# Public-private partnerships for cyber security in the Netherlands

*Making sense or non-sense?*

Master thesis
December 2019

R.W. Miedema
S1044397
Executive Master Cyber Security
Cyber Security Academy
Leiden University, TU Delft, The Hague University of Applied Sciences
Thesis supervisor: Prof. dr. Bibi van den Berg

*"Success is no accident. It is hard work, perseverance, learning, studying, sacrifice and most of all, love what you are doing or learning to do"*
Pelé (2014)

Master thesis
December 2019

R.W. Miedema
S1044397
Executive Master Cyber Security
Cyber Security Academy
Leiden University, TU Delft, The Hague University of Applied Sciences
Thesis supervisor: Prof. dr. Bibi van den Berg

# Acknowledgement

When I started the Executive Master Cyber Security in February 2018, I didn't know anything about computers, internet or cyber security. I had read the National Cyber Security Strategy and the Cyber Security Assessment Netherlands and that was all. Although I was fully motivated to obtain a second master's degree, I had many doubts whether I could do it. The first lectures were mainly about the working of computers, the internet, ones and zeros. My doubts only increased.

Now – almost two years later – you are reading my thesis; the final part of this master and I am very happy to say: I did it! In fact, this master was fantastic! The world of cyber security opened up to me, I have met a lot of new, inspiring people and learned a lot. This master broadened my horizon and my career perspective. But it did not happen by itself and I could not have done it without support. Therefore, I would like to thank my boyfriend Karel Goense who decided to move 200km away, which made me look into a second master in the first place. Besides this, he never complained that I paid more attention to my studies than to him. My deep gratitude goes to my parents and sister. They have provided me with unconditional support, pep talks and unlimited confidence in my abilities. I would not have reached the finish line without them. I would also like to thank my fellow students. Their presence, knowledge and experience has made the Fridays a lot of fun. Additionally, I would like to thank my interview respondents because I would not have been able to finish my thesis without them. Last but not least, I would like to express my appreciation and gratitude to my supervisor Prof. dr. Bibi van den Berg. She has been a source of inspiration for me during the master and provided me with valuable feedback to guide me through the process of finishing my master thesis.

# Executive summary

*"Public-private partnerships for cyber security in the Netherlands; Making sense or non-sense?".* The title of this thesis refers to the academic debate about the effectiveness of public private partnerships (PPPs) to increase cyber security related to national and economic security of nation states. In this debate, some scholars argue that public-private collaboration will not be successful. Nevertheless, PPPs for cyber security are actively promoted by the Dutch government. This research aims to shed light on the practice of collaboration in PPPs for cyber security in the Netherlands and to gain insight in factors that may contribute to the successful collaboration. By doing so, the second goal of this research is to determine to what extent the academic debate about the sense and non-sense of PPPs in cyber security is supported by empirical case studies. The scope of this research is limited to PPPs for cyber security in the Netherlands 2010 – 2019. The main research question is: Which factors may contribute to successful collaboration in public private partnerships for cyber security in the Netherlands?

Two types of research are combined to answer the main research question. First, desk research into scientific literature regarding PPPs for cyber security is conducted. Based on the literature review, a theoretical framework is drawn including factors that may contribute to successful collaboration in PPPs for cyber security according to previous research. These factors are (1) mutual trust between partners, (2) clear and shared goals and interests, (3) a clear division of roles and responsibilities, (4) high stakeholder support, (5) availability of financial support, (6) a formalized foundation of the PPP and (7) equality of partners. In this research, it is assumed that these factors may contribute to successful collaboration.

Then, four in-depth empirical case studies are conducted by means of semi-structured interviews and document analysis. The cases included in this research are FERM, CYSSEC, the National Internet Scam Reporting Point (LMIO) and the Electronic Crimes Taskforce (ECTF). In the case studies is analyzed which factors contributed to successful collaboration in these specific PPPs. The factors in the theoretical framework are used as starting point, but the semi-structured nature of the interviews allowed to shed light on additional factors as well.

The findings of this research indicate that there is no causal relationship between the factors included in the theoretical framework and successful collaboration. Besides this, the findings indicate that there is not one best way to shape PPPs, nor do standard criteria seem to exist that all PPPs should meet in order to ensure successful collaboration. For successful collaboration, the personalities and personal character traits of the people directly involved seem to be the most important. Therefore, it is concluded that the 'human factor' might contribute the most and may be the only factor with predictive value for successful collaboration.

Some limitations must be considered regarding this conclusion. Due to the small number of cases and the sole inclusion of Dutch cases, the findings cannot justifiably be generalized to other PPPs (outside the Netherlands). Besides this, the case studies clarified that collaboration is dynamic and subjected to time, context and interpretation. Therefore, it may be possible that repetition of this research results in slightly different findings. The findings in this research are still valuable since the importance of the human factor is not pointed out clearly in the existing literature that formed the basis for the theoretical framework. Therefore, this finding provides a contribution to existing theories on successful collaboration in PPPs. Regarding the academic debate about the sense and nonsense of PPPs, this research shows that PPPs may not be a panacea but can make sense and collaboration may be successful if 'the right people' are directly involved. It is recommended to conduct more extensive and thorough research into the extent that the human factor contributes to successful collaboration in PPPs.

# 1 Index

# 1 Introduction

## 1.1 Introduction

According to the Dutch National Coordinator for Security and Counterterrorism, societal disruption is lurking in the Netherlands. This is mainly due to the digitalization of critical infrastructures, the lack of analogue alternatives and the lagging resilience of society (NCTV, 2019: 7). The physical and digital domains are so intertwined in that an incident in one domain, may have consequences for the other domain. Society is made vulnerable in new ways now cyber incidents related to critical infrastructures may have disruptive consequences (WRR, 2019: 20). According to the Netherlands Scientific Council for Government Policy (2019: 22) it is not the question *if* but *when* society will be confronted with the consequences of a large-scale cyberattack. Consequently, cyber security has become an essential condition for a safe, secure and well-functioning society.

Traditionally, preventing societal disruption is seen as a responsibility of the state. Yet in the digitized world this is not evident, as more than 80 percent of all critical infrastructures and processes in the Netherlands are owned and operated by private companies (NCTV, 2017). Therefore, national security and social welfare depend to a large extent on the actions of private parties (WRR, 2019: 11). Although private parties will invest in security, it does not seem fair to expect them to take the necessary measures for national security matters (Ibid., 80). National security remains the responsibility of the national government. Hence, the national government proactively promotes the establishment of public-private partnerships (PPPs) to increase cyber security and safeguard national security (NCTV, 2017).

It is not the first time that the government actively promotes the establishment of PPPs. The first PPPs in the Netherlands were established in the eighties and mainly concerned infrastructural projects (Hueskes, Koppenjan & Verweij, 2016: 4; Eversdijk & Korsten, 2015). Since then, PPPs have been implemented in many sectors, for many purposes and may be considered 'the third way of governance' in addition to market and hierarchy (Hodge & Greve, 2007: 545). PPPs have mainly been established because they would increase efficiency, effectiveness and quality of services. Increasing efficiency has been the driving force behind the rise of many PPPs (Klijn & Van Twist, 2007: 156). Therefore, it can be questioned to what extent PPPs are a suitable means to increase cyber security.

Many studies have been conducted on PPPs and some specifically on PPPs for cyber security. This resulted in an ongoing debate between opponents and proponents, arguing why PPPs will or will not work in the context of cyber security (see Dunn-Cavelty & Suter, 2009; Clinton, 2015; Carr, 2016). In general, it can be said that there is skepticism about the use of PPPs to increase cyber security. However, not many empirical studies on PPPs for cyber security have been conducted. Regarding PPPs for cyber security in the Netherlands, not much is known about their working in practice. The lack of empirical research on PPPs for cyber security in the Netherlands is worrying given their importance for national security. This research attempts to increase the knowledge about PPPs for cyber security in the Netherlands by conducting empirical research into the practice of four PPPs. With this empirical study, an attempt will be made to find evidence for the arguments presented in the academic debate about the use of PPPs to enhance cyber security in the context of national security. The main question of this study is: "Which factors may contribute to successful collaboration in public-private partnerships for cyber security in the Netherlands?".

## 1.2 Research goal

The goal of this research is twofold. First, this research aims to shed light on the practice of collaboration in PPPs for cyber security in the Netherlands and gain insight in factors that may contribute to successful collaboration. By doing so, the second goal of this research is to determine to what extent the academic debate about the sense and nonsense of PPPs in cyber security is supported by real cases of PPPs for cyber security in the Netherlands.

## 1.3 Main question

The main question of this research is: “Which factors may contribute to successful collaboration in public-private partnerships for cyber security in the Netherlands?”.

## 1.4 Sub questions

To provide an answer on the main question, several sub-questions will be answered. First, a theoretical background on PPPs will be presented to provide insight in the characteristics of this concept. Besides this, arguments in the ongoing academic debate about PPPs will briefly be discussed. In the literature review, the following sub-questions will be answered:

1. What are public-private partnerships?
2. Why are they considered to be relevant for cyber security in the Netherlands?
3. Which factors may contribute to successful collaboration in public-private partnerships according to existing academic literature?

The case studies focus on the question: To what extent do the factors in the theoretical framework contribute to successful collaboration in real cases of public-private partnerships for cyber security in the Netherlands? Insight will be provided in the practice of collaboration in PPPs and the following items will be discussed:

a) The main reason to establish the PPP
b) The course of the process of establishment
c) The division of roles, responsibilities and accountability
d) The main goals and interests of the partners involved
e) The presence of the factors included the theoretical framework

By answering all the sub questions, it is aimed to gain theoretical insight in the concept PPPs and to determine factors that contribute to successful collaboration according to existing scientific theories. The intended outcome of this research is to gain insight in the practice of PPPs for cyber security in the Netherlands to be able to take a stand in the academic debate about PPPs. Additionally, it is intended to either validate, invalidate or supplement the theoretical insights about factors that may contribute to successful collaboration in PPPs based on empirical research.

## 1.5 Scoping

The scope of this research is limited to PPPs for cyber security in the Netherlands 2010 – 2019. Since 2010, cyber security is an item on the political agenda of the Dutch national government. This is reflected by the publication of the first “*Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010*” by GOVCERT, the publication of the first National Cyber Security Strategy (NCSS) in 2011 and the establishment of the National Cyber Security Center (NCSC) on January 1st 2012 (Opstelten, 2011b). The first national cyber security strategy of the Netherlands stressed the importance of an integral approach towards cyber security, and PPPs were recommended as a starting point to increase cyber security in the Netherlands (Ministry of Security and Justice, 2011: 5). Therefore, it can be argued that the conscious commitment to PPPs for cyber security in the Netherlands started in this period as well. Since 2010, PPPs are actively promoted by the government, which resulted in the establishment of several PPPs for cyber security. This is the reason why the scope of this research is limited to PPPs for cyber security in the Netherlands since 2010.

## 1.6 Scientific relevance

“*Public-private partnerships are no silver bullet*”, is the title of a well-known academic article written by Dunn-Cavelty & Suter (2009) about the role of PPPs for cyber security. This article represents one side of the ongoing and extensive academic debate about the effectiveness of PPPs to enhance cyber security. At this moment, both proponents and opponents of PPPs for cyber security exist, and both seem to have good arguments for their position. PPPs received a lot of attention by academia, but there seems to be a discrepancy between the attention that the topic PPPs receives in theoretical academic

discussions, and the number of empirical studies that have been conducted on the practical functioning of PPPs. As argued by McQuaid (2000: 30), empirical evidence is needed to determine whether partnerships offer real benefits or not. This research aims to narrow the gap between the theoretical discussions and practice by conducting empirical research on PPPs for cyber security in the Netherlands. Empirical research allows to verify which theoretical claims about PPPs for cyber security are supported in practice. Can collaboration in PPPs be successful or is public-private cooperation doomed to fail? Or can both be possible? And which factors are key in this? This research aims to shed light on these questions. Knowledge about collaboration in PPPs and factors that contribute successful collaboration is important, since this knowledge allows to understand if PPPs can be an effective tool to increase cyber security and why some PPPs collaborate more successfully than others.

## 1.7 Societal relevance

In the National Cyber Security Agenda 2018 of the Netherlands, the following ambition is formulated by the National Cyber Security Center: "*The Netherlands has an integrated and strong public-private approach to cybersecurity*" (NCTV, 2018a: 13). This presumes that the NCSC considers PPPs as an important and effective means to increase cyber security. However, there is a lack of research regarding PPPs in cyber security that supports this assumption. An exploration of previous research on PPPs for cyber security showed that most existing research focuses on the role of PPPs in national cyber security strategies. A comparison of different PPPs for cyber security based on in-depth case studies was not found in the exploration. This research aims to narrow this gap by conducting case studies on PPPs for cyber security in the Netherlands and to determine factors that may contribute to successful collaboration. In this way, this research contributes to knowledge and understanding about the actual working of PPPs regarding cyber security in the Netherlands. Gaining insight in the practice of PPPs is valuable, as this may contribute to empirical support for the sense or non-sense of the promotion of PPPs in the Dutch National Cyber Security Agenda. Furthermore, an increased understanding of factors that may contribute to successful collaboration in PPPs may help to improve policy development and implementation, as these factors can be considered when new PPPs are established or to improve collaboration in existing PPPs. It may also be possible that the case studies reflect the criticism voiced by academia. This would be valuable as well, as this could be a reason to start a serious discussion with policy advisors whether PPPs actually provide a useful means to increase cyber security or not. By increasing the knowledge of the practice of PPPs for cyber security, advantages and disadvantages of this approach will be clarified and can be taken into account by future policy development.

## 1.8 Reading guide

The structure of the remaining part of this thesis will now be elaborated. In chapter two, the methodology and research design will be discussed. Then, insight will be provided in the concept 'public-private partnerships' (section 3.2) and their relevance for cyber security in the Netherlands (section 3.3). Based on a review of existing academic literature regarding factors that may contribute to successful collaboration in PPPs, a theoretical framework will be drawn (section 3.6). In chapter four, the cases will be briefly introduced, followed by in-depth case studies in chapter five. In chapter six, the findings of this research will be presented, with a focus on the findings that are related to the research goal and theoretical framework. Chapter seven contains the conclusion of this thesis, presenting an answer on the main research question. A reflection on the research implementation, discussion of the results and recommendations for future research will be presented in chapter eight.

# 2 Methodology

## 2.1 Introduction

In order to get a thorough understanding of collaboration in PPPs in practice, a literature review will be combined with a document analysis and in-depth case studies. The research approach will be further explained in this chapter.

## 2.2 Type of research

To answer the research question two types of research are combined. First, desk research into scientific literature regarding PPPs for cyber security will be conducted. Based on this literature review, a theoretical framework will be drawn including factors that may contribute to successful collaboration in PPPs for cyber security according to previous research. Then, empirical case studies will be conducted, which allows to test whether the factors in the theoretical framework are supported in practice.

### 2.2.1 Case studies

The basis of the research consists of in-depth case studies. Four cases of PPPs for cyber security in the Netherlands will be examined, analyzed and compared. Although there is a growing body of (inter)national research on PPPs for cyber security, empirical research including multiple in-depth case studies in one specific country is lacking. By conducting multiple case studies, this research design enables to create a thorough understanding of the practice of these specific PPPs. Due to the time frame of this research, the scope is limited to PPPs in the Netherlands and the number of cases is limited to four. The reason to limit the scope to one specific country, is because this excludes cultural, geographical and language differences and may increase the generalizability of the results. The reason to include only four cases, is because this allows – within the set time frame – a comparison between cases, and to focus on two different types of PPPs: for critical infrastructure and for financial cybercrime. Including both PPPs for critical infrastructure and financial cybercrime is relevant, because both are established to fulfill an important task: contributing to Dutch national and economic security. Given this importance task, it is interesting to examine how these PPPs work in practice. Based on this examination, lessons may be drawn which could be used to learn from each other.

### 2.2.2 Selection criteria for the cases included

The PPPs that are included in this research are FERM, CYSSEC, the National Internet Scam Reporting Point (LMIO) and the Electronic Crimes Taskforce (ECTF). FERM and CYSSEC are the PPPs established in the Port of Rotterdam and the airport Schiphol Amsterdam respectively. Specifically these two PPPs are included in the research, because they have some similarities. They were established in the same period: between 2015 and 2016. Both aim to increase the cyber resilience of the main ports of the Netherlands, which are both classified as critical infrastructure by the Dutch government.[1] The security of the ports depends to a large certain extent on the security of chain processes. As a result, both PPPs focus on developing awareness activities to increase cyber resilience of the ports' ecosystems. Finally, both ports accommodate a wide variety of private businesses: from small and medium sized enterprises (SME's) to multinationals. This may create a specific dynamic, which may influence the PPPs.

The other PPPs included in this research are the LMIO and ECTF. Like FERM and CYSSEC, these PPPs are chosen because they have certain similarities. Being established in 2010/2011, both belong to some of the first PPPs for cyber security in the Netherlands. Besides this, they both aim to combat financial cybercrime (fraud) and represent a cooperation between (at least) the police, the public prosecutor's office and the major Dutch banks. In contrast to FERM and CYSSEC, the main focus of

[1] Besluit beveiliging netwerk- en informatiesystemen

LMIO and ECTF is on information sharing. Based on information that is shared, each partner aims to implement measures that contribute to combating cybercrime.

## 2.3 Data collection

For each case study, data is collected through interviews and a document analysis. The primary sources of data for the document analysis are reports, notes and policy documents related to the PPPs. These documents are available online or provided by the interview respondents. Besides this, for each case at least one partner of the PPP has been interviewed. In total, eleven interviews have been conducted with in total twelve respondents between July and September 2019. The respondents are professionals who are directly involved in the PPPs. In the next paragraph, the interview method and selection criteria for respondents will be elaborated.

### 2.3.1 Interview method

The interviews have been conducted by a semi-structured in-depth method. This method has been adopted because it allows to create a thorough understanding of the practice of PPPs. It offers the possibility to ask theoretically driven questions, but leaves room for the respondents' own input as well. Hence, it is possible to discuss perceptions and opinions of respondents regarding the practice of PPPs and continue to ask questions for clarification of answers (Barriball & While, 1994: 30). In this way, the specific context and lived experiences of the different PPPs could be taken into account, and empirical and theoretical research could be combined (Galletta & Cross, 2013: 24). The factors in the theoretical framework have been the basis for the interview setup. To discuss the factors with the respondents, several questions have been formulated in advance. An overview of the factors and interview questions is provided in attachment one. Because the interviews have been conducted in Dutch, the interview questions in the attachment are in Dutch as well. A translation of the questions is available upon request. Due to the interview set up, not every question has been answered by each respondent and other topics have been discussed as well. Every interview has been recorded to make a transcript afterwards. These transcripts have been used for the analysis and are also available upon request.

### 2.3.2 Selection criteria for respondents

Twelve respondents have been interviewed in total. Most respondents have been introduced to the researcher by other students of the Cyber Security Academy, or were already part of the network of the researcher. Other respondents have been recruited by the snowball method. According to Biernacki & Waldorf (1981: 141), the snowball method is suitable for this type of research due to the closed character of the research topic. On an abstract level, some information could be found online about the partners of the PPPs. Yet, information about people who are directly involved in practice was not publicly available. Therefore, knowledge of insiders was required to identify the people that are directly involved in the PPPs. To identify other relevant respondents, the researcher asked the initial respondents who else could be interviewed to obtain a more complete picture of the PPP. In most cases, the researcher was referred to a new respondent, originating in a different organization. The number and diversity of respondents has been increased in this way. The most important selection criterion for the respondents was their direct involvement in the PPPs. By using the snowball method, the researcher was referred to respondents that participate in the PPPs at different levels. The respondents either participate at strategic level (i.e. the Harbor master), at tactical level (team leaders) or at operational level (project managers, advisors). Hence, the practice of the PPPs has been discussed from multiple perspectives. Attachment two provides an overview of the respondents, their organization, job description, and date and place of the interview.

## 2.4 Data analysis

The main part of the data has been collected through interviews, which all have been transcribed. To organize the data in a replicable and systematic way, the transcripts have been converted into a dataset. In order to do this, the researcher started with reading all transcripts carefully. This resulted in a general understanding of the respondent's answers, a first impression of logical themes and tensions within the data. Then, all transcripts were processed into one dataset, in which for each question the answers of all respondents were collected. This resulted in an overview of nineteen questions on the vertical axis, and per question the answers of the respondents on the horizontal axis. In this way, the transcripts were converted in a meaningful dataset. Next, an unique code was assigned to each answer of every respondent. This code consists of the number of the respondent (R) and the number of the question (Q). This means that the answer of the first respondent to the first question has been labeled with "R1Q1". This code has been added to be able to refer to specific answers of respondents in the case studies.

The dataset has been analyzed in a structured way by means of a content analysis. This is a method to interpret the meaning from the content of a qualitative dataset (Hsieh & Shannon, 2005: 1277). A content analysis can be conducted by different approaches, of which the directed content analysis approach has been applied in this research. Compared to other content analysis approaches, the directed content analysis is a more structured approach. It is suitable for this research, as it can be used to validate or extend a theoretical framework (Ibid., 1281). In this research, a theoretical framework has been drawn based on existing theories about collaboration in PPPs. The theoretical framework includes factors that may contribute to successful collaboration in PPPs for cyber security in the Netherlands. To operationalize these factors, a coding scheme has been created. The factors included in the theoretical framework correspond to the themes in the coding scheme (e.g. level of trust). Every theme is divided into two categories, which represent the value of the factor (e.g. high or low). For each category, multiple keywords have been identified which represent an indicator for that specific category (e.g. close relationship). The indicators have been identified using several sources, such as the literature review, a discussion between the researcher and a peer regarding potential indicators and by searching for words and sentences with equal meaning. Creating a coding scheme based on existing theories is also known as *deductive category application* (Mayring, 2000). In this way, the initial coding scheme has been created. After the interviews were conducted, the indicators in the coding scheme have been supplemented and improved.

