for Incident Response and Cyber Crisis Cooperation*. https://doi.org/10.2824/967546

ENISA. (2017a). *Information Sharing and Analysis Centres (ISACs)*. https://doi.org/10.2824/549292

ENISA. (2017b). *Public Private Partnerships (PPP) - Cooperative models*.

Erp, J. van. (2017). New governance of corporate cybersecurity: a case study of the petrochemical industry in the Port of Rotterdam. *Crime, Law and Social Change*, *68*(1–2), 75–93. https://doi.org/10.1007/s10611-017-9691-5

EY. (2011). *The digitisation of everything*.

Faraj, S., von Krogh, G., Monteiro, E., & Lakhani, K. R. (2016). Online Community as Space for Knowledge Flows. *Information Systems Research*, *27*(4), 668–684. https://doi.org/10.1287/isre.2016.0682

Ferlie, E., Crilly, T., Jashapara, A., & Peckham, A. (2012). Knowledge mobilisation in healthcare: A critical review of health sector and generic management literature. *Social Science and Medicine*, *74*(8), 1297–1304. https://doi.org/10.1016/j.socscimed.2011.11.042

FERM. (2019). No Title. Retrieved June 18, 2019, from https://ferm-rotterdam.nl/

Fetterman, D. M. (2002). Empowerment Evaluation: Building Communities of Practice and a Culture of Learning. *American Journal of Community Psychology*, *30*(1), 89–102. https://doi.org/10.1023/A:1014324218388

Friedrichs, J., & Kratochwil, F. (2009). On Acting and Knowin: How Pragmatism Can Advance International Relations Research and Methodology. *International Organization*, *63*(4), 701–731.

Fteimi, N., & Lehner, F. (2018). Analysing and classifying knowledge management publications – a proposed classification scheme. *Journal of Knowledge Management*, *22*(7), 1527–1554. https://doi.org/10.1108/JKM-07-2017-0284

Gagnon, M. L. (2011). Moving knowledge to action through dissemination and exchange. *Journal of Clinical Epidemiology*, *64*(1), 25–31. https://doi.org/10.1016/j.jclinepi.2009.08.013

Galán-Muros, V., van der Sijde, P., Groenewegen, P., & Baaken, T. (2017). Nurture over nature: How do European universities support their collaboration with business? *Journal of Technology Transfer*, *42*(1), 184–205. https://doi.org/10.1007/s10961-015-9451-6

Gibson, J., & Meacheam, D. (2009). The individual and organizational commitments needed for a successful diabetes care community of practice. *Health Services Management Research*, *22*(3), 122–128. https://doi.org/10.1258/hsmr.2008.008018

Haaften, W. van. (2018). *Strategic cybersecurity management in port industries - an asset point-of-view*. Erasmus University.

Hakkaja, M. (2006). The evolution of WARPs. ENISA.

Hall, H., & Graham, D. (2004). Creation and recreation: Motivating collaboration to generate knowledge capital in online communities. *International Journal of Information Management*, *24*(3), 235–246. https://doi.org/10.1016/j.ijinfomgt.2004.02.004

Handley, K., Sturdy, A., Finchman, R., & Clark, T. (2006). Within and Beyond Communities of Practice: Making Sense of Learning Through Participation, Identity and Practice. *Journal of Management Studies*, *43*(3), 641–653. Retrieved from http://www.google.com.mx/search?q=http://escholarship.org/uc/item/3h33n5z5&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:es-MX:official&client=firefox-a&source=hp&channel=np#hl=en&client=firefox-a&hs=UHW&rls=org.mozilla:es-MX:official&channel=np&sclient=psy-ab&q

Hara, N., Shachaf, P., & Stoerger, S. (2009). Online communities of practice typology revisited. *Journal of Information Science*, *35*(6), 740–757. https://doi.org/10.1177/0165551509342361

Ho, L. A., & Kuo, T. H. (2013). How system quality and incentive affect knowledge sharing. *Industrial Management and Data Systems*, *113*(7), 1048–1063. https://doi.org/10.1108/IMDS-01-2013-0015

Hong, D., Suh, E., & Koo, C. (2011). Developing strategies for overcoming barriers to knowledge sharing based on conversational knowledge management: A case study of a financial company. *Expert Systems with Applications*, *38*(12), 14417–14427. https://doi.org/10.1016/j.eswa.2011.04.072

Hong, J. (2017). A method for identifying the critical success factors of CoP based on performance evaluation. *Knowledge Management Research and Practice*, *15*(4), 572–593. https://doi.org/10.1057/s41275-017-0066-6

Hosseini, S. M., Akhavan, P., & Abbasi, M. (2017). A knowledge sharing approach for R&D project team formation. *VINE Journal of Information and Knowledge Management Systems*, *47*(2), 154–171. https://doi.org/10.1108/VJIKMS-05-2015-0031

Hsiao, Y. C., Chen, C. J., Lin, B. W., & Kuo, C. I. (2017). Resource alignment, organizational distance, and knowledge transfer performance: the contingency role of alliance form. *Journal of Technology Transfer*, *42*(3), 635–653. https://doi.org/10.1007/s10961-016-9505-4

Huistra, A. W., & Krabbendam-Hersman, T. H. E. E. A. (2017). *Verkenning Cybersecurity Informatiedeling binnen de Topsectoren*.

Jaegersberg, G., & Ure, J. (2011). Barriers to knowledge sharing and stakeholder alignment in solar energy clusters: Learning from other sectors and regions. *Journal of Strategic Information Systems*, *20*(4), 343–354. https://doi.org/10.1016/j.jsis.2011.03.002

Jeon, S., Kim, Y. G., & Koh, J. (2011). An integrative model for knowledge sharing in communities-of-practice. *Journal of Knowledge Management*, *15*(2), 251–269. https://doi.org/10.1108/13673271111119682

Kalmár, E. (2016). *Building a model for virtual collaboration readiness*. Delft University of Technology.

Kamp, H. G. J. (2017). Kamerbrief: Verkenning Cybersecurity informatiedeling binnen de topsectoren. *Kamerbrief: Verkenning Cybersecurity Infomratiedeling Binnen de Topsectoren*. Ministry of Economic Affairs.

Kaplan, W. S., & Thomson Reed, A. F. (2007). KM: From concept to theory to practice: Knowledge leadership at Acquisition Solutions, Inc. *Vine*, *37*(2), 219–232. https://doi.org/10.1108/03055720710759982

Kelly, M. J., Schaan, J. L., & Joncas, H. (2002). Managing alliance relationships: Key challenges in the early stages of collaboration. *R&D Management*, *32*(1), 11–22. https://doi.org/10.1111/1467-9310.00235

Kitchenham, B. (2004). *Kitchenham_Procedures for Performing Systematic Reviews_2004.pdf*. https://doi.org/10.1.1.122.3308

Koh, C. E., Ryan, S., & Prybutok, V. R. (2005). Creating value through managing knowledge in an E-government to constituency (G2C) environment. *Journal of Computer Information Systems*, *45*(4), 32–41. https://doi.org/10.1080/08874417.2005.11645853

Kruss, G., & Visser, M. (2017). Putting university–industry interaction into perspective: a differentiated view from inside South African universities. *Journal of Technology Transfer*, *42*(4), 884–908. https://doi.org/10.1007/s10961-016-9548-6

Lathlean, J., & Le May, A. (2002). Communities of practice: An opportunity for interagency working. *Journal of Clinical Nursing*, *11*(3), 394–398. https://doi.org/10.1046/j.1365-2702.2002.00630.x

Lave, J., & Wenger, E. (1991). *Situated learning: legitimate peripheral participation*. Cambridge University Press.

Lee, H., & Choi, B. (2003). Knowledge Management Enablers, Processes, and Organizational Performance: An Integrative View and Emperical Examination. *Journal of Management*

Information Systems, *20*(1), 179–228. https://doi.org/10.1080/07421222.2003.11045756

Lee, H. S. (2017). Knowledge Management Enablers and Process in Hospital Organizations. *Osong Public Health and Research Perspectives*, *8*(1), 26–33. https://doi.org/10.24171/j.phrp.2017.8.1.04

Li, L. C., Grimshaw, J. M., Nielsen, C., Judd, M., Coyte, P. C., & Graham, I. D. (2009). Evolution of Wenger's concept of community of practice. *Implementation Science*, *4*(11). https://doi.org/10.1186/1748-5908-4-11

Li, Y. M., & Jhang-Li, J. H. (2010). Knowledge sharing in communities of practice: A game theoretic analysis. *European Journal of Operational Research*, *207*(2), 1052–1064. https://doi.org/10.1016/j.ejor.2010.05.033

Liu, F. C., Cheng, K. L., Chao, M., & Tseng, H. M. (2012). Team innovation climate and knowledge sharing among healthcare managers: mediating effects of altruistic intentions. *Chang Gung Medical Journal*, *35*(5), 408–419. https://doi.org/3505/350506 [pii]

Lyons, K., Acsente, D., & van Waesberghe, M. (2008). Integrating knowledge management and quality management to sustain knowledge enabled excellence in performance. *Vine*, *38*(2), 241–253. https://doi.org/10.1108/03055720810889879

Mabery, M. J., Gibbs-Scharf, L., & Bara, D. (2013). Communities of practice foster collaboration across public health. *Journal of Knowledge Management*, *17*(2), 226–236. https://doi.org/10.1108/13673271311315187

Machuca, M. M., & Costa, C. M. (2012). A study of knowledge culture in the consulting industry. *Industrial Management and Data Systems*, *112*(1), 24–41. https://doi.org/10.1108/02635571211193626

Margaryan, A., Milligan, C., & Littlejohn, A. (2011). Validation of Davenport's classification structure of knowledge-intensive processes. *Journal of Knowledge Management*, *15*(4), 568–581. https://doi.org/10.1108/13673271111151965

Muller, P. (2006). Reputation, trust and the dynamics of leadership in communities of practice. *Journal of Management and Governance*, *10*(4), 381–400. https://doi.org/10.1007/s10997-006-9007-0

Municipality of Rotterdam. (2014). Verslag conferentie 'A Trusted Dialogue.' Rotterdam: Municipality of Rotterdam.

Municipality of Rotterdam. (2015). Invitation Conference Policing Global Cities. Rotterdam: Municipality of Rotterdam.

Municipality of Rotterdam, & 100 Resilient Cities. (2016). *Rotterdam Resilience Strategie*. Rotterdam.

NCSC. (2015). *CSIRT Maturity Kit: A step-by-step guide towards enhancing CSIRT Maturity*.

NCSC. (2018a). *Starting a collective CSIRT*.

NCSC. (2018b). *Starting a regional collaboration*.

NCSC. (2018c). *Starting a supply chain collaboration*.

NCSC. (2018d). *Starting an ISAC: Sectoral collaboration*.

NCSC. (2019). No Title. Retrieved June 18, 2019, from https://www.ncsc.nl/organisatie

NCTV. (2017). *Factsheet Weerbare vitale infrastructuur*.

NCTV. (2018). *Cybersecuritybeeld Nederland (CSBN) 2018*.

Nielsen, M. F. (2012). Using artifacts in brainstorming sessions to secure participation and decouple sequentiality. *Discourse Studies*, *14*(1), 87–109. https://doi.org/10.1177/1461445611427211

NISCC. (2002). *An Information Sharing Vision to improve Internet Security*.

NISCC. (2006). WARPs - the business case.

Noblit, G. W., & Hare, R. D. (1988). *Meta-ethnography: Synthesizing qualitative research*. Sage.

Noort, W. van. (2017). Havenhack kost Nederland tientallen miljoenen. *NRC*. Retrieved from https://www.nrc.nl/nieuws/2017/06/28/havenhack-kost-nederland-tientallen-miljoenen-11332811-a1564856

OM. (2019). Openbaar Ministerie - Het werk van het OM. Retrieved June 18, 2019, from https://www.om.nl/organisatie/werk/

Orr, J. (1986). Narratives at work: Story telling as cooperative diagnostic activity. In *Proceedings of the 1986 ACM conference on Computer-supported cooperative work*.

Orr, J. (1987). *Talking about Machines: Social Aspects of Expertise, Report for the Intelligent Systems Laboratory*. Palo Alto, CA.

Orr, J. (1990a). haring Knowledge, Celebrating Identity: War Stories and Community Memory in a Service Culture. *Collective Remembering: Memory in Society*.

Orr, J. (1990b). *Talking about Machines: An Ethnography of a Modern Job*. Cornell University.

Parkhe, A. (1998a). Building Trust in International Alliances. *Journal of World Business*, *33*(4), 417–437.

Parkhe, A. (1998b). Understanding trust in international alliances. *Journal of World Business*, *33*(3), 219–240. https://doi.org/10.1016/S1090-9516(99)80072-8

Pharo, E., Davison, A., McGregor, H., Warr, K., & Brown, P. (2014). Using communities of practice to enhance interdisciplinary teaching: lessons from four Australian institutions. *Higher Education Research and Development*, *33*(2), 341–354. https://doi.org/10.1080/07294360.2013.832168

Pirkkalainen, H., & Pawlowski, J. M. (2014). Global social knowledge management - Understanding barriers for global workers utilizing social software. *Computers in Human Behavior*, *30*, 637–647. https://doi.org/10.1016/j.chb.2013.07.041

Politie. (2019). Zeehavenpolitie. Retrieved June 18, 2019, from https://www.politie.nl/themas/zeehavenpolitie.html

PoR. (2015). Vergadering Raad van Commissarissen Havenbedrijf Rotterdam N.V. d.d. 10 september 2015 - Update Cyber Security. Port of Rotterdam.

PoR. (2016). *Port of Rotterdam - Annual report 2015*.

PoR. (2017a). *Port of Rotterdam - Annual report 2016*. Rotterdam. Retrieved from https://jaarverslag2016.portofrotterdam.com/download_pdf

PoR. (2017b). *Port of Rotterdam - Annual report 2017*.

Preece, J. (2004). Etiquette, empathy and trust in communities of practice: Stepping-stones to social capital. *Journal of Universal Computer Science*, *10*(3), 294–302. https://doi.org/http://dx.doi.org/10.3217/jucs-010-03-0294

Price, D. W., & Felix, K. G. (2008). Journal Clubs and Case Conferences: From Academic Tradition to Communities of Practice. *Journal of Continuing Education in the Health Professions*, *28*(3), 123–130. https://doi.org/10.1002/chp

Ramos-Vielba, I., Sánchez-Barrioluengo, M., & Woolley, R. (2016). Scientific research groups' cooperation with firms and government agencies: motivations and barriers. *Journal of Technology Transfer*, *41*(3), 558–585. https://doi.org/10.1007/s10961-015-9429-4

Robards, M. D., Huntington, H. P., Druckenmiller, M., Lefevre, J., Moses, S. K., Stevenson, Z., … Williams, M. (2018). Understanding and adapting to observed changes in the Alaskan Arctic: Actionable knowledge co-production with Alaska Native communities. *Deep-Sea Research Part II: Topical Studies in Oceanography*, *152*(February), 203–213. https://doi.org/10.1016/j.dsr2.2018.02.008

Roberts, J. (2006). Limits to communities of practice. *Journal of Management Studies*, *43*(3), 623–639. https://doi.org/10.1111/j.1467-6486.2006.00618.x

Rooke, C. N., Rooke, J. A., Koskela, L., & Tzortzopoulos, P. (2010). Using the physical properties of artefacts to manage through-life knowledge flows in the built environment: An initial exploration. *Construction Management and Economics*, *28*(6), 601–613. https://doi.org/10.1080/01446193.2010.489925

RTV Rijnmond. (2017). Containerterminals APM wereldwijd plat door hack. *RTV Rijnmond*. Retrieved from https://www.rijnmond.nl/nieuws/156499/Containerterminals-APM-wereldwijd-plat-door-hack

Sabel, C. F. (1993). Studied Trust: Building New Forms of Ccooperation in a Volatile Economy. *Human Relations*.

Salo, A. (2001). Incentives in technology foresight. *International Journal of Technology Management*, *21*(7/8), 694–710. https://doi.org/10.1504/IJTM.2001.002944

Sanden, M. C. A. van der, & Meijman, F. J. (2004). Evidence-Based Science Communication: An Essay. *Science Communication*, *25*(3), 272–287. https://doi.org/10.1177/1075547003262662

Scarso, E., Bolisani, E., & Salvador, L. (2009). A systematic framework for analysing the critical success factors of communities of practice. *Journal of Knowledge Management*, *13*(6), 431–447. https://doi.org/10.1108/13673270910997105

Schwab, W., & Poujol, M. (2018). *The State of Industrial Cybersecurity 2018*.

Sheffield, J., & Lemétayer, J. (2013). Factors associated with the software development agility of successful projects. *International Journal of Project Management*, *31*(3), 459–472. https://doi.org/10.1016/j.ijproman.2012.09.011

Sonnenwald, D. H. (2003). *Managing Cognitive and Affective Trust in the Conceptual R&D Organization*. (M. Iivonen & H. Huotari, Eds.), *Trust in Knowledge Management and Systems in Organizations*. Idea Publishing.

Sonnenwald, D. H. (2007). Scientific Collaboration. *Annual Review of Information Science and Technology (ARIST)*, *41*(1), 643–681. https://doi.org/10.1002/aris.2007.1440410121

Swain, D. E., & Ekionea, J. P. B. (2008). A Framework for Developing and Aligning a Knowledge Management Strategy. *Journal of Information & Knowledge Management*, *7*(2), 113–122. https://doi.org/10.1142/S0219649208002019

Tan, C. N. L., & Noor, S. (2013). Knowledge management enablers, knowledge sharing and research collaboration: a study of knowledge management at research universities in Malaysia. *Asian Journal of Technology Innovation*, *21*(2), 251–276. https://doi.org/10.1080/19761597.2013.866314

Tayal, S. P. (2013). Engineering Design Process. *International Journal of Computer Science and Communication Engineering*, 1–6.

Timmermans, S., & Tavory, I. (2012). Theory construction in qualitative research: From grounded theory to abductive analysis. *Sociological Theory*, *30*(3), 167–186. https://doi.org/10.1177/0735275112457914

TNO. (2015). Gr!p op cyber - TNO cyberchallenge. TNO.

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management*, *14*(3), 207–222. https://doi.org/10.1111/1467-8551.00375

UKERNA. (2006). CSIRTs and WARPs: Improving Security Together. UKERNA and Crown.

Verhagen, H. (2016). *De economische en maatschappelijk noodzaak van meer cybersecurity - Nederland digitaal droge voeten*.

Verkiel, J. W. (2016). Cyber Resilience Officer A4 Voorstel. Rotterdam: Port of Rotterdam.

Verkiel, J. W., & Hoitink, R. J. (2016). Werkgroep Organisatie en Communicatie. Port of Rotterdam.

Vermeij, R. (2016). *Reciprocity in Wind Farm Development*. Delft University of Technology.

Wang, J., Wei, W., Ding, L., & Li, J. (2017). Method for analyzing the knowledge collaboration effect of R&D project teams based on Bloom’s taxonomy. *Computers and Industrial Engineering*, *103*, 158–167. https://doi.org/10.1016/j.cie.2016.11.010

Wang, X., Wong, T. N., & Wang, G. (2012). An ontological intelligent agent platform to establish an ecological virtual enterprise. *Expert Systems with Applications*, *39*(8), 7050–7061. https://doi.org/10.1016/j.eswa.2012.01.042

WEF. (2012). Partnering for Cyber Resilience. *World Economic Forum*. World Economic Forum.

WEF. (2016). Recommendations for Public-Private Partnership against Cybercrime. *World Economic Forum*. World Economic Forum.

WEF. (2018). *Digital Transformation Initiative*.

Wenger, E. (1998a). *Communities of practice: learning, meaning and identity*. Cambridge University Press.

Wenger, E. (1998b). Communities of Practice: Learning as a social system. *Systems Thinker*, 1–10. https://doi.org/10.2277/0521663636

Wenger, E. (2000). Communities of Practice and Social Learning Systems. *Organization*, *7*(2), 225–246. https://doi.org/10.1177/135050840072002

Wenger, E. (2011). *Communities of Practice: a brief introduction*. Retrieved from http://hdl.handle.net/1794/11736

Wenger, E., McDermott, R., & Snyder, W. M. (2002). *Cultivating Communities of Practice: A guide to managing knowledge*. Harvard Business Press.

Wenger, E., & Snyder, W. M. (2000). Communities of practice: The organizational frontier. *Harvard Business Review*, 139–145. https://doi.org/10.1177/0170840603024003909

Wenger, E., Trayner, B., & De Laat, M. (2011). *Promoting and assessing value creation in communities and networks: A conceptual framework*. Retrieved from http://www.social-learning-strategies.com/documents/Wenger_Trayner_DeLaat_Value_creation.pdf

Witherspoon, C. L., Bergner, J., Cockrell, C., & Stone, D. N. (2013). Antecedents of organizational knowledge sharing: A meta-analysis and critique. *Journal of Knowledge Management*, *17*(2), 250–277. https://doi.org/10.1108/13673271311315204

Wu, G. D. (2013). Knowledge collaborative incentive based on inter-organizational cooperative innovation of project-based supply chain. *International Journal of Engineering and Management*, *6*(4), 1065–1081. https://doi.org/10.2507/IJSIMM13(1)CO3

Yin, R. K. (2009). *Case study research: Design and methods.* (4th ed.). Los Angeles: Sage.

8. Appendices

A. Overview of trends and developments

The digitalization of our world is increasing by the day making the world more interconnected then ever (Dobs et al., 2016; EY, 2011). The digital flows have multiplied 45 times in the period from 2005 to 2014 and further increasing is expected (Dobs et al., 2016). This change poses new challenges and opportunities to businesses. On one hand, the digital changes provide new business models, more transparency, participation of emerging economies, and an easier market entrance for SMEs (Dobs et al., 2016; EY, 2011). On the other hand, new threats need to be counteracted such as the protection of data, information and systems (Dobs et al., 2016; Schwab & Poujol, 2018).

This protection is not guaranteed anymore. Malware has been taken to unprecedented levels of sophistication and impact, making it more dangerous for consumers and businesses. Malicious actors are also adopting new strategies to avoid detection and to exploit undefended gaps in the digital security of systems (Cisco, 2018). It is estimated that cybercrime costs the global economy around $400 billion in annual losses through consumer data breaches, financial crimes, market manipulation, and theft of intellectual property (Dobs et al., 2016; Verhagen, 2016). For example, an cyber-attack on the America credit bureau Equifax in September 2017 resulted in a data leak that affected nearly 148 million Americans which costed $85,5 million in the third quarter of 2018 (NCTV, 2018). While most losses are still confined to the IT space, the further digitization of Operational Technology (OT) and Industrial Control Systems (ICS) could also result in physical damage (Dobs et al., 2016; Schwab & Poujol, 2018).

Luckily, cyber security is becoming a more integral part of this digital change. A recent study of the Kaspersky Lab (Schwab & Poujol, 2018) shows that the cyber security of OT and ICS is a major priority for 77% of the interviewed companies (n=320). These companies show more awareness and attribute a higher concern to consequences of a cyber security breach, but they also believe they have become more likely to be a target even though 51% didn’t experience a breach the past 12 months. However, when a breach occurred, 54% report to have noticed damage to their products or services compared to 29% in the previous year. This suggest that the impact of a breach has increased greatly, even when the occurrence of a breach remained moderate.

Naturally threats differ per country and it can be deduced that countries with more global digital flows and a better digital infrastructure are a more likely target. The Netherlands is such a country due to our excellent digital infrastructure making it a leader in digitalization (Dobs et al., 2016; Verhagen, 2016). Some even dare to note that the digital economy is the third main port of the Netherlands besides the airport hub of Schiphol and the Rotterdam port area (Verhagen, 2016). But similar to the international trends, the cyber threats are also present in the Netherlands (CBS, 2018; NCTV, 2018): 50% of the companies with more than 10 employees encountered a cyber security incident in 2016, and for 49% of these companies this incident had financial consequences; 10.009 notifications of data leaks were received in 2017 compared to 5.617 notifications in 2016; and 11% of the Dutch citizens were victim of one or more cybercrimes such as identity fraud, sales fraud, hacking, or cyber bullying. The counter terrorism unit (NCTV) mentions that the cyber threats will be a permanent one and that the activities of cybercriminals have great impact. Although the amount of threat has not fundamentally changed the past few years, the diversity of the threats has increased. It can be said that the situation in the Netherlands can be a reason for concern due to the increasing vulnerabilities and threats against Dutch economic, societal and geopolitical interests (Verhagen, 2016, p. 17).

Certain processes are so important for the (Dutch) national interests that a disturbance or outage would lead to severe societal disruption and are a threat to national safety. These processes are deemed to be part of the vital infrastructure (NCTV, 2017). Ship management, the production, processing and storage of (Petro-) chemicals, and oil and gas supply are examples of these sort of processes as well as processes that exist in the Rotterdam port area. This area houses multiple vital processes and the port of Rotterdam is therefore seen as a vital piece of Infrastructure. However, this infrastructure is not safe from the cyber threats as was shown in June 2017 with the terminal hack of APM (Bremmer & van Heel, 2017; Noort, 2017; RTV Rijnmond, 2017). This hack closed down one of the biggest and advanced terminals and the financial damage is estimated to range from $200-300 million (NCTV, 2018). Although these facts are already quite disturbing, what's even more scary is that this hack was done with non-targeted ransomware meaning that the terminal was not even a designated target.

B. History of the CoP concept

The concept CoP has a long history in which it changes quite a bit. The term CoP is first mentioned by Lave and Wenger (1991) in their book about situated learning as part of the field of social learning. Social learning was a rising field starting in the 1970s that proposed that active participation and social interaction were essential for effective learning (Blackmore, 2010). Lave and Wenger (1991) propose a theory of newcomer learning where learning is a continuous, active, engaged, situated and identity forming process. Learning takes place in the workplace through informal and social interaction and is more about identity change than acquiring knowledge. They position the CoP as setting where such learning can happen, but never fully define this new concept.

However, the CoP itself is not completely new, especially within the field of social learning. The book with collected papers edited by Blackmore (2010) provides a good overview. The concept of a learning system was used in 1970 to indicate systems of interest where learning occurred that could be identified by an observer. Schön (Blackmore, 2010, Chapter 1) uses this concept and transfers it on national governments and states to show how entire societies evolve and learn. Vickers (Blackmore, 2010, Chapter 2) alters the concept slightly and calls it appreciative systems, since he believes people first need to show interest and value into a topic before actual learning can take place. The Hawkesbury group in Australia (Blackmore, 2010, Chapters 3–6) experimented with such systems and their practices become known internationally. They focused on the epistemology, ethics and systemic praxis within their communities to improve learning.

This foundation of research and ideas constituted to the rise of the CoP-concept after its introduction, even though no definition was given by Lave and Wenger (1991). The development of the concept is best followed using four sources (Cox, 2005; L. C. Li et al., 2009):

1) The book *Situated learning: legitimate peripheral participation* by Lave and Wenger in 1991,
2) The paper *Organizational learning and communities of practice: toward a unified view of working, learning and innovation* by Brown and Duguid in 1991,
3) The book *Communities of practice: learning, meaning and identity* by Wenger in 1998,
4) The book *Cultivating communities of practice* by Wenger, McDermott and Snyder in 2002.

As mentioned, Lave and Wenger (1991) introduce their theory of legitimate peripheral participation. This states that individuals do not receive knowledge, but they become a member of a group or community that deals with a certain practice that holds knowledge. Their membership starts on the periphery and they slowly move toward the center by becoming more connected to the community and thus acquiring the skills and knowledge. The learning occurs informally and in the workplace. This process of learning also creates their identity. The concept of CoP is introduced here to describe how workers engage in informal group both at work and off the job to share information and to develop solution of job-related problems (Cox, 2005; L. C. Li et al., 2009).

Brown and Duguid (1991) combine the insights from Lave and Wenger's work with concepts of Orr (1986, 1987, 1990b, 1990a) and Daft and Weick (1984) to link working, learning and innovation. They interpret learning as an improvement to create a new practice instead of acquiring the knowledge and skills of a practice as was done by Lave and Wenger. Their new perspective is aimed at organizations and encourages workers to engage in different communities and to create CoPs in order to learn, improve their work and to innovate for their organizations (Cox, 2005; L. C. Li et al., 2009). This is a distinct shift how Lave and Wenger (1991) understand learning and view CoPs, since they take it more towards an organizational setting and the field of Knowledge Management (KM).

Wenger (1998a) takes the next step by expanding on the concept of CoPs and by providing a first definition. He defines a CoP as a "*group that coheres through mutual engagement on appropriated enterprise and by creating a common repertoire"*. This definition shows that elements of a CoP are mutual engagement, a joint enterprise and a shared repertoire. The mutual engagement represents the continuous interaction between members that creates a shared meaning on issues and binds them together. The joint enterprise is the process or practice that the member are engaged in and work together on. The shared repertoire concerns all the common resources and products that are used and created by the members to negotiate meaning and facilitate learning. He refers to three "modes of belonging" that connect people to a CoP: engagement, imagination and alignment. They connect through the engagement with each other, by imagining themselves part of a group, and by aligning their own ideas and practices towards the group.

In his work, the CoPs are represented as self-organizing systems that occur in all sort of organizations with members from all sorts of different other CoPs. Wenger also puts emphasis on the role of identity shaping, since the CoP shapes and alters the identity of its members. Wenger (1998a) remains close to social learning practice and does (initially) not go along with ideas presented by Brown and Duguid (1991).

A twist begins with a publication of Wenger and Snyder (2000) that positions CoP in the organizational and managerial setting, thus also placing CoP in the field of KM. It is claimed that CoP helps to drive strategy, start new lines of business, solve problems quickly, transfer best practices, develop skills and help to recruit and retain talent. Even though CoPs cannot be mandated by managers, ingredients can be put together to support the creation of a CoP.

This twist is completed by the book of Wenger, McDermott and Snyder (2002). The definition of a CoP changes to *"groups of people who share a concern, a set of problems, or a passion about a topic, and who deepen their knowledge and expertise in this area by interacting on an ongoing basis"*. They further pursue the notion on how to create and foster CoP to enhance the competitiveness of firms ((L. C. Li et al., 2009). Three main characteristics of CoPs are presented and explained. The first is the domain, the common ground and boundaries that enable members to share and decide if it is worth spending time on. The second is the community, the social structure that facilitates learning through interaction. And the third is practice, the set of shared repertoires of resources. These three characteristics could be shaped and created. The role of leaders and facilitators is also introduced in order to create the CoPs. This book is sometimes seen as an inspirational and practical handbook with little value for research, especially since its contents are not empirically tested (Cox, 2005). However, this book did place the concept of CoP in the KM field.

The ideas on CoP provided by Wenger, McDermott and Snyder (2002) were taken as the basis by many in the KM field and build on by other researchers. The current research on CoPs is diverse and ranges from theoretical models on its functioning (Borzillo, 2017; Du Plessis, 2008; Edwards, 2005; Handley et al., 2006; Jeon et al., 2011; Y. M. Li & Jhang-Li, 2010) to empirical descriptions in real world situations such as schools (Chu, 2016), hospitals (Blackmore, 2010, Chapter 9; Cornes et al., 2014; Egan & Jaye, 2009; Lathlean & Le May, 2002; Mabery et al., 2013), and businesses (Machuca & Costa, 2012). This diverse set of research all pushed the concept of CoP forward and made it accepted as a KM tool for practices in the new knowledge-based economy.

There have been comments and critiques on the concept of CoP (Blackmore, 2010, Chapter 11; Roberts, 2006), especially concerning power and its influence on a CoP, the degree of informality, the tension between the goals of a CoP and an organization, and size and spatial reach. There have also been researchers who believe that the concept of CoP should return to its original field of social learning (Handley et al., 2006). However, none have been able to stop the popularity of this concept in organizational settings as a KM-tool.

However little can be found on the establishment, creation or design of a CoP; sometimes they are designed, sometimes they just exist, and sometimes they are just named as such. The only reference found is the book of Wenger, McDermott and Snyder (2002) that spurred the interest of many, but as mentioned above, the ideas from this book have not all been empirically tested. New insights are needed on the design and establishment of CoPs.

C. Timeline FERM

Table 8-1 presents the timeline of FERM. The first column shows the date and the second column presents the significant event on that date.

Table 8-1: Timeline FERM

Time	Event
2012	• The major of Rotterdam visits Singapore. Port cyber security is one of the discussion topics due to two small cyber incidents. These discussions started a set of discussions with the Driehoek of Rotterdam.
2013	
April 13th, 2013	**Approval by the Driehoek to operationalize the theme "resilience of cyber risks of the Rotterdam port area"** (Duin & Zeer, 2015) • Operationalization means a collaboration of public, private and knowledge organizations.
June 2013	Marijn van Schoote is appointed as the Information Security & Risk Officer of PoR.
Sep. 10th, 2013	**Meeting item "Roadmap Cyber security" is explained during the Supervisory Board meeting of PoR** (PoR, 2015) • Context: Digital threats are a risk for the safety and reputation of PoR and the Rotterdam port area. • The Capability Maturity Model (CMM) of Deloitte is used as reference. The aim is to rise PoR from level 2 to level 4.
2014	• Rotterdam becomes a member of the 100 Resilient Cities Program (100RC) • AIVD (Dutch intelligence agency) publishes a threat prognosis of the Rotterdam port area. This shows that there are numerous threats.
May 26th, 2014	**Conference "A trusted Dialogue"** (Municipality of Rotterdam, 2014) Representatives of government, business and science discuss several topics regarding the cyber security in Rotterdam. The covenant SEARS is signed; a PIB-consortium to export cyber knowledge to Southeast Asia.
2015	• Ineke Nierstrasz, Marijn van Schoote and Deltalinqs organize (three) masterclasses Information security for directors and high officials in Rotterdam. (partially in 2014) ○ The target audience are both public and private organizations. ○ At the first, the CEO of PoR takes part, but the Harbourmaster participates later on. ○ The Harbourmaster is informally asked by the major to take up the position as Cyber Resilience Officer (CRO) during the last masterclass. • The annual report of PoR makes a first mention of digitalization and cyber security. There is also a first mention of the operational risk "Cyber Crime". (PoR, 2016)
May 2015	**Deltalinqs, the Police's Sea Division, and the Port ISAC asks TNO to perform a research** (Duin & Zeer, 2015) • Aim: provide insight in the cases involved during a cyber incident for the port logistic chain. • Product aim: a generic concept to shape and execute a cyber resilience strategy • Sub aim: a vision on how to realize cyber resilience.

June 9-10, 2015	**Conference “Policing Global Cities”** (Municipality of Rotterdam, 2015) This international conference focusses on the current and new safety and security risks and developments in big cities. Cyber security is a small part of this.
Sep. 14-18th, 2015	**TNO presents the results of the Cyberchallenge** (TNO, 2015) • **Research questions**: How can big and small organizations of the port logistic chain gain insight in their shared needs and vulnerabilities and what are the starting points for them to improve their cyber resilience? • Explanation of resilience thinking. The main capacities are resistance, resilience and adaptability. • Assumption: To join individual strengths can create a unique set of resilience capacities. • Six Building blocks: - **Cyber Co-Op**: A cooperation of port companies to increase resilience capacities, to share knowledge, to buy collectively, to have shared representation, and to collaborate on training. - **Cyber Threat intelligence Watch**: an early warning system for threat information, cyber incidents, and the signals of the notification desk. This strategic building block helps to learn from incidents and to increase situational awareness. - **Cyber Community of Practice**: An exchange platform to 1) develop best practices, 2) judge and monitor new technology, and 3) create its own technology. - **Cyber Security & Response Team**: A specialists’ group to solve problems, provides advices, and trains. - **Cyber notification desk:** A central point for notifications regarding cyber. Its tasks consist of 1) collecting, analyzing and correlating information, 2) identifying organisations to share information with, and 3) alarming the Cyber Security & Response Team. - **Port Resilience Officer:** The official face of the digital port program that 1) holds control over training and agreements, 2) builds and facilitates a community, 3) is a liaison to other ports, and 4) helps to develop the other building blocks.
26 okt 2015	**Strategic vision document based on the findings of TNO** This document was created in collaboration with the Workgroup Cyber Resilience Rotterdam, DHVM, Municipality of Rotterdam, Directie Veilig Rotterdam, NCSC, Veiligheidsregio Rotterdam, Public Prosecution Service, and the Police’s Sea Division. (Duin & Zeer, 2015) It mentions that: • the original aim, to gain insights into shared needs and vulnerabilities of small and big companies in the port logistic chain, could not be achieved to the high complexity of the port area. • An innovative approach was used to think about cyber resilience in broad terms. Resilience was pushed here and buildings blocks were presented to realise the vision on resilience. These building blocks are the foundation of the entire strategy. • Seven building blocks (Communication was added) - **Cyber Co-Op:** A collective organization for shared acquisition of products and to share knowledge.

	- **Cyber Treat Intelligence Watch:** an early warning system for threat information, cyber incidents, and the signals of the notification desk. This strategic building block helps to learn from incidents and to increase situational awareness, but also to create their own intelligence. - **Community of Practise:** A knowledge management instrument to connect organizations informally. The aims are 1) to use each other's knowledge, expertise, network and resources, 2) to improve the network and the trust, 3) to have quicker and better connection in case of emergency, 4) to start collective initiatives. The target audience is generalists. - **Cyber Security & Response Team:** a team for early notice and quick action. The team consists of partners in the logistic chain and back-up specialists. This block has a lot of interaction with other blocks. - **Cyber Notification Desk:** a notification desks for real time threats and disruptions. The aim is to reduce response time through an efficient process. - **Port Resilience Officer:** The official leader of cyber security and resilience in the port area. He connects the organisations and acts like an ambassador. He is actively connected to 100RC. His position transcends the individual public and private organizations. - **Communication:** To ensure structured communication. It is created for the complex port network and it aims to connect organizations and to have them stay connected.
2016	• Consultation report Rotterdam Resilient Strategy is published with seven building blocks (Municipality of Rotterdam & 100 Resilient Cities, 2016). • The HbR annual report mentions digitalisations as a focus point of 2016. A port CRO is also appointed and an internal Information Security Awareness campaign is started. The operational risk "Cyber Crime" remains. • The Harbourmaster decides to develop the concepts of a CRO and to present the results to the Driehoek. • Jan Willem Verkiel (DHVM) starts with the creation of the CRO programme using the building blocks that were presented by TNO.
March 2016	**A first concept for the CRO program** Involved organizations: VRR, Deltalinqs, Police's Sea Division, Municipality of Rotterdam, and PoR. • There is, to this point, no knowledge of the legal possibilities and responsibilities. There is also no insight in important initiatives and networks regarding cyber. • Seven focus points (inspired on the findings of TNO) are presented. - **Communication and increasing cyber awareness**: the aim is to promote the CRO and increase the cyber awareness in the port area. - **Education**: The target audience is broad; ranging from high schoolers to employees of PoR and other organizations. A part of this focus point is to provide information.

	- **Legal framework**: the connection between the Port Security Office (PSO) and the Cyber Resilience Officer (CRO) need to be established and researched. - **Self-Assessment**: a tool that enables organizations to test themselves. A connection is made with other PoR-tools (such as the Port Security Toolkit). This tool can be developed by PoR or by another organization. - **Cyber Risk Management:** to monitor, analyse and react to cyber incidents. The first step is gaining an overview of the cyber risks and to operationalize these risks. - **Training:** it is expected that VRR will lead this focus point. - **Community Management:** networks need to be connected in order to create a "new" community. • The total expected costs are set to €100.000.
April 2016	**A proposal for the CRO program** PoR has a leading position. The other involved organizations are: Police's Sea Division, Deltalinqs, and the Municipality of Rotterdam. (Verkiel & Hoitink, 2016) • The building block education is added, making a total of eight building blocks. • Four workgroups are created - **Organisation and Communication** led by PoR: **Organisation** is led by Jan Willem Verkiel and Robert Jan Hoitink. The main task is to define the part of the Port Resilience Officer. Then they will focus on the CoP and the Co-Op. They want to set up the strategy for the entire CRO program. **Communication** led by Nadine Vos (PoR) and Jasper Nagtegaal (Deltalinqs). Their tasks are to create a communication strategy, a corporate identity, and a website. - **Legal Framework** led by PoR (Elsa Martens and Reinout Gunst). Their task is to determine the legal responsibilities and obligations of the Harbourmaster and to provide an advice regarding his position. This focuses more on PoR. - **Risk Management** led by Police's Sea Division (Peter Duin and Marielle Zeer). Their task is to create Cyber Notification Desk, Cyber Threat Intelligence Watch, and Cyber Security & Response Team. - **Education, Training and Awareness** led by Deltalinqs (Jasper Nagtegaal) and Police's Sea Division (Peter Duin). Their task is to provide training, training materials and checklists. • There is a general set of deadlines for deliverables. • There is a proposal on how to finance the program using support from four partners. **Document CRO** (Verkiel, 2016) • The aim of the CRO program is a balance between prevention and authority. • The following list of agreements are agreed. - Starting at June 1st 2016, a programme manager starts for FERM - Police's Sea Division, Deltalinqs and PoR provide the funds of €100.000.

	- The CRO program is launched in Sep. 2016 with a seminar. The following are clear by that time: goals, tasks, authorisations, organization, communication strategy and the legal framework. - Police’s Sea Division continues with Cyber Notification Desk, Cyber Threat Intelligence Watch, and Cyber Security & Response Team. This will be monitored by the CRO since it is part of the building blocks. - An important objective is to promote knowledge exchange between port-related organizations instead of just awareness. This will be done by expanding on the Cyber Café meetings organized by Police’s Sea Division. - The following need to be done or constructed: Do’s & Don’ts flyer, a self-assessment tool, a port cyber exercise (led by VRR, supported by the CRO), a nautical chain partners exercise (led by the CRO). - Deltalinqs will collaborate with the CRO in order to develop training modules.
June 2016	Sarah Olierook is assigned as the program manager of FERM
June 6th, 2016	Port Cyber Top 2016: a (international) summit with regards to cyber security in ports.
June 8th, 2016	PoR announces that the Harbourmaster will also fulfill the position of Port CRO. He will execute this position with the help of four workgroups.
June 23th, 2016	**FERM Workgroup meeting 1** • The composition of the Steering board is discussed and decided on. • The official launch of the PCRO will be at the Deltalinqs autumn lecture on Nov. 30th. Deltalinqs are in the lead on this project. Jasper Nagtegaal resigns and leaves his responsibilities with Peter van Loo. • The corporate identity, logo, and website are ready for the autumn lecture. PoR took the lead in this project. • The cyber exercises of VRR and the nautical chain partners will be combined. PoR will lead this in collaboration with the Police’s Sea Division and VRR. • The autumn lecture will be used to see if organizations are interested in the self-assessment tool. Police’s Sea Division has the lead in this project. • A memo is drafted regarding the legal framework. This memo can be discussed during the autumn lecture. • Peter Duin is exploring the options for the Cyber notification desk and the Cyber Response team.
Sep. 30th, 2016	**FERM Steering Board meeting 1** • 4 workgroups: Organisation and Communication, Legal Framework, Education, Training and Awareness, and Risk Management • The group Task Force Cyber security (consisting of the Public Prosecution Service, the Municipality of Rotterdam and the Police) is disincorporated. • People from the Public Prosecution Service and DCMR are added to the workgroups. • Communication: - The official launch of the PCRO will be at the Deltalinqs autumn lecture on Nov. 30th.

	- The corporate identity and the website are currently being constructed. - On Oct. 3th, the AIVD will present some of her findings regarding the cyber security in the port area. • Legal Framework: - Documents were drafted with several frameworks and propositions. This provides a baseline for further discussion. - It is considered to let the VRR become part of the PCRO. • Risk Management: The risk heat map will be checked by the NCTV • The total budget is agreed on by the members. **Attachment: Vision and Communication CRO** • The buildings blocks presented by TNO are the foundation. The aim of the PCRO program is aimed to have port-related organizations collaborate to become the most secured port against cyber aggression. (translated from: “*Het PCRO wil de havenbedrijven samen laten werken en awareness creëren om de best beveiligde haven tegen cyber agressie te worden.”)* • The aims of the PCRO are 1) to improve the resilience, 2) to increase awareness, and 3) to strengthen collaboration. • The PCRO takes the position of an ambassador and leader of the companies in the Rotterdam port area. The main stakeholders are the Port ISAC, the CRO partners (Public Prosecution Service, Police’s Sea Division, Municipality of Rotterdam, and PoR), NCSC, VRR, secondary municipalities and residents. • The focus of the program is communication. Communication is aimed to ensure connection and trust. • The ambitions of the PCRO are 1) to communicate with the target group using the website and corporate identity, 2) to create training programs, 3) to manage risks, 4) to set legal conditions. These ambitions are led by the program manager. • The Police’s Sea Division will set up a Response team, but port-related companies also need to create an expert group. • Deadlines are set.
Oct. 3th, 2016	the AIVD presents some of her findings regarding the cyber security in the port area.
Oct. 13th, 2016	**FERM Workgroup meeting 2** • Claudia Agricola (Public Prosecution Service) and Ramon Dohmen (DCMR) join the workgroup • The meeting consisted mostly of updates from each member.
Oct. 27th, 2016	A law is issued that states that companies within vital infrastructure are required to notify the NCSC.
Nov. 2nd, 2016	A port Cyber exercise with nautical chain partners led by VRR • MPA Singapore attends this exercise.
Nov. 10th, 2016	**FERM Workgroup meeting 3** • An interesting topic of discussion is the SME cybertoolkit created by the municipality steering group Veilig Ondernemen. Sarah Olierook explains and shares this with the group.

	• A presentation is given with a concept for the corporate identity. This also consists of a self-scan tool. Clockwork presents her concept. - Assumption: The aim of the platform is 1) to create awareness, 2) to share information and resources, and 3) to connect knowledge and people. - A trademark is presented: FERM. - The design values are trust and connection. - The initial colour scheme for the corporate identity and the logo are presented. • The program of the Deltalinqs autumn lecture is discussed. • The exercise of Nov. 2nd is evaluated. • Membership to the consortium HSD is considered and discussed.
Nov. 30th, 2016	Launch of FERM and the CYSSEC website on the Deltalinqs autumn lecture with the theme Security Awareness.
8 dec 2016	**FERM Workgroup meeting 4** • This meeting mainly focused on updates and finishing up the details of 2016.
2017	• Cyber security has its own header in the section Safety in the PoR annual report. This means that cyber security is officially separated from digitalization. The operational risk “Cyber Crime” remains. FERM is explicitly mentioned with regards to cyber security. • The aim of FERM for 2017 is to gain hold in the IT Security networks and to improve on the strategy of 2016. • FERM becomes a member of the HSD Consortium.
Feb. 9th, 2017	**FERM Workgroup meeting 5** • NCSC joins the workgroup meetings. • A small overview of the activities in 2016 is presented. The conclusions are: - 2016 was used to set up the PCRO, create a brand and build an initial network. - The aim for 2017 is to gain hold in the IT Security networks and to improve on the strategy of 2016 by organizing activities. • A proposition regarding a new Workgroup structure is proposed and discussed. - Communication: the focus becomes the media campaign and to further develop the website. PoR is leading this. - Event *Sta jij FERM?* an event organized for SMEs and is led by PoR. - Training: A cyber exercise as well as a follow-up on the exercise of past November. PoR is leading. - Education: the aim is to improve the knowledge level in the partners’ organizations. Deltalinqs and the Police’s Sea Division are leading this. - Legal affairs: monitoring and translating new laws and regulations. PoR has the lead. - Risk management: this is led by Police’s Sea Division - Contact has also been made with Schiphol and the airport ISAC. • The Marketing & Communication Strategy of FERM is presented.

	- Central aim: To create awareness at companies in the Rotterdam port area regarding cyber resilience and the risks and vulnerabilities of cyber security and cybercrime. To develop a space in which collaboration and knowledge exchange regarding cyber resilience can take shape between actors in the Rotterdam port area. (translated from: "*Awareness creëren bij bedrijven in de haven van Rotterdam m.b.t. cyber resilience en de risico's en kwetsbaarheden van cyber security en –crime. Een omgeving creëren waarin samenwerking en kennisuitwisseling op het gebeid van cyber resilience tussen bedrijven in de haven centraal staat.")* - Target group: Companies in the Rotterdam port area. - Responsibilities: 1) legal knowledge, 2) training and education, 3) notification desk, 4) keep an overview of the general safety and security level. - Goals: 1) **Awareness** of the FERM initiative, 2) **Knowledge** of FERM's aims and tasks 3) positive **attitude** regarding the improvement of cyber resilience, knowledge exchange and pro-active collaboration.
March 16th, 2017	**FERM Workgroup meeting 6**
March 23th, 2017	**Event: Sta jij FERM?** • 178 participants of which 48 are Port Facility Security Officer (PFSO)
March 24th, 2017	**FERM Steering board meeting 2** • The Steering Board accepts a multi-annual financial commitment until Dec. 31st 2019 regarding the FERM program. - The contribution of every partners is €25.000 excl. per year. - There is an addition in special cases the annual contribution can be increased. - The work is done using workgroups. PoR focuses on Communcation, the Municipality focuses on the legal framework, Deltalinqs has the lead on training and awareness. PoR will organize the big training exercise and the Police's Sea Division performs the risk management. • Port Cyber Cafés (PCCs) are set as a regular activity of FERM. • An update is given regarding the NIB-regulation. • Awareways has become the permanent M&C office of FERM. The M&C approach and the communication strategy is presented. • FERM is approached for SBIR co-funding starting from €250.000,-. **Memo Ambitions FERM 2017** Three additional goals are formulated: • **Being able to control large scale cross-company cybercrisisses** - Creating a team of ICT-specialist from current specialists in the port area, from collaborations and from external organizations (FOX-IT) - This team can be contacted in case of emergency. - These Cyber-specialists provide advice. This team will become the Building Block Cyber Security & Response Team. The following activities should be pursued: 1) mapping the ICT-

	specialists in the port area, 2) training ICT-experts with specific skills 3) mapping the ICT-systems used in the port area, 4) creating a cyber-disaster contingency plan. • **Improve the readiness in event of a large scale cross-company cybercrisis** - Performing a cyber-exercise with all partners. The following needs to be done: 1) write a realistic scenario, 2) prepare scripts, 3) have a facilitator from the private sector, 4) implement the project management for the exercise. • **Gaining insights in the current level of security in the process systems of vital parts of the port of Rotterdam.** - This can be performed by a university.
April 13th, 2017	**FERM Workgroup meeting 7**
May 11th, 2017	**FERM Workgroup meeting 8**
June 27th, 2017	APM terminal hack (Bremmer & van Heel, 2017; Noort, 2017; RTV Rijnmond, 2017)
July 20th, 2017	**Port Cybercafé 1**: Ransomware and Threadstone 47 participants, 8 no shows
Aug. 3th, 2017	**FERM Workgroup meeting 9**
Sep. 11th, 2017	Themasession on Cyber Security for the Veiligheidsdirectie
Sep. 14th, 2017	**Port Cybercafé 2**: Information security and awareness 41 participants of which 8 attended PCC1 and 33 were new. There were 14 no shows.
Sep 28th, 2017	**FERM Workgroup meeting 10** • Focuses on Education, but there is no concept or proposal on the focus point fort his building block.
Oct 26th, 2017	**FERM Workgroup meeting 11** • InnovationQuarter reached out to FERM for a collaboration regarding the PCCs.
Nov. 2nd, 2017	• **Cybernautics 2017** (first edition) – Board level exercise - Berenschot facilitates and presented a final report. • **Port Cybercafé 3**: Incident response 35 participants of which 10 attended PCC2 and 17 were new. There were 22 no shows.
Dec 13th, 2017	**FERM Steering board meeting 3** • There is a discussing regarding a cyber KPI for PoR. A first measurement should be done to gain insights. • It is decided that FERM will not actively seek collaboration with other network organizations, since it is not connected to FERM's goals. • A annual plan is presented containing the following highlights: - There is a concept report regarding the APMT hack from COT. - A scheme with notification criteria its resulting scale is presented. - The workplan for 2018 consists of 1) mapping what the sector wants from FERM, 2) setting up a notification desk, 3) perform a

	friendly hack, 4) organize 6 PCCs, 5) look into the Response team, 6) starting the building block Education, 7) developing a KPI
2018	
Jan. 18th, 2018	**Port Cybercafé 4**: Hacking the new year 31 participants of which 8 attended PCC3, 17 were new, and 20 no shows.
Feb. 2nd, 2018	**Handover of the FERM cartoon** NCSC offers FERM a cartoon as a token of appreciation for the positive and constructive collaboration between NCSC and FERM in 2017 and for the trust in the continuation of this collaboration in 2018.
March 12th, 2018	The first FERM graduation student starts a research regarding the building blocks Community of Practice.
March 29th, 2018	**FERM Workgroup meeting 12** • Discussions with Avans started regarding collaboration for education. They can offer the following: 1) financed research, 2) thesis projects, 3) interns, 4) project-directed education. • A questionairre must be send to companies to perform an initial measurement for the KPI and to gain insights for the workgroup Education. • DTC subsidy is considered.
April 5th, 2018	**Port Cybercafé 5**: Cybercrisis exercise with FOX-IT 22 participants of which 7 attended PCC4 and 7 were new. There were 13 no shows.
April 10th, 2018	**FERM Workgroup meeting 13** • The DTC subsidy is discussed to gain funding for an explorative research on implementing a CERT. • The schedule for the PCCs is discussed.

D. Overview of the FERM building blocks

This appendix provides an overview of the different interpretation of the building blocks based on the an internal document of the Police's Sea Division (Duin & Zeer, 2015) and the initial presentation of TNO (2015). TNO presented only the first six building blocks and the Police's Sea Division added the building block Communication quite quickly. No description was found on the last building block Education. The activities and results were found during the creating of the FERM timeline. Appendix B thus provides these in a the proper historical sequence and with some more detail.

Cyber Co-Op

TNO

This cooperation of port organizations improves the resilience capacities of her members independently and in collaboration by the collective purchase of products and exchange of knowledge. It can also look after the needs of her members, organize activities and exercises. Other building blocks can also be enabled through this cooperation, such as the building blocks Cyber Security & Response Team, the Cyber Notification Desk, and the Cyber Intelligence Watch.

Products and services can be offered more economically making it possible to increase the cyber resilience. The Co-Op also increases the awareness for cyber resilience and the knowledge and skills of her members. Lastly, it can serve as a helpdesk for issues concerning installation, configuration and other practical problems.

Police's Sea Division

The cooperation is support organization for the collective purchase of cyber security products as well a contact point for its members. It can also act as a knowledge and network facilitator. The Co-Op stimulates and accelerates a higher and better security level, collaboration, innovation and knowledge exchange.

Activities and results

- The self-assessment tool of Threadstone that is available on the FERM website.
- The awareness test that is available on the FERM website.

Community of Practice

TNO

This platform offers professional the possibility to exchange knowledge, to develop best practices and technologies, or to monitor and judge recent new technologies. It can share examples, new knowledge and perspectives on cyber security. This increases the general knowledge level, provides new ideas on possible actions, and signals new technologies.

Police's Sea Division

The CoP is a knowledge management tool aimed to connect generalists. The meetings provide insights in recent developments and provoke discussion. New initiatives can also be shared here.

The aim is to use each other's diversity in knowledge, expertise, network and resources, to create trust and networks, and to create better connections in case of emergency.

Activities and results

- Five Port Cybercafés (PCCs) have been organised that shares knowledge.

- There is a blacklist on storage spoofing.

Port Cyber Resilience Officer (PCRO)

TNO
The PCRO is the guardian of the digital port. He supervises the cyber exercises and agreements in the Rotterdam port area. He helps to build a community and to improve the other building blocks.

Police's Sea Division
The PCRO is the face and ambassador of the cyber reputation in the Rotterdam port area. He connects organizations and networks.

Activities and results

- René de Vries is appointed as PCRO.
- He is the face of the FERM program and attends most activities.
- He is part of a multitude of networks.

Cyber Threat Intelligence Watch

TNO
An early warning systems that collects, analyzes and enriches information as a means to prevent cyber incidents. This information can be shared with other organizations. It improves the situational awareness in the Rotterdam port area.

Police's Sea Division
Het fungeert als een early warning systeem voor mogelijke dreigingen. Dit wordt gedaan op basis van (inter)nationale dreigingsinformatie, cyberincidenten in andere domeinen en signalen via de cyber notification desk. Deze strategische bouwsteen verzorgt een actueel en gezamenlijk beeld van de haven en helpt om te leren van incidenten. Het doel is om incidenten te voorkomen.

Activities and results

-

Cyber Security & Response Team

TNO
This team consists (ICT) specialists that solves immeadiate disturbances and problems as well as provides advice when needed. They practice together and have a lot of knowledge of the Rotterdam port area. It shortens the downtime in case of an incident and it offers suggestions to improve the cyber security. This team can also serves a training ground.

Police's Sea Division
This is a team of seasoned specialists that act quickly and effectively in case of emergency. This building block is connected to the two other building blocks: the cyber notification desk and the CoP. It differs from the cyber notification desk in the sense of the focus in time. The Cyber Security & Response Team focuses on the short term, while the notification desk focuses the long term. It differs from the CoP, since the CoP focuses on knowledge exchange and the Cyber Security & Response Team on training.

Activities and results

-

Cyber Security Notification Desk

TNO

This is point of contact in case of disturbances and threats. This information is collected, analyzed and correlated after which it is shared with the significant organizations. It lowers the reaction time and stimulates a proactive determination of issues as a means to prevent incidents. This building block works well in combination with the building block Cyber Security & Response Team.

Police's Sea Division

This is a point of contact in case of real-time cyber-related threats and disturbances and it provides the information to counter this threats such as the determination of the issue and quick response measures. It also spreads information relevant to its members. It can lower the response time.

Activities and results

- Notifications concerning storage spoofing were noticed and a blacklist website was created and kept up-to-date.

Communication

Police's Sea Division

This is condition for the success of the other building blocks. It focuses on the network of and in the Rotterdam port area. The communication varies from providing general information to proclaiming new policy, from sharing knowledge to providing more background information.

Activities and results

- The FERM website was created and launched.
- News items and blogs are shared on the website.
- There were 2 large announcement events: at the autumn lecture of Deltalinqs and the "Sta jij FERM?" event
- Five PCCs have been organized.
- Information on storage spoofing has be shared using a storage spoofing website with the blacklist.

Education

Activities and results

- Cyber exercises were done in 2016 and 2017.

E. Questions in Questionnaire

A questionnaire was issued by the PoR as part of an exploratory research into cyber security in the Rotterdam port area. The questionnaire was only available in Dutch. Therefore the added questions for this research are translated and are presented. The next subsection shows the all (Dutch) questions in the original sequence. The added questions are:

1. Are you familiar with the initiative FERM?
   - *Yes*
   - *No*

2. Is your organization open to explore modes of collaboration with other organizations in the Rotterdam port area concerning cyber security?
   - *Yes*
   - *No*
   - *I don't know*

3. Is your organization open to share knowledge and experience concerning cyber security with other organizations in the Rotterdam port area?
   - *Yes*
   - *No*
   - *I don't know*

4. Is your organization open to develop knowledge and experience in cyber security with other organizations in the Rotterdam port area?
   - *Yes*
   - *No*
   - *I don't know*

5. The following activities would be useful for my organization:
   - *Sharing threat information (intelligence watch)*
   - *Inform organizations concerning cyber security*
   - *Guidance and help in case of a cyber-attack or incident*
   - *To facilitate knowledge exchange between organizations concerning cyber security*
   - *To train and educate organizations concerning cyber security*
   - *To facilitate collective purchase for affiliated organizations*
   - *Other…*

Questionnaire

This subsection presented the complete questionnaire in Dutch.