After the dataset had been prepared, every segment of the text has been systematically coded by using the keywords from the coding scheme. Each time a piece of text matched a keyword, the piece of text was highlighted with a specific color indicating the category related to that keyword. In this way, it became visible whether a certain category was present in the dataset. Segments of text that did not match the pre-set keywords, have been highlighted with a specific color as well. When the initial coding was finished, these segments have been reviewed again to determine whether they represented a new category or theme. The coding of the dataset has been done by hand, using a hardcopy of the dataset and by highlighting pieces of text that matched a specific code. The coding scheme is available in attachment three, and the coded dataset is available upon request.

The analysis from the interview transcript dataset has been supplemented with an analysis of relevant documents. The themes and categories in the coding scheme have been used as starting point for the document analysis. The documents have been carefully read and segments of text that were related to a certain theme or category (e.g. a paragraph about the goals of the PPPs) were highlighted with a specific color indicating the score on that category (e.g. score 'shared goals and interests'). It proved to be more difficult to extract information from the documents that is more related to latent subjects, such as 'level of trust'.

The findings from the data analysis have been used in the case studies. Based on the case studies, it will become clear to what extent the theoretical framework can be supported by empirical research. Besides this, the case studies may point out other factors that may contribute to successful collaboration in PPPs for cyber security in the Netherlands. In this way, it may be possible to enrich the theoretical framework based on empirical research.

## 2.5 Validity and reliability of the research

The value of this research partly depends on the on the extent that the research is conducted in a valid and reliable manner. In this section, the validity and reliability of this research will be discussed.

### 2.5.1 Validity

Being deductive research, existing theories about factors that may contribute to successful collaboration in PPPs formed the bases for the theoretical framework. This has resulted in the inclusion of some factors with a latent character (such as 'interests', 'trust' and 'power relationship'). To determine the presence and nature of these factors, it is necessary to move beyond the manifest content in the dataset and focus on the underlying meaning of the message as well. As a result, focusing on the validity of the research becomes more important. Validity refers to the extent that is measured what is supposed to be measured (Bollen, 1989: 184-185). The validity of this research is increased by using a thorough coding scheme with a theoretical foundation. The coding scheme consisted of themes and categories derived from the concepts that are defined in existing scientific theories. With the accurate application of this theoretical driven coding scheme, the researcher tried to increase the validity of the measurements. The use of expert interviews and the representativeness of the interview respondents provides another challenge to validity (Bryman, 2008: 291). The interview respondents may be biased or give socially desirable answers to the interview questions. Besides this, the respondents may not be representative for all possible relevant respondents. An attempt has been made to decrease the impact of socially desirable answers and increase the representativeness of the respondents. The representativeness has been increased by including respondents with different sexes, age, professional background, job title and level of involvement in the PPPs. In addition, it was tried to interview respondents originating from different public and private organizations related to the PPPs. Nevertheless, it is hard to argue that the interview respondents are representative for all possible relevant respondents. This is partly due to the snowball method, which has been applied to recruit respondents. This method does not aim to come to a representative sample.

### 2.5.2 Reliability

Reliability refers to the consistency of measurement (Bollen, 1989: 206). Research is reliable if the same outcome will be generated by repetition of the research. In this research, a content analysis is conducted. By making the coding scheme available and explaining the procedure for recruitment of interview respondents, the research can be repeated. Bryman (2008: 288) states that this makes a content analysis a transparent research method, which increases the reliability of the research. As argued in the previous section, the validity of the research is increased by the use of a theoretically driven coding scheme. To increase reliability, extra attention has been paid to the accurate and consistent application of the coding scheme. Yet, some scholars argue that it is not realistic to expect objectivity in the coding of latent content (Potter & Levine-Donnerstein, 1999: 265-266). By coding latent content, the researcher makes judgements about the implicit meaning of content. These judgements are biased to a certain extent, as they are informed by the own interpretation of the researcher. A well-known problem is the confirmation biases, which means that the interpretation of the data by the researcher is partially subject to existing beliefs and expectations (Nickerson, 1998: 175). Consequently, repetition of the research may result in slightly different outcomes. According to Potter & Levine-Donnerstein (1999: 266), this does not necessarily make the research unreliable and invalid. Yet, it increases the importance to stress that the coding is subject to interpretation. By making the clean dataset, the coding scheme and the coded dataset available, it is possible to repeat the data

analysis and check whether other researchers come to the same judgements. Previous research has shown that by using a theoretically driven coding scheme and applying this in a systematic and accurate way, a high percentage of researcher coded latent data in the same way (Ibid.).

## 2.6 Limitations

In the previous sections, validity and reliability issues have been discussed. However, there are still some other limitations of this research. Case study research requires an extensive data collection process, which is time consuming. Since this research is conducted for a master thesis, the timeframe is limited and only a small number of cases could be included. Besides the small number of cases included in the research, the scope of the research is geographically demarcated. The reason that the scope is geographically demarcated is because it is tried to limit the influence of cultural differences on the outcome of this research. Inclusion of cultural differences would make the data analysis more complex and time consuming and would make it more difficult to draw meaningful conclusions. Due to the small number of cases and the sole inclusion of Dutch cases, findings cannot justifiably be generalized to other PPPs (outside the Netherlands). Nevertheless, the study is still valuable as it provides in-depth empirical knowledge about the practice of the four Dutch PPPs that has been examined.

Another limitation of the research is the small number of relevant documents that have been included in the document analysis. Prior to the research, the researcher assumed that several documents would be available which could be used in the case studies. However, it turned out that the documentation related to the PPPs was limited. This can partly be explained by the relatively confidential nature of the PPPs. As two of the cases aim to combat cybercrime, they do not publicly communicate about all their partners, methods and procedures. Therefore, the researcher asked every respondent if it was possible to share relevant documents related to the PPPs. In most cases, this turned out to be impossible due to the non-existence of documents or the confidential character. Because of the involvement of the researcher in one of the PPPs, documents were available for this case. For the other case studies, publicly available information on the internet has been used. Because of the lack of documents and the qualitative nature of the research, the study is mainly based on self-reported data in the interviews. Self-reported data has some inherent limitations, such as the selective memory of respondents and attribution of positive events to one's own agency (USC Libraries, 2019). It is tried to decrease the impact of these biases by interviewing professionals from different organizations and covering different perspectives.

# 3 Public-private partnerships

## 3.1 Introduction

PPPs already existed long before the internet and the need for cyber security, and a lot of research has already been conducted on PPPs. In this chapter, the concept of PPPs is examined more in-depth and a theoretical background is provided. Based on an analysis of scientific literature, factors that may contribute to successful collaboration in PPPs are distinguished. The factors that are derived from the existing academic literature are included in a new theoretical framework that is used in the case studies in chapter four.

## 3.2 What are public private partnerships?

The concept of PPPs is thoroughly discussed in academic literature, yet nobody seems to know precisely what they are (Hogde & Greve, 2007: 545). Scholars approach the concept from multiple perspectives and scientific disciplines, such as Network Governance Theory and New Public Management. As a result, various conceptions and meanings of PPPs exist. Linder (1999: 42) argues that the term PPP is used to describe at least six types of partnerships, all with a different understanding of the meaning and purpose of the PPP. Brinkerhoff & Brinkerhoff (2011: 13) state that "*the permutations of partnership purposes, structures, and processes are enormous*". Among other things, the concept of PPPs is used to describe management reforms, new ways of governance or as a method of contracting out public services (see for more details Linder, 1999; Osborne, 2000; Hogde & Greve, 2007; Provan & Kenis, 2007).

An entire thesis could be written to answer the question "what are public-private partnerships". Because this thesis concerns another topic, the researcher looked for concepts that scholars seem to agree on. Despite the wide variety of conceptions and definitions, scholars seem to agree on one basic principle regarding PPPs: PPPs can be described as a collaboration between at least one public and one private party. Ideally, parties enter this partnership because there is a mutual belief that the partnership results in positive gains for both partners (Osborne, 2000: 14). Benefits associated with PPPs are: achieving goals that cannot be achieved alone, increasing cost-efficiency, effectiveness, legitimacy, capacity, spreading (financial) risks, increasing flexibility and enhanced learning (Linder, 1999; Osborne, 2000; Provan & Kenis, 2007; Manley, 2015). Besides this, parties may feel that they have a shared responsibility for (public) policy, and PPPs provide an opportunity to achieve public policy outcomes (Vaillencourt-Rosenau, 1999: 12; Osborne, 2000: 1). In short, proponents of PPPs argue that PPPs provide a cost-efficient and effective instrument to achieve (public) goals that cannot be achieved by one party without the partnership. Opponents on the other hand, argue that in practice partnering is not straightforward and point out several problems associated with PPPs. These problems include among other things: lack of accountability, lack of transparency, problems of coordination, inequalities between partners, lack of public participation, and conflicts of interests (Vaillancourt-Rosenau, 1999; McQuaid, 2000; Wettenhall, 2003; Hodge & Greve, 2007; Carr, 2016).

The wealth of research on PPPs has resulted in a comprehensive debate in the academic literature between proponents and opponents of PPPs. Scholars do not agree on the meaning, form or nature of PPPs, and confusion about the concept remains (Hodge & Greve, 2007: 545). To provide some clarity, it will now be explained what is meant by PPPs in this research. In this research, four different PPPs will be analyzed. As will be clarified in the analysis, these PPPs have been initiated by public organizations. The reason that these PPPs have been initiated is 1) because the government was not able to combat financial cybercrime successfully without private parties, and 2) there was a need to increase cyber resilience of critical infrastructures for national security reasons. A rise in cybercrime, or a cyberattack on critical infrastructure may have disruptive consequences for society (WRR, 2019: 9). Combating cybercrime, safeguarding national security and preventing societal disruption are public goals for which the government bears the final responsibility. Extending this line of reasoning, it can be argued that these PPPs have been initiated by public organizations to contribute to the achievement of

public goals because the public organizations could not effectively address these public goals without the partnership. Therefore PPPs are defined in this research as:

> *"A public-private partnership is a partnership between at least one public and one private organization to achieve a public outcome that the public organization cannot achieve without the private organization."*

As argued before, there is a wide variety of types of PPPs and the concept is not cast in stone. Hence, the concept is defined rather broad to encompass all types of PPPs and to respect all specific circumstances, forms and natures of the PPPs included in this research.

## 3.3 Cyber security & PPPs in the Netherlands

It seems like the rise of PPPs for cyber security in the Netherlands is almost equal to the awareness about the importance of cyber security. In the first National Cyber Security Strategy (NCSS) of the Netherlands in 2011, PPPs are presented as one of the basic principles to increase cyber security (Ministry of Security and Justice, 2011: 5). The minister of Security and Justice stated in the second NCSS: "*The purpose of the NCSS1 was to realize a secure, reliable and resilient digital domain through an integral cyber security approach based on public-private partnerships"* (NCTV, 2013: 3*).* This indicates that from the very beginning, the establishment of PPPs has been a goal in itself. The importance of PPPs is confirmed again by the publication of the National Cyber Security Agenda (NCSA) in 2018. The NCSA contains seven ambitions, one of which is: "*The Netherlands has an integrated and strong public-private approach to cybersecurity*" (NCTV, 2018a: 7). There has been an emphasis on the need for PPPs from the moment the Dutch government actively started to invest in cyber security, which shows that cyber security and PPPs are inextricably linked to each other. This raises some questions: why does the government invest in cyber security? And why is so much emphasis placed on PPPs? Madeline Carr (2016: 50) wrote a famous article about this and posed three questions to clarify the meaning of cyber security in the context of national cyber security strategies. These questions are: *cyber security for whom, from what, and by what means*? Since 2016, a yearly Cyber Security Assessment Netherlands (CSAN) is published by the National Coordinator for Security and Counterterrorism. The CSAN provides insight into the cyber security threats emanating from different actors against different targets. It is used to answer the questions posed by Carr (2016: 50).

### 3.3.1 Cyber security for whom

In the Netherlands, almost all critical infrastructures and processes are completely dependent on IT, and analogue alternatives have almost completely disappeared (NCTV, 2019: 7). It can be said that "*the Internet has become an indispensable element of our social, professional and economic lives*" (Van den Berg & Keymolen, 2017: 188). Society is vulnerable in new ways as cyberattacks that cause an outage of the internet or other critical infrastructures may result in socially or economically disruptive damage. Disruption of or damage on critical infrastructures may result in such serious social disruption that the continuity of our society cannot be guaranteed anymore (WRR, 2019: 26). One could argue that this puts national security at risk. This argument is support by the Dutch government, as it is stated in the NCSA that cyber security and national security are inextricably linked to each other and that national security interests are vulnerable to digital attacks (NCTV, 2018a: 7). In addition to the threat of social disruption due to a cyberattack on critical infrastructures, cybercrime poses another threat for the Dutch society. The Dutch economy is the most IT intensive economy in Europe, which makes the Dutch economy vulnerable to cyberattacks and cybercrime (Verhagen, 2016: 5). Research shows that (small) businesses often lack the expertise, capacities and resources to be resilient against cyberattacks (Leukfeldt, 2018: 12). Cybercrime may result in direct damage such as costs for recovery and prevention, and indirect damage such as missed transactions or reduced customer confidence (CPB, 2018: 1). Besides this, cybercrime can be committed by abusing services of legit private businesses, which harms the businesses as well. Criminals may also launch rogue online stores and defraud customers. In this way, cybercrime may damage confidence in the digital economy which in turn may

harm the Dutch economy (NCTV, 2018b: 5). To sum up, cyber security is needed to protect Dutch national and economic security and safeguard the sustained functioning of the Dutch society (Ibid).

### 3.3.2 Cyber security from what (and from whom)

In the previous paragraph it was argued that cyber security is needed for national and economic security of the Netherlands. As mentioned, disruption of or harm to critical infrastructures may quickly result in socially disruptive damage (NCTV, 2019: 7). Cyber security is needed to protect these critical infrastructures against harm. Harm can be caused intentionally (cyberattack) or by accident (breakdown/failure). This implies that cyberattacks on and/or outage of critical infrastructures pose significant threats to the Dutch national and economic security. Although this provides an initial answer on the question posed by Carr (2016) '*cyber security from what'*, it has become clear that these are two different threats with different threat actors and require further explanation. This poses a new question and addition to the questions posed by Carr (2016): '*cyber security from whom*?'.

Regarding cyberattacks several threat actors can be distinguished. In the CSAN 2019 is stated that: "*the biggest cyber threat affecting national security is posed by nation-state actors*" (NCTV, 2019: 15). Several countries actively execute espionage or (preparation for) sabotage activities aimed at the Dutch state, enabling them to pose harm to critical infrastructures (Ibid). This became publicly known in April 2018, when a cyber espionage operation was obstructed which was being carried out in the Netherlands by the Russian Military Intelligence Agency (Ministry of Defense, 2019). In the CSAN 2019, criminals are identified as second substantial threat actor. The easy scalability and relatively low risks of conducting cybercrime ensure that the threat emanating from criminals remains high (NCTV, 2019: 7). Examples of cyberattacks by criminals are DDOS-attacks on Dutch banks and the Dutch Tax and Customs Administration (Ibid., 15-19). Although this does not pose a direct national security threat, it may harm businesses and reduce trust in the digital economy. Customers will be less likely to buy goods or services online if they do not trust the system, so trust is key for the digital economy to function (Van den Berg & Keymolen, 2017: 195). In the CSAN 2019 is stated that no cyberattacks by terrorists have been identified recently (NCTV, 2019: 15). Yet, it is not unimaginable that terrorists will try to use a cyberattack on critical infrastructures for a terrorist attack. Due to the anonymity and relatively easy and cheap implementation, The Netherlands Scientific Council for Government Policy describes a cyberattack on critical infrastructures as "*the perfect weapon*" (WRR, 2019: 46). Other malicious threat actors that pose an intentional threat are hacktivists, scriptkiddies and insiders (NCTV, 2019: 17). In addition to the intentional threats, the Dutch national and economic security can be harmed unintentionally, by accident (Ibid., 22). The increasing dependence on ICT systems increases the probability of unintentionally caused harm to critical infrastructures. Unintentional breakdowns or failure of critical infrastructures can be caused by, for example, natural disasters. Since the modern technology that is used in critical infrastructures is increasingly complex and interconnected, unintentional harm can also be caused by technical or human errors. Therefore, one minor failure may affect multiple systems and have major consequences (Ibid., 29).

In sum, cyber security is needed because Dutch national and economic security are threatened. The biggest intentional threats are cyberattacks such as espionage and (preparation for) sabotage. The biggest unintentional threats are breakdowns or failure of critical infrastructures. Regarding intentional threats, the main threat actors are state actors and criminals. Unintentional threats emanate mainly from natural causes, technical errors and human mistakes.

### 3.3.3 Cyber security by what means

In the previous sections has been explained that cyber security is needed, among other things, to protect the Dutch national and economic security against intentional and unintentional cyberthreats aimed at critical infrastructures. According to the social contract theory by Hobbes, the state is responsible for safeguarding national security (Hobbes, 1651). This would imply that the state also takes care of the cyber security in the context of national security. In 2011, the Dutch minister of Security

and Justice publicly acknowledged the responsibility of the national government for cyber security (Opstelten, 2011a: 3). In cooperation with the private sector and scientists, the national government set up an integral approach to enhance cyber security in the Netherlands. Initially, this approach consisted of three actions: publishing the first Cyber Security Assessment Netherlands, clarifying the legal framework for cyber security, and the establishment of the National Cyber Security Center (NCSC) (Opstelten, 2011b). It can be argued that these actions provided the initial means for the government to increase cyber security. The main goal of the NCSC is to increase the digital resilience of the Dutch society. Hence, the NCSC shares insights in trends, threats and vulnerabilities, provides security advice for owners and operators of critical infrastructures and provides support with incident response capacities (Ibid., 12). Over time, new legislation to increase cyber security has been made. Derived from the European Directive on Security of Network and Information Systems, owners and operators of critical infrastructures are now required by Dutch law to take appropriate and proportional technical and organizational measures to manage cyber security risks and prevent incidents.[2] Besides this, another law was created, extending the authority of the police and public prosecutor's office to combat cybercrime.[3]

Despite these legal, administrative and organizational measures, the ability of the national government to increase cyber security to safeguard national or economic security remains limited in practice. This is due to the fact that more than 80 percent of all critical infrastructures and processes in the Netherlands are owned and operated by private companies (NCTV, 2017). This includes, among others, internet service providers, payment services, flight- and aircraft handling and electricity supply (Ibid.). Because they are privately owned and operated, the government cannot directly determine the necessary level of cyber security, nor implement measures to increase cyber security. The government depends to a large extent on private companies to increase cyber security in relation to national and economic security (WRR, 2019: 75). In order to gain some influence and control over the cyber security of critical infrastructures and processes, public-private partnerships are a necessity for the government (Ibid., 80; NCTV, 2017).

Apart from enhancing cyber security for national security matters, the national government has an interest in increased cyber security of private businesses, not being critical infrastructure. Although these private business are primarily responsible for their own cyber security, it is in the interest of the government that they maintain an adequate level of cyber security as this decreases the opportunities for cyber criminals. A decrease in cybercrime results in less victims, less work for the police and public prosecutor's office and more confidence in the digital economy. The government has implemented several measures to increase cyber security of private businesses and combat cybercrime. The government plans to invest 26 million euros in the coming years to combat cybercrime. Among other things, this budget will be used to recruit new cyber security professionals for the police organization and to conduct more cybercrime-related research (Rijksoverheid, 2019). As mentioned before, a new law was created as well, extending the authority of the police and public prosecutor's office.[4] To provide support to private businesses to increase their cyber security, the Digital Trust Center (DTC) has been established in 2018. The target group of the DTC are all 1,6 million businesses in the Netherlands not being critical infrastructure or processes (DTC, 2019a: 2). The DTC supports businesses by sharing accurate, up-to-date and reliable security advices via their website and by granting subsidies to so called "cyber resilience networks". In these networks, groups of businesses cooperate to increase the cyber resilience of their supply chain, region or sector (Ibid., 3). As said, the government does not have control over the cyber security of these private businesses. Despite these legal, financial and administrative measures taken by the government, practice shows that it is difficult to combat cybercrime effectively when public and private organizations operate on their own. Besides this, the investment needed to increase cyber security may be too high for small businesses (Olsthoorn & Koot,

[2] Wet beveiliging netwerk- en informatiesystemen (Wbni)

[3] Wet Computercriminaliteit III

[4] Ibid.

2017). For this reason, the government is again stimulating cooperation and invests in the establishment of public-private partnerships (Grapperhaus, 2019).