1. Wat is de naam van uw organisatie?

2. Wat is uw naam en mailadres?

3. Tot welke sector behoort uw organisatie?
      - *Havenlogistiek*

- *Maritieme dienstverlening*
- *Industriële dienstverlening*
- *(Proces)industrie*
- *Anders, namelijk …*

4. Hoeveel medewerkers telt uw organisatie, inclusief de eigenaar(en)/directie?
    - *1-9*
    - *10-49*
    - *50-249*
    - *250-999*
    - *>1000*

5. Bent u uitvoerend belast met en/of bent u verantwoordelijk voor de informatiebeveiliging, cyberbeveiliging, informatie technologieën of iets gerelateerd met digitale veiligheid binnen uw organisatie ?
    - *Ja*
    - *Nee*

6. Zijn deze apparaten met het internet verbonden?
   Kruisje zetten

	Ja, deze is/zijn allemaal aan het internet verbonden	*Sommigen zijn aan het internet verbonden, niet allemaal*	*Nee, deze is/zijn niet aan het internet verbonden*
Desktop (vaste computer)			
Laptop			
Tablet			
Smartphone			

7. Zijn er binnen uw organisatie nog andere apparaten aanwezig die verbonden zijn met het internet? (meerdere antwoorden mogelijk)
    - *Ja, apparaten voor het primaire proces*
    - *Ja, apparaten voor gebouw beheer systemen (zoals bijvoorbeeld camera's, hek- en sluitwerk)*
    - *Ja, apparaten voor industriele controlesystemen of procesbeheersing (zoals bijvoorbeeld het bestuur en bewaking van productieprocessen)*
    - *Nee, dit ben ik op dit moment aan het ontwikkelen*
    - *Nee, dit ben ik op de lange termijn van plan*
    - *Nee, dit ben ik niet van plan*
    - *Anders, namelijk …*
    - *Weet niet*

8. Stelling: Ik ben mij bewust van de online kwetsbaarheden van deze aan het internet verbonden apparaten?
   Een 5 puntsschaal

9. Door wie wordt de server van uw organisatie beheerd?

- *Dat doe ik zelf*
- *Door een interne IT-specialist/afdeling*
- *Door een externe IT-specialist*
- *Anders, namelijk: …*

10. Welke netwerkvoorzieningen komen voor in het bedrijfsnetwerk van uw organisatie?

- *Wi-Fi Access point*
- *Firewall*
- *ADSL-access point*
- *VPN (Virtual Private Netwerk)*
- *Geen van allen*
- *Anders, namelijk: …*
- *Weet ik niet*

11. Door wie wordt de website van uw organisatie beheerd?

- *Die is in eigen beheer*
- *Door een externe partij*
- *Weet ik niet*

12. Heeft de website van uw organisatie een beveiligingscertificaat (uw website begint met https://www)

- *Ja*
- *Nee*
- *Weet ik niet*

13. Van welke back-up voorzieningen maakt uw organisatie gebruik?

- *Externe mobiele opslag (Externe harde schijf, USB-stick)*
- *Aparte interne server*
- *Aparte externe server*
- *Back-up voorzieningen via Cloud-diensten (Google Drive, Dropbox)*
- *Gespecialiseerde back-up via een externe partij*
- *Wij maken geen back-up*

14. Maakt uw organisatie gebruik van Cloud-diensten?

- *Ja*
- *Nee*
- *Weet ik niet*

15. Welke technologieën gebruikt uw organisatie (meerdere antwoorden mogelijk)?

- *Global Positioning Systems (GPS) of Differential GPD (GDPS)*
- *Electronic data interchange (EDI)*
- *Radio-frequency identification (RFID)*
- *Real-time location systems (RTLS)*

- *Wireless sensor networks (WSN)*
- *Mobile devices (smart phones etc.)*
- *Information Communication Technologies (ICT) (for example e-mail, Instant Messaging (IM) and virtual meeting systems)*
- *Anders, namelijk …*

16. Welke algemene informatiesystemen gebruikt uw organisatie ?
    - *Executive Support Systems (ESS)*
    - *Management Information Systems (MIS)*
    - *Decision-Support Systems (DSS)*
    - *Transaction Processing Systems (TPS)*
    - *Enterprise Resource Planning (ERP)*
    - *Customer Relationship Management (CRM) systems*
    - *Knowledge Management Systems (KMS*
    - *Supply Chain Management (SCM) systems*

17. Welke haven- en industrie gerelateerde informatiesystemen gebruikt uw organisatie?
    - *National single window*
    - *Port community systems (PCSs)*
    - *Port Authority Management / Havenmeester Management Information System (HaMIS)*
    - *Vessel Traffic Services (VTS)*
    - *Shackle and pole reservation system*
    - *Automatic Identification Systems (AID)*
    - *Port River Information Systems (PRIS)*
    - *Terminal Operating Systems (TOS) Automated Yard Systems*
    - *Gate appointment systems*
    - *Automated Gate Systems*
    - *Warehouse management system (WMS)*
    - *Port Road and Traffic Control Systems*
    - *Intelligent Transport Systems (ITS)*
    - *Port Hinterland Intermodal Information Systems (PHIIS)*
    - *Douane aangiftesystem (AGS) / Custom declaration system*
    - *Supervisory Control And Data Acquisition (SCADA) systems*
    - *Distributed Control Systems (DCS)*
    - *Manufacturing Execution Systems (MES)*
    - *Product Lifecycle Management (PLM) systems*
    - *Anders, namelijk …*

18. Hebben de medewerkers binnen uw organisatie toegang tot gevoelige digitale informatie?
    - *Ja, alle medewerkers hebben toegang tot alle digitale informatie*
    - *Gedeeltelijk, medewerkers hebben alleen toegang tot die digitale informatie die zij nodig hebben voor het uitvoeren van hun werkzaamheden*

- *Nee, de medewerkers hebben geen toegang tot de digitale informatie van de organisatie*
- *Weet ik niet*

19. Zijn er externen die toegang hebben tot gevoelige digitale informatie? (Denk hierbij aan contractors, partners, adviseurs)
    - *Ja, (enkele) externen hebben toegang tot alle digitale informatie*
    - *Gedeeltelijk, (enkele) externen hebben alleen toegang tot die digitale informatie die zij nodig hebben voor het uitvoeren van hun werkzaamheden*
    - *Nee, externen hebben geen toegang tot de digitale informatie van het organisatie*
    - *Weet ik niet*

20. Met welke organisaties werkt uw organisatie digitaal samen (Denk bijv. geautomatiseerde koppelingen?
    - *Portbase*
    - *Secure Logistics*
    - *Havenbedrijf Rotterdam N.V.*
    - *Divisie Havenmeester van het Havenbedrijf Rotterdam N.V.*
    - *DirkZwager*
    - *Douane*
    - *DCMR*
    - *Gezamenlijke Brandweer*
    - *Anders, namelijk …*

21. Stelling: De bedrijfsprocessen in mijn organisatie zijn volledig afhankelijk van computers en internet (ICT)?
    5 puntsschaal

22. Stelling: Ik ben mij bewust van de online veiligheidsrisico's (cybercrime) die mijn organisatie loopt?
5 puntsschaal

23. Stel, er wordt ingebroken in de systemen van uw organisatie, wat zou de schade kunnen zijn?
- *Er wordt geld gestolen*
- *Er worden gastgegevens gestolen*
- *Er worden bedrijfsgegevens gestolen*
- *Bedrijfsprocessen liggen stil*
- *Er kan imagoschade optreden*
- *Er kunnen juridische en/of contractuele problemen ontstaan*
- *Anders, namelijk: …*

24. Hoe groot is de **economische** schade die een cyberaanval op uw organisatie zou kunnen hebben (bijv. financiële schade, imago schade etc)?
    Schaal van 1 tot 7 (waarbij 1 heel weinig en 7 heel veel is)

25. Hoe groot is de **financiële** schade door cybercriminaliteit bij uw organisatie ongeveer? Graag afronden op hele bedragen)
    - *Zeg ik liever niet (maar er was wel sprake van schade)*
    - *Weet ik niet*
    - *… euro (tekstueel antwoord)*

26. Hoe groot is de **fysieke** schade die een cyberaanval op uw organisatie zou kunnen hebben? *Schaal van 1 tot 7 (waarbij 1 heel weinig en 7 heel veel is)*

27. Welke technische maatregelen heeft uw organisatie genomen om online risico's (zoveel mogelijk) uit te sluiten?

	Ja	*Nee*	*Weet ik niet*
De computers van het organisatieorganisatie zijn voorzien van virusscanner			
De virus scanner(s) is(/zijn) up-to-date			
De computers/het network van het organisatie zijn/is voorzien van een firewall			
De firewall(s) is(/zijn) up-to-date			
Het (draadloze) network is beveiligd			
De software op het bedrijfsnetwerk wordt up-to-date gehouden			
(Internet)activiteiten op het bedrijfsnetwerk worden geregistreerd (gemonitord/gelogd)			
De logs worden (regelmatig) bekeken/geëvalueerd			
Bestanden met vertrouwelijke informatie worden versleuteld opgeslagen (bijvoorbeeld middels encryptie)			
Bestanden met vertrouwelijke informatie worden versleuteld verstuurd (bijvoorbeeld middels encryptie)			
Er wordt gebruik gemaakt van biometrische beveiligingsmethode, zoals vingerafdruklezers			

28. Welke beleidsmaatregelen heeft uw organisatie genomen om online risico's (zoveel mogelijk) uit te sluiten?

	Ja	*Nee*	*Weet ik niet*
Er wordt gebruikt gemaakt van biometrische beveiligingsmethoden, zoals vingerdruklezers.			
Er is een schriftelijke weergave aanwezig van de huidige ICT infrastructuur (netwerk/computersystemen)			
Er zijn scenario's ontwikkeld waarin is beschreven hoe het organisatie slachtoffer kan worden van cybercrime (een ex-medewerker die bijvoorbeeld inlogt op het bedrijfsnetwerk en vertrouwelijke informatie steelt)			
Er is een protocol opgesteld waarin is beschreven hoe te handelen bij cybercrime			
Er is een informatiebeveiligingsbeleid aanwezig			
Werknemers worden bewust gemaakt van online risico's			

Werknemers hebben geleerd om geen email van potentieel onbetrouwbare afzenders te openen			
Werknemers hebben geleerd online betalingsopdrachten te verifieren langs een extra kanaal alvorens uit te voeren (bijv. om CEO/CFO fraude te voorkomen)			
Werknemers hebben geleerd om goed op te letten bij het doen van onlinebetalingen (bijvoorbeeld op de 's' achter de http of op het slotje in de webbrowser)			
Werknemers hebben geleerd om geen gevoelige informatie, privé en zakelijk, op het internet te verstrekken (bijv. social media)			
Werknemers moeten verschillende sterke wachtwoorden voor online accounts gebruiken (combinatie van minstens 8 cijfers en letters)			
Het is verplicht om wachtwoorden met regelmaat te wijzigen			
Er worden regelmatig (veiligheids)audits uitgevoerd			
Het is toegestaan dat werknemers privé apparatuur aan het bedrijfsnetwerk koppelen (BYOD)			
Er zijn (schriftelijke) regels opgesteld over het gebruik van ICT voor privé doeleinden			
Er zijn (schriftelijke) regels opgesteld voor het doen van online betalingen (bijv. 4 ogen principe)			
Er zijn (schriftelijke) regels opgesteld over het omgaan met vertrouwelijke informatie, zoals persoonsgegeven van u, uw medewerkers en/of gasten			
Er zijn (schriftelijke) regels opgesteld over het openen van onbekende bestanden (zoals bijlagen in e-mails)			
Er zijn (schriftelijke) regels opgesteld over het (op verzoek) afgeven van bedrijfsgegevens			
Het is verplicht om wachtwoorden met regelmaat te wijzigen			
De toegang tot de digitale informatie geblokkeerd nadat de gebruiker deze niet meer nodig heeft			
Er worden maatregelen getroffen op het gebied van detectie (bijv. door een Intrusion Detection System)			

29. In hoeverre heeft uw organisatie te maken gehad met de volgende incidenten?

	Meerdere keren slachtoffer	*Één keer slachtoffer*	*Een of meerdere mislukte pogingen (dus geen slachtoffer*	*Niet mee te maken gehad*	*Weet ik niet*
Afpersing via internet (het moeten afgeven van geld of goederen door bedreiging en/of geweld)					
Chantage via internet (het moeten afgeven van geld of goederen door bedreiging met smaad, smaadschrift of openbaarmaking van een geheim)					
Denial of Service (Dos-)aanval (digitale aanvallen op het systeem waardoor dit wordt overbelast en niet meer					

beschikbaar is, bijvoorbeeld het platleggen van de website)					
Defacing (het zonder toestemming veranderen/bekladden, vervangen of vernielen van de website van uw organisatie					
Diefstal van datadragers (zoals pc, laptop, usb-sticks)					
Diefstal van gegevens (opzettelijk afgetapte of opgenomen gegevens die niet voor de dader bestemd zijn)					
Fraude/oplichting via internet (financiële schade oplopen middels bedrog)					
Hacking (inbraak op de computersystemen van uw organisatie)					
Identiteitsmisbruik via internet (het misbruik maken van de identiteitsgegevens van uw organisatie)					
Malware (infectie van computersystemen middels virussen, trojan horses, spyware en/of wormen)					
Ongeautoriseerd gebruik van het bedrijfsnetwerk (bijvoorbeeld voor het downloaden/verspreiden van illegale software, kinderpornografie, SPAM of het plaatsen van berichten van racistische of discrimineerde aard)					
Phishing (het via digitale middelen – zoals e-mail – met een verzinsel informatie over uw organisatie ontfutselen via mensen binnen uw organisatie)					
Ransomware (een programma dat een computer (of gegevens dier erop staan) blokkeert en vervolgens van de gebruiker geld vraagt om de computer weer te "bevrijden")					
Skimming waarbij op een onrechtmatige wijze pinpas- of creditcardgegevens van uw organisatie zijn bemachtigd en gekopieerd					
Smaad/laster via het internet (het via ICT opzettelijk aantasten van de goede naam van uw organisatie)					
Spionage via internet (het via digitale middelen verkregen van vertrouwelijke bedrijfsinformatie van economische of politieke waarde)					
Vernieling van gegevens via internet (gegevens die opzettelijk veranderd,					

gewist, onbruikbaar of ontoegankelijk gemaakt worden)					

30. Hoe groot acht u het vermogen van uw organisatie om te herstellen van een groot cyberincident?
5 puntsschaal

31. Hoe groot schat u de kans dat een vergelijkbaar organisatie in Nederland in een periode van 12 maanden slachtoffer wordt van een cybercrime (pogingen niet meegerekend)?
Beantwoord met een numerieke waarden tussen 1-100

32. Tot op welke hoogte maakt uw organisatie **plannen** met betrekking tot cyber security? (Denk daarbij aan het vaststellen van de rol van de organisatie m.b.t de omgeving, het vaststellen van organisatorische rollen en verantwoordelijkheden m.b.t. cyber security, toewijding vanuit het management en het vaststellen van een policy m.b.t. cyber security)
Schaal van 1 tot 7 (waarbij 1 heel weinig en 7 heel veel is)

33. Tot op welke hoogte **operationaliseert** uw organisatie de plannen met betrekking tot cyber security? (Denk daarbij aan het uitvoeren van risicobeoordelingen en risicobehandelingen, het opstellen van doelen m.b.t. cyber security en het vrijmaken van middelen voor cyber security)
Schaal van 1 tot 7 (waarbij 1 heel weinig en 7 heel veel is)

34. Tot op welke hoogte **controleert** uw organisatie de activiteiten op het gebied van cyber security? (Denk daarbij aan het monitoren, meten, analyseren en evalueren van de prestaties van de activiteiten op het gebied van cyber security, het uitvoeren van interne audits en beoordelingen vanuit het management m.b.t cyber security)
Schaal van 1 tot 7 (waarbij 1 heel weinig en 7 heel veel is)

35. Tot op welke hoogte **verbetert** uw organisatie de activiteiten op het gebied van cyber security naar aanleiding van de controles? (Denk daarbij aan verbeteren op het moment dat er incidenteel iets fout gaat of het op continue verbeteren van de activiteiten op het gebied van cyber security)
Schaal van 1 tot 7 (waarbij 1 heel weinig en 7 heel veel is)

36. Bent u bekend met het initiatief FERM?
    - *Ja*
    - *Nee*

37. Hoe belangrijk vindt uw bedrijf de scholing en training omtrent cyber security?
Schaal van 1 tot 7 (waarbij 1 heel weinig en 7 heel veel is)

38. Hoe belangrijk vinden uw medewerkers scholing en training omtrent cyber security?
Schaal van 1 tot 7 (waarbij 1 heel weinig en 7 heel veel is)

39. Aan wat voor opleidingen en trainingen heeft uw bedrijf medewerkers laten deelnemen m.b.t. cyber security?

- *Op operationeel niveau*
- *Voor ICT medewerkers*
- *Voor risk (security) management en beleids- & crisis medewerkers*
- *Voor functioneel beheer*
- *Op strategische niveau*
- *Op tactisch niveau*
- *Anders..*

40. Bij welke organisaties of partner heeft u deze opleidingen en trainingen omtrent cyberveiligheid afgenomen?

    Openvraag

41. Aan welk type opleidingen en trainingen, aansluitend op eerder gedane opleidingen en trainingen heeft uw bedrijf behoefte?
    - *Op operationeel niveau*
    - *Op tactisch niveau*
    - *Op strategisch niveau*
    - *Voor risk (security) management en beleids- & crisis medewerkers*
    - *Voor ICT medewerkers*
    - *Voor functioneel beheer*

42. Staat uw organisatie er voor open om met andere bedrijven in het Rotterdams havengebied **samen te werken** omtrent cyber security?
    - *Ja*
    - *Nee*
    - *Weet ik niet*

43. Staat uw organisatie er voor open om met andere bedrijven in het Rotterdams havengebied **kennis en ervaring uitwisselen** omtrent cyber security?
    - *Ja*
    - *Nee*
    - *Weet ik niet*

44. Staat uw organisatie er voor open om met andere bedrijven in het Rotterdams havengebied **nieuwe kennis te ontwikkelen** omtrent cyber security?
    - *Ja*
    - *Nee*
    - *Weet ik niet*

45. Bent u bekend met het concept Computer Security Incident Response Team (CSIRT)?
    - *Ja*
    - *Nee*

46. Bent u bereid zich aan te sluiten bij een Cyber Security Incident Response Team (CSIRT)? (Een CSIRT is een expertgroep die zich focust op cyber security voor een organisatie of groep van organisaties.)
    - *Ja*
    - *Nee*
    - *Weet ik niet*

47. De volgende activiteiten zouden zinvol kunnen zijn voor mijn bedrijf:
    - *Dreigingsinformatie delen (intelligence watch)*
    - *Voorlichten van organisaties over cyber security*
    - *Begeleiden en te hulp schieten bij een cyber-aanval of incident*
    - *Kennis uitwisseling faciliteren tussen organisaties over cyber security*
    - *Organisaties trainen en opleiden op het gebied van cyber security*
    - *Gezamenlijk inkoop faciliteren voor de aangesloten organisaties*
    - *Other*

F. Results of the questionnaire

This appendix contains the complete results on the five questions from the questionnaire that were posed for this research. Highlights of these results are presented in section 4.1.3. The results are presented with the use of tables and graphs.

Company size and company type

Table 8-2 shows the numerical results of the general details of the organizations that participated in the questionnaire. Figure 8-1 provides a visual overview of these results.

Table 8-2: Overview of the company type for every size

Companies	Micro	Small	Middle	Large	Giant	Total
Port logistics	1	10	11	10	2	34
Maritime service provider	3	6	6	7	1	23
Industrial service provider	3	1	3	3	2	12
(Process)industry	3	4	9	5	3	24
Total	10	21	29	25	8	93

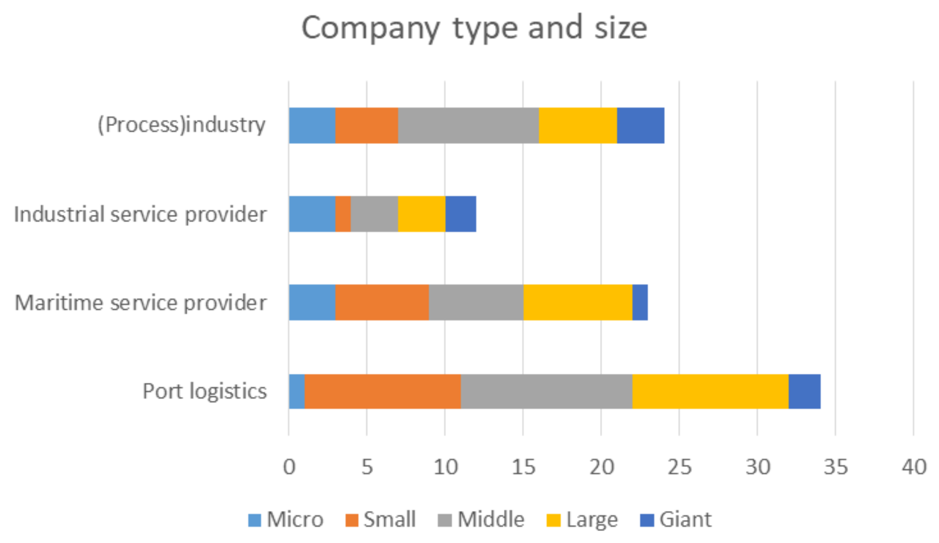

Figure 8-1: Graphical overview of the companies types and sizes

Table 8-3 and Table 8-4 show which companies are familiar with FERM. This is visualized in Figure 8-2 and Figure 8-3.

Table 8-3: Overview of the companies familiar with FERM per size

Familiar with FERM?	Micro	Small	Middle	Large	Giant	Total
Yes	6	12	19	16	5	58
No	4	9	10	9	3	35

Table 8-4: Overview of companies familiar with FERM per type

Familiar with FERM?	Port logistics	Maritime service provider	Industrial service provider	(Process) industry	Total
Yes	20	13	8	17	58
No	14	10	4	7	35

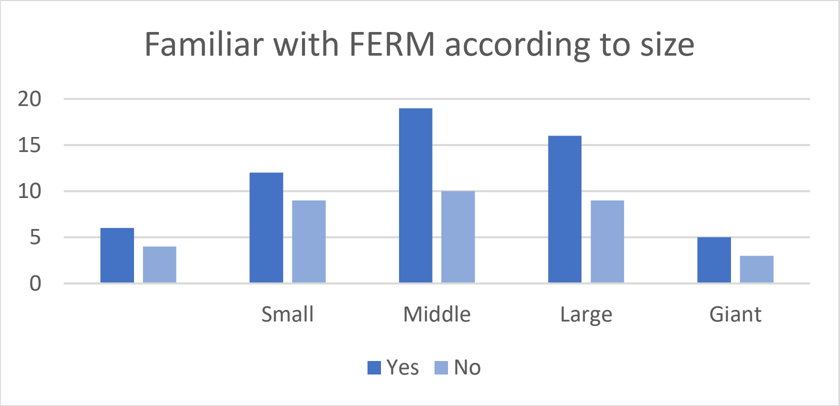

Figure 8-3: Familiarity with FERM according to size

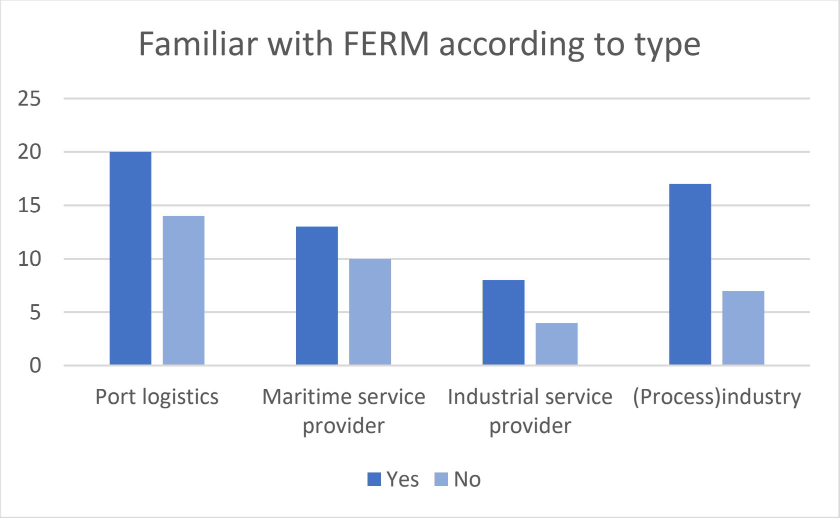

Figure 8-2: Familiarity with FERM according to type

Importance of cyber security

The importance of cyber security from an organization's perspective is presented in

Table 8-5 and Table 8-6. This is visualized in bar-charts in Figure 8-5 and Figure 8-6.