Summarizing the previous sections, it can be argued that cyber security is predominantly needed in the Netherlands to protect national and economic security against breakdowns of, or cyberattacks on, critical processes and high levels of cybercrime. The biggest threats emanate from state actors, criminals and several unintentional causes. The Dutch government aims to protect Dutch national and economic security through different administrative, organizational, technical and legal means. It remains difficult to exert direct influence on the level of cyber security because the government does not own and/or operate critical infrastructures and processes in most cases. Establishing PPPs is therefore a key strategy for the government. Examples of PPPs that have been established for cyber security of critical infrastructures are FERM (Port of Rotterdam) and CYSSEC (Schiphol Airport). Examples of PPPs that have been established to increase cyber security of private businesses and combat cybercrime are LMIO (Marktplaats) and ECTF (Dutch banks). Based on this observation, it can be stated that PPPs provide an important means for the Dutch government to enhance cyber security and to protect Dutch national and economic security from intentional and unintentional cyberthreats. Figure one provides an overview of the main answers on the questions posed by Carr (2016), complemented with an extra question posed in this research: *cyber security for whom, from what, from whom and by what means?*

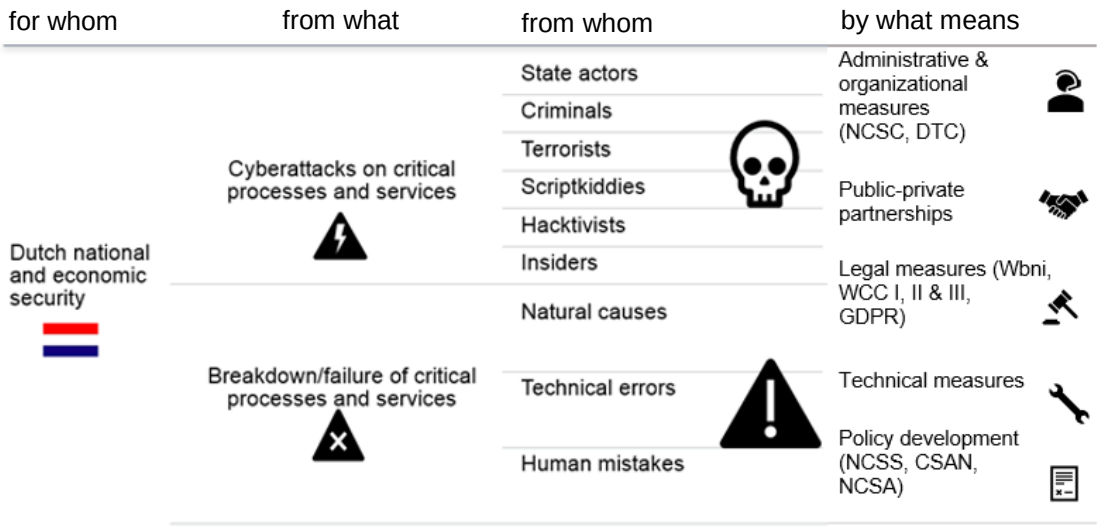


*Figure 1 Cyber security in the Netherlands: for whom, from what, from whom and by what means?*

## 3.4 PPPs for cyber security, a panacea?

In the previous section has been explained that PPPs are implemented as a means to enhance cyber security and protect the Dutch national and economic security. Considering the extent that the government promotes and relies on PPPs, they almost seem to be a panacea. Yet, they are a frequent topic of academic debate, and some even doubt whether the idea of cooperation between the government and private businesses is realistic at all. It would be naïve of the government to assume that private business would fund national security needs, including defending against potential nation-state attacks against critical infrastructures (Clinton, 2015: 55). Furthermore, PPPs are expected to create synergy, drawing on the strengths and weaknesses of each partner and leading to results that no partner can achieve without the PPPs. The partnership should be more than the sum of its parts, but research by Vaillancourt-Rosenau (1999: 10) shows that this is not always the case. It is argued that PPPs have substantial problems, as they do not lead to superior performance in criteria of equity, access and democracy. Besides this, they seem to increase regulation instead of reducing it (Ibid).

Other research shows that the expectations of partners about roles, responsibilities and authority diverge (Carr, 2016: 44), and that interests and goals of partners are only partially convergent (Dunn-Cavelty & Suter, 2009: 181).

The academic debate about PPPs resulted in a wealth of both theoretical and (foreign) empirical studies regarding this topic. These studies show that it proves to be a challenge to establish successful collaboration within the PPPs (Osborne, 2000: 2). However, authors have identified factors that contribute to successful collaboration within PPPs. A literature study has been conducted to get an overview of the factors that are identified by multiple researchers. These factors will be outlined in the next section. Due to the wealth of the existing research on PPPs, it is impossible to discuss every publication. An attempt has been made to include the factors which appear to be mentioned the most, but no claim to comprehensiveness can be made.

## 3.5 Literature review

### 3.5.1 Factors that contribute to successful collaboration in PPPs

From the literature study it becomes clear that there are similarities among the factors that scholars have identified as key factors for successful collaboration within the PPPs. The factor that is identified by the most scholars and referred to as 'most critical' for successful collaboration, is *trust*. Dunn-Cavelty & Suter (2009: 184) devoted an article to the challenges of PPPs for cyber security and actually advocate another approach. Still, they state that PPPs *can* be successful if the actors involved have established mutual trust. They consider mutual trust to be more important than control and regulation (Ibid.). McQuaid (2000: 30) and Osborne (2005) support this argument by emphasizing the necessity of trust and stating that 'trust between the partners' is the most important key aspect for successful partnerships. Also Manley (2015: 85) and Brinkerhoff & Brinkerhoff (2011: 4) refer to mutual trust as a key factor for successful collaboration. Huxam & Vangen (2000: 319) state that "*trust and respect lies at the heart of partnering".* An important finding of these authors is that establishing mutual trust within a partnership provides a fundamental challenge: "*trust can only be developed through collaboration, which in turn depends on trust"* (Dunn-Cavelty & Suter, 2009: 182). To build and maintain mutual trust several measures are mentioned: creating a mutual belief in positive gains for both partners, investing in personal relationships, increase transparency and understanding the challenges each partner faces (Manley, 2015; Huxham & Vangen, 2000; Carr, 2016).

The second key factor for successful collaboration that has been mentioned by many authors is related to *the goals and interests* of the partners and the PPPs. If the goals and interests of partners are not clear or do not align, there is a potential for conflicts of interest and misunderstanding between partners (Vaillancourt- Rosenau, 1999: 22; McQuaid, 2000: 22). This hinders successful collaboration. Therefore, it is important that the partners have shared and undisputed goals (Dunn-Cavelty & Suter, 2009: 180). Ideally, the goals of the PPPs are jointly determined and formalized (Brinkerhoff & Brinkerhoff, 2011: 4; Clinton: 2015: 64; Carr, 2016: 55).

*Clarity about roles and responsibilities* presents a third aspect that has been identified by many authors as key aspect for successful collaboration with PPPs. Clarity about roles and responsibilities of partners is important because research shows that successful collaboration within PPPs is hindered by differences in expectations about the roles of different partners and the unwillingness of parties to take responsibility for specific tasks (Huxham & Vangen, 2000: 319). A problem with accountability may arise if partners do not feel responsible for the activities of the PPPs. Therefore, many authors state that it is important that the division of roles, responsibilities and authorities is made clear at the start of the collaboration (Ibid.; Vaillancourt-Rosenau, 1999: 25; McQuaid, 2000: 30; Dunn-Cavelty & Suter, 2000: 180; Clinton, 2015: 59; Carr, 2016: 60).

Derived from the literature study, it can be argued that a fourth key factor for successful collaboration is the level of *stakeholder support*. This refers to the extent that public, political and other stakeholders

encourage and support the partners to tacking the issue at stake by joining the PPP. Clinton (2015: 64) finds that early involvement of the industry and reaching out to stakeholder is important for successful collaboration as it creates support for the PPP and the decisions made. Vaillancourt-Rosenau (1999: 25) argues that PPPs may be more successful when there is community or societal agreement on the importance of the public goal at stake and support for the establishment of a PPP. Manley (2015: 85) amplifies this argument by stating that public and political pressure to join a PPP can convince parties to do so.

Another factor identified by many scholars is the level of *financial support* for the partnership. This refers to two things: 1) are the partners willing to contribute financial resources to the partnership (Huxham & Vangen, 2000: 320), and 2) are there financial incentives for (private) partners to join the PPP (Vaillencourt-Rosenau, 1999: 25; McQuaid, 2000: 20; Manley, 2015: 93; Carr, 2016: 57). The financial contribution of partners is needed to ensure that overhead costs associated with maintaining the partnership can be covered, and that there is budget available for the PPP's activities (Huxham & Vangen, 2000: 32). Without budget, successful collaboration may be hindered. The financial incentives for parties may be necessary to convince them to join the PPP and to contribute to a public goal rather than achieving their own objectives (Carr, 2016: 57). Besides financial incentives, private parties may be convinced by the availability of other resources of value through the PPP, such as information and expertise previously not available in their organization (McQuaid, 2000: 20).

In addition to the above, authors have identified that collaboration is more successful when there is a *contract or another document that formalizes the collaboration* of partners in the PPP. Case study research by Clinton (2015: 61) shows that collaboration in PPPs was less successful if there was no common document or framework governing the PPP. Other scholars support this argument by pointing out that a clear and formal foundation of the PPP is a precondition for successful collaboration (Dunn-Cavelty & Suter, 2009: 180; Huxham & Vangen, 2000: 293-300; Brinkerhoff & Brinkerhoff, 2011: 4). Carr (2016: 62) argues that in case of diverging interests, PPPs must be governed by rules in order to be successful. Manley (2015: 93) seems to agree with this, arguing that a clear legal framework is an essential element for successful collaboration. Collaboration will be easier if there is a legal framework which determines the terms and conditions of the collaboration and clarifies what partners may expect from each other.

In most articles and books included in the literature study are 'equality of partners' and 'consensus-based decision making' identified as key aspect of successful collaboration. *Equality of partners* contributes to successful collaboration because partners will be more willing to collaborate if they feel that every partner is equal (Manley, 2015: 94). Besides this, inequality of partners may cause tensions if one partner tries to achieve objectives other than the objectives of the partnership, and may pose problems for decision making (Huxham & Vangen, 2000: 23-24). The importance of collaborative and consensus-based decision making for successful collaboration is also mentioned by Brinkerhoff & Brinkerhoff (2011: 4) and Clinton (2015: 94). According to McQuaid (2000: 23), being in a partnership suggests that power is equally distributed between all partners. This is not a necessity according to Huxam & Vangen (2000: 23). They argue that equality of partners does not necessarily mean that all partners should have equal power. Some partners might have a legitimate claim for more power due to their role, responsibilities or because they make a greater contribution to the PPP. Hence, equality between partners is not, by definition, equality in power.

In sum, an outline is provided from the factors that have been identified by many authors as key factors for successful collaboration in PPPs. Although these authors argue that these factors contribute to successful collaboration, the importance of some of these factors has become apparent because in the cases that were examined by these authors collaboration in PPPs was unsuccessful. According to some authors, the unsuccessful collaboration was partly due to the absence of these factors (see Vaillancourt Rosenau, 1999; Clinton, 2015; Manley, 2015). As their absence contributed to unsuccessful

collaboration, the authors assumed that the opposite - their presence - contributes to successful collaboration. In this way, they identified factors that contribute to successful collaboration by ascribing a binary value to factors that contributed to unsuccessful collaboration. This assumption is also adopted in this research. Therefore, it can be argued based on previous studies that the following factors may contribute to successful collaboration in PPPs:

1. Mutual trust between partners in the PPPs
2. Clear and shared goals and interests of the partnership
3. Clarity about roles, responsibilities and authority at the beginning of the collaboration
4. High stakeholder support
5. Availability of financial support for the PPPs activities and incentives for collaboration
6. A formal foundation of the collaboration in the PPP
7. Equality of partners

### 3.5.2 Other factors that may affect successful collaboration

In addition to the factors discussed in the previous section, the literature study showed that there are other factors that may play a role in the collaboration in PPPs. Yet, the existing literature does not clarify if these factors contribute to successful collaboration. One of these factors is the governance form of PPPs.

The literature study illustrated that PPPs can be governed in different ways and several governance forms can be distinguished. Wettenhall (2003) and Provan & Kenis (2007) both argue that the governance of PPPs can be categorized along two different dimensions. Wettenhall (2003) divides the governance of partnerships in broadly two ideal types, each representing a pole on a scale. In the first ideal type, the governance structure of the partnership can be characterized as horizontal and non-hierarchical. All parties are directly involved, and decisions are made based on consensus. In the other ideal type, the governance is characterized by hierarchy. It can be described as a vertical arrangement, with one party in a controlling role. The superior party exercises control over the partnership, and steers the actions of others to achieve the intended goals. Based on these ideal types, Wettenhall (2003: 91-92) distinguishes three categories of governance forms:

1. Mixed enterprises: *"all types of government ownership arrangements, ranging from "sole" to "dominant" to "passive" investor*".
2. Outsourcing or contracting-out: "*arrangements in which a public authority retains ownership or policy control of a function but contracts with a private operator to discharge that function*".
3. Subsidization, controlled competition, regulation: "*a mix of public and private elements where a government pays subsidies to private companies to get them to do things the government did not want to do itself*".

These types of partnerships can be placed on a scale with the poles representing the ideal types, as presented in figure two. According to Wettenhall, true partnerships should be on the left side (non-hierarchical) of the scale.

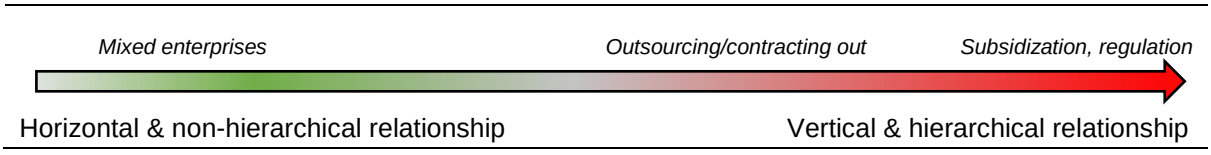


*Figure 2: Typology of governance forms of PPPs by Wettenhall (2003: 90-93)*

A similar categorization is provided by Provan & Kenis (2007: 234). Just like Wettenhall, they argue that network governance forms (e.g. PPPs) can be categorized on a scale. At one side of the scale, the network is highly decentralized and governed by the parties that compromise the network. This is referred to as "shared governance". On the other side, the network is governed centrally, with a single entity executing the governance activities. Besides being decentral or centrally governed, they argue that networks can be participant-governed or externally governed. Participant-governed networks can

be governed in two ways: either though shared governance by network members, or by a single network member taking the role of lead-organization. By externally governed networks, the network is governed by a unique network administrative organization (NAO). The NAO can be either formally mandated as part of the network formation process or established voluntarily by network members. Based on this categorization, Provan & Kenis (2007: 234-237) distinguish three forms of network governance:

1. Participant-governed networks: decentralized and shared governance by network members themselves, based on equality of network members.
2. Lead organization-governed networks: a more centralized and hierarchical form of governance. The lead organization is responsible for the coordination of activities and decisions within the network.
3. Network administrative organization: centralized form of governance by a separate and external entity.

This typology of governance forms can be placed on a similar scale as the typology by Wettenhall (2003). This is presented in figure three.

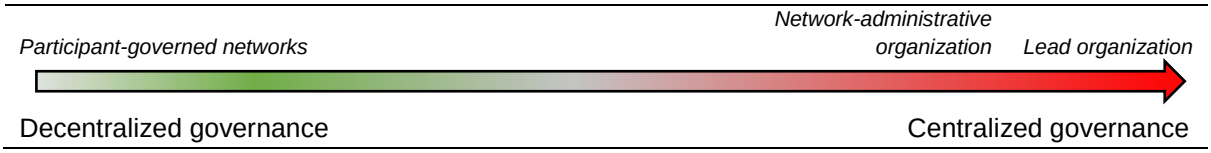


*Figure 3: Typology of governance forms of PPPs by Provan & Kenis (2007: 234-237)*

In the existing literature, not one specific governance form as identified by Wettenhall (2003) and Provan and Kenis (2007) has been identified as key factor for successful collaboration. When discussing governance forms, Manley (2015: 86) stresses the importance of a bottom-up approach. Brinkerhoff & Brinkerhoff (2011: 4) explicitly mention the importance of non-hierarchical and horizontal structures and processes. On the other hand, McQuaid (2000: 28) argues that collaboration is likely to be more successful in hierarchies, because this governance form facilities sustainable, long term relationships and thus may increase trust between partners. In addition, he argues that hierarchical organizations promote a more stable collaboration because it will be less likely that there are many changes in personnel and responsibilities.

The absence of a clear point of view regarding the governance form in the literature makes it hard to argue that a certain governance form contributes more to successful collaboration than others. In order to examine to what extent a specific governance form contributes to successful collaboration in the cases in this research, a new framework is created by the researcher including the governance forms of both Wettenhall (2003) and Provan and Kenis (2007). The governance forms distinguished by Wettenhall (2003) and Provan and Kenis (2007) have been combined in order to get a more comprehensive typology of governance forms. In figure four, the governance forms have been placed on a scale ranging from horizontal and decentralized governance to vertical and centralized governance. On the basis of the factors that have been identified, there seem to be pro's and con's for both governance forms. One could possibly argue that in a 'shared' or 'network' governance form, it will be more likely that PPPs have a positive score on 'stakeholder support', 'mutual trust between partners' and 'shared goals'. On the other hand it could possibly be argued that a more 'vertical' and 'centralized' governance form may contribute to 'clarity about roles, responsibilities and authority', and that it will be more likely that sufficient 'financial support' is available. Although one would expect that 'equality of partners' would be higher in 'shared' or 'network' governance forms, Huxham & Vangen (2000: 23) argue that this is not necessarily the case. In order to determine whether a specific governance form contributes to successful collaboration in PPPs, the governance forms of the cases in this research will be categorized based on this framework.

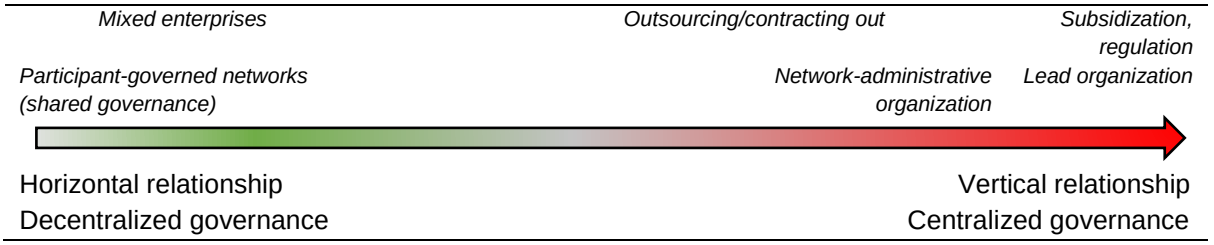


*Figure 4: Typology of governance forms of PPPs, based on the type of relationship between partners (Wettenhall, 2003) and the degree of centralization of governance activities (Provan & Kenis, 2007)*

Another factor that is mentioned in the literature in relation to collaboration in PPPs, is the number of parties involved in the PPPs. However, the literature review it did not result in a clear point of view whether the number of parties involved in the PPPs contribute to successful collaboration. The only authors that make a clear statement about this are Dunn-Cavelty & Suter (2009). They argue that given the importance of mutual trust, a PPP "*can only be carried out with selected companies and must be small*" (Ibid., 184). Although it is not really apparent from previous research, it may be possible that the number of partners involved affects the collaboration in the PPP. In order to gain more insight in the relationship between the number of parties involved in the PPP and successful collaboration, this will be examined in the analysis as well.

## 3.6 Theoretical framework of factors that may contribute to successful collaboration

Based on the factors that have been identified in section 3.5.1 as factors that contribute to successful collaboration according to existing literature the researcher created new theorical framework. In order to determine which factors may contribute to successful collaboration in practice, the cases will be analyzed by means of this theoretical framework. Due to the nature of the factors that have been identified, some have nominal values (e.g. the formal foundation of the PPP) and others have ordinal values (mutual trust to a greater or lesser extent). As the presence (to a certain extent) of these factors may contribute to successful collaboration in the PPPs, it can be argued that the absence of a factor may contribute to unsuccessful collaboration in the PPPs to a certain extent. As mentioned, in section 3.5.1, this assumption has also been made by the authors of the articles included in the literature review. The researcher combined the factors to create a new theoretical framework which is presented in table one and will be used for this research. Because the literature review did not clarify whether a specific governance form and the number of parties involved in the PPP contribute to successful collaboration, these factors have not been included in the theoretical framework and will be analyzed separately.

*Table 1:*
*Factors that may contribute to successful and unsuccessful collaboration in PPPs for cyber security*

| | **Mutual trust** | **Goals & interests** | **Roles & responsibilities** | **Stakeholder support** | **Financial support** | **Foundation of PPP** | **Relationship between partners** |
|---|---|---|---|---|---|---|---|
| **Successful** | *High* | *Clear/shared* | *Clear* | *High* | *Available* | *Formalized* | *Equal* |
| **Unsuccessful** | *Low* | *Unclear/diverging* | *Unclear* | *Low* | *Unavailable* | *Not formalized* | *Unequal* |

Now it is clarified which factors may contribute to successful collaboration PPPs, one thing still needs clarification: the meaning of "successful" and "unsuccessful". It is challenging to provide an all-encompassing definition of these concepts, as they have different meanings in different contexts and to different people. The Cambridge Dictionary (2019) provides the following definitions:

- Success: "*the achieving of the results wanted or hoped for*".
- Failure: "*the fact of someone, or something, not succeeding*".

If these definitions would be used for this research, collaboration in the PPPs would be seen as successful if the intended goals of the PPPs were achieved. The collaboration in the PPPs would be seen as unsuccessful if goals were not achieved. However, this does not touch upon the essence of this research. In this research, it is examined whether the collaboration itself is successful. According to previous research, the degree of successful collaboration depends on the level of trust, alignment of goals, clarity of roles & responsibilities etc. and not (solely) on goal achievement. This implies that in this research, a PPP can be determined as successful even though the intended goals have not been achieved.

In this research, "successful" refers to the collaboration in the PPPs. There is not a specific outcome a priori designated as "successful", as each PPP has specific characteristics which result in different ways of collaborating. Collaboration in PPPs will be considered successful when partners engage in collective and mutually supportive action to achieve certain goals, and satisfaction about the cooperation exists. Factors that may contribute to this according to existing literature have been included in the theoretical framework (table one). Collaboration in PPPs will be considered unsuccessful if the partners do not operate in the interest of the partnership and the 'greater good', and the actions and goals of partners are not complementary. Unsuccessful collaboration is characterized by inequality and distrust among partners, conflicts of interest and coordination problems.