Table 8-5: Importance from an organization's perspective for every company size

Organization's perspective	Micro	Small	Middle	Large	Giant	Total
Low 1	1	0	0	0	0	1
2	1	0	3	0	0	4
3	1	1	1	0	0	3
4	1	3	4	4	0	12
5	4	4	10	9	1	28
6	2	6	6	4	3	21
7	0	6	5	8	4	23
8	0	0	0	0	0	0
9	0	0	0	0	0	0
Very high 10	0	0	0	0	0	0

Table 8-6: Importance from an organization's perspective for every company type

Organization's perspective	Port logistics	Maritime service provider	Industrial service provider	(Process) industry	Total
Low 1	0	0	1	0	1
2	1	0	1	2	4
3	0	3	0	0	3
4	7	2	1	2	12
5	12	5	5	6	28
6	8	4	2	7	21
7	5	9	2	7	23
8	0	0	0	0	0
9	0	0	0	0	0
High 10	0	0	0	0	0

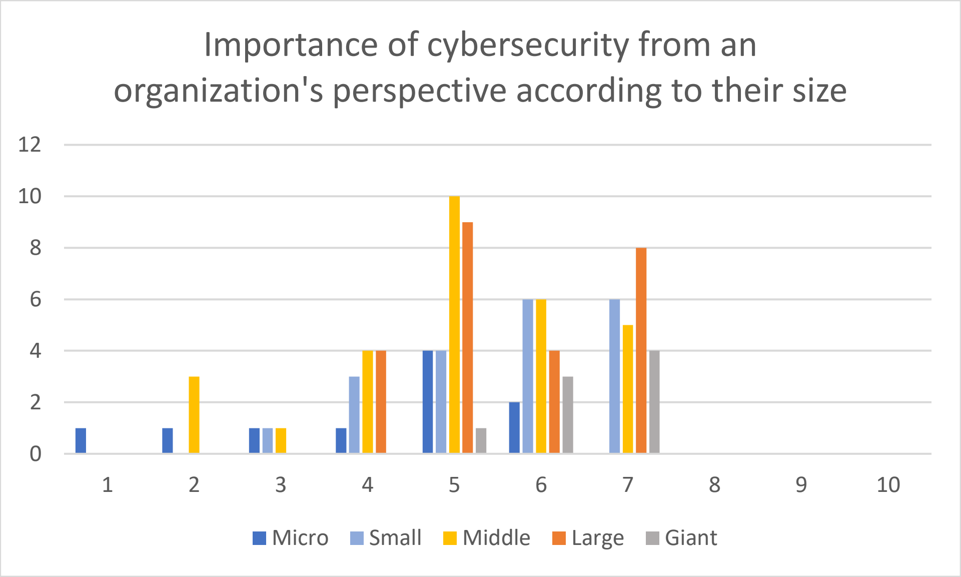

Figure 8-5: Importance of cyber security from an organization's perspective according to their size

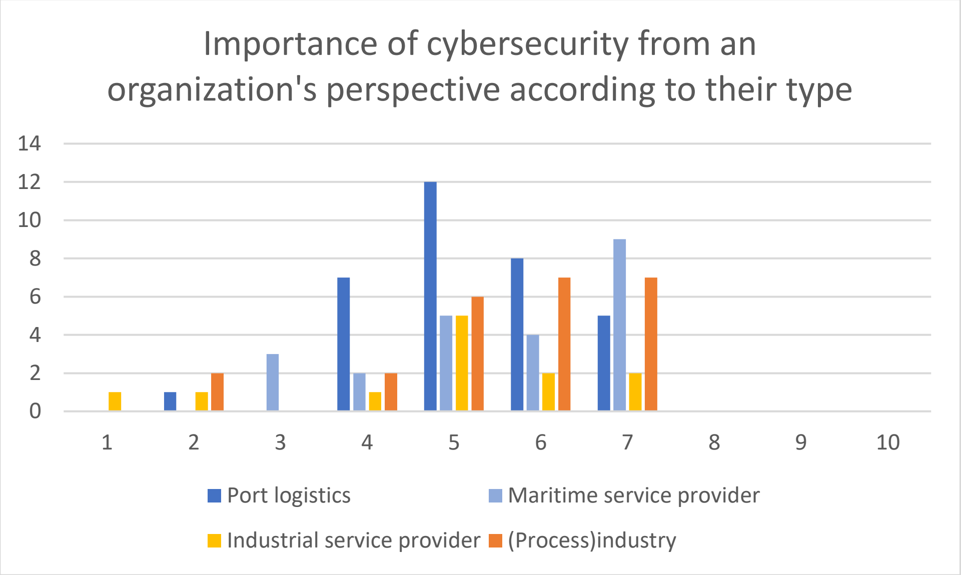

Figure 8-4: Importance of cyber security from an organization's perspective according to their type

The importance of cyber security from an employee's perspective is presented in

Table 8-7 and Table 8-8. This data is shown visually in Figure 8-6 and Figure 8-7

Table 8-7: Importance from an employee's perspective for every company size

Employee's perspective	Micro	Small	Middle	Large	Giant	Total
Low 1	1	1	0	0	0	2
2	0	0	3	0	0	3
3	2	3	0	4	1	10
4	2	5	7	8	3	25
5	4	5	13	6	1	29
6	1	5	3	6	1	16
7	0	1	3	1	2	7
8	0	0	0	0	0	0
9	0	0	0	0	0	0
High 10	0	0	0	0	0	0

Table 8-8: Importance from an employee's perspective for every company type

Employee's perspective	Port logistics	Maritime service provider	Industrial service provider	(Process) industry	Total
Low 1	0	1	1	0	2
2	1	0	1	1	3
3	4	2	1	3	10
4	11	5	2	7	25
5	11	4	5	9	29
6	4	9	1	2	16
7	2	2	1	2	7
8	0	0	0	0	0
9	0	0	0	0	0
High 10	0	0	0	0	0

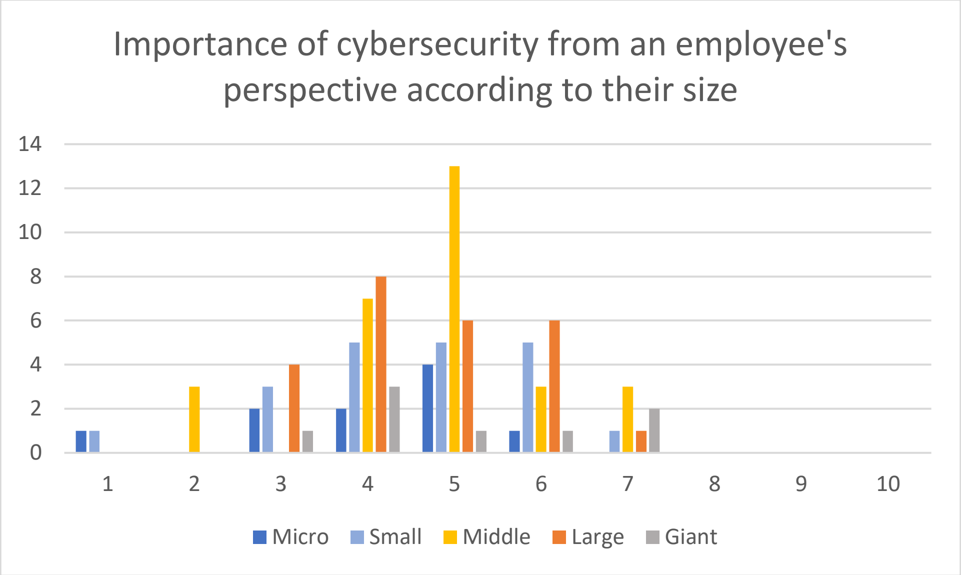

Figure 8-6: Importance of cyber security from an employee's perspective according to their size

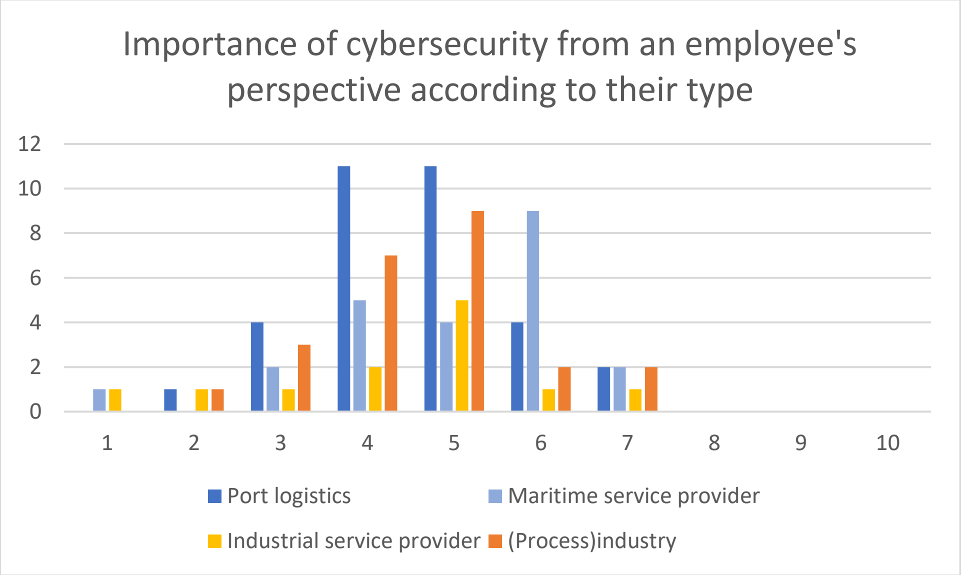

Figure 8-7: Importance of cyber security from an employee's perspective according to their type

Interests of the organizations

Table 8-9 and Table 8-10 provide insights into the interest that companies have in the options: collaboration, exchange of information and knowledge and knowledge development. This is visualized in Figure 8-8 and Figure 8-9.

Table 8-9: Overview of the interests of companies according to their size

	Open to	Collaboration	Exchange of information and knowledge	Knowledge development	Total
Micro	Yes	7	8	6	21
	No	0	0	2	2
	I don't know	3	2	2	7
Small	Yes	12	14	9	35
	No	3	2	3	8
	I don't know	5	4	8	17
Middle	Yes	21	22	20	63
	No	4	1	2	7
	I don't know	4	6	7	17
Large	Yes	14	16	17	47
	No	1	1	0	2
	I don't know	10	8	8	26
Giant	Yes	4	5	5	14
	No	1	1	1	3
	I don't know	3	2	2	7
Total	Yes	58	65	57	180
	No	9	5	8	22
	I don't know	25	22	27	74

Table 8-10: Overview of the interests of companies according to their type

	Open to	Collaboration	Exchange of information and knowledge	Knowledge development	Total
Port logistics	Yes	23	25	21	69
	No	5	2	3	10
	I don't know	5	6	9	20
Maritime service provider	Yes	16	16	13	45
	No	3	3	3	9
	I don't know	4	4	7	15
Industrial service provider	Yes	7	9	8	24
	No	1	0	1	2
	I don't know	4	3	3	10

(Process) industry	Yes	12	15	15	42
	No	0	0	1	1
	I don't know	12	9	8	29
Total	Yes	58	65	57	180
	No	9	5	8	22
	I don't know	25	22	27	74

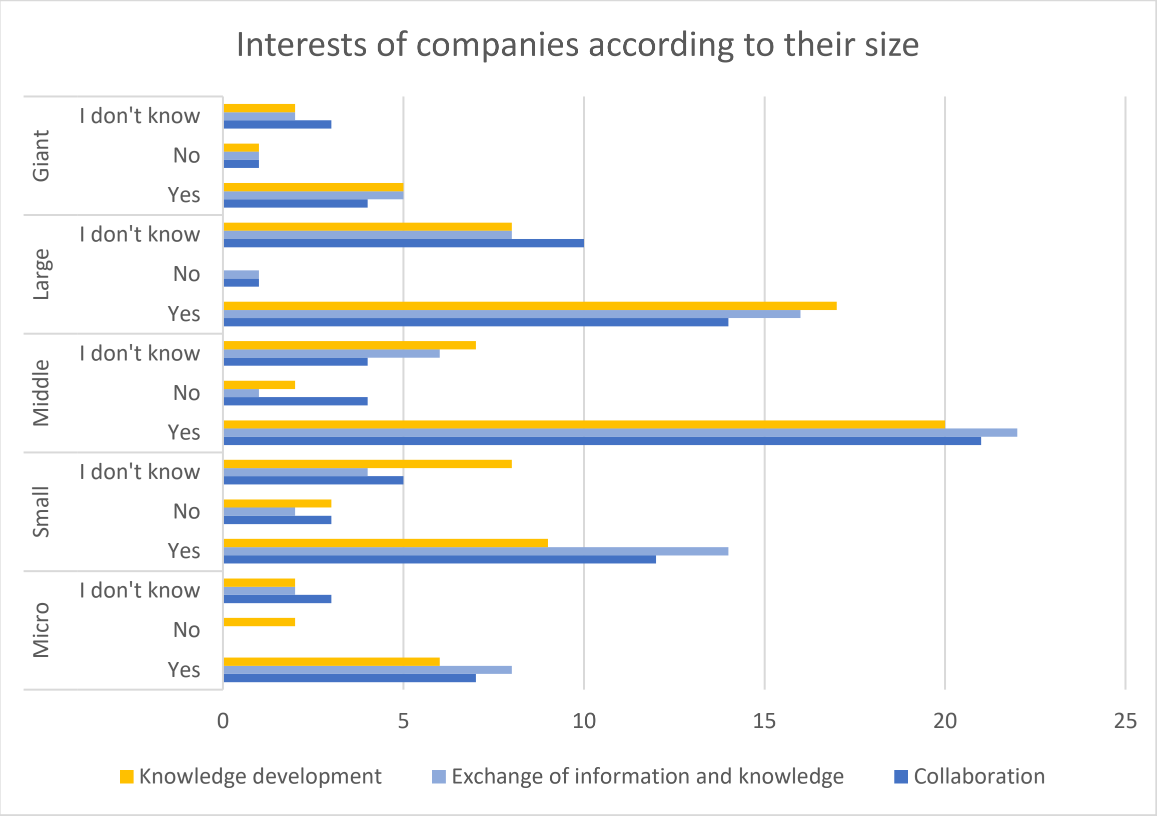

Figure 8-8: Interests of companies according to their size

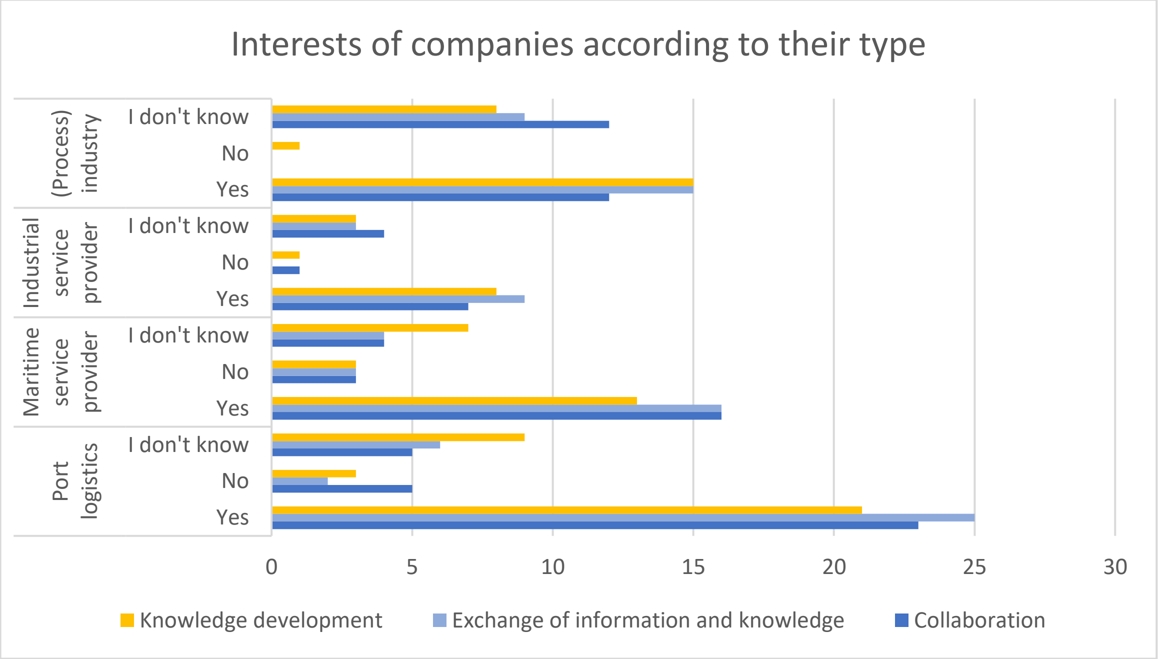

Figure 8-9: Interests of companies according to their type

Table 8-11 and Table 8-12 provide insights in what activities the organizations found useful. Visualization are shown in Figure 8-11 and Figure 8-10.

Table 8-11: Overview of interest in useful activities per company size

Useful activities	Micro	Small	Middle	Large	Giant	Total
Inform organizations concerning cyber security	6	13	18	18	3	58
To facilitate knowledge exchange between organizations concerning cyber security	1	6	13	12	4	36
Sharing threat information (intelligence watch)	4	10	23	20	4	61
To train and educate organizations concerning cyber security	1	3	12	12	3	31
Guidance and help in case of a cyber-attack or incident	5	7	17	14	2	45
To facilitate collective purchase for affiliated organizations	2	2	4	3	1	12

Table 8-12: Overview of interest in useful activities per company type

Useful activities	Port logistics	Maritime service provider	Industrial service provider	(Process) industry	Total
Inform organizations concerning cyber security	25	17	7	9	58
To facilitate knowledge exchange between organizations concerning cyber security	12	10	4	10	36
Sharing threat information (intelligence watch)	23	16	7	15	61
To train and educate organizations concerning cyber security	15	7	3	6	31
Guidance and help in case of a cyber-attack or incident	16	13	5	11	45
To facilitate collective purchase for affiliated organizations	6	2	1	3	12

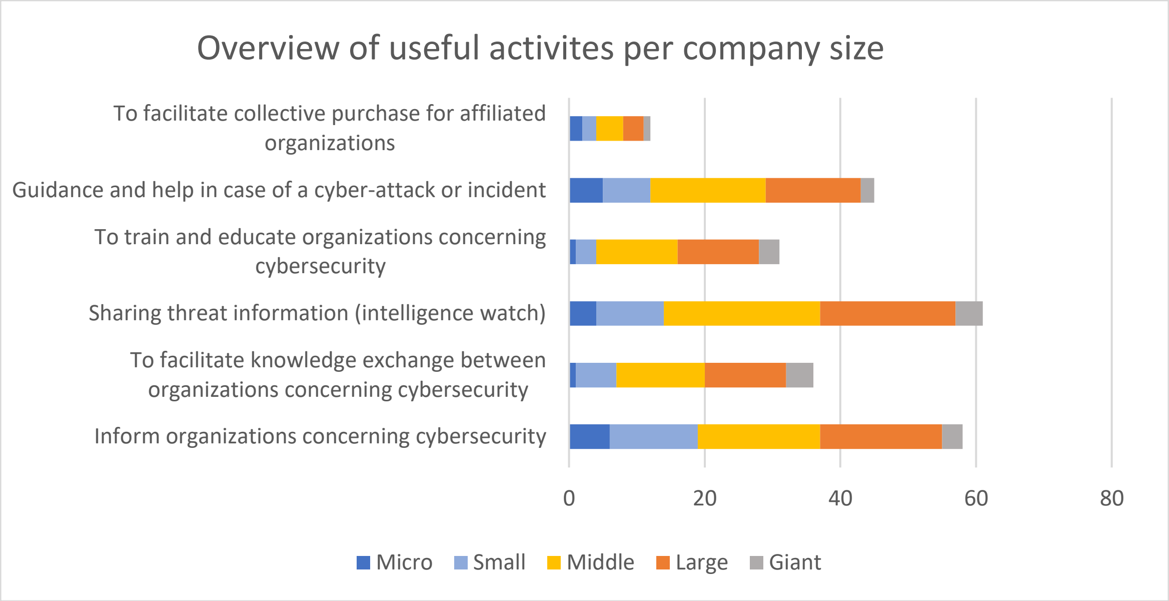

Figure 8-11: Overview of useful activities per company size

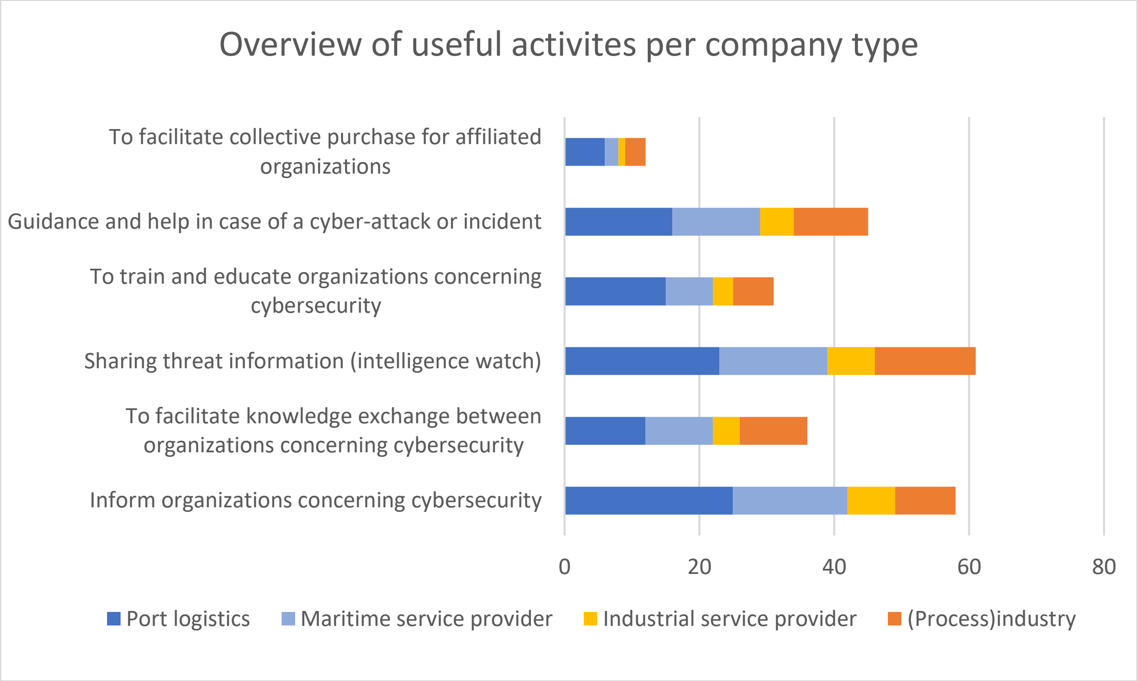

Figure 8-10: Overview of useful activities per company type

G. Overview of main actors

Port of Rotterdam (PoR)

PoR is the administrator, exploiter and developer of the Rotterdam port area. Its mission is to create economical and societal value through the realization of sustainable growth in this world renowned port in collaboration with its clients and stakeholders. This is achieved by focusing on two goals. The first is the development, construction, management and exploitation of the Rotterdam port and industrial area. This goal is pursued by the commercial departments of PoR. The second goals is the improvement of effective, safe, and efficient maritime logistics. This aim is linked to the public obligations that PoR has and is carried out by the Division Harbour master (PoR, 2017b, p. 20). One can see a clear division between the private and public aims and this is a results of the history of PoR. It started as a municipality service, but grown into a state-owned private company.

PoR is aware of digitalization trend and its connected threats (PoR, 2016, 2017b, 2017a). Therefore it intends to increase the cyber resilience in the Rotterdam port area, increase the cyber-awareness, and improve the readiness and risk management of companies in cyber security. It realizes that it should be collectively, so it has been a partner and co-initiator of FERM.

Its main interest in FERM is to activate companies in the Rotterdam port area to improve their cyber security as a means to ensure safe maritime operations, one of PoR's main goals. The Division Harbourmaster, the part of PoR responsible for FERM, realizes that a hard approach using rules and regulations is not desirable at this point and therefore has focused on a soft approach using FERM's awareness program. PoR offers both its annual contribution as well as 1,5 FTE to the program taking a leading and executive role in the FERM program.

PoR holds several resources within the network. Their first and most important resource is their role as administrator enabling them to set rules and regulations to the other organizations in the Rotterdam port area. This can force companies to obey them, however this resources must be used with moderation in order to remain in good relations with the organizations. A second resource is their level connectivity with all relevant parties and people in the Rotterdam port area and beyond. This enables PoR to gain a lot of information, use this information effectively and to lobby their interest. A last resource is their excellent image with most actors. PoR is seen a high quality and reliable partner.

Municipality of Rotterdam

The municipality of Rotterdam concerns itself with the prosperity of the citizens and the city of Rotterdam. The Rotterdam port area is the pride of the city as well as an important asset concerning employment. However, the port also has its darker sides with issues such as drugs trafficking. The Rotterdam port area used to be managed by a municipality service until 2004 when it became a state-owned private company. The municipality still is the main stakeholder in the Port of Rotterdam (70,8%) together with the Dutch Government (29,2%) in the Port of Rotterdam.

The municipality made cyber security an important topic and has focused on the port area since its first appearance. It believes that the port area was the best target and therefore the best starting point. It is a partner of FERM as well a co-initiator. Its main interest is that the port area remains protected as well as to ensure connection between overlapping parties within the organizations. The municipality offers the annual contribution and takes a strategical and networking position.

The resources of the municipality are limited in this case, since it has less influence in the Rotterdam port area. However, it remains a well-connected actor with all public organizations. It also possesses a leading role due to subsidies and initiatives that it can support or start. These two resources present the municipality with leverage to influence aspects in the Rotterdam port area.

Police's Sea Division

The Police's Sea Division ensures the safety of the Rotterdam port area. This is done in collaboration with several partners including the Custom office and the Port of Rotterdam. Her work focuses on nautical supervision, environmental enforcement, crime reduction and prevention, border control and nautical incident response (Politie, 2019).

The Police realized and experienced that cyber-related crime increased and it expected that this would grow. The Sea Division realized the threats to the port area. They are a co-initiator and partner of FERM, so it contributes the annual contribution. Their main interest is to gain better overview of the affairs in the port area in order to improve their services as well as to position themselves as an easy point of contact in case of crime. Their main focus is preventing and avoiding crime. FERM undoubtedly deals with prevention. The Police's Sea Division has taken a network position, but has often tried to execute actions for FERM. However, the results of these actions has remained somewhat limited due to some internal strife.

The resources of Police Sea Division start with one of the police's fundamental function to fine and fight crime based on law. This can influence parties in the Rotterdam port area. A stronger resource is their expertise in cybercrime and cyber security. They can share this knowledge and use it to fight crime. This knowledge can be very interesting for other parties. They also hold a strong network with other cyber experts, thus adding a lot of knowledge to the actors.

Deltalinqs

Deltalinqs promotes common interests of over 95% of all logistic, ports and industrial enterprises in mainport Rotterdam. Over 700 companies from fourteen different sectors are joined in the association of entrepreneurs. They are striving to strengthen Rotterdam's competitiveness, sustainable growth and social and political acceptability for all activities within the port and industrial area; all for the benefit of their members (Deltalinqs, 2016).

Deltalinqs is a direct partner of FERM. It represents the private part of the PPP using its role as entrepreneur's association. Its main interest is to keep aware of the latest news in the port area related to the companies. Within FERM, they are also seen as a linking pin to the companies. They have taken a networking position.

Deltalinqs is actor with three resources. Firstly, their representative position of the port organizations provides them with influence with the public actors. Secondly, they maintain a well-developed network with the port organizations and therefore know their issues as well as influence their actions. This is important for this case. A third resource is their knowledge in facilitating services for the port organizations that fit their needs. This makes them a reliable and preferred partner for companies.

DCMR

DCMR is the collective environmental service that works for the South Holland province, the 15 municipalities of Rijnmond and Goeree-Overflakkee. Ìt aims to offer a safe and clean place to live for the 1,2 million inhabitants of this area. The main tasks of DCMR are: the inspection and enforcement of environmental rule, the creation of licenses, and the license creation, supervision and enforcement for high-risk companies (DCMR, 2019).

DCMR foresees the consequences of cyber threats to the environmental goals, however their mandate and power is too little to act at this point. They became an informant of FERM and hold a networking position. Their main interest is to be aware of the developments concerning cyber in the port area as well as remain connected with the other relevant parties.

The resources of DCMR are limited in this case since it is restricted to environmental aspects. They inspect organizations on their environmental policy and can hold them accountable. However, this still remains far from the cyber security topic.

Public Persecutor Service (OM)

The OM is a national organization that is responsible to trace and prosecute criminal facts. It aims to find a fitting punishment for the perpetrator, to support victims and next of kin, and to ensure proper dealing of the law. The OM and the judges form the Jucidiary power of the Netherlands. The main tasks of the OM are: to lead the police in tracing criminal facts, to persecute criminal facts and present suspects to a judge, and to solve criminal facts without intervention of a judge (OM, 2019).

The OM joined FERM as an informant. Their main interest is the networking position on cyber-related issues. A program “de Integere Haven” of the OM put some focus on cybercrime. The OM felt that this program connected with some of the aims of FERM.

The OM has the little resources since cyberlaw is still in its infancy.

National Cyber Security Centre (NCSC)

NCSC is the central information hub and centre of expertise for cyber security in the Netherlands. NCSC's mission is to contribute to the enhancement of the resilience of Dutch society in the digital domain, and thus to create a secure, open and stable information society. On an international level the NCSC is the Dutch point of contact in the field of ICT threats and cyber security incidents. The primary target group of the NCSC is the Dutch national government and the vital infrastructure. Its main activities are: to response to threats and incidents, to provide perspective and action prospects, to improve crisis management, and to offer a collaboration platform on cyber security (NCSC, 2019).

NCSC simulates cyber security related collaboration in the Netherlands, especially around vital infrastructure. They quickly joined FERM as an informant in order to make this initiative grow.

The NCSC hold high level knowledge and information which is a great resource since organizations are in desperate demand for information and expertise on cyber security. Their position as a central information hub supported by the central government also strengthens their image and position with other actors. A third resource they possess is their vast experience with cyber collaboration in other situations. They can provide good advice on how to further advance FERM as well as collaboration in the Rotterdam port area.

Companies

The Companies actors is very diversified group. The Rotterdam port area consists of around 700 companies in several different sectors and ranging from small to multinational companies. They all rent land from the PoR and are checked by the PoR on safety regulations. This group can be described as conservative. Cyber security is a topic that they have heard of, but it isn’t their top priority. Companies are the target audience for the FERM activities.

The Companies-actor holds one mayor resource: they are the target audience. This makes their opinion, view and needs crucial, since other organizations cannot easily force them to comply. From another perspective, this can also be seen as weak resource, since it only holds power in unity while most companies are diverse and thus less unified.

H. Definitions of the Theoretical overview

H.1 Characteristics

This pillar is aimed to collect and organize the different characteristics of CoP and related concepts such as alliances and collaborations. In total 11 files contained 102 quotes concerning the characteristics. These quotes can be organized in 11 themes: Learning, Knowledge management, Network, Social capital, Informality, Self-leading, Problem solving, Identity, Mutuality, Community, and Social.

The theme **Community** notes the group feeling with shared rituals and characteristics.

The theme **Identity** makes clear that a CoP provides and creates an identity of its own that is used by its members. This is strengthened by the theme mutuality.

The theme **Informality** shows that a CoP possess equivalence between the members, causing informal and horizontal connections that can overcome formal structures and relationships. There are no restrictions and no hierarchy between members. Members are also able to enter and leave voluntarily.

The theme **Knowledge management** shows that a CoP is a place where people share and discuss their explicit and tacit knowledge to make sense of it and to create new insights and practices. The knowledge in a CoP is a responsibility of the entire group of members. It covers the exchange, sharing, and development of knowledge.

The theme **Learning** tells that a CoP is a place for collective learning through peer-to-peer connection and learning activities or opportunities. Learning is done together and also focuses on learning, meta-learning and epistemic learning. This is strongly based on Social Learning Theory.

The theme **Mutuality** involves that a CoP gives form to its identity through shared values, ideas and resources that create mutuality between members.

The theme **Network** focuses on the fact that a CoP provides a network where experts can interact and work together with peers.

The theme **Problem solving** shows that a CoP holds knowledge and ideas that can offer quick solutions for new problems. It is quicker than formal organizational units to determine problems and find suitable solutions.

The theme **Self-constructing** focuses on the aspect that a CoP is strongly focused on itself and reinventing itself. Therefore the members negotiate with each other, organize themselves, critically reflect on itself and determine the best course of action. It possess and creates its own leadership and stewards the competencies of its members.

The theme **Social** tells us that a CoP is created through the social interactions of its members, therefore it is constantly changing along with its members and has it a high personal connection for the members. It is therefore essential to view a CoP as a social process where the interactions between persons are a key element.

The theme **Social capital** tells us that a CoP is a place for members to build social capital in the broadest sense.

H.2 Needs

This pillar is aimed to collect and organize the different needs that organizations can have to start or be part of a CoP. 4 files contained 11 quotes regarding this pillar. This pillar showed great overlap with other pillars, such as characteristics and drivers. Furthermore, needs are very specific for every case and are hard to determine after the process, since then they have become a driver or barrier.

H.3 Goals

This pillar is aimed to collect and organize the different goals that can be chosen for a CoP and related concepts such as alliances and collaborations. 11 files contained 37 quotes regarding this pillar. These quotes can be organized in 6 themes: Knowledge management, Learning, Network, Finance, Problem solving, and Information.

The theme **Finance** relates to goals that provide advantages for the involved organizations. These advantages can differ greatly from gaining access to resources or equipment, to spreading risks or to gain prestige, but in the end all these provide an organization with a financial advantages.

The theme **Information** relates to the goal to gain access to new sources of information by exchanging and interpreting information.

The theme **Knowledge management** relates to the goals to share, exchange, improve, develop and manage knowledge for a specific practice within or between organizations. A common goal is to use a CoP to gain access to knowledge and distribute it effectively and efficiently in order to reduce an information overload.

The theme **Learning** relates to goals to teach to and learn from each other with regards to a practice in order to build capabilities without formal programs. Learning can empower people with understanding, knowledge and skills which contributes to the capabilities of that person and its organization. A CoP also provides cross-fertilization across disciplines which contribute to the learning.

The theme **Network** relates to the goal to establish a community with a network of expert peers. There is however a difference between a network and a community.

The theme **Problem solving** relates to the goal to solve problems more creative and systematic.

H.4 Drivers

This pillar aimed to collect and organize the drivers that stimulate the creation of a CoP or related concepts and that are attributed to the successful implementation. 19 files contained 135 quotes regarding this pillar. These quotes can be organized in 11 themes: Characteristics of the CoP, Commitment, Communication, Culture, Identity, Initial phase, Learning, Management, Relationship Management, Structure, and Trust.

The theme **Characteristics of the CoP** relates to characteristics that are inherently present in a CoP, but most be supported or stimulated to improve a CoP. The four most important characteristics to support are the autonomy/self-organization, voluntary engagement, reflectiveness and the sense of community.

The theme **Commitment** tells us that a driver is to improve the commitment of the members. The passion and the responsibility that members feel for their practice is a great intrinsic motivator that fuels the commitment to the CoP. It also stimulates the autonomy of the CoP.

The theme **Communication** says that developing and maintaining good communication in both quality and frequency, is driver for a CoP. Both formal as informal forms of communication must be used. Communication creates transparency, trust building and reduces misunderstanding and uncertainty, especially in the initial phase.

The theme **Culture** explains that a culture that values community and where members want to contribute to the overall goals in an autonomous fashion are essential for a CoP. This is highly dependent on the corporate culture and context of the members.

The theme **Identity** tells that an strong identity of the CoP is a driver for its success, since it is socially empowering and strengthens participation of members. This can be created through shared experiences, interactive activities, multimember ship, and shared values and interest.

The theme **Initial Phase** shows that the startup phase is crucial for future success, since it sets the tone for the community, its members and the relationships between the members. The "right" tone can be set by stimulating a spirit of enquiry and mutual discovery, and by establishing trust-based relationships. It's important to create norms or etiquette for good behavior, different types of leadership and communication lines both formal and informal. This contributes to transparency and reduces uncertainty.

The theme **Management** relates to the actions of (top) management that can act as drivers for a CoP. First of all, management has influence on the emergence of CoPs in their organizations using the companies policies, the corporate culture, the designing of a CoP, and the organizational environment. Secondly, management can influence the success of a CoP through the support it provides to a CoP. CoP need financial support, effective infrastructure, and help with coordination and resource finding. Thirdly, management can provide soft support to a CoP by recognizing the value, providing time for members to spent on the CoP, providing vision on their aim and (strategic) objectives and helping them connect. Lastly, management has a direct influence in the CoP by creating a foundation for trust and playing a leadership or facilitator role.

The theme **Learning** shows that learning is a great driver for a CoP. Reflexivity, informal learning and mutual understanding must be improved to enable learning.

The theme **Relationship management** focuses on the effect of strong personal relationships between members of a CoP. CoPs are inherently a social endeavor, thus an important driver for success is the relationship management in a CoP. The relationships are also important for trust and learning. Multi membership, reciprocity and empathy are building blocks for relationships to unite members.

The theme **Structure** relates to how CoPs are structured to gain success. The structure should support the natural characteristics of a CoP.

The theme **Trust** focuses on the importance of trust between members for the success of a CoP. Trust provides a basis for mutual understanding, mutual confidence and openness making a collaboration more robust and creating strong relationships and learning opportunities. If trust is high, then the economic factors also become secondary. Trust can be cultivated by having an early and continuing dialog between members, minimizing perceptions of asymmetry in value creation, having a long "shadow of the future".

H.5 Barriers

This pillar aims to collect and organize the barriers that hinder the creation of a CoP or related concepts and those that limit the continuation of a CoP. 15 files contained 99 quotes regarding this pillar. These quotes can be organized in 10 themes: Finance, Uncertainty, Characteristics of a CoP, Management, Initial phase, Communication, Technology, Culture, Trust, and Operational.

The theme **Characteristics of the CoP** relates to the inherent characteristics of a CoP that can hinder its own progress or creation. Firstly, the strong personal bonds between members can create groupthink, decrease reflexivity, hinder change and overshadow concerns. Secondly, there is a natural tension between the CoPs and (traditional) management both in values as well as in nature/culture. Lastly, the informality and difficulty in measuring results or value can cause a CoP to lose priority.

The theme **Communication** focuses on barriers that impede the workings of a CoP by creating misunderstandings, uncertainty and lack of interaction between members. The lack of communication in general is a great barrier, but ineffective communication also is a barrier. Inefficiency in communication can be caused by existing relationships, but also by the members itself, for example by not being open or not communicating personal intentions and expectations.

The theme **Culture** shows that culture differences and the culture within organizations can hinder CoPs. Culture difference are seen in the broadest sense. It can cause conflict or make members unable to understand certain problems.

The theme **Finance** focuses on financial reasons that hinder CoPs. This can range from a lack of funding or the dependence on sponsorship to financial incentives to keep a competitive advantage.

The theme **Initial phase** considers the starting phase of a CoP and the challenges it faces. Important challenges are establishing (social) norms, creating an identity for the community, an creating homogenous expectations and shared assumptions. Another issue are challenges created by existing practices, such as existing patterns of interactions or power relations.

The theme **Management** focuses how management and its policies can hinder the success of a CoP. An important factor is implementing hierarchy on a CoP impeding learning and limiting freedom. There are also several ways in which management can hinder (voluntary) participation to a CoP such as short-term pressure and blindness for success.

The theme **Operational** involves all sort of practical barriers that are case specific. For example, technological infrastructure is not compatible. It also shows a that lack of understanding of each other’s product can impede collaboration.

The theme **Technology** shows that technological infrastructure can also impede collaboration, since it influence how members collaborate.

The theme **Trust** relates to the barrier of a lack of trust. Trust is brittle and difficult to recover. It also takes time to create. When trust is lacking, sharing decreases, development of social capital decreases and incentives to work reduces.

The theme **Uncertainty** tells that uncertainty regarding future events, partners responses, resources, roles and responsibilities hinder a CoP.

H.6 Forms & activities

This pillar aims to collect and organize the different forms that CoP can have and which activities they can pursue. 10 files contained 28 quotes regarding this pillar. These quotes were organized in 5 groups: **Digital infrastructure & tools**, **Indirect communications**, **Forms**, **Activities**, and **Meeting each other**. These groups mostly contain concrete examples.

I. Literature of the systematic review

Table 8-13: Results of sytemic review by author and aspect

Authors	Goals	Drivers	Barriers	Forms
Alali & Salim, 2016		x		x
Borzillo, 2017	x			
Bos et al., 2007			x	x
Chen, Lin, & Yen, 2014	x			
Cheung, Lee, & Lee, 2013	x			
Chu, 2016		x		
Cochrane, 2014		x		
Cochrane, 2011		x		
Cornes et al., 2014	x			
Crowley et al., 2018				x
Dahlander & O'Mahony, 2011				x
Dawson et al., 2018	x			
Del Giudice, Della Peruta, & Maggioni, 2015		x		
Du Plessis, 2008	x	x		
Dube, Bourhis, & Jacob, 2006				x
Ekberg et al., 2010				x
Faraj, von Krogh, Monteiro, & Lakhani, 2016				x
Ferlie, Crilly, Jashapara, & Peckham, 2012				x
Fetterman, 2002	x			
Gagnon, 2011				x
Galán-Muros et al., 2017		x		
Gibson & Meacheam, 2009				x
Hall & Graham, 2004		x		
Hara, Shachaf, & Stoerger, 2009				x
Ho & Kuo, 2013		x		
Hosseini et al., 2017	x			
Hong, Suh, & Koo, 2011			x	
J. Hong, 2017		x		
Hsiao et al., 2017				x
Jaegersberg & Ure, 2011			x	
Kaplan & Thomson Reed, 2007			x	
Koh, Ryan, & Prybutok, 2005				x
Kruss & Visser, 2017		x		
Lathlean & Le May, 2002	x			
Lee & Choi, 2003		x		
H. S. Lee, 2017		x		
Y. M. Li & Jhang-Li, 2010		x		
Liu, Cheng, Chao, & Tseng, 2012	x			
Lyons, Acsente, & van Waesberghe, 2008			x	
Mabery, Gibbs-Scharf, & Bara, 2013		x		
Machuca & Costa, 2012				x
Margaryan, Milligan, & Littlejohn, 2011				x

Nielsen, 2012		x		
Pharo, Davison, McGregor, Warr, & Brown, 2014		x		
Pirkkalainen & Pawlowski, 2014			x	
Price & Felix, 2008			x	
Ramos-Vielba et al., 2016			x	
Robards et al., 2018				x
Rooke, Rooke, Koskela, & Tzortzopoulos, 2010			x	
Salo, 2001		x		
Scarso, Bolisani, & Salvador, 2009		x		
Sheffield & Lemétayer, 2013		x		
Swain & Ekionea, 2008				x
Tan & Noor, 2013		x		
Wang, Wong, & Wang, 2012	x			
J. Wang et al., 2017		x		x
Witherspoon, Bergner, Cockrell, & Stone, 2013	x			
Wu, 2013		x		

J. Meta-ethnography

This appendix provides an overview of the literature that supported the theoretical elements found in the meta-ethnography. The definition of every element is explained in section 4.2.2.

J.1 Goals

Table 8-14 presents the sources that were used to create the Goal elements. All element have at least nine sources that contribute to their creation.

Table 8-14: Sources of the Goal-elements

Goal	Sources
Company Improvement	(Borzillo, 2017; Cornes et al., 2014; Crowley et al., 2018; Gibson & Meacheam, 2009; J. Hong, 2017; H. S. Lee, 2017; Lyons et al., 2008; Ramos-Vielba et al., 2016; Scarso et al., 2009; Swain & Ekionea, 2008)
Knowledge management	(Alali & Salim, 2016; Borzillo, 2017; Bos et al., 2007; Crowley et al., 2018; Du Plessis, 2008; Dube et al., 2006; Gagnon, 2011; Hall & Graham, 2004; H. S. Lee, 2017; Mabery et al., 2013; Ramos-Vielba et al., 2016; Scarso et al., 2009; Swain & Ekionea, 2008)
Learning	(Borzillo, 2017; Bos et al., 2007; Cornes et al., 2014; Crowley et al., 2018; Du Plessis, 2008; Dube et al., 2006; Hall & Graham, 2004; H. S. Lee, 2017; Scarso et al., 2009)
Network and Interactions	(Alali & Salim, 2016; Cornes et al., 2014; Crowley et al., 2018; Du Plessis, 2008; Dube et al., 2006; Gibson & Meacheam, 2009; Mabery et al., 2013; Pharo et al., 2014; Ramos-Vielba et al., 2016; Scarso et al., 2009)
Strategic (company) advantage	(Crowley et al., 2018; Du Plessis, 2008; Ho & Kuo, 2013; H. Lee & Choi, 2003; Liu et al., 2012; Ramos-Vielba et al., 2016; Scarso et al., 2009; Swain & Ekionea, 2008; Tan & Noor, 2013; Witherspoon et al., 2013)

J.2 Drivers

Table 8-15 presents the sources that were used to create the Driver elements. There is big variety in the amount of sources used to create the elements. The least amount of sources used is five for Awareness of knowledge and information, and six for Strategy. Since these elements were less often mentioned, it could be that either these elements are less important compared to the others, that these elements are less accepted by the scientific community, or that these elements have to be researched more. On average the elements are mentioned in 15 sources. The elements Culture and Social are mentioned the most in the found literature, respectively by 31 and 30 sources.

Table 8-15: Sources of the Driver-elements

Drivers	Sources
Awareness of knowledge and information	(Ekberg et al., 2010; J. Hong, 2017; Kaplan & Thomson Reed, 2007; Lathlean & Le May, 2002; Y. M. Li & Jhang-Li, 2010)
Commitment	(Alali & Salim, 2016; Chen et al., 2014; Cheung et al., 2013; Cornes et al., 2014; Dahlander & O'Mahony, 2011; Ekberg et al., 2010; Faraj et al., 2016; Galán-Muros et al., 2017; Gibson & Meacheam, 2009; Ho & Kuo, 2013; Lathlean & Le May, 2002; Y. M. Li & Jhang-Li, 2010; Mabery et al., 2013; Machuca & Costa, 2012; Pharo et al., 2014; Witherspoon et al., 2013)
Communication	(Chen et al., 2014; Chu, 2016; Cornes et al., 2014; Du Plessis, 2008; Galán-Muros et al., 2017; D. Hong et al., 2011; J. Hong, 2017; Jaegersberg & Ure, 2011; Koh et

	al., 2005; H. Lee & Choi, 2003; Y. M. Li & Jhang-Li, 2010; Liu et al., 2012; Lyons et al., 2008; Machuca & Costa, 2012; Robards et al., 2018; Scarso et al., 2009; Tan & Noor, 2013; J. Wang et al., 2017; Witherspoon et al., 2013)
Culture	(Alali & Salim, 2016; Borzillo, 2017; Chen et al., 2014; Cheung et al., 2013; Chu, 2016; Cornes et al., 2014; Dawson et al., 2018; Du Plessis, 2008; Dube et al., 2006; Ekberg et al., 2010; Faraj et al., 2016; Gagnon, 2011; Galán-Muros et al., 2017; Hall & Graham, 2004; Ho & Kuo, 2013; J. Hong, 2017; Hsiao et al., 2017; Kaplan & Thomson Reed, 2007; Koh et al., 2005; Lathlean & Le May, 2002; H. Lee & Choi, 2003; H. S. Lee, 2017; Liu et al., 2012; Mabery et al., 2013; Machuca & Costa, 2012; Pharo et al., 2014; Ramos-Vielba et al., 2016; Robards et al., 2018; Tan & Noor, 2013; J. Wang et al., 2017; Witherspoon et al., 2013)
Facilitator & leadership	(Alali & Salim, 2016; Borzillo, 2017; Chen et al., 2014; Chu, 2016; Cochrane, 2011; Cornes et al., 2014; Crowley et al., 2018; Ekberg et al., 2010; Gibson & Meacheam, 2009; Hara et al., 2009; J. Hong, 2017; Kaplan & Thomson Reed, 2007; Lathlean & Le May, 2002; H. S. Lee, 2017; Liu et al., 2012; Lyons et al., 2008; Pharo et al., 2014; Price & Felix, 2008; Robards et al., 2018; Scarso et al., 2009)
Management	(Borzillo, 2017; Chu, 2016; Cornes et al., 2014; Crowley et al., 2018; Ekberg et al., 2010; Gagnon, 2011; Galán-Muros et al., 2017; Gibson & Meacheam, 2009; Hall & Graham, 2004; Hara et al., 2009; J. Hong, 2017; Kaplan & Thomson Reed, 2007; Koh et al., 2005; Lathlean & Le May, 2002; H. S. Lee, 2017; Y. M. Li & Jhang-Li, 2010; Liu et al., 2012; Lyons et al., 2008; Mabery et al., 2013; Robards et al., 2018; Swain & Ekionea, 2008; Tan & Noor, 2013; J. Wang et al., 2017; Witherspoon et al., 2013)
People	(Alali & Salim, 2016; Ekberg et al., 2010; Faraj et al., 2016; Gagnon, 2011; Hosseini et al., 2017; Kaplan & Thomson Reed, 2007; Lathlean & Le May, 2002; H. Lee & Choi, 2003; Mabery et al., 2013; Pharo et al., 2014; Robards et al., 2018; Scarso et al., 2009; J. Wang et al., 2017)
Reward and recognition	(Alali & Salim, 2016; Faraj et al., 2016; Galán-Muros et al., 2017; Hall & Graham, 2004; Ho & Kuo, 2013; Hosseini et al., 2017; Kaplan & Thomson Reed, 2007; Kruss & Visser, 2017; H. S. Lee, 2017; Y. M. Li & Jhang-Li, 2010; Liu et al., 2012; Ramos-Vielba et al., 2016; Scarso et al., 2009; Tan & Noor, 2013; J. Wang et al., 2017; Witherspoon et al., 2013)
Shared and negotiable goals	(Borzillo, 2017; Chen et al., 2014; Chu, 2016; Du Plessis, 2008; Faraj et al., 2016; Gagnon, 2011; Gibson & Meacheam, 2009; Hall & Graham, 2004; D. Hong et al., 2011; J. Hong, 2017; Lathlean & Le May, 2002; Liu et al., 2012; Mabery et al., 2013; Pharo et al., 2014; Robards et al., 2018; Scarso et al., 2009; Witherspoon et al., 2013)
Social	(Alali & Salim, 2016; Borzillo, 2017; Bos et al., 2007; Chen et al., 2014; Chu, 2016; Cochrane, 2011; Cornes et al., 2014; Crowley et al., 2018; Dawson et al., 2018; Del Giudice et al., 2015; Du Plessis, 2008; Ekberg et al., 2010; Faraj et al., 2016; Gagnon, 2011; Gibson & Meacheam, 2009; Hall & Graham, 2004; Ho & Kuo, 2013; D. Hong et al., 2011; J. Hong, 2017; Hosseini et al., 2017; Kaplan & Thomson Reed, 2007; Lathlean & Le May, 2002; H. Lee & Choi, 2003; Liu et al., 2012; Lyons et al., 2008; Mabery et al., 2013; Pharo et al., 2014; Robards et al., 2018; Tan & Noor, 2013; Witherspoon et al., 2013)
Strategy	(Chen et al., 2014; Cochrane, 2011; Dube et al., 2006; Gibson & Meacheam, 2009; Koh et al., 2005; Scarso et al., 2009)
Structure	(Borzillo, 2017; Cochrane, 2011; Cornes et al., 2014; Galán-Muros et al., 2017; Hall & Graham, 2004; Hara et al., 2009; D. Hong et al., 2011; Hsiao et al., 2017;

	Lathlean & Le May, 2002; H. Lee & Choi, 2003; H. S. Lee, 2017; Y. M. Li & Jhang-Li, 2010; Pharo et al., 2014; Scarso et al., 2009)
Tools & ICT	(Alali & Salim, 2016; Chu, 2016; Cochrane, 2011; Dahlander & O'Mahony, 2011; Del Giudice et al., 2015; Hall & Graham, 2004; Ho & Kuo, 2013; J. Hong, 2017; Koh et al., 2005; Lathlean & Le May, 2002; H. Lee & Choi, 2003; H. S. Lee, 2017; Y. M. Li & Jhang-Li, 2010; Lyons et al., 2008; Machuca & Costa, 2012; Swain & Ekionea, 2008; Tan & Noor, 2013; Witherspoon et al., 2013)
Trust	(Alali & Salim, 2016; Borzillo, 2017; Chen et al., 2014; Chu, 2016; Cornes et al., 2014; Dawson et al., 2018; Du Plessis, 2008; Ekberg et al., 2010; Faraj et al., 2016; Gagnon, 2011; Hall & Graham, 2004; J. Hong, 2017; H. Lee & Choi, 2003; H. S. Lee, 2017; Liu et al., 2012; Mabery et al., 2013; Machuca & Costa, 2012; Pharo et al., 2014; Ramos-Vielba et al., 2016; Robards et al., 2018; Tan & Noor, 2013; Witherspoon et al., 2013)

J.3 Barriers

Table 8-16 presents the sources that were used to create the Barrier elements. There is less variety in the amount of sources used to create the elements. The least amount of sources used is seven for Alignment & focus, Communication, and Structure. The elements Culture is mentioned the most in the found literature, by 20 sources. On average, the elements are mentioned by 11 different sources.

Table 8-16: Sources of the Barrier-elements

Barriers	Sources
Alignment & focus	(Bos et al., 2007; Jaegersberg & Ure, 2011; Lathlean & Le May, 2002; Mabery et al., 2013; Pirkkalainen & Pawlowski, 2014; Scarso et al., 2009; Swain & Ekionea, 2008)
Commitment & Participation	(Bos et al., 2007; Cochrane, 2011; Dube et al., 2006; Hall & Graham, 2004; Ho & Kuo, 2013; D. Hong et al., 2011; Hsiao et al., 2017; Lathlean & Le May, 2002; Mabery et al., 2013; Pharo et al., 2014; Scarso et al., 2009)
Communication	(Bos et al., 2007; Dahlander & O'Mahony, 2011; D. Hong et al., 2011; Jaegersberg & Ure, 2011; Koh et al., 2005; Pirkkalainen & Pawlowski, 2014; Scarso et al., 2009)
Culture	(Alali & Salim, 2016; Bos et al., 2007; Chu, 2016; Dawson et al., 2018; Du Plessis, 2008; Faraj et al., 2016; Ferlie et al., 2012; Ho & Kuo, 2013; D. Hong et al., 2011; Hsiao et al., 2017; Koh et al., 2005; Kruss & Visser, 2017; H. Lee & Choi, 2003; H. S. Lee, 2017; Machuca & Costa, 2012; Pharo et al., 2014; Pirkkalainen & Pawlowski, 2014; Ramos-Vielba et al., 2016; Scarso et al., 2009; Witherspoon et al., 2013)
Management	(Bos et al., 2007; Dawson et al., 2018; Du Plessis, 2008; Dube et al., 2006; D. Hong et al., 2011; Hsiao et al., 2017; Koh et al., 2005; Kruss & Visser, 2017; Lathlean & Le May, 2002; H. S. Lee, 2017; Mabery et al., 2013; Pharo et al., 2014; Pirkkalainen & Pawlowski, 2014; Price & Felix, 2008; Ramos-Vielba et al., 2016; Scarso et al., 2009)
Structure	(Dahlander & O'Mahony, 2011; Dawson et al., 2018; Galán-Muros et al., 2017; Kaplan & Thomson Reed, 2007; Mabery et al., 2013; Pharo et al., 2014; Scarso et al., 2009)
Tools & ICT	(Bos et al., 2007; Chu, 2016; Cochrane, 2011; Du Plessis, 2008; Dube et al., 2006; Ho & Kuo, 2013; D. Hong et al., 2011; Kaplan & Thomson Reed, 2007; Lathlean & Le May, 2002; H. Lee & Choi, 2003; Pirkkalainen & Pawlowski, 2014; Scarso et al., 2009)

Trust and social relations	(Bos et al., 2007; Crowley et al., 2018; Du Plessis, 2008; Dube et al., 2006; Ferlie et al., 2012; D. Hong et al., 2011; Lathlean & Le May, 2002; H. Lee & Choi, 2003; H. S. Lee, 2017; Mabery et al., 2013; Machuca & Costa, 2012; Pirkkalainen & Pawlowski, 2014; Ramos-Vielba et al., 2016; Scarso et al., 2009)

K. Interview protocol semi-structured interviews

Table 8-17: Interview protocol semi-structured interviews

Part	Question	Rationale
Introduction	Introduce yourself	
	Tell about research goals and connection to interview	Introduce the research and aim of the interview. Highlight some key elements of research to create a basic understanding.
	- Theme of the research is collaboration and knowledge exchange between companies in the port area in the field of cyber security	
	- My focus will be on the concept of Community of Practice: "a group of people informally bound together by shared expertise and passion for a joint enterprise." (Wenger and Snyder, 2000)	
	- A Community of Practice is commonly characterized by three activities: 1) knowledge exchange, 2) learning and 3) collaboration.	
	- My research question is: *"How can a Community of Practice on cyber security be established (in a logistic ecosystem)?"*	
	- With this interview I want to determine factors that influence CoPs and explore how a CoP can be created for the Rotterdam port area.	
	Tell about structure of interview	Manage expectations of the interview and my role as interviewer.
	- Consists for 4 parts: Short warm up, Goals, Drivers, Barriers.	
	- The goal is for you to tell about your experiences and ideas and I will ask questions to gain a better understanding.	
	- The interview will take around 1 hour.	
	Ask permission to record	
Warm up	What is your name	For the record and simple warm up
	What does your function and responsibilities entail?	For the record and simple warm up
	Do you have personal experiences in collaboration, knowledge exchange or learning with regards to cyber security or resilience?	Establish experience and expertise of the person
	Do you believe that a CoP on cyber security will work for the Rotterdam port area?	gauge point of view
Goals	What do you believe could be goals to establish a CoP?	Determine goals (SQ1b)
	What do you believe should be the goal for a CoP on cyber security for the Rotterdam port area? Why?	Zoom in on casus (SQ2)
	(ask about goals found in literature?)	

Success factors	What factors do you believe would help the establishment and working of a CoP?	Determine drivers (SQ1b)
	What factors do you believe would help the establishment of the CoP on cyber security in the Rotterdam port area? Why?	Zoom in on casus (SQ2)
	What do you believe is the most critical success factor for the establishment of a CoP on cyber security in the Rotterdam port area?	Determine critical node (SQ2)
	Which steps do you believe should be taken to reach these factors? By whom?	Gain insight in vision of companies (SQ3)
Barriers	What factors do you believe would hinder or impede the establishment of a CoP?	Determine Barriers (SQ1b)
	What factors do you believe would hinder or impede the establishment of a CoP on cyber security in the Rotterdam port area?	Zoom in on casus (SQ2)
	What do you believe is the most critical factor that can hinder the establishment of a CoP on cyber security in the Rotterdam port area?	Determine critical node (SQ2)
	Which steps do you believe should be taken to prevent these factors? By whom?	Gain insight in vision of companies (SQ3)

L. Interview summaries

Participant P1

Participant details

Name	Position	Size organization	Private/public	Rotterdam Port area
P1	CISO	Medium	Public	No

Summary

P1 works for a public organization that is part of national network of organizations with a similar goal. The ICT is done completely internally and cyber security is handled by 4 people.

P1 wants to gain (practical) information and help when the situation becomes dire. There exists a CERT for their network that fulfils this role and P1 is positive about its function. Furthermore he wished to collaborate with organizations in the network that have similar troubles in order to create a collective product or service. He believes this is more efficient and effective.

P1 mentioned that trust and “knowing each other” are an important drivers for collaboration, but they are difficult to achieve as well. A sense of awareness and urgency can increase the priority making it easier to start with a collaboration. This needs to happen on all levels. A clear vision or goal were seen as very helpful to create commitment. He/she has a neutral view on the role of management. It can be helpful to have their support as well as completely block any form of collaboration. A block from management was usually caused by more political reasons or that there is no priority. A bigger barrier is to establish commitment and participation by the different organizations. He/she also mentions that cultural differences can make collaboration more difficult and can hinder the creation of trust and social connections. He/she also experienced that it is not as self-evident or common to make contact with each other.

Elements

Table 8-18 provides an overview of the goals, drivers and barriers that were mentioned by this participant. The elements are arranged according to the perceived focus and priority that was given to them by the participant.

Table 8-18: Prioritization of elements of P1

Goals	Drivers	Barriers
Collective Cyber unit (New)	Trust (Theory)	Commitment and Participation (Theory)
Knowledge management (Theory)	Commitment (Theory)	Management (Theory)
	Social (Theory)	Priority (New)
	Awareness and Urgency (New)	Culture (Theory)
	Shared and Negotiable goals (Theory)	Trust and Social relations (Theory)
		Lack of knowledge and awareness (New)
		Mutual differences (New)

Other

P1 noted that it was easier to find connections for collaboration on a lower organizational level than through higher levels. This could suggest that the goals or aims are more similar on lower levels.

Participant P2.1/P2.2

Participant details

Name	Position	Size organization	Private/public	Rotterdam Port area
P2.1	Terminal manager	Small	Private	Yes
P2.2	ISPS manager	Small	Private	Yes

Summary

P2.1 and P2.2 are part of a small private organization in the Rotterdam port area. Their organizations is mostly faced by fake emails and the phenomena Storage spoofing. They are exchanging descriptions of potential culprits of storage spoofing with other organizations in the area.

Their main aim is to stop criminal activities that can cause damage of any sort to their organizations. They wish to see how other organizations are securing themselves and learn what is possible in order to gain some practical insights to take their own organizations to a higher level. It is mentioned several time that they feel dependent on the knowledge of others.

Their curiosity in how others handle themselves is an important driver, but direct relevance and making connection with others is important too. P2.1 also believes that distinguishing between the different branches and problems in the area can help to make better connections, since this will also make the group more manageable. The group size is important, because it can drive conversation or impede it. P2.1 also notes that it is difficult for companies to contact each other, because there can be no contact concerning commercial purposes. This could suggest a somewhat tense and distrustful culture.

They note that they expect more feedback from the Port of Rotterdam concerning cyber security, possibly using the ISPS. They also believe that the Port of Rotterdam should facilitate the meetings concerning cyber security, since they are responsible.

Elements

Table 8-19 provides an overview of the goals, drivers and barriers that were mentioned by this participant. The elements are arranged according to the perceived focus and priority that was given to them by the participant.

Table 8-19: Prioritization of elements of P2.1/P2.2

Goals	Drivers	Barriers
Company improvement (Theory)	Interest in Others (New)	Group size (New)
Learning (Theory)	Group size (New)	Culture (Theory)
Knowledge management (Theory)	Direct relevance (New)	Trust and Social relations (Theory)
Strategic (company) advantage (Theory)	Distinctions (New)	Commitment & Participation (Theory)
	Social (Theory)	Communication (Theory)
	Facilitator (Theory)	Mutual differences (New)

Other

It is mentioned that make the current storage spoofing website more known and using specialized cyber police officers would also help a lot. This could suggest that they also see that a part of the responsibilities is with the authorities.