# 4 PPPs for cyber security in The Netherlands: short introduction per case

## 4.1 Introduction

To examine factors that may contribute to successful collaboration in PPPs, four in-depth case studies have been conducted. In this chapter, a concise description is provided of each case in which the establishment, goals, financial model and organization structure of the PPPs will briefly be discussed.

## 4.2 FERM

In 2015, the Mayor, the Police Chief and the Chief Public Prosecutor of Rotterdam went on a business trip to Singapore. During a visit to the port of Singapore, they were informed about cyber security risks of modern ports. Because the processes and operations in the port of Rotterdam were automating and digitizing at a rapid pace, they decided that something had to be done to increase the cyber resilience of the port of Rotterdam. Research organization TNO was hired to develop a strategy to increase the cyber resilience of the Port of Rotterdam. This resulted in eight 'building blocks' which are presented in figure five. According to TNO, giving substance to these building blocks would increase cyber resilience of the Port of Rotterdam. To do this, the harbor master had been appointed as Port Cyber Resilience Officer. He became responsible for "FERM" the port cyber resilience program which was officially launched on January 1st, 2016 with an initial duration of four years [R5Q3]. The main goals of FERM are increasing cyber resilience in the port, increasing cyber security awareness of organizations operating in the port, intensifying the cyber security skills of organizations and building risk management in this area (Havenbedrijf Rotterdam, 2016).

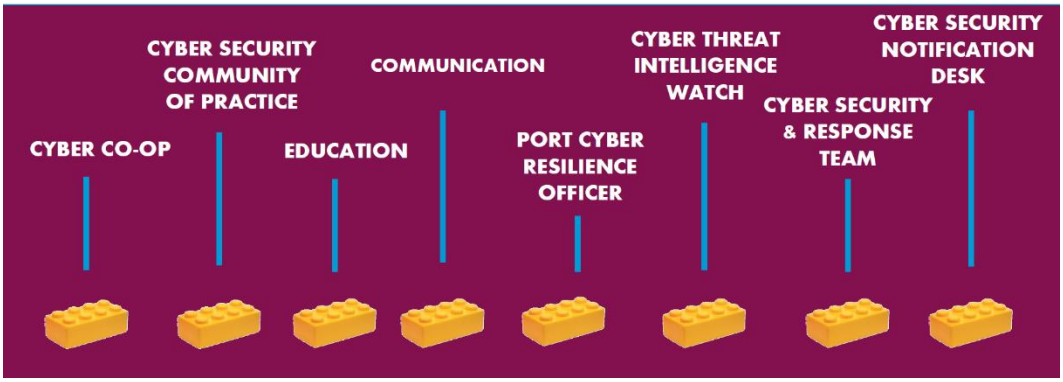


*Figure 5: FERM building blocks (Reprinted from Deltalinqs, personal communication, April 15th 2019).*

At the operational level, a working group was established consisting of employees from the Port of Rotterdam, the City of Rotterdam, the Seaport Police, the Public Prosecutor's office and the business representation organization Deltalinqs. An employee of the Port of Rotterdam was appointed as program manager of FERM. At the strategic level, a steering committee was established consisting of the Port Cyber Resilience Officer, the alderman of the City of Rotterdam responsible for the Port of Rotterdam, the Police Chief of Rotterdam, the Chief Public Prosecutor and the Chairman of the Board of Deltalinqs. All parties in the steering committee, except from the Public Prosecutor, invested €25.000 per year for four years. Due to the lack of financial resources, the Public Prosecutor's Office did not make a financial contribution. This was generally accepted by the steering committee [R2Q7; R5Q5]. The yearly budget of €100.000 has been available to give substance to the building blocks and managed by the program manager of FERM [R5Q5; R2Q19]. Over time, the joint environmental protection agency of the province of South Holland (DCMR), the NCSC and the Safety Region Rotterdam-Rijnmond (VRR) joined the working group. They did not join the steering group nor become an official (paying) partner of FERM [R1Q1; R2Q17; R3Q17].

FERM can be considered a PPP because it is a collaboration between public (City of Rotterdam and Seaport Police) and private (Port of Rotterdam and Deltalinqs) parties to achieve the public goal 'increasing cyber resilience of the Port of Rotterdam'. Yet, the parties have a somewhat differing status within the partnership. The core of the PPP consists of only four 'official members' based on their financial contribution and membership of the steering committee. The Public Prosecutor is involved at the strategic level as a member of the steering committee but does not make a financial investment [R5Q5]. The other parties take a more peripheral role by not making a financial investment, nor being a member of the steering group. In addition to the yearly budget, a subsidy of € 200.000 was granted by the Ministry of Justice and Security in 2018 [R2Q26].

Although officially all partners in the steering committee are equals, accountability is not equally divided. The Port Resilience Officer is mainly responsible for the implementation of the Port Cyber Resilience Program. This responsibility is delegated to the program manager FERM. The program manager is accountable to the Port Cyber Resilience Officer, which is in turn held accountable by the steering committee [R2Q19; R3Q19; R5Q19]. Figure six contains a visual representation of the PPP.

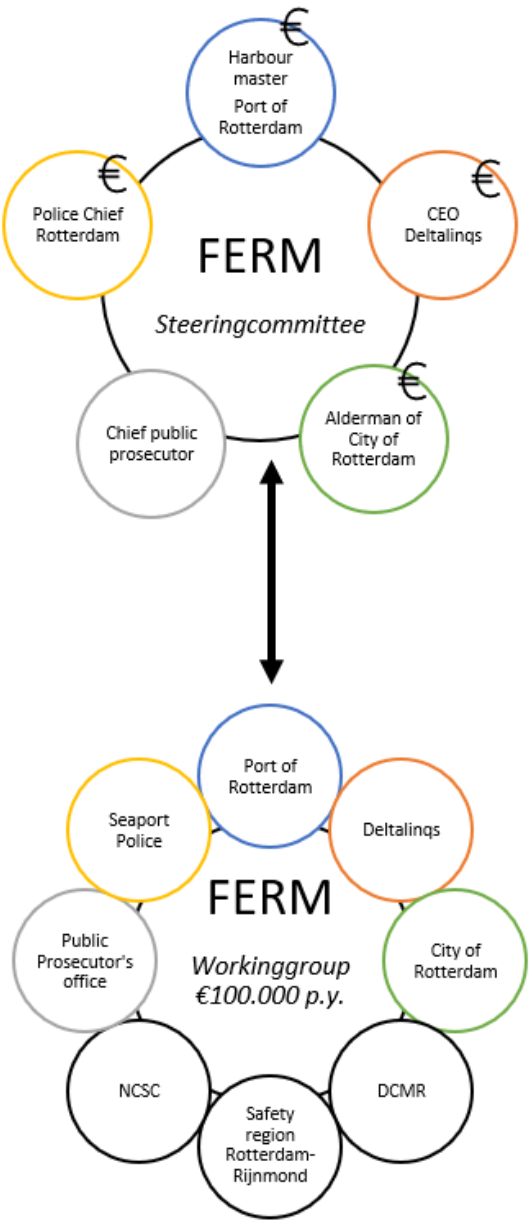


*Figure 6: Visual representation of the PPP FERM*

## 4.3 CYSSEC

Schiphol Airport is owned by the Royal Schiphol Group (ie. Schiphol), but the settlement of air traffic and the operation of the airport depends on many parties in the Schiphol ecosystem. There is a significant chain dependence in safety and security of the ecosystem, which is why Schiphol felt the urgency to increase the ecosystem's cyber resilience. In order to do this, Schiphol hired a consultant from Capgemini to set up a community program [R10Q8]. This resulted in the launch of CYSSEC in 2017. CYSSEC (**'**Cyber Synergie Schiphol Ecosysteem') is a cyber security initiative in the Schiphol community. It is described as 'a platform which aims to increase cyber resilience of the Schiphol ecosystem (all businesses and organizations at Schiphol)' (CYSSEC, 2019). In the pursuit of this goal, extra attention is paid to co-creation with the businesses and organizations at Schiphol and the specific chain dependencies in the ecosystem [R10Q4].

The core of CYSSEC is a project organization operated by a project lead and a project employee. Besides this, there is a group of twelve ambassadors which are working for public and private business and organizations in the Schiphol ecosystem, such as the Royal Schiphol Group, the Royal Netherlands Marechaussee, Menzis Aviation, the Safety Region Kennemerland, Aircargo Nederland and several small and medium enterprises [R10Q8; R10Q16]. The only condition for being an ambassador is the willingness and motivation to participate. To officially become an ambassador of CYSSEC, the ambassadors have to sign a Memorandum of Understanding on personal title [R10Q13]. On strategic level, the project lead of CYSSEC has regular contact with the Director Safety, Security and Environment of Schiphol. Additionally, the NCSC contributes to CYSSEC by sharing their knowledge and relevant up-to-date information about cyber security threats (CYSSEC, 2019). Given the public goal of CYSSEC and the parties involved in the initiative, CYSSEC can be considered a PPP.

At this moment, CYSSEC is mainly financed by Schiphol as Schiphol still hires the consultants of Capgemini to be the project lead and project employee [R10Q8]. The ambassadors of CYSSEC do not make a financial contribution. In 2019, CYSSEC was granted a subsidy of € 200.000 by the Digital Trust Center [R10Q14].

The project organization initiates the projects and activities of CYSSEC. By signing the MoU, the ambassadors have expressed commitment to the implementation of the projects and activities, yet they do not have any formal obligation to the project organization [R10Q16]. Figure seven contains a visual representation of the PPP.

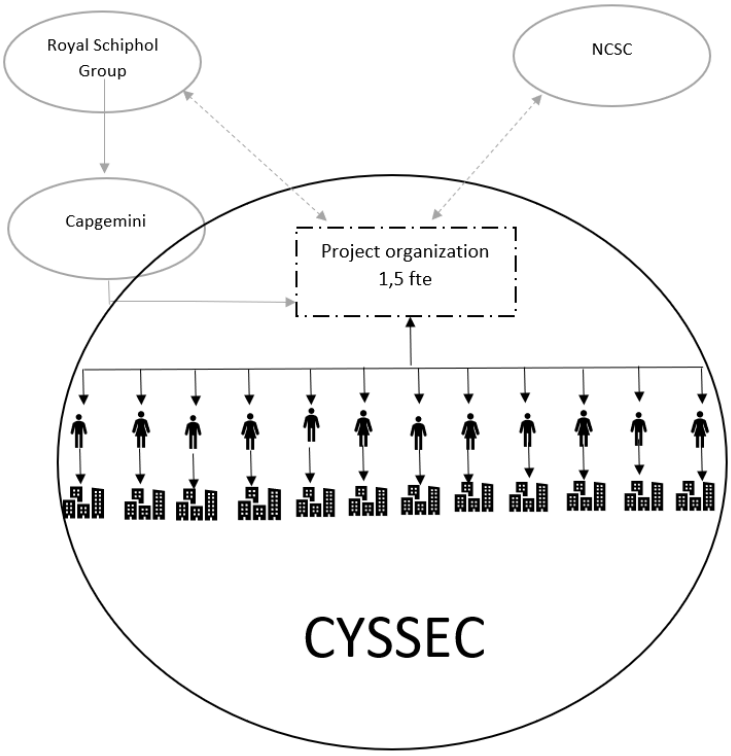


*Figure 7: Visual representation of the PPP CYSSEC*

## 4.4 LMIO

The internet gave rise to the existence of online trading platforms such as Marktplaats. Although these platforms have been established to facilitate online buying and selling of goods, they are also used to defraud people. This resulted in several problems for different parties:

- Marktplaats's reputation was damaged and faced a decrease in customer confidence [R9Q2]
- All the 26 police regions were confronted with many police reports regarding online buying and selling fraud and all had to deal with it individually. Potentially, this resulted in 26 different investigations regarding the same offender [R7Q3, R8Q3]
- The police and public prosecutor's office were confronted with a major increase in police reports regarding online buying and selling fraud (40.000 – 50.000 per year) and were not able to handle all of them [R8Q18].

Because of the issues Marktplaats was facing, a consultant was hired to initiate a cooperation with the investigation authorities. Soon this consultant realized that Marktplaats was not the only online trading platform that was searching for ways to deal with online buying and selling fraud. To create a single point of contact for the government, he established the 'Overleg Online Handelplaatsen' (OOH), which represented 90% of the online trading platforms. Because the investigative authorities were also looking for ways to reduce online buying and selling fraud, they decided to examine possibilities for cooperation with the OOH. Meetings between Marktplaats, the police, the public prosecutor's office and the ministry of Security and Justice started. After a start-up phase of more than three years, the pilot project 'National internet scam reporting point' (LMIO) was launched in 2010 (Van der Steur, 2015; [R9Q2]). The main goal of LMIO is to establish an effective way to decrease online buying and selling fraud [R7Q2; R9Q2].

LMIO is a single point of contact for all police reports regarding online buying and selling fraud. All police reports are collected and analyzed by one police team in collaboration with one public prosecutor. LMIO also prepares a file if there are indications for criminal investigations. These files are handed over to local police forces for further investigation (Van der Steur, 2015). In addition to the criminal investigation part, a covenant was signed between LMIO and the OOH in which they agree on collaboration to combat online selling and buying fraud. In practice this means that the trading platforms will be informed by LMIO when police reports include fraud related to their platform. This allows the platforms to take measures to prevent more criminal activities by the same account [R7Q15; R8Q3]. LMIO has been expanded over the years and several partnerships have been set up with relevant partners such as the major Dutch banks, the Dutch Payment Association, payment service providers and the Authority for Consumers and Markets [R7Q7; R8Q8; R7Q15; R9Q16]**.** Almost all partnerships between LMIO and the other parties consists of the same aspects: LMIO collects and analyses police reports related to online buying and selling fraud, and informs partners when the reports are related to their products or services. Based on this information, the partners can take measures to prevent more cases of fraud. For example, if the police receives three or more reports regarding fraud by a certain Marktplaats account, Marktplaats is informed about this. Based on this information, Marktplaats may decide to block this account. The same applies to banks and bank account numbers [R8Q8].

At the operational level, LMIO consists of around eight FTE police officers (ten people), including a team leader. The team leader is responsible for LMIO and accountable to the Chief of Police. He works in close collaboration with one specific public prosecutor [R7Q2; R8Q6]. At this moment, the core of LMIO is formed by a separate team within the Dutch national police organization, but efforts are being made to embed LMIO in the regular organization. At the strategic level, two consultative bodies have been set up. For the partnership with the OOH, the 'steering committee LMIO' is established including the representative of the OOH, the team leader of LMIO and the public prosecutor [R9Q16]. For the partnership with the major Dutch banks, the 'Expertpool Internetoplichting Banken' has been set up, including representatives of the banks, the team leader of LMIO and the public prosecutor [R8Q18]. In these consultative bodies, the long-term strategy is discussed and strategic decisions are taken. However, each partner is responsible for the implementation in its own organization [R7Q15; R8Q18].

In addition, each organization bears its own costs, meaning that there is no collectively available budget for LMIO [R7Q8; R9Q14]. Given the parties involved in the partnerships of LMIO and the official commitment of both public and private partners to contribute to a public goal by signing a covenant, LMIO can be considered a PPP. In figure eight, a visual representation of LMIO is provided. The different colors indicate different aspects of LMIO. Red represents the criminal investigations part, green represents the strategic level and blue represents the partnerships related to LMIO. Apart from the formal partnerships shown in figure seven, there are also informal partnerships between LMIO and the media, the 'Consumentenbond' and the ministry of Security and Justice [R8Q24].

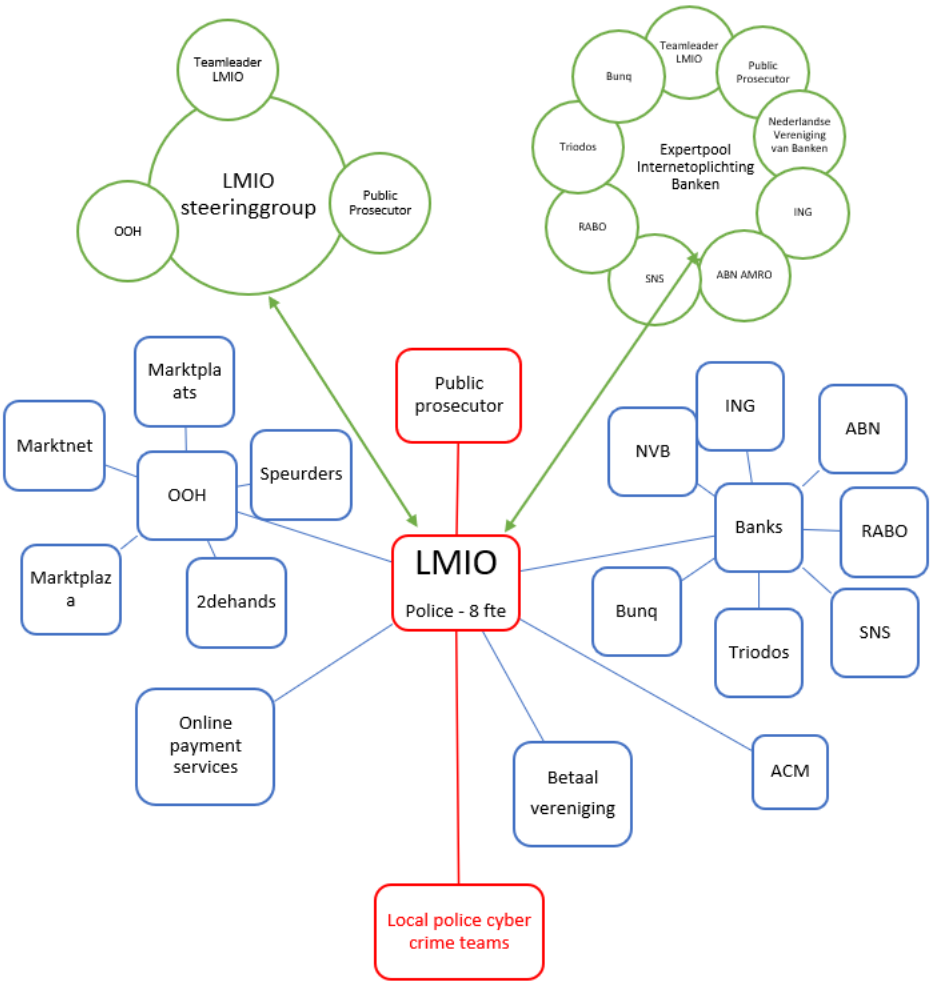


*Figure 8: Visual representation of the PPP LMIO*

## 4.5 ECTF

The increase in the use of internet led to a new form of banking: online banking. Online banking became a very popular method, with as a consequence digital payment traffic becoming an attractive target for criminals. The financial damage caused by fraud involving online banking increased from 1,2 million euros in 2009 to 9,8 million euros in 2010 (Government of the Netherlands, 2011). Because secure and reliable payment traffic is crucial for the stable and adequate functioning of the financial system, the Team High Tech Crime (THTC) of the national police, the national public prosecutor's office and the major Dutch banks started to cooperate to fight online banking fraud. The 'Electronic Crimes TaskForce' (ECTF) was launched in March 2011, when a covenant was signed by the minister of Security and Justice, the president of the Dutch Banking Association, directors of the ABN Amro bank, ING bank, Rabobank, SNS Bank, the Chief Police and the Chief Public Prosecutor (Ibid.). Given that the ECTF consists of a combination of public and private parties, joining forces to achieve a public goal (decreasing online banking fraud), the ECTF can be considered a PPP.

The main goal of the ECTF is to fight cybercrime that undermines society's confidence in the integrity of the financial system. Activities of the ECTF include mitigation, detection and disruption of criminal activities involving online banking and victim notification [R6Q4]. In order to do this specific knowledge, information and expertise of all partners is collected, analyzed and shared. Based on the reinforced information position, the banks take measures to mitigate and disrupt criminal activities. The police and public prosecutor use the information to investigate and prosecute criminal suspects (Government of the Netherlands, 2011). In addition to the formal collaboration on paper, the parties are physically joining forces by working together in one operational team which is located at the location of THTC. The ECTF team consists of six police officers (a financial specialist, a digital specialist, two analysists, a tactical detective and a team leader) and one representative of each bank [R6Q8]. The public prosecutor's office is not part of the operational ECTF team. When it is necessary to consult a public prosecutor, the team leader of the ECTF contacts the public prosecutor linked to the THTC [R6Q8]. A supervisory committee has been set up to guide the ECTF at the strategic level. The supervisory committee consists of the parties that signed the covenant. They meet once every six weeks to discuss the course of events, strategic issues and finances [R6Q17]. A visual representation of the ECTF is provided in figure nine.

The ECTF team leader is responsible for the daily operations of the ECTF. She is accountable to the supervisory committee. Regarding personnel-related matters, she is only responsible for the police officers. The other organizations bear their own responsibility regarding human resources. Additionally, they bear the responsibility to take measures based on the information that is shared in the ECTF. If an organization fails to take measures, it will be discussed in the supervisory committee [R6Q19]. The employees working for the ECTF are paid by each organization individually. When additional budget for the ECTF is needed, a request for budget is made at the supervisory committee. If there is an agreement on the budget, each partner makes a contribution. The other costs, such as the location and the screening of employees are paid by the police [R6Q8].

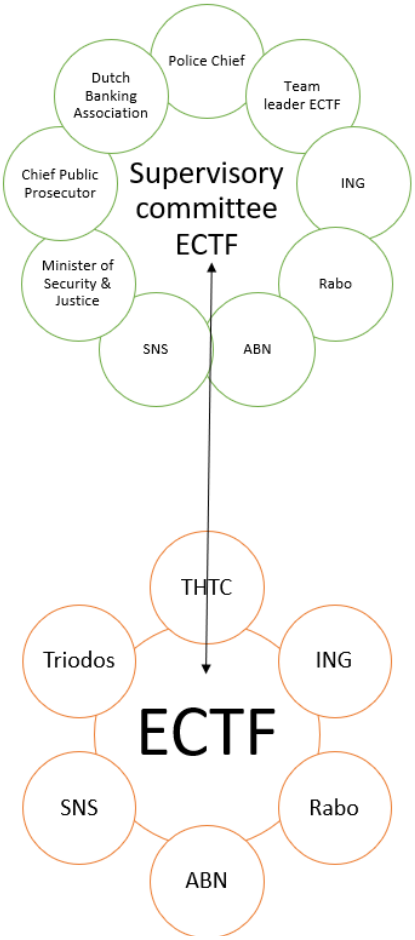


*Figure 9: Visual representation of the PPP ECTF*

# 5 Case studies

## 5.1 Introduction

In this chapter, the PPPs that have been introduced in chapter 4 will be analyzed using the theoretical framework created in paragraph 3.6. The analysis is divided in two parts instead of an analysis per case. The analysis of FERM and CYSSEC, and of LMIO and ECTF respectively are combined because these cases largely relate to the same goals (ie. cyber resilience of critical infrastructure and reducing financial cybercrime). Given the relatively corresponding goals, it is interesting to examine if the PPPs are similar to a certain extent as well. By combining them, a comparison is possible which may shed light on similarities and differences, and the extent that the collaboration is considered successful. Based on this comparison, it may become clear why collaboration in some PPPs is more successful than in other PPPs, and which factors play a role in this. First FERM and CYSSEC will be analyzed, then LMIO and the ECTF will be analyzed. Each factor from the theoretical framework is discussed in relation to the specific cases. Quotes from respondents have been used to substantiate the analysis. For matters of consistency and readability, these quotes have been translated from Dutch to English. An attempt has been made to stick to the original text as much as possible. However, due to language differences it has not always been possible to translate a sentence literally.

## 5.2 FERM & CYSSEC

**Mutual trust**

The literature study showed that mutual trust between partners is crucial for successful collaboration. This is affirmed by the partners of both FERM and CYSSEC. During the interview, the importance of trust has been mentioned many times by different respondents. It was argued that "*trust between partners is necessary to get something done"* [R3Q9]. Besides stressing the importance, all respondents argued independently from each other that the level of trust between partners is high. This can be illustrated by the following statements:

> "*A real strength of the partnership is the strong mutual bond between the partners, we know each other well and trust each other"* [R2Q9]

> *"(..) we can just talk about it, openly and confidently. That's why I feel comfortable at FERM. What you see if what you get, we respect each other for who we are. There is no politics in the working group. That gives a relaxed and comfortable feeling*". [R3Q10]

Trust has also been expressed when respondents were asked about the sharing of sensitive information. In the case of FERM was mentioned: *"We easily share sensitive information with each other. There is a lot of trust and a familiar atmosphere between the partners in the working group"* [R3Q11]. Also in the case of CYSSEC there seems to be a sufficient level of trust to share sensitive information: *"We really have a circle of trust, so we encourage people to share what went wrong so others can learn from that"* [R10Q11].

In this way, the interviews clarify that also in practice mutual trust between partners is considered to be important, and that the level of trust is high in both cases.

**Goals & interests**

In the interviews with respondents involved in FERM it became clear that different conceptions about the main goal of FERM exist. Goals that have been mentioned were "*increasing cyber resilience of the Port of Rotterdam*" [R2Q3], "*gaining insight in the vulnerabilities in the port's infrastructure and processes and measures to mitigate these vulnerabilities*" [R3Q4; R4Q4] and "*increasing resilience by creating awareness"* [R5Q5]. The respondents agreed that of these goals, hitherto only awareness has been created. The reasons why other goals have not been achieved differ. One respondent argued that

"*if the Port of Rotterdam has a different opinion, it will not happen*" [R4Q4]. A similar reason is provided by another respondent which states the following:

> *"The Port of Rotterdam has a special interest. They have formal duties in the port and are responsible for FERM. I can see them struggling with this because it costs a lot of money. So they focus on their primary interest. If others want something not related to the port as 'critical infrastructure', but for example related to small and medium enterprises companies in the port, then it soon becomes a bit more complicated" [R3Q4].*

The main goal of FERM and the partners' individual goals or interests have not been discussed nor clarified at the start of the PPP [R3Q4]. One respondent states: "*it has not been discussed what each partner considers to be important to do, or what their goals and interests regarding FERM are*" [R3Q5]. This shows that in the case of FERM the goals and interests of partners are to a certain extent unclear and diverging.

The goal of CYSSEC seems to be more clear as both respondents agreed on the goal "*increasing the cyber resilience of the Schiphol ecosystem with specific focus on the chain dependencies*" [R10Q14]. This statement corresponds with the goal that is mentioned on the website of CYSSEC. Although CYSSEC is initiated by the Schiphol Group, it seems that joining CYSSEC is also in the interest of other parties. In contrast to FERM, it is not decided at strategic level which parties are part of the PPP. Being an ambassador of CYSSEC is voluntarily, on personal title and based on intrinsic motivation of individuals. As argued by the respondents: "*just because it is voluntarily and on personal title, you can be sure that the people around the table really want to be there, and that they are not there because they are forced to be there*" [R10Q16]. The individual interests and exact reasons to join CYSSEC may differ, but at least it can be argued that all ambassadors have a shared interest in being a member of CYSSEC. If being an ambassador of CYSSEC was not in their own interest, they probably won't become an ambassador. This illustrates that in the case of CYSSEC partners have clear and shared goals and interests.

**Roles & responsibilities**

The harbor master from the Port of Rotterdam is appointed as Port Cyber Resilience Officer (PCRO) and thereby responsible for FERM. This responsibility is delegated to an employee of the Port of Rotterdam, which is appointed as program manager FERM [R3Q19; R5Q19]. The program manager is accountable to the PCRO, which in turn is accountable to the steering committee. The Alderman of the City of Rotterdam is chairman of the steering committee [R2Q19; R5Q19]. Except from this, roles and responsibilities are not clearly divided or assigned. One respondent states "*there is no division of roles and responsibilities. It has a high 'ik doe het er bij'-gehalte"*[R4Q18]. Taking into account the answers of the other respondents, some distinction in roles can be made. "*The Port of Rotterdam is in the lead and has a pioneering role. The role of the other partners is relatively small and equally divided*" [R1Q18; R2Q18]. "*This means that the Port of Rotterdam facilitates the organization of the working group and sets the agenda. The other partners provide knowledge, substantive input and financial support. The Port of Rotterdam takes care of the daily operations of FERM*" [R1Q18]. Regarding responsibilities the following statements are made:

> "*nobody is responsible for anything*" [R4Q19]

> "*we did not arrange this properly. We have no idea who is accountable when it goes wrong. In practice, the PCRO is accountable, but the Alterman is chair of the steering committee. The steering committee approves strategic decisions, so in that sense they may also be accountable*" [R2Q19].

> *"When something needs to be done, we just look around the table and discus whether or not we will do it. We just look at each other like "are we going to do this? And who is going to do it? And when are we going to do it?" And then we just do it.."* [R3Q20]

> *"There is no structure. I would like to have an organization chart, not to place everyone in that organization chart but to be able to understand what we are doing, why and with whom. Then we can get started. Now everything is a bit fuzzy"* [R3Q18].

This illustrates that roles and responsibilities are not clear and not equally divided among the partners of FERM.

In case of CYSSEC, there seems to be more clarity about the division of roles and responsibilities. Two consultants of Capgemini are hired by Schiphol to take care of the day-to-day project management. One of them, the project lead, is mainly responsible for CYSSEC and accountable to the Director Safety, Security and Environment of Schiphol. When individuals want to join CYSSEC and become an ambassador, they have to sign a Memorandum of Understanding (MoU). In this MoU, the roles and responsibilities of the ambassadors are clearly described: ambassadors function as sparring partners, contribute to the implementation of CYSSEC campaigns, represent the ideas of CYSSEC and provide access to the wider community [R10Q8; R10Q10]. Besides this, they are expected to attend the CYSSEC meetings. If ambassadors do not adhere to the MoU, the project lead will confront them [R10Q10]. This shows that the division of roles and responsibilities in CYSSEC is clear.

**Stakeholder support**

During the analysis of the interviews it has become clear that it is difficult to give a clear answer with regard to stakeholder support. This is because there are much more stakeholders involved in the PPPs than expected, and they are too diverse to place them all in one category. The category 'stakeholder support' was derived from the literature review and it was expected that 'stakeholders' would mainly refer to society in general or the management boards of the parties involved in the PPPs. During the analysis, it became clear that there are multiple stakeholders at many different levels: the community, media, politics, the broader society, colleagues, management boards, the executive and administrative level etc. All these parties can be stakeholders and may affect the collaboration in the PPPs. Due to the differences in roles and interests of these stakeholders, the degree of support from these parties can vary greatly and change over time as well. This implies that there can be high stakeholder support and low stakeholder support in one PPP at the same time. This was the case with FERM. In its core, the reason that FERM has been initiated is because the Mayor, the Police Chief and the Chief Public Prosecutor of Rotterdam wanted something to be done to increase cyber resilience of the Port of Rotterdam. Together with the Port of Rotterdam and Deltalinqs, they made budget available to launch a program [R1Q14]. Therefore, it seems fair to argue that stakeholder support at executive/ administrative level was high. However, it was stated in the interviews that a new financial model is needed because some partners actually do not want to make budget available after 2020 [R2Q26; R5Q18]. This could indicate that stakeholder support at executive/administrative level is low. The interviews also clarified that from the outset an attempt has been made to expand the PPP and to include more businesses originating in the Port of Rotterdam. So far this has not been achieved and as a result FERM has remained a PPP including only two private parties [R5Q18]. This would indicate a low score on stakeholder support regarding the community. In any case, it shows that stakeholder support is not a constant variable. Besides this, it shows that it is hard to provide a conclusive score on stakeholder support because it can differ per stakeholder and over time.

It does not seem right to make a comparison between FERM and CYSSEC regarding the level of stakeholder support, because the timeframe may influence the level of support and CYSSEC has only been operational for 1,5 years and FERM for almost four years. Nevertheless, it can be argued that in case of CYSSEC there is a high level of support from different stakeholders at this moment. According to the respondents, there is support from the board level of Schiphol. "*They really realize that this is very important and therefore are willing to invest in it*" [R10Q14]. Besides this, CYSSEC has been established with the aim to become a 'community initiative'. Hitherto, twelve ambassadors originating from twelve different companies voluntarily have become CYSSEC ambassador [R10Q8]. This

indicates high stakeholder support from the private parties in the Schiphol community. However, the ambassadorship is on personal title instead of as a representative from a business [R10Q16]. This makes the actual involvement of businesses and their support for CYSSEC unclear, which is why it is difficult to provide a conclusive score on the level of stakeholder support in case of CYSSEC as well.

**Financial support**
As mentioned before, all parties in the steering committee except from the Public Prosecutor made a commitment to invest €25.000 per year for four years when FERM was established. In addition to the yearly budget of €100.000, a subsidy of € 200.000 has been granted by the Ministry of Justice and Security in 2018. This indicates that financial support is available. Yet it should be noted that at this moment, it is not clear if there will be budget available after 2020 and that this is considered worrisome by respondents [R1Q14].

The financial model of CYSSEC differs from FERM. CYSSEC is financed by Schiphol, which comes down to paying the costs for hiring two consultants from Capgemini. Being project lead and project employee, they do most of the work in arranging meetings, developing content and setting up campaigns. There are relatively few other costs according to them [R10Q20]**.** A subsidy of €200.000 has been granted to CYSSEC by the Digital Trust Center in 2019 [R10Q14] (DTC, 2019b). This subsidy is only granted once and it is not known if the financing from Schiphol will be unlimited. Regarding the long-term financial model, the respondents argued: *"I can imagine that we will move towards a financial model where the strongest shoulders carry the heaviest burden*" [R10Q14]. Therefore, it can only be argued that at this moment there is financial support available but that it is not known if and how this will be arranged on the long term. The respondents did not express worries about a lack of financial support.

**Foundation of the PPP**
A formal decision to establish FERM has never been made. Nor a formal founding document, a contract, covenant or MoU exists. One of the respondents states: "*there is no founding document or covenant. People always say "the local triangle decided to establish FERM and appointed the PCRO", but there is no document that says so. If we quit doing it, it will just stop*" [R5Q13]. Additionally, no agreements have been made about confidentiality, results or how the budget should be spent [R3Q5; R5Q19]. One respondent states: "*I think FERM is a PPP, but not an institutionalized PPP. FERM is nothing and that makes things difficult*" [R3Q5]. Statements of other respondents confirm that collaboration is hampered by the lack of a formal agreement and organization structure. "*The open and informal atmosphere contributes to trust, but it is also a weakness or a risk. It can lead to nothing, that nothing happens or people are not committed. An advantage of a tight business setting is that it results in action, that you really go somewhere. The Port of Rotterdam pays attention to this, that is good because the risk is that we talk more than we do things*" [R3Q9]. The respondents express the need for a less voluntary form of cooperation in which mutual expectations, roles and responsibilities are clarified [R2Q16]. This indicates that the foundation of FERM is not formalized and that this hinders effective collaboration.

In case of CYSSEC, the collaboration has been formalized through the signing of a MoU between the project lead of CYSSEC and all ambassadors [R10Q13]. The MoU does not provide a legal obligation for ambassadors but ensures that they take their ambassadorship more serious and increases commitment. A respondent stated: *"by signing the MoU, we have intensified the connection between parties*" [R10Q13]. Besides this, it is argued that "*the MoU has been a practical means to show that being an ambassador is not entirely without obligations. It also helped to clarify the role of the ambassadors*" [R10Q14]. The MoU illustrates that the foundation of CYSSEC is formalized. Besides this, it shows that a formal foundation contributes to clarity about roles and responsibilities [R10Q10; R10Q13]**.**

**Relationship between partners**

The lack of formal agreements, organization structure and internal rules makes it difficult to determine how partners of FERM formally relate to each other. The positions of the members of the steering committee indicate that theoretically speaking, all partners of FERM are equal. They operate at the same level (executive board) and do not have a hierarchical relationship with each other. The same principle applies to the working group. Regarding decision-making procedures, a respondent states: "*Anyone can submit a proposal, everyone can say everything. Making decisions sounds so serious.. I think we just develop a shared good feeling and then we say "this feels good and it aligns with the goals of FERM so maybe we should do it. That is a decision for me*" [R3Q18]. Some nuance has been brought by other respondents. It is argued that in the working group, the voice of the parties that have made a financial investment in FERM prevails [R2Q17]. On top of this, all respondents state that the Port of Rotterdam has the most influence and that the Port of Rotterdam basically decides what happens [R2Q17; R3Q17; R1Q18; R2Q18; R5Q19]. This is not considered to be a problem by most respondents, but rather logical [R1Q18]. A respondent from The Port of Rotterdam argues the following about this:

> "*I think that our vote counts the most, simply because we are the one that facilitates FERM. The other parties are always behind because they have too little time to deal with this. So it is logical that we have the most influence, but I think we never made a decision that anyone really disagreed on. In the end we are a partnership and not a group that works against each other*" [R2Q17].

Although it remains difficult to provide a concrete finding regarding the relationship between parties in FERM, it seems fair to argue that the relationship is unequal because the Port of Rotterdam has more influence than the other parties.

In case of CYSSEC, the interview indicates that there is one dominant party as well. Schiphol has initiated CYSSEC and hires two consultants from Capgemini to take care of the daily operations. Schiphol provide financial support for CYSSEC and functions as a sparring partner at strategic level. Therefore, one could assume that Schiphol exerts more influence and plays a larger role in CYSSEC than other parties. A respondent states:

> "*Schiphol is most actively involved, so we have a kind of guidance from their cyber security center and management. We discuss the future of CYSSEC with them. Yet, we are responsible for the implementation and we discuss this with the ambassadors. Because Schiphol provides the funding of CYSSEC, the role of the ambassadors in practice is just agreeing on the plans. It has never happened that they did not agree or wanted to change plans. If so, we would have complete autonomy to do that"* [R10Q20].

However, the respondents argue that Schiphol made a deliberative choice to hire external consultants to set up CYSSEC as "*this would make it easier to make CYSSEC a neutral community initiative. If Schiphol would be in the lead parties would possibly feel that big brother determines everything. CYSSEC is organized in such a way that all parties get the impression that they are equal*" [R10Q18]. In this way, the consultants argue that they work for the CYSSEC community and not for Schiphol. Besides this, an employee of Schiphol has become an ambassador of CYSSEC and officially signed the MoU. This has also been a deliberate choice to show that they are equal to the other ambassadors. Although the CYSSEC project organization facilitates the collaboration and invests most time and effort in the partnership, it is argued that they are also equal to the ambassadors. The ambassadors cannot be forced to do things by the CYSSEC project organization, even if they have signed the MoU [R10Q19]. It can therefore be concluded that although informally Schiphol and the CYSSEC project organization may have more influence, formally all parties are equal. Additionally, the effort made to emphasize the equality of partners and neutrality of the initiative shows that equality and neutrality are considered to be important for successful collaboration.

## 5.3 LMIO & ECTF

**Mutual trust**

The literature review showed that mutual trust between partners is crucial for successful collaboration. The importance of mutual trust is affirmed by the partners of LMIO and ECTF. The essence of the collaboration in LMIO and ECTF is sharing sensitive information. All respondents argue that therefore trust is key [R8Q11; R9Q8; R7Q17; R6Q9]. It is also argued that trust is not self-evident. Trust needs to grow, which requires certain preconditions. In both cases of LMIO and the ECTF, special attention was paid to establishing trust. Regarding LMIO, respondents state:

> "*From the beginning it was my job to create trust between partners. You can define 'trust' in many ways, but at least you have to make sure that everybody works together with integrity, and that you give a fair representation of things*" [R9Q8].

> *"Successful collaboration and trust is not self-evident, you will have to invest in it to make it work"* [R9Q23]

> "*I told the people involved: it does not matter to me how we arrange it on paper. What is important for me is that we know each other, that we can call each other, that we build a basic level of trust and that we do this with similar intentions. Then, the collaboration comes naturally [R7Q17].*"

A respondent involved in ECTF argues:

> "*What is a real strength is the high level of trust. I think this is very important. The people involved meet often, they know what information they can share and that the information will be treated confidentially. What is not allowed to be shared, will not be shared. Hence, trust has been proven*" [R6Q9].

This shows that trust is considered to be important, and that is there is mutual trust between partners of LMIO and the ECTF according to the respondents. However, the interviews also made clear that trust alone is not sufficient to share information. Sharing information between the police and private parties is strongly regulated, and a legal basis is required to share personal data and information. In the case of LMIO and the ECTF, the police is allowed to share information based on article 18 and 20 of the Police data law[5] [R7Q11]. A respondent from the ECTF states:

> "*Our goal is combating digital banking crime. We are only allowed to share information in relation to this goal, and in the covenant it is defined on which themes we cooperate. These themes are phishing, malware, online trading fraud, DDos-attacks and cyberattacks on banks. Considering these types of cybercrimes, it is important to be able to share information quickly. This happens within the legal borders of the covenant. For example, if we look in our police systems and we see that a suspected person has a criminal record not related to cybercrime, we do not share this information. We are gatekeepers for our own organization, so we ensure that we do not share information that we are not allowed to share. However, sometimes we do share information beyond the limits of the covenant, but then the public prosecutor has given permission" [R6Q11]*

Without legal basis, private companies are not allowed to share personal data either. This has become even more difficult by the introduction of the new General Data Protection Regulation (GDPR). In case of LMIO and ECTF, a way was found to deal with this. A respondent argues: "*If we want information from private parties, it is claimed by the public prosecutor based on the Procedural Criminal Law*[6]*. With the claim, we give the private parties a legal basis to share the information. Besides this, we create a system in which information is not shared without any control, as the public prosecutor checks whether*

[5] Wet Politiegegevens
[6] Wetboek van Strafrecht

*it is appropriate or not* [R7Q11]. The above analysis illustrates that in both cases of LMIO and ECTF, the respondents confirmed that mutual trust is important and that it is present in the PPPs. It is considered to be so important that specific attention is paid to the creation of specific circumstances to increase trust. However, trust alone is not sufficient to share information. In order to achieve the main objective of the PPPs, a legal basis to share information may be as important as trust.

**Goals & interests**

In the existing literature on PPPs, the importance of clear and shared goals and interests has been emphasized by many researchers. This was also emphasized by the respondents in the interviews regarding LMIO and ECTF. The respondents have mentioned several reasons why shared goals and interests are important:

> *"after you have found a common goal and mutual interest by the existence of the PPP, it will be easier to find a way to work together" [R7Q7].*
>
> *"long-term collaboration will be very difficult if there is no common goal" [R2Q26].*
>
> *"a shared goal ensures commitment from all parties" [R6Q7].*
>
> *"this kind of partnerships will never work if there is no shared interest. I think the crux is that you can define a clear common goal" [R9Q8].*
>
> *"The added value of the PPP is that there a network with the same people meeting regularly. Things go faster because you know each other and work on the same goal" [R7Q17].*

However, most respondents also stressed that besides shared goals and interests it is important that the PPP serves individual goals and interests. If the PPP does not align with the individual interests, it will be hard to collaborate successfully [R9Q23]. In case of LMIO, a respondent argues: *"we have thought about the advantages for each party involved, because collaboration works best if it is in everyone's own interest. So we thought: what is the advantage of the police, the public prosecutor, Marktplaats and for the Dutch society? A 'common interest' sounds nice, but in the end every individual is held accountable by its own organization and then the common interest does not count. That is reality'. [R9Q14].* In case of the ECTF, a respondent argues: "*the good thing in this collaboration is that we all have an individual interest in the success of the collaboration. The banks have an interest and the police has an interest. So in the end we have a common interest and we are all committed*" [R6Q7]. It is argued that the one does not exclude the other: "*different interests can coexist, as long as there is a shared interest as well*" [R9Q8].