Participant P3

Participant details

Name	Position	Size organization	Private/public	Rotterdam Port area
P3	PFSO	Medium	Private	Yes

Summary

P3 is part of a private organization in the Rotterdam port area. The IT is outsourced and all P3's colleagues have to provide are functional demands after which the service provider will start to facilitate it.

P3 believes that the threats from cyber are low for his organizations due to three reasons. Firstly, he/she believes his organization is not interesting to hack. Secondly, their operations are not sensitive to cyber-related issues. And finally, they have not encountered any trouble themselves or at direct competitors. He/she admits that these believes are somewhat baseless, since he/she also possess little knowledge over cyber security and its possibilities. This shows that a great barrier is the priority given to cyber, but also the lack of knowledge and awareness. The management therefore does not support it.

P3 thinks a goal of collaboration should be prevent people from doing double work ("opnieuw het wiel uitvinden") and to create a standard and shared level of security. This also supports his/her thought that the differences between organizations in branch, knowledge level and priority should be taken in account. This will help to provide a shared goal. A first step will remain to make be people become aware and let them experience a form of urgency.

Elements

Table 8-20 provides an overview of the goals, drivers and barriers that were mentioned by this participant. The elements are arranged according to the perceived focus and priority that was given to them by the participant.

Table 8-20: Prioritization of elements of P3

Goals	Drivers	Barriers
Company improvement (Theory)	Awareness and Urgency (New)	Priority (New)
Knowledge management (Theory)	Distinctions (New)	Lack of awareness and knowledge (New)
	Shared and negotiable goals (Theory)	Mutual differences (New)

Other

Participant P4

Participant details

Name	Position	Size organization	Private/public	Rotterdam Port area
P4	Security consultant	Small	Private	Yes

Summary

P4 is a PFSO-expert that advises and provides services for several private organizations in the Rotterdam port area. Cyber security has become part of the PFSO and he believes it is an important issue.

P4 is skeptical regarding collaboration in the Rotterdam port area. He/she believes that organizations are somewhat distrustful of each other, will always try to solve it on their own, and will never tell the full story. A low sense of awareness will also prevent organizations to act, since the priority will be lower as well. Collaboration can only work if the awareness is high, and when it is on the rise, then in turn the urgency will increase. P4 also makes distinctions between organizations based on prolife and urgency for cyber security. Furthermore he/she notes that collaboration need time to grow.

P4 thinks the only solution would be a centralized cyber security shop where organizations can buy all the products and services they need. This will ensure the cyber security of the port of Rotterdam. If collaborations were possible, it would be aimed to speak with the other actors in order to know what they are doing and how they are doing.

Elements

Table 8-21 provides an overview of the goals, drivers and barriers that were mentioned by this participant. The elements are arranged according to the perceived focus and priority that was given to them by the participant.

Table 8-21: Prioritization of elements of P4

Goals	**Drivers**	**Barriers**
Collective Cyber security Unit (New)	Awareness and Urgency (New)	Trust and Social relations (Theory)
Knowledge management (Theory)	Distinctions (New)	Culture (Theory)
Network & Interactions (Theory)	Time (New)	Lack of awareness and knowledge (New)
		Priority (New)
		Commitment and Participation (Theory)

Other

Participant P5

Participant details

Name	Position	Size organization	Private/public	Rotterdam Port area
P5	CISO	Large	Public	No

Summary

P5 works for public organization that is connected to a network of similar organizations. The ICT-provider for all the organizations in this network set up an CERT and SCIRT that show great similarities with a CoP. P5 is positive about how these CERT and SCIRT work as well, but notes that it took some time to develop to what it is now.

The main aims of the CERT and SCIRT are to exchange information; for example on cyber threats or malfunctions/bugs in software. It has quite the natural aim to create networks as well. It is also noted that specific products and services are developed in collaborations with the organizations. It should be remembered that the CERT and SCIRT were established by the ICT providers, so this aim coincides with the aim of such a stakeholder.

P5 believes that trust is an important, maybe the most important, driver, since it enables lots of the information sharing and social interaction. He/she also notes the importance of direct relevance for the members in order to keep them interested and connected. This also helps to keep management support. P5 describes that social interactions arise naturally as well as drive the community. This is further strengthened by the shared culture due to the similarities between the organizations in the network.

A big barrier is the lack of trust, since trust itself is such an enabler. The participation of people with unaligned aims or a manager instead of a CISO as well as resistance of management can be barriers as well.

Elements

Table 8-22 provides an overview of the goals, drivers and barriers that were mentioned by this participant. The elements are arranged according to the perceived focus and priority that was given to them by the participant.

Table 8-22: Prioritization of elements of P5

Goals	Drivers	Barriers
Knowledge management (Theory)	Trust (Theory)	Trust and Social relations (Theory)
Network & Interactions (Theory)	Direct relevance (New)	People (New)
Creation of products and services (Personal)	Management (Theory)	Management (Theory)
	Social (Theory)	
	Time (New)	

Other

This interview was not recorded in its entirety, therefore the notes made by the researcher after the interview play an important role in the summary. This may mean that some observations cannot be directly found in the transcript.

Participant P6

Participant details

Name	Position	Size organization	Private/public	Rotterdam Port area
P6	Strategic advisor	Large	Public	Yes

Summary

P6 is part of a public organization related to FERM. He/she is very positive about how the FERM group works and notes that the safe and open culture makes collaboration easy. The main goal of this group is to establish a strong network.

P6 believes that the main goals for a CoP are exchanging information and making it possible for board-level stakeholders to make proper decisions. This can also include agenda setting for board-level members. He/she also notes the importance of creating awareness as a goal for a CoP.

P6 notes quite a lot of drivers, most of them related to shared (cultural) values. He/she believes that a shared culture consisting of safety, openness, informality and honesty are crucial. He/she also focuses on the personal and social driver. The connection and trust between people is quite important. It is noted that these three drivers also take time to develop. An important driver that is named at the end is urgency. This can be a strong driving force to make stakeholders collaborate. Other drivers that were briefly named were shared goals, support from management, a facilitator and commitment from both management as well as the participants.

P6 focuses on three barriers explicitly, but mentions several others as well. She notes that the social drivers are almost instantly barriers if they are not treated right. In addition, an important barrier is the people involved and their attitude towards the CoP. If people are too self-centered or unconstructive, then it will limit the CoP. Management is another barrier that can block the participation of people and develop of the CoP. A last important barrier is the difference between companies.

Elements

Table 8-23 provides an overview of the goals, drivers and barriers that were mentioned by this participant. The elements are arranged according to the perceived focus and priority that was given to them by the participant.

Table 8-23: Prioritization of elements of P6

Goals	Drivers	Barriers
Knowledge management (Theory)	Culture (Theory)	Culture (Theory)
Network & Interactions (Theory)	Social (Theory)	People (New)
Enabling board-level members (Personal)	Trust (Theory)	Trust and Social relations (Theory)
	Time (New)	Mutual differences (New)
	Awareness and Urgency (New)	Management (Theory)
	Management (Theory)	Commitment and Participation (Theory)
	Shared and negotiable goals (Theory)	Communication (Theory)

	Commitment (Theory)	
	Facilitator (Theory)	
	Direct relevance (New)	

Other

P6 also shows some distrust towards the aims of private organizations. It is mentioned that their only aim is profit maximization which can be destructive for the whole.

Participant P7

Participant details

Name	Position	Size organization	Private/public	Rotterdam Port area
P7	CISO	Large	Public-Private	Yes

Summary

P7 is in touch with quite a few organizations in the Rotterdam port area, although less with the SMEs. P7's view is practical and aimed on the tactical and operational level.

P7 believes the aim of the CoP should be to establish and share best practices for the Rotterdam port area as well as share threat intelligence information. This indicate a form of knowledge management on a more practical level as well as the aim for direct company improvements. Furthermore, he/she indicated that collective training exercises or awareness programs would also be a good aim. Lastly, he/she noted that a product investment collective was also a possible aim.

P7 believes that there are three important conditions for the CoP: a proper IT-support system in order to encourage collaboration and communication, a facilitator that leads and supports the process of the CoP, and some initial trust between the partners. From these three conditions, organizations can commit themselves for the long term with shared goals. He/she briefly mentioned other drivers as well.

The main barrier was the lack of priority that organizations have for cyber security which is further strengthened by the lack of knowledge about the subject. Therefore, organizations are late to act. There are also difference between the organizations in the Rotterdam port area that impede sharing as well as easy communication. This limits the creation and working of a CoP as well.

Elements

Table 8-24 provides an overview of the goals, drivers and barriers that were mentioned by this participant. The elements are arranged according to the perceived focus and priority that was given to them by the participant.

Table 8-24: Prioritization of elements of P7

Goals	Drivers	Barriers
Company improvement (Theory)	Tools & ICT (Theory)	Priority (New)
Collective Training or exercise (New)	Facilitator (Theory)	Lack of awareness and knowledge (New)
Knowledge management (Theory)	Trust (Theory)	Mutual differences (New)
	Commitment (Theory)	Limited sharing (New)
	Shared and negotiable goals (Theory)	Communication (Theory)
	Social (Theory)	Trust and Social relations (Theory)
	Confidentiality (New)	Tools & ICT (Theory)
	Direct relevance (New)	
	Distinctions (New)	

Other

Participant P8

Participant details

Name	Position	Size organization	Private/public	Rotterdam Port area
P8	Researcher	Large	Public	Yes

Summary

P8 is co-organizer of knowledge events in his own organizations that are show similarities with CoP. He/she also wholeheartedly believe in the power of these sort of events.

P8 thinks the main aim for CoP is to create and strengthen networks between similar and like-minded people. This can help to increase the set of "objective knowledge" as well as exchange experiences and knowledge. He/she envisions the CoP as a neutral meeting ground where generic themes can be discussed. He/she points out that the CoP can also act as an information point and communication canal, but this is from the point of view of his organization.

P8 puts a lot of focus on the practical and organizational aspects of CoP meetings such as proper location, network breaks and plenty of coffee. He/she highlights the social aspects of the CoP and the driving force of this. Emphasis is also put on the right type of attendants and the moderator/facilitator. These two are important to create the right setting for exchange and interaction. Repetition (and inherently, time) also is important for the CoP to grow and to gain the right status.

P8 shows concern about the current culture in the Rotterdam port area. A safe environment to speak your mind is important, but is not yet present. Furthermore, Rotterdam is in general less focused on knowledge exchange than other cities such as Amsterdam. This work ethos can hinder a CoP. This can hinder the social interactions and creation of trust. The heterogeneity of the Rotterdam port area plays a critical role in this as well.

Elements

Table 8-25 provides an overview of the goals, drivers and barriers that were mentioned by this participant. The elements are arranged according to the perceived focus and priority that was given to them by the participant.

Table 8-25: Prioritization of elements of P8

Goals	Drivers	Barriers
Network & Interactions (Theory)	Social (Theory)	Culture (Theory)
Knowledge management (Theory)	People (Theory)	Trust and Social relations (Theory)
	Facilitator (Theory)	Mutual Differences (New)
	Time (New)	People (Theory)
	Culture (Theory)	
	Direct relevance (New)	
	Trust (Theory)	
	Communication (Theory)	

Other

Participant P9

Participant details

Name	Position	Size organization	Private/public	Rotterdam Port area
P9	Policy advisor	Medium	Semi-public	Yes

Summary

P9 has quite a lot of experience with different parties in the Rotterdam port area and meeting structures. The result is that P9 has a distinct vision on how the CoP should be shaped and what is important.

P9 thinks the goals of a CoP have a certain flow. It starts with establishing an understanding of the state-of-the-art knowledge after which practical experience is gather among organizations. The combination of these two can lead to a perspective of action (handelingsperspectief). This perspective can focus on learning new things, deeper investigations or lobby actions depending on the situation. This string of goals are most focused on knowledge management and may lead to some form of learning. A natural goal of a CoP is establishing connections between people and creating a network.

An important driver is creating fun or “jeux” in order to create an open and positive atmosphere. This helps to create a proper culture trustful connections. A good facilitator and moderator as well as the right people are quite important for this as well. P9 believes that a positive and fun setting can be combined with useful sharing. Useful sharing can be established by direct relevance and confidentiality.

A combination of barriers were thought of as essential. The culture in the Rotterdam port area is somewhat tense causing people to perceive certain topics too fearful and with too much emotion. This creates distrust and limited sharing. Sharing is further limited when confidentiality is secured causing distrust to further increase.

Elements

Table 8-26 provides an overview of the goals, drivers and barriers that were mentioned by this participant. The elements are arranged according to the perceived focus and priority that was given to them by the participant.

Table 8-26: Prioritization of elements of P9

Goals	Drivers	Barriers
Knowledge management (Theory)	Jeux (Personal)	Culture (Theory)
Network & Interactions (Theory)	Culture (Theory)	Trust & Social relations (Theory)
Learning (Theory)	Social (Theory)	Limited sharing (New)
	Trust (Theory)	People (New)
	Facilitator (Theory)	Group size (New)
	People (Theory)	Communication (Theory)
	Confidentiality (New)	
	Direct relevance (New)	
	Distinctions (New)	
	Time (New)	

Other

P9 thinks one principle can be important: right to take, obligation to bring (haal-recht, breng-plicht). Organizations must always bring in new information and have the right to take information.

Participant P10

Participant details

Name	Position	Size organization	Private/public	Rotterdam Port area
P10	Board member	Large	Public-private	Yes

Summary

P10 clearly takes a management level perspective on CoPs as well as shows clear positions with regards to the function of collaboration in the field of cyber security.

P10 envisions stronger connections both physically as well as digitally. He/she uses the the metaphor of digital firemen force, a PPP that resolves crisis by providing operational support as well as advises in the implementation phase by sharing knowledge and expertise.

P10 focuses on the a shared sense of responsibility, commitment, trust and social interactions that can drive a CoP. The culture needs to be right and the pride that people for being part of the Rotterdam port area can contribute to this. Management level support and commitment also play a key part and can be further improved by establishing shared goals and communicating the urgency.

The greatest barrier that P10 sees is the culture of competition and direct profitability. Therefore management will not support CoPs on cyber security and it will not be financed. It also hinders the sharing of information of knowledge.

Elements

Table 8-27 provides an overview of the goals, drivers and barriers that were mentioned by this participant. The elements are arranged according to the perceived focus and priority that was given to them by the participant.

Table 8-27: Prioritization of elements of P10

Goals	Drivers	Barriers
Collective Cyber unit (Theory)	Commitment (Theory)	Culture (Theory)
Knowledge management (Theory)	Culture (Theory)	Management (Theory)
Network & Interactions (Theory)	Management (Theory)	Priority (New)
	Pride for Rotterdam (New)	Communication (Theory)
	Social (Theory)	Limited sharing (New)
	Trust (Theory)	
	Awareness and Urgency (New)	
	Shared and negotiable goals (Theory)	
	Distinctions (New)	
	Communication (Theory)	

Other

Participant P11.1/P11.2/P11.3

Participant details

Name	Position	Size organization	Private/public	Rotterdam Port area
P11.1	Asset manager	Medium	Private	Yes
P11.2	Director of Operations	Medium	Private	Yes
P11.3	QHSE	Medium	Private	Yes

Summary

The people from this organizations all understand the importance of cyber security, however their interest in the subject is very limited since it's not related to their core business. They use an external firm that deals with the ICT, but they realize they themselves need to have some knowledge of it too.

The main aim of a CoP would be to gain and share practical information and knowledge. This can be examples or casus of other companies such as other IT solutions or new methods. Organizations can learn from each other in this manner, which can lead to direct improvement of their own organization. There are some hints that they are very interested in the level of other companies and want their branch as a whole be at similar level of security. The motivation for this aim is not clear-cut.

The most important drivers are relevance and interest in others. If the CoP address relevant issues especially of other organizations, then commitment and attendance is natural. The social relations and trust in others also proves to be important, since they show some distrust to others and unknown parties. This also aligns with their statement that their opinion of FERM is positive due to the trust they have in the public organizations that established FERM. They also wish for some sort of screening for the participants in order to secure the confidentiality. A great factor for their current interest in cyber security is the APM-terminal crash in June 2017. This made them and all other companies in the Rotterdam port area aware of the dangers of cyber security.

The biggest barriers is their distrust in others especially when they are not familiar with some of the participants. They also don't want sales people to be part of the meeting, since they don't wish to be bother with sales-related emails and calls from IT suppliers.

Elements

Table 8-28 provides an overview of the goals, drivers and barriers that were mentioned by this participant. The elements are arranged according to the perceived focus and priority that was given to them by the participant.

Table 8-28: Prioritization of elements of P11.1/P11.2/P11.3

Goals	Drivers	Barriers
Company improvement (Theory)	Direct relevance (New)	Trust and Social relations (Theory)
Knowledge management (Theory)	Interest in others (New)	People (New)
Learning (Theory)	Social (Theory)	Culture (Theory)
	Trust (Theory)	
	Awareness and Urgency (New)	
	Confidentiality (New)	
	Pride for Rotterdam (New)	
	Structure (Theory)	

Other

Participant P12

Participant details

Name	Position	Size organization	Private/public	Rotterdam Port area
P12	Security manager	Large	Private	Yes

Summary

P12 is proud on the safety and security, both physical as well as digital, of his organization. This organizations puts quite a lot of focus on this theme, therefore P12 has a lot of support as well as strong connections with other organizations.

P12 believes the main aim is to exchange experiences and to look each other in the eye. Furthermore, he/she believes that exchanging experiences and building networks happen in two different settings.

The main driver is the social connections between people that creates trust. P12 also stresses the importance of a confidentiality protocol which sets clear rules on how and when information will be shared. Support of management is given for P12, but he realizes that other security manager might not be as fortunate. Therefore, he notes that management plays an important role in support as well as in setting a culture in which security and safety are central themes. This culture is a show of commitment. A similar or shared culture is also essential when collaborating with other organizations, since it also contributes to a shared goal. Lastly, P12 notes that management as well as employees need awareness of cyber security in order start improving and collaborating.

A big barrier is the initial lack of openness and trust between organizations. Furthermore, P12 notes that there is also a limit to the information and knowledge that is shared. Some part will also remain private. P12 notes that a lack of management support and priority are great barriers too. When the amount of participants increase, this can also hinder the creation of connections and trust, thus hindering the process of a CoP.

Elements

Table 8-29 provides an overview of the goals, drivers and barriers that were mentioned by this participant. The elements are arranged according to the perceived focus and priority that was given to them by the participant.

Table 8-29: Prioritization of elements of P12

Goals	Drivers	Barriers
Knowledge management (Theory)	Social (Theory)	Trust and Social relations (Theory)
Network & Interactions (Theory)	Trust (Theory)	Culture (Theory)
	Management (Theory)	Limited sharing (New)
	Confidentiality (New)	Priority (New)
	Culture (Theory)	Group size (New)
	Commitment (Theory)	Communication (Theory)
	Shared and negotiable goals (Theory)	
	Awareness and Urgency (New)	
	Pride for Rotterdam (New)	
	Group size (New)	

Other

Participant P13

Participant details

Name	Position	Size organization	Private/public	Rotterdam Port area
P13	QESH manager	Medium	Private	Yes

Summary

Cyber security is P13's responsibility, but an external firm handles the technical details and the tests. P13 is currently trying to do more testing herself, since UH believes the current way of testing is limited.

P13 sees it as a main goal to exchange and share tips & tricks related to practical cases with other companies in order to directly improve, but also to do collective training exercises. P13 has a firm believe that training and exercising are crucial and therefore he/she wants to increase its difficulty and size. The interviews revealed several barriers and drivers. A barriers is that P13 only wants to share information and details to a certain degree. This seems to be caused by an overall culture of secrecy and a lack of trust between organizations. P13 also need to gain permission from higher management if he/she wished to explore collaboration on this field. A driver is, as P13 puts it, "knowing people", "being able to contact easily" and "to be part of Rotterdam". P13 also notes that the incident at APM terminal in June 2017 made the entire port area more aware of the urgency of cyber security.

P13 is critical about the current way of working of the PoR. He/she noted that no constructive feedback is given and that the mandatory training exercise are not critical enough. P13 believed that PoR should be more firm as well as play a facilitator role for collaboration.

Elements

Table 8-30 provides an overview of the goals, drivers and barriers that were mentioned by this participant. The elements are arranged according to the perceived focus and priority that was given to them by the participant.

Table 8-30: Prioritization of elements of P13

Goals	Drivers	Barriers
Collective training or exercise (New)	Social (Theory)	Limited Sharing (New)
Company improvement (Theory)	Management (Theory)	Culture (Theory)
Knowledge management (Theory)	Awareness and Urgency (New)	Trust and Social relations (Theory)
	Culture (Theory)	Management (Theory)
	Pride for Rotterdam (New)	Mutual Differences (New)
	Facilitator (Theory)	

Other

M. Theoretical elements mentioned in interviews.

The process of transcribing, coding and translating explained in section 3.3.4 made it possible to determine if any of the theoretical elements were mentioned by the participants. Overviews per aspects were created and are presented in Table 8-31, Table 8-32 and Table 8-33. The overviews show how many times a theoretical element of a certain aspect is mentioned by a specific participant as well as a sum of how many of the participant mentioned a certain element. These overviews provide some first information on the recognition of the theoretical elements by stakeholders.

M.1 Goals

The overview of the Goal aspect are shown in Table 8-31. When examining the individual participants (P1-P13), it can be seen that, in general, Goals were not mentioned often during the interviews. Only P7 mentioned two goals for five times, while most only referred to a certain goal once or twice. It can also been seen that most refer only to a maximum of two goals; only P1, P5 and P9 mentioned more than two possible goals for a CoP.

When examining the sum, it can be easily seen that two goals are mentioned most often: Knowledge Management and Network & Interactions.

Table 8-31: Overview of the theoretical goals mentioned in the interviews

Theoretical Goals	**Sum**	**P1**	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**	**P10**	**P11**	**P12**	**P13**
Company improvement	5		4	1				2				2		2
Knowledge management	13	1	3	1	1	3	2	2	5	5	1	4	2	2
Learning	3		3							1		1		
Network & Interactions	7				1	1	1		8	1	1		1	
Strategic (company) advantage	1		2											

M.2 Drivers

The overview of the driver aspect is presented in Table 8-32. Upon examination of the responses of the participants, it can be seen that there is more variation in the amount of references compared to the Goal elements. This suggest that participants talked more about the Drivers and tried to stress it the importance of certain elements more.

An examination of the sum-column shows that some elements were not or barely mentioned by participants: Awareness of knowledge, Communication, People, Reward & Recognition, Strategy, Structure, and ICT & Tools. The Drivers Social and Trust were mentioned most often. A group of Drivers are mentioned by approximatively half of the participants: Commitment, Culture, Facilitator, Management, and Shared & negotiable goals.

Table 8-32: Overview of the theoretical drivers mentioned in the interviews

Theoretical Drivers	Sum	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13
Awareness of knowledge	0													
Commitment	5	1					4	2			2		1	
Communication	2								1		1			
Culture	6						8		3	1	3		2	1
Facilitator	6		1				1	3	3	3				1
Management	5					1	4				2		1	1
People	2								1	1				
Reward & recognition	0													
Shared & negotiable goals	6	1		1			4	3			1		2	
Social	11	1	2			3	4	2	1	2	2	1	1	3
Strategy	0													
Structure	1											1		
Tools & ICT	1							2						
Trust	9	2				4	5	3	1	3	3	1	3	

M.3 Barriers

The overview of the Barrier aspect is presented in Table 8-33. Upon examination of the responses of the participants, it can be seen that there is more variation in the amount of references compared to the Goals elements, but less than with the Driver elements. This suggest that participants talked moderately about the barriers and put more focus on the Drivers.

The examination of the sum-column shows that some elements were not or barely mentioned by participants: Alignment & Focus, Commitment & Participation, Structure, and ICT & Tools. Two Barriers are mentioned by most participants: Culture and Trust & social relations.

Table 8-33: Overview of the theoretical barriers mentioned in the interviews

Theoretical Barriers	Sum	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13
Alignment & focus	0													
Commitment & participation	4	3	1		2		2							
Communication	6		1				1	1		1	1		1	
Culture	10	3	1		2		1		3	4	2	1	2	1
Management	5	4				1	2				2			2
Structure	0													
Tools & ICT	1							1						
Trust & social relations	11	3	3		3	1	1	1	1	3		1	1	2

N. NEW ELEMENTS MENTIONED IN THE INTERVIEWS

The process of transcribing, coding and translating explained in section 3.3.4 made it possible to create new elements. These elements were created according to the three aspects Goals, Drivers, and Barriers. Table 8-34, Table 8-35, Table 8-36 provide an overview of the new elements for their respective aspect and how often they are referred to by the participants. The amount of reference were the basis to create the element. The definition of the elements can be found in section 4.3.1.

N.1 New Goals

The new Goal elements are shown in Table 8-34. Two new elements were found: Collective cyber security unit and Collective training or exercise. The table shows that the references to these new Goals is low, except for P10 on the Collective cyber unit. This is in line with the observation on the references at the theoretical Goals in Table 8-31.

Table 8-34: Overview of new goals mentioned in the interviews

New Goals	Sum	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13
Collective cyber unit	3	2			2						4			
Collective training or exercise	2							1						2

N.2 New Drivers

The new Driver elements are shown in Table 8-35. A total of 7 new elements were synthesized from the interviews, among which the Drivers Awareness & Urgency and Direct Relevance are mentioned by more than half of the participants. In general, the amount of references to a new Driver element per participant remains low, but is somewhat in line with the findings of Table 8-32.

Table 8-35: Overview of new drivers mentioned in the interviews

New Drivers	Sum	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13
Awareness & urgency	8	1		2	6		2				1	1	1	1
Confidentiality	4							1		3		1	4	
Direct relevance	7		2			1	2	1	1	2		2		
Distinctions	6		2	3	2			1		2	1			
Group size	2		2										1	
Interest in others	2		2									1		
Pride for Rotterdam	4										2	1	1	1
Time	5				1	1	1		2	1				

N.3 New Barriers

The new Barrier elements are shown in Table 8-36Table 8-35. A total of 6 new elements were synthesized from the interviews, among which the Barrier Mutual Differences is mentioned by more than half of the participants. In general, the amount of references to a new Barrier element per participant remains low, but is somewhat in line with the findings of Table 8-33Table 8-32.

Table 8-36: Overview of new barriers mentioned in the interviews

New Barriers	**Sum**	**P1**	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**	**P10**	**P11**	**P12**	**P13**
Group size	3		2							1			1	
Lack of awareness and knowledge	4	1		3	2			1						
Limited sharing	5							1		3	1		1	2
Mutual differences	7	1	2	2			2	2	1					2
People	5					1	2		1	1		1		
Priority	6	2		4	1			2			1		2	

O. Summary of narrative review

O.1 Existing concepts

The literature presented several concepts that could be useful for this case. These concepts could be used as a solution on their own or as a source of inspiration. This section will describe the concepts themselves and will elaborate on them. Furthermore, the most promising concepts for the case of PoR will be highlighted. Section 5.1.2 describes the solutions of the conditions which are based on the findings in literature and thus on these concepts.

Table 8-37 presents the concepts found in literature. The first and second column show respectively the abbreviation and the full name of all eleven concepts. The third column presents the definitions for the concepts. Several documents differed in their definition for a concept with the same name. Therefore all definitions are listed in the third column.

Several sets of concepts can be discerned upon closer examination of the definitions. The first set of concepts comes from the field of cyber security. This set includes the concepts: ISAC, CERT, CSIRT, WARP and Abuse Team. These concepts were conceived with a focus on cyber security. Their difference lies mostly in their connection to direct operations. An ISAC is more focused on sharing information and supporting each other, while an Abuse Team is directly operational.

Special attention must be given to CERT and SCIRT, since at this moment both terms are used as synonyms. The concept CERT was established in the late 1980s in the USA after one of the first major IT incidents. This concept was the inspiration for the SCIRT concept in Europe in the 1990s. CSIRT is currently considered the more precise term (ENISA, 2006b, p. 6).

Another set is formed by the CoP-related concepts which are all mentioned by Wenger et al. (2002). This set includes the CoP, the distributed CoP, and the community-based knowledge initiative. This set is connected by the idea of learning, and developing knowledge at the same time. The difference between the concepts is mainly the physical distance and formality. For example, the members of a CoP are physically close for face-to-face interactions and to establish a group, while a distributed CoP works completely digitally.

The contents of the last set are related to each other, since they are general collaboration formats: the PPP, the regional ecosystem, and the supply chain. These formats are used in a wider area than cyber security and for all sorts of reasons. They have been shown to be effective in certain situations.