This illustrates that the importance of shared goals and interests is confirmed by real life practitioners. Besides this, it illustrates that in both cases of LMIO and the ECTF partners have shared goals and interests. Yet, an important finding is that besides shared goals and interests, it is considered important that the PPP aligns with individual goals and interests of the parties involved.

**Roles & responsibilities**

The literature study clarified that a clear division of roles and responsibilities of partners is important for successful collaboration. In the case of LMIO, the division of roles and responsibilities seems to be clear. There was a need for a single point of contact for all police reports regarding online buying and selling fraud. Since only the police has the authority to collect and analyze police reports, a police team was established and made responsible for collecting and analyzing these reports. In the police team, different roles can be distinguished: team leader, tactical detective, analyst, administrative assistant and work planner [R7Q8]. This team has been accommodated by the police district Kennemerland [R9Q14]. Police investigations take place under the authority of a public prosecutor. Therefore it was necessary to appoint a public prosecutor that would be ultimately responsible for the police

investigations of LMIO. The police investigations of the Kennemerland district take place under the authority of the North Holland Public Prosecution Service, so they appointed a 'Public Prosecutor Internet Scams'. The public prosecutor that has been appointed was chosen because he had already been involved in fraud cases [R7Q2].

Some private parties have become a facilitator of online buying and selling fraud against their will because cybercriminals abuse their legal platforms and infrastructures for cybercrime. By signing the covenant, these parties expressed to take responsibility and to take repressive measures that stop their role as facilitator of cybercrime. Besides this, they expressed the intention to take preventative measures to decrease cybercrime. What these measures are depend on the organizations' role in the process of online buying and selling fraud. For example, Marktplaats can take measures in cases of online buying and selling fraud related to their platform. A possible measure could be the removal of fraudulent advertisements. The banks can take measures to ensure that bank accounts cannot be used several times when it is known that the owner of that bank account is involved in online buying and selling fraud. A possible measure could be that banks block a banking account if the owner of the account is reported at the police several times [R8Q8]. Besides private parties that have become a facilitator of online buying and selling fraud, there are parties involved in LMIO that can play a role in the prevention of online buying and selling fraud. For example, the ACM can play a role in the prevention of online buying and selling fraud by creating awareness by owners of online platforms and online stores, and by carrying out checks. By signing the covenant, the partners have become responsible to take measures to fight and prevent online buying and selling fraud. However, they are free to decide about the way they give substance to this responsibility. A respondent states: "*we have not officially determined what measures a partner must take because that is up to themselves. We cannot tell a bank what to do. We give each other information so everyone can take responsibility and implement the measures that they consider necessary*" [R7Q15]. Another respondent states that the measures are not fixed because partners do not want that: "*then you pin them down and they do not want that. They want to decide themselves and I understand that*" [R8Q8].

In the above analysis shows that in case of LMIO the division of roles and responsibilities is relatively clear. The police collects and analyses reports, and starts investigations under the authority of the public prosecutor. The team leader of LMIO is responsible for the daily operations of the police, and the public prosecutor has the responsibility to ensure that the police operates within the legal borders. Although certain people have been appointed for these roles, the formal roles and responsibilities of the police and public prosecutor have not been assigned but are legally determined. The roles and responsibilities of the other partners of LMIO depend on their role as facilitator in the process of online buying and selling fraud or in the ability to prevent this. The private parties are responsible to take measures they consider necessary to fight fraud based on the information they have received from the police. Each person involved in LMIO is accountable to his or her formal boss in his or her own organization.

In case of the ECTF, the division of roles and responsibilities is relatively similar. By signing the covenant, the partners have become responsible to fight cybercrime that affects the integrity of the digital banking system (eg. phishing, malware, online fraud, DDoS-attacks). In the covenant is stated that the partners of the ECTF collaborate on the basis of three i's: intelligence, investigations and interventions. In practice this means that they share information which allows to take measures to prevent and fight cybercrime [R6Q13]. The role of the police is to collect and analyze reports to put forward criminal investigations. The role of the banks is to take measures like blocking bank accounts, increase internal cyber security measures, inform customers about phishing mails etc.

A difference between the ECTF and all other PPPs included in this research, is that the ECTF is the only case in which all partners physically form a team and sit together in one room. A respondent states: "*You should not only express commitment, but also do it. So when I started as team leader I said: if you think this is important, I need a team with dedicated people. Then I was allowed to recruit them. You*

*have to make strong agreements regarding commitment so you do not have to worry about staff. The banks committed themselves to make one employee available that becomes a part of the ECTF and everybody sticks to it.*" [R6Q9]. The ECTF team consists of a team leader, a financial specialist, a digital specialist, two analysts, one tactical detective and one employee of the fraud department from each bank involved [R6Q18]. For the position of financial specialist, a vacancy has been found on the internet including a job description (see attachment four). This job description shows that the roles and responsibilities of the partners in the ECTF are clearly defined.

Another difference between the ECTF and LMIO is that the public prosecutor is not a regular partner of the ECTF. This is because the ECTF does not conduct criminal investigations, but forwards indications for criminal investigations to the local police units. Because the ECTF team is housed in the office of the Team High Tech Crime (THTC), permission is requested at the public prosecutor of THTC when it is necessary [R6Q7]. The team leader is responsible for the police officers and the daily operations of the ECTF. She is accountable to the supervisory committee. The supervisory committee decides about the long-term strategy and finances of the ECTF. The employees of the banks are responsible for ensuring that what is agreed on or shared within the ECTF, is implemented by their banks. If a bank does not implement the measures or execute other actions, this will be discussed by the team leader in the supervisory committee [R6Q19].

These findings show that the division of roles and responsibilities is relatively clear. In case of LMIO, the division of roles and responsibilities is based the legal powers of the police and the public prosecutor, the role of some parties as facilitator of online buying and selling fraud and the internal (technical) capacities to take measures. In case of the ECTF, the role of the police is also based its legal powers. The role of the banks if based on their analytical and technical capacities to detect and prevent cybercrime. There is a covenant in both cases that has been signed by all parties. In these covenants, the purpose of the cooperation and the associated roles and responsibilities have been described. Because the roles and responsibilities are described in the covenant, their division has been clear right from the start.

**Stakeholder support**

As mentioned in the previous case studies, it has become clear that the category 'stakeholder support' has been defined too broad in the theoretical framework. Similar to the previous cases, LMIO and the ECTF have multiple stakeholders at many different levels with different roles and interests. Therefore, the degree of support can vary greatly per stakeholder and over time.

In case of LMIO, all partners and broader society are stakeholders in the first place. LMIO has been established bottom-up, as a result from a shared need of all partners. Therefore, there has always been a high level of support for LMIO among the founding partners. Yet, this high level of support applies primarily to the people who have been directly involved and has not always been given by the organizations these people belong to. A respondent argues: "*sometimes we really had to defend ourselves hand and tooth against people who had other interests and wanted to abandon the project or take it over because then they could get a subsidy*" [R9Q8]. Yet, it seems like this has changed over time. LMIO was established in 2010 as a program with temporary funds from the police to develop innovative measures against cybercrime [R7Q8]. Already in 2015, the Minister of Security and Justice informed the parliament that LMIO had proven to be effective and that LMIO would be embedded within the new police organization (Van der Steur, 2015). Yet it took till 2019 before a decision was made within the police organization about embedding LMIO. It is decided to embed the functionalities of LMIO instead of the team itself [R8Q18]. Nevertheless, this means that LMIO will remain to exist as a regular part of the police. In the interview, a respondent representing Marktplaats argued that there has always been a high level of support for LMIO within Marktplaats. Among other things, this can be illustrated by the fact that Marktplaats has been a founding partner and a main initiator behind LMIO. Furthermore, there have been cases in which Marktplaats provided funding for costs of systems that the police

needed but could finance [R9Q23]. These findings illustrate that there is a high level of support for LMIO among the partners.

The interviews clarified that the media are an important stakeholder for LMIO as well. A reason for Marktplaats to initiate a collaboration with the police in the first place, was because of negative media attention. According to a respondent, many articles have been published about the lack of effort from Marktplaats to prevent fraud. This resulted in damage to the brand image and provided an incentive for Marktplaats to do something against online buying and selling fraud [R9Q2]. To a certain extent the same applies to the police, since the media wrote about the police that "they did not do anything about it" [R9Q2]. In the last years, this has changed and the media have become an informal partner of LMIO. Tv-shows and magazines such as 'Radar', 'Opgelicht' and 'de Consumentenbond' support LMIO by broadcasting and publishing warnings provided by LMIO [R8Q24]. This illustrates that at this moment, there is a high level of support for LMIO from the media as well.

The ECTF has been established to fight cybercrime that undermines society's confidence in the integrity of the financial system. A respondent argued that this is in the interest of the banks, the police and of society which ensures that all partners are committed to the partnership [R6Q7]. This shows that at least the banks, police and society are stakeholders of the ECTF. It has become clear that not a lot of information is publicly available about the ECTF. This may be due to the fact that this information is related to the cyber security of organizations in the financial system and therefore confidential. This makes it difficult to provide a substantiated answer regarding the level of stakeholder support. However, when the ECTF was established a covenant has been signed by the minister of Security and Justice, the president of the Dutch Banking Association, directors of the ABN Amro bank, ING bank, Rabobank, SNS Bank, the Chief Police and the Chief Public Prosecutor (Government of the Netherlands, 2011). Given that these high placed officials signed the covenant, it seems fair to argue that at least there has been support for the ECTF at the highest levels of the partner organizations at the start. Another expression of support for the ECTF is found in the annual report 2015 of the national police. In this report is stated that the effort of the ECTF results in a better common information position and more effective interventions against cybercrime (Politie, 2015: 34). The high level of support for ECTF is also confirmed by an statement of a respondent: "*There is commitment from all partners. This is also apparent now we need a new covenant due to the GDPR and all partners have said "we want to continue doing this". We are still a bit of a role model PPP"* [R6Q7].

The category 'stakeholder support' is rather broad, making it difficult to provide a comprehensive answer. Nevertheless, the above analysis includes examples of support for both LMIO and the ECTF from different stakeholders at different moments in time. Besides this, both LMIO and ECTF already exist for almost ten years and have become part of the regular police organization. This illustrates that in general the level of stakeholder support for LMIO and ECTF has been high.

**Financial support**

From the moment LMIO was established, several investments have been made by partners. Until now, the police team working for LMIO has always been financed with temporary funds from the police, made available to develop innovative measures against cybercrime. The public prosecutor's office has not provided financial support but contributes in manpower by appointing a dedicated public prosecutor. The private parties such as Marktplaats and the banks have always taken care of their own costs [R7Q8]. Costs that have been made include hiring new employees for fraud, trust and safety departments, software development costs and costs for hiring external consultants [R9Q14]. There has not been a collective budget available for the LMIO as such, but costs have been spread over the partners who could bear the costs at that time. A respondent argues: *"if an API had to be built by the police but they did not have budget available, then Marktplaats paid the bill. So there was a high level of reciprocity"* [R9Q23]. Another respondent states:

> *"there is no collective budget available to build a public-private consortium. We are now exploring how we should continue in the future. I do not think there will ever be a collective budget available including funds from private parties because then the outside world will argue "these private parties have bought influence in criminal investigations". Therefore I think it will continue like this where each partner takes care of its own costs and maybe in the future we will be more like the ECTF and also physically meet up"* [R7Q8].

LMIO will soon be embedded in the regular police organization, making permanent budget available [R7Q8]. A respondent emphasized the importance of a sound financial model and states that this is well arranged in case of LMIO: "*Partnerships like this require that each partner invests. If you are not willing to invest it will never work. A sound financial model is very important because if this is not arranged, you will get unsolvable problems later on. That is why LMIO is a success, each partner contributed either with funding or other resources*" [R9Q23].

Even though there is no collective budget available for LMIO, it is demonstrated that there still is a high level of financial support from the partner organizations. The lack of a collective budget is not considered to be a problem since each partner contributes in a certain way. Besides this, partners seem to be willing to take care of costs that are in the common interest of LMIO and cannot be paid by other parties.

In case of the ECTF, financial support is arranged in a similar way. There is no collective budget available and the costs incurred by the partners are paid by themselves. For example, each bank has made one FTE available for the ECTF team. For matters of continuity, this one FTE is divided over two people that alternate in their presence at the ECTF. In this way, there is always an employee of each bank available. Based on the information that is shared within the ECTF, banks may want to implement new (cyber security) measures to detect unusual patterns and malicious transactions. The activities of banks resulting from their participation in the ECTF are paid by the banks themselves. The national police also provides financial support for the ECTF by employing approximately six FTE that work full time for the ECTF [R6Q8]. Other costs, such as the security screening of new ECTF-employees and housing are paid by the police as well. The lack of a regular collective budget is not considered to be a problem. A respondent argues: "*if we need budget, this is discussed in the supervisory committee. There, the budget will be divided between partners and everybody delivers its part*" [R6Q8]. This analysis illustrates that just like in case of LMIO, the level of financial support is high even though there is no regular collective budget available. The lack of a collectively available budget is not considered a problem as partners are willing to provide financial means in case it is necessary.

**Foundation of PPP**

The interviews clarified that the PPP LMIO can better be described as a network of PPP's than as one demarcated PPP. A team of the police district Kennemerland acts as pivot in the 'LMIO network'. This team operates as the single point of contact for police reports regarding online buying and selling fraud. The first PPP was established when a collaboration agreement was signed between this police team and the 'Overleg Online Handelsplaatsen'. It can be argued that with the establishment of this PPP, the foundation of LMIO has been formalized. The interviews illustrate that three other partnerships have been established between this police team and private parties in name of LMIO. The police team of LMIO has also signed formal collaboration agreements with (1) the major Dutch banks and the Dutch Payments Association, (2) the Authority for Consumers and Markets and (3) Payment Service Providers [R8Q8]. Although the PPP LMIO initially only concerned the collaboration between the police and the 'Overleg Online Handelplaatsen', do the other partnerships also operate in name of LMIO.

The organization structure of LMIO is rather complex, making it challenging to provide a concise answer regarding the foundation of LMIO. Yet, several formal agreements have been signed and LMIO soon will be embedded in the regular police organization. This illustrates that the foundation of LMIO is formalized.

The collaboration within the ECTF has been formalized by a single covenant. At the start of the ECTF, this covenant has been signed by representatives of all partners (Government of the Netherlands, 2011). The formal covenant was necessary to legalize sharing personal information between public and private parties on a regular basis [R6Q11]. Besides this, the covenant has created a shared commitment and allows to address each other if agreements are not met [R6Q7; R6Q9]. Due to the implementation of the GDPR, the current covenant of the ECTF must be renewed [R6Q13]. The new covenant is not finished yet, but given the fact that it will be there in the future it can be argued that the ECTF has a formal foundation as well.

**Relationship between partners**

The relationship between partners in both cases of LMIO and the ECTF is similar. In both cases, partners are relatively equal. There is no hierarchical relationship and decision-making is consensus based [R6Q20]. Roles and responsibilities have been divided between partners and each partner is responsible for the follow-up within its own organization. Implementing the follow-up generally means that the police starts or forwards a criminal investigation and private parties take appropriate measures based on the information they receive from the police. Regarding these measures, a respondent states: "*it is not defined what measures partners need to take exactly, because this is up to the partners themselves to decide. I cannot tell a bank what to do. So we share information and enable everyone to take responsibility"* [R7Q15]. This clarifies that power is equally distributed in the PPPs and that there is no dominant party who decides what needs to be done. However, the public prosecutor has the legal authority to demand information from private parties. The private parties have a legal obligation to comply with this demand. Therefore, the relationship in a PPP between the police, public prosecutor and private parties can never be 100 percent equal. Nevertheless, the level of autonomy of private parties to determine what measures they take and the fact that partners cannot tell each other what to do, shows that partners are relatively equal.

# 6 Findings

## 6.1 Theory vs. practice

In the previous chapter, the case studies have been conducted. It has been examined how the factors included in the theoretical framework are reflected in practice. Based on the case studies, it will now be determined whether the collaboration in the PPPs included in this research can be considered successful, and to what extent the factors in the theoretical framework contributed to this.

### 6.1.1 Factors that may contribute to successful collaboration

In section 3.2, successful collaboration has been defined as: "partners engage in collective and mutually supportive action to achieve certain goals, and satisfaction about the cooperation exist". Given this definition, the findings in the analysis illustrate that all PPPs included in this research collaborate successfully. In all cases, partners seem to be mutually supportive and join forces to achieve a certain public goal. The interviews illustrated a high level of satisfaction and enthusiasm about the PPPs among the partners. Besides this, all respondents have explicitly expressed that they consider the collaboration in the PPPs to be successful [R1Q9; R2Q9; R3Q9 R3Q22; R5Q23; R6Q9; R6Q21; R7Q21; R8Q21; R9Q23; R10Q23]. In order to determine to what extent the factors in the theoretical framework contributed to this success, scores have been assigned to these factors for each case respectively. The overviews of the factors and the scores for each case are provided in tables 2, 3, 4 and 5.

*Table 2:*
*Score of FERM on factors that may contribute to successful and unsuccessful collaboration in PPPs for cyber security*

| | **Mutual trust** | **Goals & interests** | **Roles & responsibilities** | **Stakeholder support*** | **Financial support** | **Foundation of PPP** | **Relationship between partners** |
|---|---|---|---|---|---|---|---|
| **Successful** | ***High*** | *Clear/shared* | *Clear* | *High* | ***Available**** | *Formalized* | *Equal* |
| **Unsuccessful** | *Low* | ***Unclear/diverging*** | ***Unclear*** | *Low* | *Unavailable* | ***Not formalized*** | ***Unequal*** |

Notes:
* Too diverse to provide one comprehensive score
** Collective budget available from 2016-2020, looking for new financial model

*Table 3:*
*Score of CYSSEC on factors that may contribute to successful and unsuccessful collaboration in PPPs for cyber security*

| | **Mutual trust** | **Goals & interests** | **Roles & responsibilities** | **Stakeholder support*** | **Financial support** | **Foundation of PPP** | **Relationship between partners** |
|---|---|---|---|---|---|---|---|
| **Successful** | ***High*** | ***Clear/shared*** | ***Clear*** | *High* | ***Available**** | ***Formalized*** | ***Equal*** |
| **Unsuccessful** | *Low* | *Unclear/diverging* | *Unclear* | *Low* | *Unavailable* | *Not formalized* | *Unequal* |

Notes:
* Too diverse to provide one comprehensive score
**Collective budget available until 2021, unclear after 2021

*Table 4:*
*Score of LMIO on factors that may contribute to successful and unsuccessful collaboration in PPPs for cyber*

| | Mutual trust | Goals & interests | Roles & responsibilities | Stakeholder support | Financial support | Foundation of PPP | Relationship between partners |
|---|---|---|---|---|---|---|---|
| **Successful** | ***High*** | ***Clear/shared*** | ***Clear*** | ***High*** | ***Available*** | ***Formalized*** | ***Equal*** |
| **Unsuccessful** | *Low* | *Unclear/diverging* | *Unclear* | *Low* | *Unavailable* | *Not formalized* | *Unequal* |

*Table 5:*
*Score of ECTF on factors that may contribute to successful and unsuccessful collaboration in PPPs for cyber security*

| | Mutual trust | Goals & interests | Roles & responsibilities | Stakeholder support | Financial support | Foundation of PPP | Relationship between partners |
|---|---|---|---|---|---|---|---|
| **Successful** | ***High*** | ***Clear/shared*** | ***Clear*** | ***High*** | ***Available*** | ***Formalized*** | ***Equal*** |
| **Unsuccessful** | *Low* | *Unclear/diverging* | *Unclear* | *Low* | *Unavailable* | *Not formalized* | *Unequal* |

It appears that in three out of four cases, a 'positive' score can be assigned to most of the factors that may contribute to successful collaboration. According to the existing literature, this would imply that collaboration in these PPPs is successful. Yet, the analysis did not demonstrate that these factors cause successful collaboration. Only for two factors the respondents stated that that they contributed to successful collaboration in these specific cases. These factors are high mutual trust and a formal foundation. Regarding the other factors, the interviews provided the following insights from practice: there is a clear division of roles and responsibilities in most cases, but it is not demonstrated that this contributes to successful collaboration. About 'goals and interests', respondents have argued that it is specifically important that each partner has an own interest in the PPPs besides or instead of a shared common goal. A common goal would not be sufficient for a partner to be committed to a PPP, because in the end he/she will be held accountable by his/her own boss for achieving goals in the interest of the own organization instead of the PPPs' interest. Furthermore, the case of FERM illustrated that collaboration might be successful just because the relationship between partners is unequal and this is accepted by the partners because it is the most workable situation given the context of this specific PPP. Additionally, the cases of LMIO and the ECTF illustrated that the lack of financial support in form of a collectively available budget does not have to be a problem and does not result in unsuccessful collaboration. This illustrates a 'positive' score on the factors in the theoretical framework is not an absolute condition for successful collaboration

Combining these insights results in the following observation: in all cases included in this research, the collaboration in the PPPs is considered successful by the people directly involved. In three out of four cases, mainly positive scores can be assigned to the factors included in the theoretical framework. However, the analysis did not illustrate that collaboration is successful *because* of the positive scores of these factors. It may be possible in practice that there is clarity about roles, a high level of financial support, a formal foundation, shared goals and a high level of stakeholder support, but the collaboration in the PPPs is not successful because the people directly involved are not committed, flexible or willing to work outside their comfort zone. This clarifies that a positive score on all factors included in the theoretical framework does not necessarily result in successful collaboration. Additionally, the case of FERM showed that collaboration can still be considered successful by the people directly involved, even though the analysis resulted in a 'negative' score on most of the factors in the theoretical framework.

Given that all PPPs included this research are considered to be successful by the partners involved and that there are positive scores on the factors included in the theoretical framework in three out of four cases, it is hard to argue that these factors do not contribute to successful collaboration. Yet, a causal relationship between the factors included in the theoretical framework and successful collaboration in PPPs for cyber security in the Netherlands is not demonstrated by the findings of this research. Some findings in this research indicate that there may even be a reverse causation: in some cases it seems

like the collaboration in the PPPs is successful because there is no 'positive' score on the factors. This is most clear in case of FERM, were respondents argued that the collaboration is successful because of a lack of formalities, a lack of a strict rules about roles and responsibilities, and (accepted) inequality. The same applies to the cases where it was argued that collaboration is successful because it serves the individual goals and interests of partners. Individuals goals and interest were considered more important than shared and common goals or interests. Although a causal relationship is not demonstrated by this research, it has become clear that the factors in the theoretical framework seem to fulfill another important role. This will be elaborated in the next section.

### 6.1.2 Sustainable long-term existence of PPPs

The focus of this research is on successful collaboration in PPPs. However, the findings in this research indicate that the factors included in the theoretical framework contribute to sustainable long-term existence of PPPs instead. This has become clear several times during the analysis, which will now be demonstrated.

First, in case of FERM, a yearly collective budget has been available since the beginning. However, the Port of Rotterdam no longer wants to provide financial support. As a consequence, the future of FERM is under discussion. Second, in case of LMIO it has been argued that "*long-term collaboration will be difficult without shared goals*" [R2Q16]. Shared goals are thus considered important for sustainable long-term collaboration. Third, a formal foundation is also considered important for sustainable long-term collaboration: *"then you have something that exists, and no one can just get rid of it or get around it"* [R10Q24], "*it is less voluntary*" [R2Q16]. Fourth, sustainable long-term collaboration will be threatened by a lack of stakeholder support. This can be illustrated with the case of CYSSEC, were it seems like the entire PPP depends on the support of Schiphol as they provide funding for the project organization of the PPP. Additionally, the analysis demonstrated that especially political support may be important for the long-term existence of PPPs. This can be illustrated by the following statement, derived from an interview regarding LMIO:

> "*I secretly organized political attention for LMIO. I arranged that the minister would visit LMIO and would made some promises. Then it all came down to the minister's briefing, so there the lobby comes in. I knew that if the minister would say 'I think this is important and the LMIO must continue to exist', the police chief would have to deal with it as well. It would put pressure on the police chief to ensure that LMIO would remain to exist*." [R9Q19].

This example shows that political support can be a leverage to safeguard the long-term existence of a PPP. It is not unlikely that the same applies to the other factors, as sustainable long-term collaboration may become fragile when the division of roles and responsibilities is unclear or when the level of mutual trust decreases.

It must be noted that successful collaboration and sustainable long-term collaboration are two different things. Successful collaboration is not a guarantee for sustainable long-term existence, and sustainable long-term existence of a PPP does not mean that collaboration is successful. This implies that in practice, even when collaboration within a PPPs is successful, it may be possible that the PPP ends because the preconditions for sustainable long-term collaboration have not been met. The case studies illustrated that this poses a serious challenge to the PPPs included in this research. This will now be clarified.

In all cases, the PPP has been established ad hoc, outside the regular organization structures and with temporary funding. The PPPs can be described as either project- or program based [R7Q3; R6Q8; R10Q8]. In most cases, it has not been discussed at the start of the PPPs how the collaboration would be secured on the long-term. Questions like 'what to do when the PPP is a success?', 'when do we stop?', 'how do we ensure continuity in employees to enhance trust' or 'how will structural funding be arranged?' have not been asked [R1Q24; R2Q25; R7Q24; R9Q24]. After the PPPs exist several years, some partners may begin to withdraw their support for the PPPs. As it is an 'add-on' to the regular

organization, it is easy for organizations to withdraw their (financial) support for the PPP in case of a reorganization or when budget cuts are necessary. This can be illustrated by the following statements:

> *"FERM starts to become publicly known now, but that took three years. Now we can discuss 'should we keep it this way? If so, for who? And what are we going to do exactly? In the end, you will get the question about money again: who is going to pay for it? Now there are four parties who pay 25K each year, but will they keep doing this? Or are we going to do it differently? If we are going to do it differently, will it be viable? These are difficult questions. With the current budget, we have come to a good collaboration and we have organized some nice meetings and crisis exercises. But what is needed if we want to make this sustainable and robust?" [R3Q22].*

> *"We are still working on a sustainable future of LMIO. It is established with temporary funding from the police and public prosecutor for innovative measures to combat cybercrime. (..) Up till now, it has been a temporary structure and Peter Hagenaars is now trying to convert the temporary structure into a fixed structure. The people that work for LMIO have a temporary position. This must be changed into a regular position. We are now exploring the way LMIO will be formalized in the future [R7Q8]. (…) if it is decided to invest the money and FTE's in something else than LMIO, then it will stop. That is the choice that must be made" [R7Q14].*

The fact that PPPs are mainly established ad hoc, outside the regular organization structures and with temporary funding makes the PPPs vulnerable and puts pressure on the long-term existence [R2Q25; R9Q9]. Besides this, the new privacy law (GDPR) makes it more difficult to share sensitive personal information between partners, which is the core activity of the ECTF and LMIO. A respondent argues: "*the new privacy law a provides a big challenge for the ECTF. In the end, nothing goes above the law. So everybody can say that our work is really important, but if the GDPR determines that we cannot do it anymore, than we are done*" [R6Q24]. This illustrates that in case of LMIO and the ECTF, the long-term existence is also threated by the new privacy law (GDPR).

In sum, the factors included in the theoretical framework seem to contribute mainly to sustainable long-term existence of PPPs instead of successful collaboration. Sustainable long-term existence of PPPs will be threatened if there is a "negative" score on these factors. This implies that even though partners collaborate successfully, a PPP may end because the preconditions for sustainable long-term collaboration have not been met. The case studies illustrated that this poses a serious challenge to the PPPs included in this research.

### 6.1.3 Other findings related to the theoretical framework

It has become clear that the factors included in the theoretical framework seem to contribute to a sustainable long-term existence of PPPs. Additionally, the analysis resulted in another finding as well. It seems like some of the factors relate to each other in some way. In some cases included in this research, a positive or negative score on one factor exerts influence on another factor. It may be possible that all factors relate to each other, but it is beyond the scope of this research to conduct an in-depth examination of the relationships between factors. Nevertheless, it is relevant to discuss the relationships that already have become apparent briefly, which will be done in the next paragraphs. It should be noted that these relationships are not by definition casual relationships but show that the factors relate to each other in some way.

The first relationship seems to be between the foundation of PPPs and the division of roles and responsibilities. It has become clear that a formal foundation increases the chance on clarity about roles and responsibilities, and the lack of a formal foundation increases the chance on unclarity about roles and responsibilities. This was demonstrated during the case studies as they showed that in the cases were the foundation of the PPP has been formalized (LMIO, ECTF, CYSSEC), the division of roles and responsibilities between partners has been more clear than in the case were the foundation of the PPP has not been formalized (FERM). This can be explained by the fact that in most cases the formal

contract, agreement or other official document includes a description of the division of roles and responsibilities. When partners sign the contract or agreement, they know what is expected from them and the division of roles and responsibilities is clarified. When there is no formal foundation and partners do not explicitly discuss the division of roles and responsibilities, it is more likely that the division of roles and responsibilities will be unclear. Remarkably, the case of FERM illustrated that the lack of a formal foundation and unclarity about roles and responsibilities does not necessarily result in a low level of trust. All respondents that have been interviewed in case of FERM, explicitly mentioned the high level of trust between partners [R1Q11; R2Q9; R3Q10; R2Q11; R5Q19].

Second, clear and shared goals and interests increase the chance on a high level of trust, while unclear and diverging goals and interests do not necessarily result in a low level of trust. In the cases of the ECTF, and LMIO the importance of shared and clear goals has been emphasized, just like the high level of trust. These cases showed that the more explicitly you can define a common goal that everybody agrees on and everybody has an interest in, the higher the level of trust will be. Among other things, it was argued that "*a shared goal and interest must be clear, because otherwise the collaboration will never work. It must be clear for everyone why we collectively want to do this. In this case, it was clear for all people involved why this had to succeed, so we were in it together*" [R9Q8]. The analysis showed that clear and shared goals and interests strengthens the relationship between partners and thus increases trust. However, the relationship between goals and interests and the level of trust does not seem to be straightforward. The case of FERM illustrated that unclarity about goals and interests causes confusion and creates room for own interpretation of partners. Nevertheless, this did not necessarily result in a low level of trust. As argued in the previous section, all respondents that have been interviewed explicitly mentioned the high level of trust between partners [R1Q11; R2Q9; R3Q10; R2Q11; R5Q19]. One respondent added some nuance: "*I only trust the people involved, and absolutely not the organizations. I do not want to say that the organizations do not trust each other, but in the context of FERM personal trust is higher than trust in the organizations*" [R2Q9]. This illustrates that unclear and diverging goals and interests do not necessarily result in a low level of trust. The opposite seems to be true as well: a high level of trust does not necessarily result in shared goals and interests.

Third, unclarity about goals and interest increases the chance on unclarity about roles and responsibilities. This became apparent in case of FERM but seems also rather logical: if the exact goals and common interests of the PPP are unclear, it will be difficult to determine what must be done in order to achieve the goal and to divide roles and responsibilities between partners. In case of FERM, the lack of a clear goal that would be in the interest of each partner [R2Q5; R3Q5; R4Q5; R5Q5], contributed to the fact that the division of roles and responsibilities has never been discussed [R3Q18; R4Q18]. A visual representation of the relationship between factors in shown in figure ten.

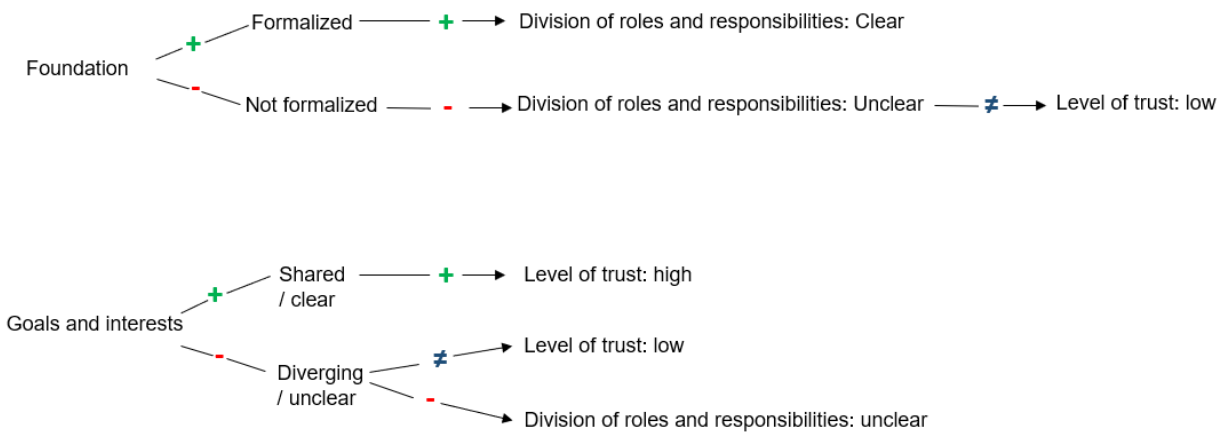


*Figure 10: Relationships between factors based on the findings of this research*

In sum, this analysis illustrates that some factors relate to each other and a positive or negative score on one factor exerts influence on the others. There seems to be a relationship between the factors: foundation of the PPP, division of roles and responsibilities and the level of trust. In addition, there seems to be a relationship between the factors: goals and interests, the level of trust and the division of roles and responsibilities.

### 6.1.4 Governance form

The literature review in chapter three illustrated that PPPs can have different governance forms. However, it did not clarify whether a specific governance form would contribute to successful collaboration. A typology of governance forms of PPPs has been provided in figure 3 in section 3.5.2. The governance forms of the PPPs included in this research will now be categorized according to this typology. Because in all cases included in this research collaboration is considered to be succesfull it is interesting to see whether they have similar governance forms. If all cases would have a similar governance form, it could be possible that this specific governance form contributes to succesfull collaboration.

In case of FERM, the governance form can be described best as a "lead organization-governed network" as defined by Provan & Kenis (2007: 234-237). The Port of Rotterdam is the lead organization in this case, which is responsible for the coordination of activities and main decisions. Although the relationship between partners is equal in theory, practice shows that the Port of Rotterdam fulfills a more important role and exerts more influence than the other partners. In case of CYSSEC, the governance form can be described best as a "network administrative organization" as defined by Provan & Kenis (2007: 234-237). This means that governance of the PPP is centralized through the establishment of a separate and external entity. CYSSEC is the separate and external entity that has been established to centralize the governance of cyber security matters in the Schiphol ecosystem. Although partners of CYSSEC are formally equal, practice shows that Schiphol exerts more influence on the PPP than the other partners. The case of LMIO is similar to CYSSEC. LMIO is the separate and external entity that has been established by the police to centrally govern matters regarding online buying and selling fraud. Even more so, one of the main reasons to establish LMIO was the need for centralization. In practice, the PPP LMIO consists of a police team entering several collaborations with different partners. This resulted in a network of partnerships that is built around the police team 'LMIO'. Even though LMIO operates on an equal basis with all partners that have entered the PPP, it seems fair to argue that the police team LMIO has a leading role in the PPP since it acts as focal point in the network. Therefore, the governance form of LMIO can also be described as "network administrative organization" as defined by Provan & Kenis (2007: 234-237). In case of the ECTF, governance is shared by all partners and there is an equal and horizontal relationship between partners. Therefore, the governance form of the ECTF can be described best as a "participant-governed network' as defined by Provan & Kenis (2007: 234-237). In figure eleven, an overview is provided of the theoretical typology of governance forms of PPPs and the governance forms of the examined PPPs in practice.

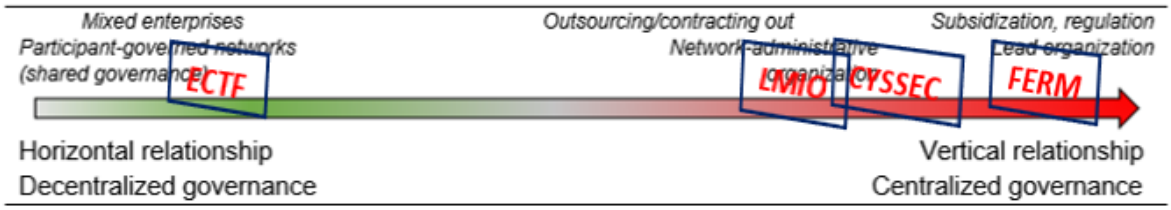


*Figure 11 Classification of the governance forms of the PPPs examined in this research based on a theoretical typology*

This analysis shows that the practical case studies confirm that different governance forms of PPPs exist. Besides this, it illustrates that there is not a specific governance form that contributes to successful collaboration because collaboration is considered successful in all the PPPs while governance forms differ. There does not seem to be one 'ideal type PPP'. The interviews did not provide sufficient information to provide a conclusive answer on the question whether the governance forms of the PPPs have been a deliberate choice or the result of circumstances. The only point that has been stressed several times and is related to governance forms, was the importance of equality and autonomy of partners and consensus-based decision making [R7Q17; R10Q18]. Remarkably, this is somewhat contrary to the governance forms in practice. Taking this into account, together with the history of the PPPs and the processes of establishment, the governance forms seem to be more the result of circumstances than a deliberate and well-considered choice.

### 6.1.5 Number of partners involved in the PPPs

Similar to the governance form, the literature review did not clarify whether the number of parties involved in the PPPs may be a key factor for successful collaboration. Only one author mentioned that given the importance of mutual trust, a PPP "*can only be carried out with selected companies and must be small*" (Dunn-Cavelty & Suter, 2009: 184). In the interviews, the number of partners in the PPPs did not seem a point of discussion. Every respondent has been asked if the PPPs should be extended. The answers of the respondents generally expressed that the PPPs should only be extended if this would contribute to goal achievement. Therefore, it seems like the PPPs have been established with the partners that were considered necessary for goal achievement; the number of partners was inferior. The importance of a small number of partners was only mentioned once: "*LMIO started as a small project. It was a deliberate choice to keep it small, because otherwise it would be too complicated to get things done*" [R9Q16]. This statement has not been verified by the other respondents involved in LMIO. Therefore, case studies have not provided sufficient findings to determine whether the number of partners in a PPP contributes to successful collaboration. By just counting the number of parties involved in the PPPs examined in this research, it becomes clear that in practice the number of parties involved in the PPPs at the operational level ranges from six (ECTF) to 14 (CYSSEC). The number of partners of CYSSEC is still growing since they are still looking for more ambassadors. Also in case of LMIO it seems like many partners are involved. Formally, there are five partnerships but each partnership consists of multiple parties. Although these are not very large numbers, it does not seem like the number of partners in the PPPs has deliberately been kept very small. Due to the lack of information a more comprehensive insight cannot be provided. Whether the number of parties involved in the PPP contributes to successful collaboration remains unclear.

## 6.2 Beyond theory: successful collaboration in PPPs in practice

During the case studies there has been a primary focus on the factors included in the theoretical framework and specific questions related to these factors have been asked during the interviews. As illustrated in section 6.1.1, the case studies did not confirm a causal relationship between the factors in the theoretical framework and successful collaboration in PPPs for cyber security in the Netherlands. When the respondents were asked what factor(s) caused successful collaboration according to them, almost all respondents explicitly mentioned the same factor. Remarkably, this factor was not included in the theoretical framework and will be clarified in the next section.

### 6.2.1 The human factor

The interviews clarified that successful collaboration depends to a large extent to be the ability of partners to make the PPP workable in practice. Workable does not mean a 'positive' score on all factors included in the theoretical framework, but that they are given substance in such a way that the intended collaboration in the PPP is made feasible for those involved. This in turn depends to a large extent on the people directly involved and the specific time and context in which the PPP is established. Practice shows that if the people directly involved in the PPPs want to make it work, they will make it work. This

illustrates that the extent to which those directly involved want to make the collaboration a success and are willing to put extra effort in the collaboration, is to a large extent a determining factor for successful collaboration. The importance of the attitude and personal characteristics of the individuals involved in the PPPs was emphasized by almost all respondents. This can be illustrated by the following statements:

> *"The people are of major importance, enthusiastic people who like to do it. They are not the old traditional police people. Public-private collaboration is a bit of pushing and pulling, giving and taking. This is all part of the game and you should like that to be successful. I think people are the most important thing in the end. It is a strategic game and everyone is aware of that. You must like it and have a feeling for it" [R6Q9].*

> *"All the people involved in the PPP must do things that others say they can't do. They swim against the tide. If the team leader of the police stayed between the lines of the regular organization structure, he would not have anything to worry about. Now he had to explain to his chef that this form of collaboration was really useful. But his chef did not recognize this in the beginning. So you need people who are really willing to go beyond borders. It only works with people who really want to go for it. In that respect we have had a great and enthusiastic team over the years. Yet, it has been a constant struggle and it could have gone wrong at many moments. It is really entirely due to the personal involvement of people such as Jesse and Gijs. If they would not have had such a high believe in it, it would have never worked… also Marktplaats has been supporting and paying over all those years. You need that. Now we are at the point that it is actually very obvious that you would have a collaboration like this, but it has not been like this for years" [R9Q19].*

> *"The high level of trust between partners in LMIO is not due to my effort. It is mainly due to the people with whom we are doing this. They all had this basic character trait allowing trust easily to grow. You have to be able to think in terms of the common interest and in the end you also have to fight sometimes, because only being nice to each other does not result in anything. You must be able to make difficult decisions together. In case of LMIO, we really had to fight and defend ourselves sometimes against people who wanted to abolish LMIO or take it over" [R9Q8].*

> *"The biggest challenge that remains is how to get public-private collaboration done within a classical bureaucratic government organizations such as the police and public prosecutor's office. What we do is sailing in opposite direction, to veer off the beaten track. That is always a struggle and will remain a challenge. Always. I hope that we will always continue to do things that do not fit within the regular organization structure. If you do what you always did, you get what you always got. It's a smasher, but it's true. You must try to be very creative here. I think it remains a major challenge" [R7Q24].*

> *"Public-private collaboration demands that you sometimes must accept things and take on things that are not necessarily up to you. It is very important for the success of such cooperation that parties are not too rigid. If someone does not want to change the things he does, then nothing will change obviously. Therefore, the people involved in the PPP need a specific mindset" [R9Q24].*

> *"(…) you must be able to understand all interests and positions of the other parties involved. It really helps if you have the skills to communicate with everyone" [R9Q19].*

> *"What you actually try to do is to change the internal organization from the outside, while you do not have mandate to make internal decisions. You want them to do things differently than what they are used to. You can just hope for a certain outcome because the only instrument you have is your own enthusiasm to show them why it is a good idea and to convince them that they should approve it" [R9Q20].*

> *"It is about the personalities of the people involved, about their personal attitude. What you see is what you get, we respect each other. There is no politics in the working group, which gives a relaxed and comfortable feeling. Perhaps that is also what we need to tackle difficult problems together. Hidden agendas are scarce in FERM. You can say everything, even if you disagree with someone. This is largely due to the people that are involved [R3Q10].*

> *"You need to get the "right" people are round the table: (1) People that understand the importance of cooperation. People need to be able to think outside their own role and beyond their own interest. You need elasticity of mind; (2) People that can combine this elasticity of*

*mind with a sufficient status in the organization to be able to bring something forward. Someone at operational level may fully agree with you but might not be able to get things done at a higher level; (3) People who want to bring parties together, because in the end everyone is busy with its own career and interest. You need to be able to understand different interests because this makes clear what drives people and why they would cooperate" [R9Q2].*

These findings indicate that the most important factor for successful collaboration in PPPs might be 'the human factor'. The human factor refers to specific personalities and personal character traits that contribute to successful collaboration in PPPs for cyber security in the Netherlands. The interviews clarified that in order to collaborate successfully, it is important that the people directly involved in the PPPs are: motivated, flexible, committed, creative, cooperative, honest, have perseverance, have a trusting personality, are strategic thinkers, are willing to work outside of their comfort zone, are able to think beyond their own interest and are able to convince others. In practice, it may be possible that there is clarity about roles, a high level of financial support, a formal foundation, shared goals and a high level of stakeholder support, but the collaboration in the PPPs is not successful because the people directly involved are not committed, flexible or willing to work outside their comfort zone. Hence, the human factor might be more important than the factors included in the theoretical framework. The importance of the human factor has not been pointed out clearly in the existing literature that formed the basis for the theoretical framework. However, the in-depth empirical case studies allowed to look beyond the theoretical framework which resulted in this new finding. The extent that the human factor contributes to successful collaboration in PPPs for cyber security in the Netherlands should be examined more extensively.