Table 8-37: Overview of existing concepts

Abbreviation	Full name	Definitions used in literature
ISAC	Information Sharing and Analysis Centre	A member driven organization or group (formal or informal) which is created to support its members in protection by cyber and physical security (ENISA, 2017a, p. 12)
		A consultative body for cyber security. In an ISAC, you create a trusted environment with organizations from the same sector in order to share sensitive and confidential information on incidents, threats, vulnerabilities, measures and lessons learnt in relation to cyber security. (NCSC, 2018d, p. 4)
CERT	Computer Emergency Response Team	CERTs started as being a reaction force to cyberattacks, but they evolved over time. Now they provide a complete security service provider, including preventative services such as alerts,

		security advisories, training and security management services. The term “CERT” was soon considered insufficient. As a result, the new term “CSIRT” was established at the end of the 1990s. (ENISA, 2006b, p. 6)
CSIRT	Computer Security Incident Response Team	A team of IT security experts whose main business is to respond to computer security incidents. It provides the necessary services to handle them and support their constituents to recover from breaches (ENISA, 2006a, p. 7).
		An organization that receives reports of security breaches, conducts analyses of the reports and responds to the senders (ENISA, 2016, p. 7)
		A form of collaboration in which CSIRT services are performed for a number of organizations. A collective CSIRT handles the coordination and collaboration in the event of threats or incidents that occur at one or more participating organizations (NCSC, 2018a, p. 4)
WARP	Warning, Advice and Reporting Points	WARP members agree to work together in a community and share information to reduce the risk of their information systems being compromised and therefore reduce the risk to their organization. This sharing community could be based on a business sector, geographic location, technology standards, risk grouping or whatever makes business sense” (ENISA, 2006b, p. 9)
		A WARP provides a service of early warnings of alerts and vulnerabilities that is specifically tailored to its community. By delivering relevant content in a language understood by the community’s users, and by taking steps together to mitigate specific threats within the community, the WARP is able to show tangible benefits for its members and to establish trust. (Hakkaja, 2006, p. 7)
Abuse Team		A group of experts that deal with large number similar incidents, are responsible for customs IPS, deal with simple incidents, take commercial interest in consideration. (ENISA, 2006b, p. 9)
CoP	Community of Practice	A group of people who share a concern, a set of problems, or a passion about a topic and who deepen their knowledge and expertise in this area by interacting on an ongoing basis (Wenger et al., 2002, Chapter 1).
Distributed CoP		A CoP where there are no means for face-to-face interaction, so all is done digitally (Wenger et al., 2002, Chapter 6).
Community-based knowledge initiative		The concept of CoP is leveraged to transform organizations in order to build the organization’s overall capacity to learn and innovate (Wenger et al., 2002, Chapter 9)
Supply chain		A group of organizations that are involved in a flow of products, services, finances and information, and in which the organizations are individually responsible for part of the flow (NCSC, 2018c, p. 4)
Regional Ecosystem		This collaboration encompasses a large number of diverse groups – private businesses, government bodies, individuals,

		processes and smart devices – which interact with each other for a range of purposes. Connected information infrastructures, processes, data and communication technologies create dependencies between these diverse groups (NCSC, 2018b, p. 4).
PPP	Public Private Partnership	A long term agreement/cooperation/collaboration between two or more public and private sectors that has developed through history in many areas (ENISA, 2017b, p. 7).

O.2 Possible Strategies and Structures

Table 8-38: Summary of narrative review focused on strategies and structures

Literature	**Strategies and structures**
(ENISA, 2017a) - ISACs	Formation process: 1) Rationale for creation: why is the ISAC started and in what context: heavy hierarchal culture thus regulatory requirement or pragmatic approach based on network 2) Decide on driving force: profit, having knowledge, government or EU institution. 3) Motivation to participate: Public: Knowledge of security, opportunity for single coordination point, better understanding of needs private sector Private: Sharing knowledge on incidents, part of group, access to knowledge, networking
	Models for ISAC - Country-focused ISAC; all experts are part of 1 initiative to make sharing and exchange easy. Funded by subsidies and mandatory fees, but no governance structure. -Sector-specific ISAC; sharing information and analysis with each other in sector to improve sector knowledge and experience. Usually has platform with shared services. Funded through mandatory fees or contribution. Clear governance structure with management and support roles by sector itself or government. - International ISAC; private sector is driving force, and cultural differences an obstacle.
	Governance model: - Structured with chair and vice-chair (and secretariat) that set goals - With support body where secretariat is a facilitator. - Flexible governance by volunteers.
	Funding strategies: - mandatory fees (based on size and involvement) - voluntary contribution - government subsidies (rare option, private sector is usually responsible)
	Basic capabilities of ISAC - Information sharing; usually formal agreement or membership agreement is required. Done through a platform or face-to-face. Types of info: incidents, threats, vulnerability, mitigations, situational awareness, best practices, strategic analysis. - Analysis; a difficult to develop capability.

	- Trust building; can be best done through personal relations, but legal forms can help. Components are: added value, punctuality, comprehensiveness, expertise, dedication. - Capacity Building; increasing and adding capabilities such as vulnerability and threat analysis, training and expertise, awareness campaigns.
(ENISA, 2017b) – PPPs	Strategies for growth: - Top down - Bottom up - Top down then grow bottom up - Bottom up then grow top down - Fire and forget - Split and merge
	Types of PPP - Institutional PPP; for vital infra. Very dependent on leadership, but public servants determine success. - Goal-orientated PPP; when cyber is seen as essential for economy and needs more support. Has strategic and policy focus. Clear structures. - Outsourcing Cyber Service PPP (OCS); government recognizes need, but cannot address it, thus creates stand-alone organization. - Hybrid PPP; combi of OCS and institutional. Governments needs more knowledge and resources to build solutions.
(ENISA, 2006a) – CSIRT	- Determine type of CSIRT (9 types) - Select services; 1) reactive, 2) proactive, 3) artifact handling, 4) security quality management. - Define initiative with business plan; have organizational structure, financial model, sharing policy. - Create business case. - Train members.
(ENISA, 2014) – Trust models	Build trust by: - Controlling entry of new members using a protocol with sponsorship or a trusted introduce (TI). - Provide activities that foster trust. - Provide additional maturity level. - Have members sign a NDA. - Have contribution.
(ENISA, 2016) – incident response and collaboration	4 baseline capabilities of CSIRT: 1) Formal capability; mandate that determines role and purpose 2) Operational-technical capability; services it provides 3) Operational-organizational capability; the resources, services delivery and business continuity 4) Co-operational capability; to be able to work with others (i.e. through SLA)
(ENISA, 2006b) – CERT collaboration	Models for cooperation: - Bilateral team-team: comes from experience and common future goal - Association: set of teams: driven by common interest and goals. Can be launch platform for networking and team cooperation. - Cooperation between associations.
	Legal bases: - Non-disclosure Agreement (NDA) - Memorandum of Understanding (MOU) - Contract

	- Terms of Reference (ToR)
	Models for trust: - Bilateral and multilateral agreements - Code of Conduct - Sponsorship - Open Community - Accreditation by TI
(NCSC, 2015) – CSIRT Maturity kit	- Organization; focus on trustworthiness and reliability with high performance. - Human; create CoC, have a small start group (3-5 members), focus on training - Tools; invest in automated tools - Processes; document steps and processes in order to make them available.
(NCSC, 2018d) – ISAC	- Explore; find like-minded parties, keep it formal, ask lots of questions and try to reach consensus - Build; formal kick-off, focus on building trust, dividing roles, and meeting structure. Also discuss membership guidelines - Continue; keep building trust, try to increase the value per meeting. Also create procedures for new members and how to change roles.
(NCSC, 2018a) - CSIRT	- explore; create support, build trust and seek consensus. 1) find possible partners, 2) create workgroup. - Consensus; define mandate, services and activities. - Grow; increase capabilities and evolve.
(NCSC, 2018c) – supply chain	- Explore: gain overview of involved parties and bring together - Demonstrate; study supply chain and establish basic level, make agreements on how to improve. - Implement; develop, do and monitor steps.
(NCSC, 2018b) – Regional collaboration	- Explore; take time to make design choices - Develop; validate ideas within large group and broaden support. Make a decision making structure - Action; expand leading group into interactive community. Create a roadmap
(NISCC, 2006) – WARP business case	Five stages in making the WARP Business case 1) Identity the community 2) Identifying benefits 3) Identify resources and costs 4) Identify funding: internal, membership supscription, member co-operative, partnership, sponsorship 5) Produce business case
(Askwith, 2006) – WARP case study	Trust building start with finding a common interest which can be translated to a business benefit to stimulate participation. Steps towards a WARP: - Identify the community; It is difficult to assess the match of possible members. Therefore an inside champion who helps to penetrate the organizations and other organizations, is very helpful. He can advise on how to engage, who to engage and to understand the needs better. - Build a business case. - sell the WARP idea to all members through the best person within every organization to engage with - Establish funding - Bring the potential members together and start. - Keep momentum going with activities using careful planning.

(NISCC, 2002) – Information sharing vision	Funding model of WARP - Commercial; members pays subscription fee to an independent agency - Corporate; internal for 1 company. - Customer; large organizations offers this (with discount) to its existing customers. - Public-private (partnership) - Cooperative; all members pay subscription and this pays the WARP's activities and services.
(Hakkaja, 2006) – Evolution of WARP	Core services of a WARP - Filtered warnings; a staff members collects information from members and external sources and distributes these according to the needs of the members. - Advice brokering; members have a safe environment to exchange knowledge and information. - Trusted sharing; an safe environment where members can share sensitive information. Development model WARP 1) Show benefit through a tailored warning service, so that everyone feels they are getting a personalized and valuable service 2) Develop trust through encouraging members to help one another by sharing and giving advice. 3) Encourage members to report their experiences on sensitive topics such as attacks and problems to improve on collective learning.
(UKERNA, 2006) – CSIRT and WARP together	
(Wenger et al., 2002)	Typology of CoP relation with organization: - Unrecognized; invisible to organization and some potential members - Bootlegged; informally known to few - Legitimized; officially sanctioned as entity - Supported; provided with direct resources to create a CoP
	CoP elements: - Domain; set of issues, create identity & purpose. - Community; people and members, create social fabric for learning - Practice; set of framework, ideas, tools that are created and shared.
	Design principles: - Design for evolution; have elements catalyze natural evolution - Open a dialogue between inside & outside perspectives - Different levels of participation; different roles such as coordinator, leader, member. Usually: core group, active group, peripheral, outsiders. - Develop both public & private community spaces - Focus on value - Combine familiarity and excitement - Create a rhythm for the community
	Stages of community development - Potential; an existing social network flock informally around a subject. Domain: set the scope, Community: connecting the network informally, Practice: identify common needs. Important features: 1) determine primary intent of community. 2) define domain and identify engagement issues.

	3) build a case for action. 4) identity potential coordinators & thought leaders. 5) interview potential members. 6) connecting members. 7) create preliminary design of community. The critical role is community coordinator. - Coalescing; official launch and focus on building trust, relationships and awareness of common interests and needs. Domain: establish value of sharing knowledge, Community: develop relationship & trust to discuss sensitive info, Practice: determine what knowledge to share and how. Nurture communities through: 1) build case for membership 2) launch community 3) initiate community events & space 4) legitimize community coordinators 5) build connections between core members 6) find ideas, insights, practice worth sharing 7) be modest with reorganizing 8) identify opportunities for value 9) gain manager support & engagement. - Maturing; focus shifts from establishing value to clarifying the focus, role, and boundaries of community. Domain: to define its role in organization and in relation to other domains, Community: managing the boundaries to ensure that the community is not distracted from its core purpose, Practice: organize knowledge and take stewardship serious. Maturing through: 1) identify gaps in knowledge and develop learning agenda 2) define role in organization 3) redefine community boundaries 4) routinize entry requirements and processes 5) measure the value of community 6) maintain cutting-edge focus 7) build and organize a knowledge repository. - Stewardship: sustain momentum while members shift. Domain: maintain the relevance and find voice in organization, Community: keep tone and focus on positive and action, Practice: keep it cutting-edge. Keep momentum: 1) institutionalize voice in organization 2) rejuvenate community 3) hold renewal workshop 4) actively recruit new people to core group 5) develop new leadership 6) mentor new members 7) seek relationships & benchmarks with outside organizations. - Transformation; change of a CoP into something else 1) fades away

	2) die by turning in social club 3) split or merges 4) becomes institutionalized.
	Distributed CoP – design/nurture - Active stakeholder alignment - Create structure that promotes both local variation and global connectivity - Build a rhythm strong enough to maintain community visibility - Develop private space of community more systematically
	Community-based knowledge initiative – design principles: - Evolutionary design - Distributed leadership - Participation across multiple structures - Dance of informal and formal - Value - Build on existing structure - Pacing the initiative
	Phases for knowledge system of multiple communities - Prepare: analyze context and conditions, and prepare possible paths. Make initial plan and get support. - Launch: find places with right people and organizational structure to start communities - Expand; when senior management is convinced, use them to start more communities. Should possess: success stories, experienced support team, network of sponsors and stakeholders. - Consolidate: helps to make communities a definite part of organization: institutionalize, integrate, align - Transform: create differences in organization by 1) becoming more integrated or 2) transforming the organization.

O.3 Practical tips and recommendations

Table 8-39: Summary of narrative review focused on practical tips and recommendations

Literature	Practical tips & recommendations
(ENISA, 2017a) - ISACs	Types of collaboration style or tools: - regular meeting - working groups - Ad hoc investigative working groups - conferences and side events.
	Recommendations: - Participate need to invest in trust to ensure right level of sharing - Facilitator need to ensure right level of attendance. - Have structure that motivates private sector; focus on addressing needs and expectations and have a sharing strategy - Use TLP strategy - Structure needs to engage public sector too - ToR or CoC should be agreed upon and signed - Produce results periodically - Agreement on cases were mandatory sharing is required - Have facilitator - Incorporate funding mechanism from the start

	- Stimulate cross-sectoral cooperation - Let law enforcement have special role - Evaluate activities regularly - Develop new services based on needs of stakeholders.
(ENISA, 2017b) - PPPs	- Focus in establishment on motivation of private sector - Agree on legal basis from the start - Public institution or national plan has the lead - Invest in internal relations. - Invest in open communications and pragmatic approach - Government representatives should be able to participate with NDA - SME should participate. - Have a catalytic manager to help build trust
(ENISA, 2006a) - CSIRT	- Make a SWOT or PEST - Combine business case with project plan for own organizations. - Have a clear communication channel for management
(ENISA, 2014) - Trust models	- use TLP - Focus on sharing and improve this by rotating speakers, vary the discussion format and proposing side activities - Set requirements for new members.
(ENISA, 2016) - incident response and collaboration	- Continuous training and exercises are essential to improve, as well as to assess organizations and stimulate collaboration. - Align response plan with existing frameworks and policies - Use legal framework to define roles and responsibilities
(ENISA, 2006b) – CERT collaboration	
(NCSC, 2015) - CSIRT Maturity kit	Write a business plan to gain support containing 1) How it fits with organizational strategy 2) Identity possible stakeholder 3) Identify issues and how to solve them.
(NCSC, 2018d) - ISAC	
(NCSC, 2018a) - CSIRT	- Gain (top level) support in every organization, since it helps to gain recognition. - Set as most important objective: “digital resilience and security of organization” - Begin with 3-5 organizations and then expend.
(NCSC, 2018c) - supply chain	- Gain support on strategic level
(NCSC, 2018b) - Regional collaboration	- Start with few organizations - 1st year is only building network. - Celebrate successes openly.
(NISCC, 2006) – WARP business case	Possible services: creation of trusted environment, information filtering, access to expert advice, strategic decision support, education, and awareness
(Askwith, 2006) – WARP case study	- WARP is usually operated by an agency on behalf of a community. - Community building and information exchange are attractive long term benefits, but the short term services and benefits usually convince the members. - Funding can be done using a 12 month seed funding which turn into a membership. Members can explore the WARP in the first 12 month and then commit. - Timing can be difficult, since wrong time can impede momentum and diminish trust.

(NISCC, 2002) – Information sharing vision	- WARP, CERT, ISAC can work in a network to strengthen each other. - The key for a successful WARP is that the staff is very familiar with the needs, capabilities and problem of their community. - Functions of a WARP • Receive warnings/advisories from other WARPs/CERTs and other sources, filter and assess them, and reissue them to their community where appropriate, perhaps with increased priority. • Provide e-mail and/or telephone advice to community members on Internet-related security matters. • Solicit and record IT-security incident reports from community. • Share (sanitised) incident reporting data with other WARPs/CERTs etc with whom a sharing agreement has been reached (formal or informal). • Contribute incident data, resources and/or expertise/knowledge to other network nodes to help deal with widespread problems. • Participate in ‘networking’ and sharing of experiences and knowledge with other network nodes. • Develop close links with selected WARPs/CERTs for support and collaboration on problems. - WARP is run by at least to part-time staff members, but preferably three to five. Every staff members has good technical knowledge.
(Hakkaja, 2006) – Evolution of WARP	- WARPs are a light version of a CERT. They can therefore be complementary to a CERT. They are easier to establish and less costly. - WARPS are best created in small communities to secure the flow of information. - A effective collaboration is to combine the two types of operation: using a WARP, or group of WARPs, to reduce the number of incidents through preventive measures, and a CSIRT to handle those incidents that do, nonetheless, occur.
(UKERNA, 2006) – CSIRT and WARP together	- CSIRT staff need good technical skills in order to understand quickly the nature of a problem and suggest how it may be contained and remedied. They must also have good inter-personal skills: most of the people CSIRTs deal with have just suffered a security incident and may be in a distressed state - CSIRTs and WAPRs can complement each other. CSIRTs would like preventive advice to be more widely adopted. WARPs, who have a closer relationship with their communities, should be able to achieve this. The most obvious area for collaboration is therefore in the sharing of information about preventive measures.
(Wenger et al., 2002)	- Public events need to contain informal networking - In potential phase focus on facilitating dialogue to know what people need. - Use teleconferences and video chat to promote aliveness. - Do fieldtrip to visit each other - Let leader make significant time and/or effort commitment - Set agenda with high goals - Start significant initiatives - Strengthen link with members - To manage knowledge system - Link processes that develop and apply knowledge in order to create value - Set goals - Use goals to reflect - Get funding for time: individual participation, budget per project - Use pilots to test and learn - Two developments always run parallel:

	- Develop internal practice for community development - Cultivate management sponsorship and stakeholder alignment.

P. Sub solutions

P.1 Sub solutions for the conditions based on the narrative review

C1. Similar ideas, customs and social behavior should be created together and agreed on.

- The rationale for creation and the driving force of the ISAC should be discussed with members during formation. (ENISA, 2017a)
- Determine the type of CSIRT, select services types, define initiative with business plan, create business case. (ENISA, 2006a)
- In the *Explore* phase, find like-minded parties, keep it formal, ask lots of questions and try to reach consensus. The next phase of *Building* should continue with discussing as well as contain a formal kick-off. There should be a focus on building trust, roles should be divided, and meeting structure should be made. (NCSC, 2015)
- Use the initial phase to seek consensus and to create a workgroup. The second phase is about reaching a consensus by defining the mandate, the services and activities. (NCSC, 2018d)
- The members of a CoP and their interaction (Community aspect) create and determine the set of issues the CoP deals with and create the identity and purpose of the CoP. (Wenger et al., 2002)
- The *Potential* phase should focus on setting the scope, connecting the network informally and identifying needs. Dialogue is essential to do this. Some important features of this phase are: 1) determine primary intent of community 2) define domain and identify engagement issues 3) build a case for action. (Wenger et al., 2002)

S1. There must be a mix of group meetings and individual meetings.

- Decide on a meeting structure in the *Build* phase. (NCSC, 2015)
- Several design principles focus the mix of interactions. They recommend a dialogue between inside & outside perspectives as well as different levels of participation by members. The balance between familiarity and excitement and the 'rhythm' of the community is also stressed. (Wenger et al., 2002)
- The *Coalescing* phase should possess a launching event. Several different community events must be initiated during this phase as well, in order to build trust and network, and to determine needs and interests. (Wenger et al., 2002)
- The community should be rejuvenated once in a while, especially during the *Stewardship* phase. A renewal workshop can help. This will keep the relevance and sustain momentum. (Wenger et al., 2002)
- Practical recommendations are to have public events with informal networking and to do fieldtrips. (Wenger et al., 2002)
- Focus on sharing and improve this by rotating speakers, vary the discussion format and proposing side activities. (ENISA, 2014)

S2. Members must be encouraged to meet each other, but individual meetings should also be arranged if deemed necessary by a third party (the facilitator).

- A governance model should contain a structure with a chair and vice-chair to set goals and a support body to facilitate interactions and meetings. (ENISA, 2017a)
- The *Potential* phase should focus on identifying potential coordinators, thought leaders, and connecting members. New members can also be recruited or sought after. (Wenger et al., 2002)
- Create structure that promotes both local variation and global connectivity. (Wenger et al., 2002)
- Have a facilitator and stimulate cross-sectoral cooperation. (ENISA, 2017a)
- Invest in internal relations using a catalytic manager to help build trust. (ENISA, 2017b)
- Strengthen link with members. (Wenger et al., 2002)

T1. Trust building exercises should be organized.

- Trust building can be best done through personal relations, but legal forms can help. Components are: added value, punctuality, comprehensiveness, expertise, dedication. (ENISA, 2017a)
- Build trust by (ENISA, 2014):
  - Controlling entry of new members using a protocol with sponsorship or a trusted introduce (TI).
  - Provide activities that foster trust.
  - Have members sign a NDA.
  - Have contribution fee
- Code of Conduct, sponsorship, accreditation by a trusted introduce can help to build trust (ENISA, 2006b)

T2. Trust and the sense of safety should regularly be discussed in the group.

- Code of Conduct and agreements can help build trust and must be discussed from time to time. They can also act as conversation starter. (ENISA, 2006b)
- Have a catalytic manager to help build trust. (ENISA, 2017b)

T3. Trust building and maintenance is a priority in the CoP.

M1. Management must be activated from the start for every actor.

- Manager support and engagement must be gained in the Coalescing phase in order let the community expand. (Wenger et al., 2002)
- Defining the role in the organizations and the community boundaries help to focus the CoP in the *Maturing* phase. (Wenger et al., 2002)
- There should be focus on management during every phase of a knowledge system of multiple communities. The *Launch* phase focuses on finding places with right people and organizational structure to start communities. The *Expand* phase is when senior management is convinced in order to start more communities. During the *Consolidate* phase: the communities become a definite part of the organization through either institutionalization, integration, or alignment. The last phase, *Transform*, is when the CoP creates differences in organization by 1) becoming more integrated or 2) transforming the organization. (Wenger et al., 2002)
- Gain (top level) support in every organization as fast as possible, since it helps to gain recognition. (NCSC, 2018a)

- Gain support on strategic level. (NCSC, 2018c)
- Let a leader make significant time and/or effort commitment (Wenger et al., 2002)

M2. Actors must be assisted in convincing their management.

- The critical role is community coordinator. (Wenger et al., 2002)
- Have a clear communication channel for management. (ENISA, 2006a)
- Write a business plan to gain support containing the fit with the organizational strategy, an identification of possible stakeholders, and a definition of issues and respective solutions. (NCSC, 2015)

FL1. The CoP must have a person that is responsible for the daily needs, a facilitator.

- Have a support body where the secretariat acts as a facilitator. (ENISA, 2017a)
- A critical role is community coordinator. The role should be initiated in the potential phase. (Wenger et al., 2002)
- Have facilitator. (ENISA, 2017a)

FL2. The facilitator of the CoP should organize events and keep in touch with the members.

- Facilitator need to ensure right level of attendance. (ENISA, 2017a)
- The community coordinators should be legitimized in the *Coalescing* phase. Stronger connections between core members should be a focus, as should be organizing several events, including a launching event. (Wenger et al., 2002)

FL3. The facilitator leads the process, but the participants make the strategic and practical decisions concerning the CoP.

- There should be a validation of ideas within a large group to broaden support in the *Develop* phase. A decision-making structure should be developed as well. (NCSC, 2018c)
- There should be active stakeholder alignment. (Wenger et al., 2002)

FL4. There are reoccurring moments for decision making by the participants of the CoP.

AU1. The facilitator should regularly talk to participants to check the value that is added.

- A design principle is to focus on value continuously. (Wenger et al., 2002)
- Opportunities for value should be identified during the *Coalescing* phase to further increase value of CoP. (Wenger et al., 2002)
- The focus shifts from establishing value to clarifying the focus, role, and boundaries of community in the *Maturing* phase. Measuring the value of the community is important now. (Wenger et al., 2002)

AU2. Results should be communicated clearly and distinctly to the participants.

- Steps should be developed, performed and monitored in the *Implement* phase. (NCSC, 2018a)
- Value of the community should be measured and a knowledge repository should be built in the *Maturing* phase. This makes the results of the CoP accessible for the members. (Wenger et al., 2002)
- Success stories can help to gain support from senior management, but communicate a clear result as well. (Wenger et al., 2002)
- Invest in open communications and pragmatic approach. (ENISA, 2017b)
- It is recommended to celebrate successes openly. (NCSC, 2018b)

AU3. Information about incidents and prospects in similar groups should be reported to the CoP.

- In a *Country-focused ISAC*, all experts are part of one initiative to make sharing and exchange easy. With a *Sector-specific ISAC*, sharing information and analysis with each other in sector is done to improve sector knowledge and experience. Usually has platform with shared services. (ENISA, 2017a)
- One of the basic capabilities of ISAC is Information sharing usually due to a formal agreement or membership agreement. Sharing is done with a platform or face-to-face meetings. Types of information: incidents, threats, vulnerability, mitigations, situational awareness, best practices, strategic analysis. (ENISA, 2017a)

AU4. Incidents or troubles of participants need to discussed.

- The motivation to participate differs for public and private parties. A motivation for the public organizations is to gain a better understanding of the needs of the private sector. For the private sector, the sharing of knowledge and the access to knowledge is more important. (ENISA, 2017a)
- A basic capability of ISAC is Information sharing, usually due to a formal agreement or membership agreement. Sharing is done with a platform or face-to-face meetings. Types of info: incidents, threats, vulnerability, mitigations, situational awareness, best practices, strategic analysis. (ENISA, 2017a)

DR1. Topics discussed in the CoP must hold direct value for its members. This must be checked with every event and should be reflected on.

- Determining and deciding on the driving force of the ISAC is an important part of the formation process. (ENISA, 2017a)
- Evaluate activities regularly. (ENISA, 2017a)
- In *Potential* phase focus on facilitating dialogue to know what people need. (Wenger et al., 2002)

DR2. The relevance must be measured and reflected on after each event in the form of feedback.

- The supply chain must be studied in the *Demonstrate* phase in order to make agreements on the improvements. Steps can be developed, performed, monitored and discussed in the *Implement* phase. (NCSC, 2018a)
- Some of the design principles are to design for evolution, to open a dialogue between inside & outside perspectives, and to focus on value. (Wenger et al., 2002)
- The shift to clarifying the focus, role and boundaries of the CoP in the *Maturing* phase lead to the organization and reflection on current activities. Gaps in the current knowledge can be identified in order to set a learning agenda. It can help to measure the current value and to build a knowledge repository. (Wenger et al., 2002)
- Results should be produced periodically. Activities should be evaluated regularly. (ENISA, 2017a)
- Set goals and use these goals to reflect on the progress and value of the CoP. (Wenger et al., 2002)

DR3. Feedback must be documented and used for future events.

- A focus point is to document steps and processes in order to make them available. (ENISA, 2006b)
- A knowledge repository needs to be built in the *Maturing* phase. (Wenger et al., 2002)

P.2 Sub solutions found in narrative literature

Promising strategies

Section 5.1.1 presented several concepts and highlighted the most interesting ones for this case. The strategies explained in literature regarding these concepts will be summarized here, since they hold more promise. Some concepts have several sources with different strategies.

WARP

The establishment of a WARP is also mentioned with two strategies. ENISA presents a development model consisting of three steps (Hakkaja, 2006). The first step is to show benefit through a tailored warning service, so that everyone feels they are getting a personalized and valuable service. The second step is to develop trust by encouraging members to help one another by sharing and giving advice. The third step is to encourage members to report their experiences on sensitive topics such as attacks and problems to improve on collective learning.

The British NISCC recommends a setup consisting of six steps. First, the community must identified to find potential member organizations. Secondly, a business case must be built in order to convince potential members. Thirdly, a person within every potential member organization must be sought and the business case must be sold to this person. This person can then convince the organization. When members are convinced, the fourth step of funding needs to be addressed and established. The fifth step is to bring the potential members together and start the WARP. The WARP is now operational, so the final step is to keep the momentum going with careful planning.

Regional collaboration

NCSC advises three phases to establish a regional collaboration (NCSC, 2018b). The *Explore* phase focuses on making design choices with a smaller group. The *Develop* phase aims to validate the ideas within large group and to broaden support. A decision making structure needs to be determined now, since decision making can be difficult with many different organization. The last phase is *Action* where the leading group is expanded into interactive community.

Supply chain collaboration

NCSC determined three phases to set up a supply chain collaboration (NCSC, 2018c). The *Explore* phase focuses to gain overview of involved parties and to them together. The *Demonstrate* phase centers on studying supply chain. A basic level of cyber security is established and agreements are made on how to improve the different organizations. The final phase is *Implement*. Now, the steps determined in the previous phase need to be develop, done and monitored.

Interesting structures

This section highlights the most interesting structures explained in literature. These structures provide options to examine or structure a collaboration or parts of the collaboration. The structures presented here are sometimes combined from multiple sources. The references will be added correctly in order to see the distinction.

Dimensions of a collaboration

Collaboration consists of several dimensions that make it a whole. These dimensions often need different things to function and to grow. Several sets of dimensions were found.

Wenger et al. (2002) present three main characteristics of CoPs that could be shaped and created. The first is the *Domain*, the common ground and boundaries that enable members to share and decide if it is worth spending time on. The second is the *Community*, the social structure that facilitates learning through interaction. And the third is *Practice*, the set of shared repertoires of resources.

The NCSC presented four components of a CSIRT (NCSC, 2015). The first component is the *Organization*, the overall structure of the collaboration. The second is *Human*, the interaction between individuals and their individual growth. The third is *Tools* which encompasses all tools needed to function optimally. The last component is *Processes*, the workflows that structure the work of the CSIRT and which need to documented.

ENISA set four baseline capabilities for the CSIRT to structure this concept (ENISA, 2016). The *Formal* capability focuses on the mandate that determines role and purpose of the CSIRT. The *Operational-technical* capability encompasses all the services provided. The *Operational-organizational* capability centers on the resources, the services delivery and the business continuity of the CSIRT. The *Co-operational* capability focuses on the ability to collaborate with other CSIRTS.

The business case

The business case of a collaboration helps to set it up. The British NISCC and the Dutch NCSC provide advice for the content of a business case. NISCC advises five stages in making a WARP business case (NISCC, 2006). First, the community needs to be identified. Second, the benefits of a WARP for this community needs to be identified. Third, the resources and costs of the WARP need to be determined. Fourth, the funding for these resources and costs needs to be identified. When all these components are clear, then the last stage of writing the business case can commence.

The NCSC advises to incorporate three parts in the business case. The first part is the fit of the initiative in the current organizational strategy. The second is the possible stakeholders of this initiative. The last is the issues that need to be solved combined with an initial impression on how to solve these issues.

Building trust

Section 4.4 is clear on the role trust plays in the setting up a collaboration. Several models to build trust are presented in literature. A first mode is the use of bilateral and multilateral agreements (ENISA, 2006b) or a NDA (ENISA, 2014). A second mode is through a monetary contribution (ENISA, 2014) or sponsorship (ENISA, 2006b, 2014). A third mode is the use of trusted introduce (ENISA, 2006b, 2014). This mode involves current members to recommend and guide new members in order to increase the members of the collaboration. A fourth mode is the creating of a Code of Conduct to ensure a baseline for the interaction between members (ENISA, 2006b).

Funding mechanisms

Funding is a reoccurring theme in the literature of the narrative review. Several options are listed for the funding of a collaboration:

- Commercially funded through a mandatory fee or membership subscription (based on size and involvement) (ENISA, 2017a; NISCC, 2002, 2006)
- A voluntary contribution (ENISA, 2017a)
- Government subsidies or sponsorship (rare option, private sector is usually responsible) (ENISA, 2017a; NISCC, 2006)
- Corporate funding as an internal project (NISCC, 2002, 2006)
- Customer service provided by large organizations to its existing customers. (NISCC, 2002)

- Public-private (partnership) (NISCC, 2002, 2006)
- Cooperative funded by all members paying a subscription which pays the WARP's activities and services (NISCC, 2002, 2006)

Governance model

ENISA offers three options for the governance of an ISAC (ENISA, 2017a). These options could also be used for other forms of collaboration. The first option is a model of chair and vice-chair that set all goals and facilitate the activities. A second option is having a chair with a secretariat that acts as support body and as a facilitator. The last options is a flexible governance form where all activities are done by volunteers.

P.3 Sub solutions for the conditions based on the brainstorm

C1. Similar ideas, customs and social behavior should be created together and agreed on.

Based on experience, structures and cultures can serve as a base for new initiatives such as a CoP. Intuitively, it is believed that creating something together is usually a long term process and therefore the focus should be on individual meetings with limited participants. It is usually easier to reach a consensus and to build trust and connection with a smaller, more intimate group. A twist can be given to these meetings by organizing speed dating between (potential) partners in order to connect them more and to break traditional structures.

S1. There must be a mix of group meetings and individual meetings.

This condition seems obvious, but can be difficult to enforce in a proper balance. A meeting organizer can support this mix and monitor it. Intuitively, it is believed that he can encourage partners to meet individually as well as organize meetings that combine team building activities and individual meetings. It could be interesting or refreshing to use a game format, such as the Virtues Cards (Deugdenkaarten) by Linda Kavelin Popov, or the 'Ontdekkaarten', by Hanneke Middelburg, for the first individual meetings to break the ice.

S2. Members must be encouraged to meet each other, but individual meetings should also be arranged if deemed necessary by a third party (the facilitator).

Based on experience, necessity is an important driver which can be created through a hierarchical role. A safe environment helps people to feel more comfortable to meet new people, since this is often seen as difficult. Dedicating moments in collective meetings to individual contact can work encouraging based on intuition. It could help to set simple ground rules for the meetings in order to help create interaction.

T1. Trust building exercises should be organized.

It's common practice to do these activities in a different setting mostly outside the normal workplace. Based on intuition, these exercises should be un-conventional for optimal bonding, but that using Us-Them structure can create a competitive spirit which can help building trust.

T2. Trust and the sense of safety should regularly be discussed in the group.

Feelings are commonly hard to discuss in a group setting and in a professional setting, so individual meetings can be used to measure the feeling of trust and safety. Intuitively, this should be a reoccurring agenda item. A creative idea is to set some ground rules that can be enforced, to guarantee a safe environment as well as regular and dedicated moments for every member's feelings.

T3. Trust building and maintenance is a priority in the CoP.

Building trust between people through interaction mostly is a slow process. However, it can easily be forgotten, or assumed that trust should be priority, so someone should have a dedicated role to guard the discussion regarding trust. Building trust becomes less difficult for members if the activities provide some form of entertainment or fun.

M1. Management must be activated from the start for every actor.

It's common practice that the aims and needs of higher management need to be determined per member in order to advice members on what and how to communicate. Intuitively, there is some general information that every management team should know, so this should be collective in a designed package. A creative idea is to use interactive sessions such as a case study or workshop to involve and activate management layers.

M2. Actors must be assisted in convincing their management.

An intuitive believe is that practice makes perfect, therefore a practical workshop should be organized to train members. Maybe the members can also improve and learn by sharing their experience with each other and role-playing with them.

FL1. The CoP must have a person that is responsible for the daily needs, a facilitator.

Usually a third party can provide a sense of neutrality and objectivity.

FL2. The facilitator of the CoP should organize events and keep in touch with the members.

It's usually so that organizing the events and keeping a personal connection with all members can be hard for one person. The facilitator should have at least someone supporting him, preferably one or more members. Based on intuition, it is expected that a more experienced professional would be better at facilitating for the PoR case.

FL3. The facilitator leads the process, but the participants make the strategic and practical decisions concerning the CoP.

A decision making process or tool makes sense intuitively, since it can enable participants to structure their decisions while keeping the facilitator out of the equation. A democracy will not work for this case.

FL4. There are reoccurring moments for decision making by the participants of the CoP.

Decision making can sometimes cause new discussions or subjects to arise. It's important to not let these new discussions or subject hinder the decision on other points. Intuitively, special moments for decision making feels right. This can be done using a certain protocol or ritual for the decision making.

AU1. The facilitator should regularly talk to participants to check the value that is added.

It could be that a standardized format can help to check it consistently. Added value should also be one of the main results measured by the members.

AU2. Results should be communicated clearly and distinctly to the participants.

A bullet-list provides a strong overview of the simple results. It may be good to combine this with a common visualization format in order to create recognition.

AU3. Information about incidents and prospects in similar groups should be reported to the CoP.

Based on experience, the relevance of the shared information should always be considered before sharing it with all members. This role can be done by the facilitator. He can play a central role in addressing incidents, but could also act as a central connector with all groups.

AU4. Incidents or troubles of participants need to discussed.

Legal documents are often used to secure confidentiality. Intuitively, a safe environment where members feel comfortable, seems most important.

DR1. Topics discussed in the CoP must hold direct value for its members. This must be checked with every event and should be reflected on.

Members can find it difficult to say what is valuable for them and what isn't. Intuitively, this can be solved by having the facilitator play a central role in finding information and knowledge. This can be done using the combination of a questionnaire with follow-up phone calls.

DR2. The relevance must be measured and reflected on after each event in the form of feedback.

The SMART-format is commonly used to make, measure and reflect on goals. It takes effort to create one's own metric based on the goals and needs of the members.

DR3. Feedback must be documented and used for future events.

Experience shows that short documents in a fixed format provide an excellent guideline to document consistently. A secretariat is helpful for archiving.

Q. MORPHOLOGICAL CHART

Table 8-40: Morphological chart

Conditions and definitions	Experience	Intuition	Creativity	Sub solution in narrative review
Strategies				Formation process (ENISA, 2017a): 1) Rationale for creation: why is the ISAC started and in what context: heavy hierarchal culture thus regulatory requirement or pragmatic approach based on network 2) Decide on driving force: profit, having knowledge, government or EU institution. 3) Motivation to participate: Public: Knowledge of security, opportunity for single coordination point, better understanding of needs private sector. Private: Sharing knowledge on incidents, part of group, access to knowledge, networking
				Process to develop a CSIRT (ENISA, 2006a): - Determine type of CSIRT (9 types) - Select services; 1) reactive, 2) proactive, 3) artifact handling, 4)

				security quality management. - Define initiative with business plan; have organizational structure, financial model, sharing policy. - Create business case. - Train members.
				Steps to build an ISAC (NCSC, 2018d): - Explore; find like-minded parties, keep it formal, ask lots of questions and try to reach consensus - Build; formal kick-off, focus on building trust, dividing roles, and meeting structure. Also discuss membership guidelines - Continue; keep building trust, try to increase the value per meeting. Also create procedures for new members and how to change roles.
				Steps to build a CSIRT (NCSC, 2018a): - explore; create support, build trust and seek consensus. 1) find possible partners, 2) create workgroup. - Consensus; define mandate, services and activities. - Grow; increase capabilities and evolve.
				Steps to build a supply chain collaboration (NCSC, 2018c): - Explore: gain overview of involved parties and bring together - Demonstrate; study supply chain and establish basic level, make agreements on how to improve.

				- Implement; develop, do and monitor steps.
				Steps to build a regional collaboration (NCSC, 2018b): - Explore; take time to make design choices - Develop; validate ideas within large group and broaden support. Make a decision making structure - Action; expand leading group into interactive community. Create a roadmap
				Steps towards a WARP (Askwith, 2006): - Identify the community; It is difficult to assess the match of possible members. Therefore an inside champion who helps to penetrate the organizations and other organizations, is very helpful. He can advise on how to engage, who to engage and to understand the needs better. - Build a business case. - sell the WARP idea to all members through the best person within every organization to engage with - Establish funding - Bring the potential members together and start. - Keep momentum going with activities using careful planning.
				Development model WARP (Hakkaja, 2006): 1) Show benefit through a tailored warning service, so that everyone feels they are getting a

				personalized and valuable service 2) Develop trust through encouraging members to help one another by sharing and giving advice. 3) Encourage members to report their experiences on sensitive topics such as attacks and problems to improve on collective learning.
				Stages of community development (Wenger et al., 2002) - Potential; an existing social network flock informally around a subject. - Coalescing; official launch and focus on building trust, relationships and awareness of common interests and needs. - Maturing; focus shifts from establishing value to clarifying the focus, role, and boundaries of community. - Stewardship: sustain momentum while members shift. - Transformation; change of a CoP into something else
Structures				Dimensions of a collaboration CoP elements (Wenger et al., 2002): - Domain; set of issues, create identity & purpose.

				- Community; people and members, create social fabric for learning - Practice; set of framework, ideas, tools that are created and shared. 4 baseline capabilities of CSIRT (ENISA, 2016): 1) Formal capability; mandate that determines role and purpose 2) Operational-technical capability; services it provides 3) Operational-organizational capability; the resources, services delivery and business continuity 4) Co-operational capability; to be able to work with others (i.e. through SLA) Components of a CSIRT (NCSC, 2015): - Organization; focus on trustworthiness and reliability with high performance. - Human; create CoC, have a small start group (3-5 members), focus on training - Tools; invest in automated tools - Processes; document steps and processes in order to make them available.
				Business case: Write a business plan to gain support containing (NCSC, 2015): 1) How it fits with organizational strategy

				2) Identity possible stakeholder 3) Identify issues and how to solve them. Five stages in making the WARP Business case (NISCC, 2006) 1) Identity the community 2) Identifying benefits 3) Identify resources and costs 4) Identify funding: internal, membership subscription, member co-operative, partnership, sponsorship 5) Produce business case
				Several models to build trust: - the use of bilateral and multilateral agreements (ENISA, 2006b) or a NDA (ENISA, 2014). - a monetary contribution (ENISA, 2014) or sponsorship (ENISA, 2006b, 2014). - the use of trusted introduce (ENISA, 2006b, 2014). - the creating of a Code of Conduct to ensure a baseline for the interaction between members (ENISA, 2006b).
				The funding of a collaboration: • Commercially funded through a mandatory fees or membership subscription (based on size and involvement)

				(ENISA, 2017a; NISCC, 2002, 2006) • A voluntary contribution (ENISA, 2017a) • Government subsidies or sponsorship (rare option, private sector is usually responsible) (ENISA, 2017a; NISCC, 2006) • Corporate funding as an internal project (NISCC, 2002, 2006) • Customer service provided by large organizations to its existing customers. (NISCC, 2002) • Public-private (partnership) (NISCC, 2002, 2006)
				Three options for the governance of an ISAC (ENISA, 2017a): - a chair and vice-chair that set all goals and facilitate the activities. - a chair with a secretariat that acts as support body and as a facilitator. - a flexible governance form where all activities are done by volunteers.
C1. Similar ideas, customs and social behavior should be created together and agreed on.	Existing structures and cultures can serve as a base for the CoP.	This is a process that takes a long time.	Organize speed dating between possible partners	The rationale for creation and the driving force of the ISAC should be discussed with members during formation. (ENISA, 2017a)
		Keep it small and focus on individual meetings		Determine type of CSIRT, select services types, define initiative with business plan, create business case. (ENISA, 2006a)
				In the exploring phase, find like-minded parties,

				keep it formal, ask lots of questions and try to reach consensus. The next phase of Building should continue with discussing as well as contain a formal kick-off. There should be a focus on building trust, roles should be divided, and meeting structure should be made. (NCSC, 2015)
				Use the initial phase to seek consensus and to create a workgroup. The second phase is about reaching a consensus by defining the mandate, the services and activities. (NCSC, 2018d)
				The members of a CoP and their interaction (Community aspect) create and determine the set of issues that the CoP deals with and create the identity and purpose of the CoP. (Wenger et al., 2002)
				The potential phase should focus on setting the scope, connecting the network informally and identifying needs. Dialogue is essential to do this. Some important feature of this phase are: 1) determine primary intent of community 2) define domain and identify engagement issues 3) build a case for action. (Wenger et al., 2002)
S1. There must be a mix of group meetings and individual meetings.	Setting individual meetings can be difficult to direct.	Individual meetings must be encouraged.	Have a game format for the first individual meetings.	Decide on a meeting structure in the Build phase. (NCSC, 2015)

	A facilitator or meeting organizer can help.	start with 1 team building activity and split quickly to individual meetings		Several design principles focus the mix of interactions. They recommend a dialogue between inside & outside perspectives as well as different level of participation by members. The balance between familiarity and excitement and the “rhythm” of the community is also stressed. (Wenger et al., 2002)
				The Coalescing phase should possess a launching event. Several different community events must be initiated during this phase as well in order to build trust and network, and to determine needs and interests. (Wenger et al., 2002)
				The community should be rejuvenated once in a while, especially during the Stewardship phase. A renewal workshop can help. This will keep the relevance and sustain momentum. (Wenger et al., 2002)
				Practical recommendations are to have public events with informal networking and to do fieldtrips. (Wenger et al., 2002)
				Focus on sharing and improve this by rotating speakers, vary the discussion format and proposing side activities. (ENISA, 2014)
S2. Members must be encouraged to	Necessity is important driver and can be	Collective meetings should	Set simple ground rules for meetings	A governance model should contain a structure with a chair and

meet each other, but individual meetings should also be arranged if deemed necessary by a third party (the facilitator).	created by hierarchical role.	contain moments of (forced) individual meeting.	that focus on the interaction.	vice-chair to set goals and a support body to facilitate interactions and meetings. (ENISA, 2017a)
	People find it difficult to meet new people. Provide safe environment			The potential phase should focus on identifying potential coordinators and thought leaders, and connecting members. New members can also be recruited or sought after. (Wenger et al., 2002)
				Create structure that promotes both local variation and global connectivity. (Wenger et al., 2002)
				Have facilitator and stimulate cross-sectoral cooperation. (ENISA, 2017a)
				Invest in internal relations using a catalytic manager to help build trust. (ENISA, 2017b)
				Strengthen link with members. (Wenger et al., 2002)
T1. Trust building exercises should be organized.	The setting must be different than the normal one, i.e. “heidag”	Be un-conventional.		Trust building can be best done through personal relations, but legal forms can help. Components are: added value, punctuality, comprehensiveness, expertise, dedication. (ENISA, 2017a)
		use us-them structure by using an external party		Build trust by (ENISA, 2014): - Controlling entry of new members using a protocol with sponsorship or a trusted introduce (TI).

				- Provide activities that foster trust. - Have members sign a NDA. - Have contribution fee
				Code of Conduct, sponsorship, accreditation by a trusted introduce can help to build trust
T2. Trust and the sense of safety should regularly be discussed in the group.	It's hard to address in groups, so use individual meetings to measure this.	Make it reoccurring agenda item.	Make ground rules.	Code of Conduct and agreements can help build trust and must be discussed from time to time. They can also act as conversation starter. (ENISA, 2006b)
	Use check-in and check out		Have moment for feelings of individual	Have a catalytic manager to help build trust. (ENISA, 2017b)
T3. Trust building and maintenance is a priority in the CoP.	Normal working experience also built trust, but don't give a big increase.	Easily forgotten or assumed, so create dedicated role to guard this	Make it fun by using activities.	
M1. Management must be activated from the start for every actor.	Management aims and needs must be determined per member in order to advice on specific communication.	Provide general information package designed for management.	Make it interactive by organizing a case study or workshop	Manager support and engagement must be gained in the Coalescing phase in order let the community expand. (Wenger et al., 2002)
				Defining the role in the organizations and the community boundaries help to focus the CoP in the Maturing phase. (Wenger et al., 2002)
				There should be focus on management during every phase of a knowledge system of multiple communities. The Launch phase focuses on finding places with right people and organizational structure

				to start communities. The Expand phase is when senior management is convinced in order to start more communities. During the Consolidate phase : he communities become a definite part of organization through either institutionalization, integration, or alignment. The last phase Transform is when the CoP create differences in organization by 1) becoming more integrated or 2) transforming the organization. (Wenger et al., 2002)
				Gain (top level) support in every organization as fast as possible, since it helps to gain recognition. (NCSC, 2018a)
				Gain support on strategic level. (NCSC, 2018c)
				Let leader make significant time and/or effort commitment
M2. Actors must be assisted in convincing their management.		Provide practical workshop to practice this	Let members share experience and practice on each other.	The critical role is community coordinator. (Wenger et al., 2002)
				Have a clear communication channel for management. (ENISA, 2006a)
				Write a business plan to gain support containing the fit with the organizational strategy, an identification of possible stakeholders, and a definition of issues and respective solutions. (NCSC, 2015)

FL1. The CoP must have a person that is responsible for the daily needs, a facilitator.	Attract someone from third party to ensure neutrality and objectivity.			Have a support body where the secretariat acts as a facilitator. (ENISA, 2017a)
				A critical role is community coordinator. The role should be initiated in the potential phase. (Wenger et al., 2002)
				Have facilitator. (ENISA, 2017a)
FL2. The facilitator of the CoP should organize events and keep in touch with the members.	Don't put the load on 1 person, but give the facilitator some support	More experienced people are usually better. Don't give it to a junior.		Facilitator need to ensure right level of attendance. (ENISA, 2017a)
				The community coordinators should be legitimized in the Coalescing phase. Stronger connections between core members should be a focus, as should be organizing several events, including a launching event. (Wenger et al., 2002)
FL3. The facilitator leads the process, but the participants make the strategic and practical decisions concerning the CoP.		Design a decision making process/tool		There should be a validation of ideas within a large group to broaden support in the Develop phase. A decision-making structure should be developed as well. (NCSC, 2018c)
		Democracy doesn't work		There should be active stakeholder alignment. (Wenger et al., 2002)
FL4. There are reoccurring moments for decision making	Decision making can also cause new discussions to arise.	Make special moments for decision making.		

by the participants of the CoP.				
		Create a "protocol" or ritual for decision making.		
AU1. The facilitator should regularly talk to participants to check the value that is added.		Make standard format		A design principle is to focus on value continuously. (Wenger et al., 2002)
		Make it one of the main results of CoP		Opportunities for value should be identified during the Coalescing phase to further increase value of CoP. (Wenger et al., 2002)
				The focus shifts from establishing value to clarifying the focus, role, and boundaries of community in the Maturing phase. Measuring the value of the community is important now. (Wenger et al., 2002)
AU2. Results should be communicated clearly and distinctly to the participants.	Use an organized bullet-list system	A common visualization format		Steps should be developed, performed and monitored in the Implement phase. (NCSC, 2018a)
				Value of the community should be measured and a knowledge repository should be built in the Maturing phase. This makes the results of the CoP accessible for the members. (Wenger et al., 2002)
				Success stories can help to gain support from senior management, but communicate a clear

				result as well. (Wenger et al., 2002)
				Invest in open communications and pragmatic approach. (ENISA, 2017b)
				It is recommended to celebrate successes openly. (NCSC, 2018b)
AU3. Information about incidents and prospects in similar groups should be reported to the CoP.	The relevance of the information for the CoP should always be considered before sharing.	Facilitator plays a central role in addressing these incidents.	Facilitator should be connected with other groups and disciplines.	In a Country-focused ISAC, all experts are part of 1 initiative to make sharing and exchange easy. With a Sector-specific ISAC, sharing information and analysis with each other in sector is done to improve sector knowledge and experience. Usually has platform with shared services. (ENISA, 2017a)
				A basic capabilities of ISAC is Information sharing usually due to a formal agreement or membership agreement. Sharing is done with a platform or face-to-face meetings. Types of info: incidents, threats, vulnerability, mitigations, situational awareness, best practices, strategic analysis. (ENISA, 2017a)
AU4. Incidents or troubles of participants need to discussed.	Use legal binding documents to secure confidentially.	Safe space in important		The motivation to participate differs for public and private parties. A motivation for the public organizations is to gain a better understanding of needs of the private sector. For the private sector, the sharing of knowledge and the access to knowledge is more important. (ENISA, 2017a)
				A basic capabilities of ISAC is Information

				sharing usually due to a formal agreement or membership agreement. Sharing is done with a platform or face-to-face meetings. Types of info: incidents, threats, vulnerability, mitigations, situational awareness, best practices, strategic analysis. (ENISA, 2017a)
DR1. Topics discussed in the CoP must hold direct value for its members. This must be checked with every event and should be reflected on.	Participants can find it difficult to say what is valuable for them and what isn't.	The facilitator plays a central role in finding this information.	Use a questionnaire with a follow-up by phone.	Determining and deciding on the driving force of the ISAC is an important part of the formation process. (ENISA, 2017a)
				Evaluate activities regularly. (ENISA, 2017a)
				In potential phase focus on facilitating dialogue to know what people need. (Wenger et al., 2002)
DR2. The relevance must be measured and reflected on after each event in the form of feedback.	SMART format can be used.		metrics must be based on the goals and needs of members to measure.	The supply chain must be studied in the Demonstrate phase in order to make agreements on the improvements. Steps can be developed, performed, monitored and discussed in the Implement phase. (NCSC, 2018a)
				Some of the design principles are to design for evolution, to open a dialogue between inside & outside perspectives, and to focus on value. (Wenger et al., 2002)
				The shift to clarifying the focus, role and boundaries of the CoP in the Maturing phase lead to the organization and

				reflection on current activities. Gaps can be identified in the current knowledge in order to set a learning agenda. It can help to measure the current value and to build a knowledge repository. (Wenger et al., 2002)
				Results should be produced periodically. Activities should be evaluated regularly. (ENISA, 2017a)
				Set goals and use these goals to reflect on the progress and value of the CoP. (Wenger et al., 2002)
DR3. Feedback must be documented and used for future events.	Short documents in a fixed format can provide a guideline.			A focus point is to document steps and processes in order to make them available. (ENISA, 2006b)
	Secretariat can do archiving.			A knowledge repository needs to be built in the Maturing phase. (Wenger et al., 2002)

R. INTERVIEW PROTOCOL EXPERT FEEDBACK

Table 8-41: Interview protocol for the expert feedback

Part	Question	Rationale
Introduction	Introduce yourself	
	Tell about current research and results	Explain the current phase of the research
	- A narrative review and brainstorm were conducted in order to determine elements that crucial to establish a CoP.	
	Explain about this interview and its structure	Explain the aim of the interview and manage expectations of the interview
	- The aim is to gain feedback based on the experience of the expert in order to prioritize elements for a concept solution.	
	- Some questions are prepared, however the focus will be on interaction and dialogue	
	- The goal is for you to give feedback based on your experiences and ideas and I will ask questions to gain a better understanding	
	- The interview has four parts: general remarks, phase 1, phase 2, phase 3	
	- The phases are based on the phases in ISAC and CoP.	
General	Do you believe that CoP has phases?	Check if phases are used in practice and to compare with insights from literature
	What phase do you discern?	
Phase 1	This phase focuses on laying the groundwork. • Which actions do you deem most important in this phase? • Can you give a examples or tips? • Do you believe higher management is important in this phase?	Gain first thought on the first phase Determine the importantce of critical node and Management conditions
	Literature focuses on establishing a network, appointing a community coordinator and setting a strategic goal. • How does this connect to your experiences? • Which organizations should provide a community coordinator? • What is your experience with a community coordinator? • Who should presume the position of leader? • Previous interviews (& literature) show that knowledge management is a prominent goal, therefore this seems an appropriate role. Do you believe this is a proper goal?	Discuss and gain feedback on the first phase. Extra focus is put on the use of a facilitator and the group size.

	• How many and what type of participants must be gather in this phase? Core group & Periphery	
Phase 2	This phase focuses on launching and providing trust and value • Trust was deemed very important, what actions can be taken to establish/create trust? • What activities can bring value to the participants in your experience? What topics are of interested/can connect members/are most important? • A barrier is the lack of priority. Are there ways to increase the priority that is given the CoP in your experience?	Discuss and gain feedback on phase 2. Extra focus is put on solutions for critical node and conditions on Awareness & Urgency and Direct Relevance
	What role do you think the community coordinator should focus on in this phase?	Gain feedback on the use of facilitator.
	Should higher management be involved in this phase?	Gain feedback on condition Management
Phase 3	This phase focuses on strengthening the CoP and setting more focus. • What type of "rhythm" will help to strengthen the CoP? Some participant said meeting every 3 months, since there is a strong sense for physical meetings? • Do you believe that digital forms of interaction can work for the Rotterdam casus? • How can more people be attracted? • New knowledge should be created in this phase. Literature suggest to secure a librarian-role in order to organize this knowledge to make it accessible? Do you believe that this is necessary? Who should take such a role? • How can you "train" new members in order to have smooth participation?	Discuss and gain feedback on phase 3. It is assumed the community will continue and expand for the sake of the argument.
	What role do you think the community coordinator should focus on in this phase?	Gain feedback on the use of facilitator.
	Should higher management be involved in this phase?	Gain feedback on condition Management

S. Summary of expert feedback

Expert E1

Participant details

Name	Position	Connected to FERM	Rotterdam Port area
E1	Researcher & advisor Cyber collaboration	Yes	No

Summary
E1 works as a researcher on cyber security collaboration and uses his research to advice organizations in the Netherlands. His work provides him with a good overview of the challenges that organization face and the solutions they find.

General feedback
E1 made some general marks about cyber security collaboration. It is noted that several modes of collaboration are used within the field of cyber security. Currently, the ISAC and PPPs models are often used. The collaboration between organizations usually arise when organizations face the same challenges due to similar systems, similar processes and similar company profiles. Collaboration can then make help the organizations involved. A large barrier is a low assessment of the cyber risks by the organizations. They are not aware of the relevance of cyber security for their organizations.

Collaboration sometimes happens voluntary, but sometimes it is demanded by a third party. A current discussion is whether a community can be initiated from a compliancy perspective or that completely different approach should be used. There still is no consensus on how communities for cyber security should be started.

An important success factor is a catalytic facilitator. This person leads the group, is the point of contact, and performs the administrative tasks. These tasks should be divided in a later stage over several people such as an account holder, an administrative employee, and a facilitating employee. The accountholder is an independent expert that can provide technical depth.
The topic of trust building is discussed through out the entire interview. E1 sees trust as a no brainer, but remains somewhat unclear on how to build it. It is mentioned that trust is a process that requires time. The NCTV's advice is referred to:

- Have a clear gentlemen's agreement
- Make agreements regarding information sharing, finding, and capturing.
- Have small groups
- Guarantee confidentiality
- Keep participants equal

Feedback on Phase 1
The start of the collaboration is always on open dialogue between all the involved parties in order to search for a shared challenge. This challenge can often be found with general activities or processes that are not company specific. This dialogue contributes to the trust and connection between parties. The facilitator is crucial in this phase to stimulate networking and building the group. The facilitator leads the process in this phase.

Feedback on Phase 2

The parties should make their participation official in this phase as well as take more lead in the facilitation and content of the collaboration. The role of the facilitator is to stay sharp and focus on gathering interesting discussion subjects. He also performs services for the collaboration such as researching and writing documents. He is an example for the group. His worth of this actions is proven to the group in order to activate the group to perform these actions themselves.

E1 stresses the point of involving higher management in this phase. The added value needs to be clear for higher management. Reporting becomes more important in order to involve higher management. This is often difficult to achieve since it's a skill that ICT-experts lack. The facilitator can help in the communication to higher management.

The end of this phase should be to close the tasks of the facilitator. The participants need to create their own financing model and action plan to continue the services offered in the current collaboration

Feedback on Phase 3

It is assumed that the members want to continue with the CoP. E1 believes that a large organization should take a leading position in this phase. A discussion arose on difficulties that arise at this point. First, it becomes more difficult to maintain the rhythm of the meetings. It's a continuous challenge to have a proper balance between physical and digital meetings. Another challenge is the group size, since in most cases the groups become too big in this phase. E1 notes that groups with more than 30 members usually interact less. Larger groups can only be connected to specific services, but then it no longer is a community. A new and common challenge is attracting new members or finding opportunities to attract new members.

The role of a librarian is discussed. In general, it is good to store knowledge and information. However, in most cases, all information is available, just not at the right time for the right person.