# 7 Conclusion

PPPs are actively promoted by the Dutch government to increase cyber security and safeguard national and economic security. However, not much is known about their working in practice. This research has been conducted to increase practical knowledge about PPPs for cyber security in the Netherlands and to gain insight in factors that may contribute to successful collaboration. By doing so, it has also been attempted to determine to what extent the academic debate about the sense and nonsense of PPPs in cyber security is supported by real cases of PPPs for cyber security in the Netherlands. In order to do this, the following research question has been examined: "*Which factors may contribute to successful collaboration in public-private partnerships for cyber security in the Netherlands?".* Based on this research, it is hard to argue that the factors included in the theoretical framework do not contribute to successful collaboration at all. Yet, the findings indicate that there is no causal relationship between the factors derived from existing literature and successful collaboration in PPPs in practice. Additionally, the findings indicate that the 'human factor' might be the most important factor for successful collaboration in PPPs. This conclusion is based on several findings in the case studies and analysis. This will be elaborated in the next paragraphs.

The following sub-questions have been examined to provide an answer on the main question:

1. What are public-private partnerships?
2. Why are they considered to be relevant for cyber security in the Netherlands?
3. Which factors may contribute to successful collaboration in public-private partnerships according to academic literature?
4. To what extent do these factors contribute to successful collaboration in real cases of public-private partnerships for cyber security in the Netherlands?

A literature review and document analysis have been conducted to examine sub-questions 1- 3. Based on the literature review, a theoretical framework has been drawn including factors that may contribute to successful collaboration according to existing theories. In order to examine sub-question 4, four case studies of PPPs for cyber security have been analyzed based on this theoretical framework. In the next paragraphs, the conclusions related to the sub-questions will be discussed first. Then, the main question will be answered more extensively.

In this research, PPPs have been defined as *"a partnership between at least one public and one private organization to achieve a public outcome that the public organization cannot achieve without the private organization".* The document analysis clarified that there has been an emphasis on the need for PPPs from the moment the Dutch government actively started to invest in cyber security. This is because in many cases the government does not own and/or operate critical infrastructures and processes, which makes it difficult to exert direct influence on their level of cyber security. Participating in PPPs enables the Dutch government to influence the level of cyber security of critical infrastructures and processes they do not own or operate. This in turn enables them to increase the protection of Dutch national and economic security from intentional and unintentional cyberthreats. In sum, it can be concluded that PPPs are relevant because they provide an important means for the government to enhance cyber security and protect national and economic security.

The literature review clarified that several scholars agree on certain factors that may contribute to successful collaboration in PPPs. The factors that are pointed out several times in existing literature are: (1) mutual trust between partners, (2) clear and shared goals and interests, (3) a clear division of roles and responsibilities, (4) high stakeholder support, (5) availability of financial support, (6) a formalized foundation of the PPP and (7) equality of partners. In this research, it has been assumed that these factors may contribute to successful collaboration. A theoretical framework has been drawn including these factors. Besides the seven factors already mentioned, some scholars have pointed out that the governance form of PPPs and the number of parties involved may also contribute to successful

collaboration. Because there did not seem to be general agreement about this, these factors have not been included in the theoretical framework. However, they have briefly been examined after the general analysis in order to determine whether the governance form and the number of parties involved contribute to successful collaboration according to this research.

To determine to what extent these factors contribute to successful collaboration in PPPs in practice, four case studies of PPPs for cyber security in the Netherlands have been analyzed based on the theoretical framework. In the cases of LMIO and the ECTF, the analysis resulted in a positive score on each factor for successful collaboration. In the case of CYSSEC, the analysis resulted in a positive score on six out of seven factors. In the case of FERM, the analysis resulted in a positive score on two out of seven factors. Considering the existing theories about successful collaboration, this would allow to conclude that the collaboration is more successful in the cases of LMIO and ECTF than in case of CYSSEC and especially FERM. However, the interviews clarified that in all cases the collaboration was considered successful. This has been explicitly mentioned by all respondents individually. Besides this, the interviews clarified that even though there is mutual trust, shared goals, clarity about roles, financial support, a formal foundation, stakeholder support and equality of partners, the collaboration in the PPPs can still be unsuccessful because the people directly involved are not committed, flexible or willing to work outside their comfort zone. This clarifies that a positive score on all factors included in the theoretical framework does not necessarily result in successful collaboration. Additionally, the case of FERM illustrated that a negative score on the factors does not necessarily result in unsuccessful collaboration. It is hard to argue that the factors do not contribute to successful collaboration at all. Yet, the findings in this research allow to conclude that there is no causal relationship between the factors derived from existing theories and successful collaboration. The analysis showed that there might even be a reverse causation: collaboration in the PPP may be successful just because of a 'negative' score on the factors derived from theory.

The findings of this research indicate that successful collaboration was predominantly due to the effort of the people directly involved. Collaboration in PPPs has been successful because these people have been able to make the PPP workable in practice. This means that they have dealt with the presence or absence of the factors included in the theoretical framework and gave substance to the PPPs based on the (im)possibilities of the specific time and context in which the PPPs have been established. As a result, all PPPs that have been examined are different. The findings show that there is not one best way to shape PPPs, nor do standard criteria exist that all PPPs should meet in order to ensure successful collaboration. For successful collaboration, the personalities and personal character traits of the people directly involved seem to be the most important. Based on this research, it can be concluded that the 'human factor' might contribute the most and might be the only factor with predictive value for successful collaboration.

Although there is no causal relationship between the factors in the theoretical framework and successful collaboration, the findings in the analysis allow to conclude that these factors seem to fulfill another important role. The sustainable long-term existence of PPPs will be threatened if there is no mutual trust, diverging goals, unclarity about the division of roles, low stakeholder support, low financial support, no formal foundation and inequality between partners. The case studies illustrated that even when collaboration within a PPP is considered successful, it may be possible that the PPP ends because the preconditions for sustainable long-term collaboration have not been met. Successful collaboration and sustainable long-term collaboration are thus two different things. Successful collaboration is not a guarantee for sustainable long-term existence of PPPs, and sustainable long-term existence of PPPs does not mean that collaboration is successful. Based on this research, it can be concluded that the factors included in the theoretical framework might contribute to a large extent to sustainable long-term existence of PPPs, while the 'human factor' might contribute to a large extent to successful collaboration. The analysis did not result in sufficient findings to determine whether a specific governance form or the number of parties involved in the PPPs contribute to successful collaboration.

To conclude, the answer on the main research question will now be elaborated. The main research question of this thesis was: "*Which factors may contribute to successful collaboration in public-private partnerships for cyber security in the Netherlands*?". Based on findings in this research it can be concluded that for successful collaboration, the 'human factor' might be the most important factor and the only factor that may have predictive value. The human factor refers to the personalities and personal character traits of the people directly involved in the PPPs. More specifically, the analysis clarified that in order to collaborate successfully in PPPs for cyber security in the Netherlands, the people directly involved should be: motivated, flexible, creative, committed, cooperative, honest, have perseverance, have a trusting personality, are strategic thinkers, are willing to work outside of their comfort zone, are able to think beyond their own interest and are able to convince others. If 'the right people' are part of the PPPs, collaboration in PPPs for cyber security in the Netherlands may be successful even though the factors that contribute to successful collaboration according to previous research are not (all) present.

# 8 Discussion

## 8.1 Reflection on research implementation

This research has been conducted to gain insight in the practice of PPPs for cyber security in the Netherlands and factors that may contribute successful collaboration. By doing so, the research resulted in practical findings that allow to take a stand in the academic debate about the sense and non-sense of PPPs for cyber security. Case studies have been conducted to create a thorough understanding of the practice of these specific PPPs. Due to the time frame of this research, the scope has been limited to PPPs in the Netherlands and the number of cases has been limited to four. Because of the small number of cases and the sole inclusion of Dutch cases, the findings cannot justifiably be generalized to other PPPs (outside the Netherlands).

To increase the validity of the research, it was intended to increase the representativeness of the respondents by interviewing at least one public and one private partner for every single case. This would have resulted in at least two interviews per case, representing both public and private perspectives on the collaboration. This has not been possible due to busy schedules and sickness of respondents. Nevertheless, twelve respondents have been interviewed of which three originated in private organizations and nine in public organizations. Due to the semi-structured nature of the interviews, it has not been possible to discuss every interview question with all respondents. Therefore, not all interview questions have been answered by all respondents. The questions that have been asked were open questions. As a result, some answers varied widely, were very comprehensive and touched upon all kind of topics not necessarily related to the core of the question. On the one hand, it proved to be difficult sometimes to deduce a concrete answer on a question during the analysis, on the other hand it resulted in valuable insights in the practice of PPPs and the discussion of topics that were not expected based on existing theories. Therefore, the findings are still considered valuable in the context of this research, even though the private perspective remained somewhat underexposed and not all questions have been answered by all respondents.

Regarding reliability, it has been intended to increase reliability by making the coding scheme available and explaining the procedure for recruitment of interview respondents. In this way, the research can be repeated. However, it has become clear that the extent that collaboration is considered successful cannot be seen as a static fact. Collaboration is dynamic and subjected to time, context and interpretation. Therefore, it may be possible that repetition of this research results in slightly different findings.

## 8.2 Expectations vs. results

The literature review (section 3.2 and 3.3) showed that PPPs are topic of extensive academic debate. Multiple studies have been conducted, but general agreement on a common definition is still lacking. The existing literature did not provide one conclusive answer on the question what a PPP actually is and there does not seem to be an ‘ideal type PPP’. Therefore, it was expected that the findings of this research would show that multiple forms of PPPs exist. The case studies (sections 5.2 and 5.3) resulted in findings that meet this expectation. The findings in this research confirm the findings of previous studies because the four PPPs that have been examined in this research all turned out to be different. They differ in the nature of the collaboration, the type of measures they take, the division of roles and responsibilities, the availability of financial support, legal aspects, the stakeholders that are involved etc.

Regarding successful collaboration, the literature review clarified that there are some factors that scholars agree on that would contribute to successful collaboration. These factors have been combined in a theoretical framework, which was tested in this research. Because several scholars agreed on these factors, it was expected that the findings of this research would confirm their contribution to

successful collaboration. Based on this research, it is hard to argue that the factors do not contribute to successful collaboration at all. Yet, the findings indicate that there is no causal relationship between the factors derived from existing theories and successful collaboration and that there may even be a reverse causality. Instead of contributing to successful collaboration, the findings indicate that the factors included in the theoretical framework might contribute to sustainable long-term existence of PPPs. As explained before, successful collaboration and sustainable long-term existence are two different things. Therefore, the results of this study do not confirm the existing theories that formed the basis of the theoretical framework.

Besides the factors included in the theoretical framework, the literature review showed that according to some scholars the governance form and number of partners involved in the PPPs would contribute to successful collaboration. Because the literature review did not provide a clear point of view regarding these factors, a specific outcome was not expected. Yet, it was interesting to see if the case studies would result in specific findings regarding these factors, as this would allow to complement existing theories. However, the findings of this research did not result in a conclusive answer either. If the governance form of the PPP and number of partners involved contribute to successful collaboration remains unclear.

## 8.3 New insights regarding successful collaboration in PPPs

In the academic debate about PPPs, some scholars argue that PPPs will not be successful in practice because of - among other things - a lack of trust between public and private parties, incompatible goals and interests and unclarity about roles and responsibilities (see section 3.4). However, the findings of this study demonstrate that the PPPs are considered successful by the people that are directly involved in the PPPs. This result may be biased due to socially desirable answers, but it should be noted that all respondents expressed that the collaboration between partners is successful. All respondents mentioned explicitly and independently from each other the same factor that, according to them, contributes the most to successful collaboration: the human factor. The human factor refers to specific personalities and personal character traits of people directly involved in PPPs. This research indicated that in order to collaborate successfully in PPPs, the people directly involved should be: motivated, flexible, committed, cooperative, honest, have perseverance, have a trusting personality, are strategic thinkers, are willing to work outside of their comfort zone, are able to think beyond their own interest and are able to convince others.

This research demonstrated that in contrast to the factors in the theoretical framework, the human factor may be the only factor with predictive value for successful collaboration. The importance of the human factor has not been pointed out clearly in the existing literature that formed the basis for the theoretical framework. Therefore, this finding provides an important contribution to existing theories on successful collaboration in PPPs. Regarding the academic debate about the sense and non-sense of PPPs, this research shows that PPPs may not be a panacea but can make sense and collaboration may be successful if ‘the right people’ are directly involved.

## 8.4 Recommendations

This research resulted in some new insights regarding successful collaboration in PPPs for cyber security. However, the generalizability of the results is rather limited due to the small number of cases and the sole inclusion of Dutch cases. It would be valuable to conduct more extensive and thorough research into the extent that the human factor contributes to successful collaboration in PPPs, and to see whether the importance of the human factor will be confirmed by other studies. Further research is required to determine whether the findings of this research can be validated by other cases of PPPs for cyber security. This could be both Dutch and foreign cases. Besides this, it would be interesting to see what specific character traits of the people directly involved result from other studies regarding successful collaboration in PPPs for cyber security. Based on this research, it has been only possible

to provide a rough estimate of the specific character traits that people directly involved in the PPPs should have in order to collaborate successfully in PPPs. Therefore, this should be examined more carefully.

Another recommendation for future research relates to the factors included in the theoretical framework. The research showed that they seem to be important preconditions for the sustainable long-term existence of PPPs. Besides this, it was demonstrated that some factors relate to each other in some way. It might be possible that all factors relate to each other, which could imply that in practice only a few of these factors have to be arranged and others will automatically follow. A more in-depth examination of the relationships between the factors would therefore be valuable.

Besides recommendations for future research, some practical recommendations can be made based on the results of this research. Given the importance of the human factor for successful collaboration in PPPs for cyber security, it can be recommended to take the specific personal character traits that have been pointed out in this research into account when new PPPs are established or new employees for PPPs are recruited. Besides this, the case studies demonstrated that all PPPs included in this research have been established ad hoc, outside the regular organization structure and with temporary funding. When the PPPs were established, it has not been determined how the PPPs would be embedded in the regular organization structures. As a result, these PPPs struggle to embed the PPPs and sustainable long-term existence is under pressure. Therefore, it is recommended to discuss at the start of a new PPPs how the PPPs will be embedded to secure sustainable long-term collaboration.

# 9 Literature


AIVD (2019a). “Cyberdreiging – Welke digitale dreigingen onderzoekt de AIVD?”. Online available at: https://www.aivd.nl/onderwerpen/cyberdreiging. Visited on September 15, 2019.

AIVD (2019b). “Offensief cyberprogramma – Een ideaal businessmodel voor staten”. Online available at: https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2019/06/27/offensief-cyberprogramma-een-ideaal-businessmodel-voor-staten/Offensief+cyberprogramma+een+ideaal+businessmodel+voor+staten_1.pdf

AIVD (2019c). “Wat is nationale veiligheid?” Online available at: https://www.aivd.nl/onderwerpen/over-de-aivd/vraag-en-antwoord/wat-is-nationale-veiligheid Visited on September 20, 2019.

Barriball, K.L. & A. While (1994). “Collecting data using a semi-structured interview: a discussion paper”. *Journal of advanced nursing* (19). Pp. 328-335.

Biernacki, P. & D. Waldorf (1981). “Snowball sampling: Problems and Techniques of Chain Referral Sampling”. *Socialogical methods & research,* 10(2). Pp. 141-163.

Brinkerhoff, D.W. & J.M. Brinkerhoff (2011). “Public-private partnerships: perspectives on purposes, publicness and good governance”. *Public Administration Development, 31*. Pp. 2-14.

Bollen, K.A. (1989). Structural equations with latent variables. New York: Wiley.

Bryman, A. (2008). Social Research Methods. New York: Oxford University Press Inc.

Carr, M. (2016). Public-private partnerships in national cyber-security strategies*. International Affairs*, 92. Pp. 43-62.

Carroll, P. & P. Steane (2000). Public-private partnerships. Sectoral perspectives. In: S.P. Osborne (Ed.), *Public-Private Partnerships: Theory and Practice in International Perspective* (pp. 36-55). London: Routledge.

Clinton, L. (2015). Best Practices for Operating Government-Industry Partnerships in Cyber Security. *Journal of Strategic Security, 8*(4). Pp. 53-68.

CPB (2018). “Risicorapportage Cyberveiligheid Economie 2018”. Online available at: https://www.thehaguesecuritydelta.com/media/com_hsd/report/215/document/cpb-notitie-15okt2018-risicorapportage-cyberveiligheid-economie-2018.pdf

CYSSEC (2019). “Fokko Dijksterhuis, projectleider bij CYSSEC: ‘Een keten is zo sterk als zijn zwakste schakel”. Online available at: https://cyssec.nl/nieuws/2019/10/cyssec-alert-online Visited at October 7, 2019.

DTC (2019a). “Factsheet Digital Trust Center English Version”. Online available at: https://www.digitaltrustcenter.nl/over-het-digital-trust center/documenten/publicaties/2018/08/06/factsheet-digital-trust-center-english-version

DTC (2019b). “Cyberweerbaarheid subsidieontvangers bekend”. Online available at: https://www.digitaltrustcenter.nl/actueel/nieuws/2019/07/25/cyberweerbaarheid-subsidieontvangers-bekend Visited on October 13, 2019.

Dunn-Cavelty, M. & M. Suter (2009). “Public-private partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection”. Center for Security Studies (CDD). *International Journal of Critical Infrastructure Protection* (2). Pp. 179-187.

Eversdijk, A. & A.F.A. Korsten (2015). 'Motieven en overwegingen achter publiek-private samenwerking', *Beleidsonderzoek Online*. Online available at: http://www.arnokorsten.nl/PDF/Samenwerking/Motieven%20achter%20publiek%20private%20samenwerking.pdf

Galletta, A., & W. Cross (2013). *Mastering the Semi-Structured Interview and Beyond: From Research Design to Analysis and Publication*. New York: London: NYU Press.

GOVCERT (2010). “Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010”. Online available at: https://www.tweedekamer.nl/kamerstukken/detail?id=2010Z16848&did=2010D45332.

Government of the Netherlands (2011). “Intensive cooperation between the police, Ministry of Justice

and banks against Internet fraud". Online available at: https://www.government.nl/latest/news/2011/03/14/intensive-cooperation-between-the-police-ministry-of-justice-and-banks-against-internet-fraud Visited on October 11, 2019.
Grapperhaus, F.B.J. (2019). Brief regering; Voortgang integrale aanpak cybercrime - Naar een veiliger samenleving. [Government letter]. Online available at: https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vkzbtbs3qhzt
Havenbedrijf Rotterdam (2016). "Havenbedrijf Rotterdam krijgt Port Cyber Resilience Officer". Online available at: https://www.portofrotterdam.com/nl/nieuws-en-persberichten/haven-rotterdam-krijgt-port-cyber-resilience-officer Visited on October 7, 2019.
Hobbes, T. (1651). Leviathan. Londen: Green Dragon.
Hodge, G.A., and C. Greve (2007). "Public–Private Partnerships: An International Performance Review." *Public Administration Review,* 67(3). Pp. 545-58.
Hsieh, H. & S.E. Shannon (2005). "Three approaches to Qualitative Content Analysis". *Qualitative Health Research,* 15(9). Pp. 1277-1288.
Hueskes, M., Koppenjan, J.F.M & S. Verweij (2016). "Publiek-Private Samenwerking in Nederland en Vlaanderen: Een Review van Veertien Proefschriften". *Bestuurskunde*, 25 (2), Pp. 90-104.
Huxham, C. & S. Vangen (2000). What makes partnerships work? In: S.P. Osborne (Ed.), *Public-Private Partnerships: Theory and Practice in International Perspective* (pp. 293-310). London: Routledge.
Klijn, E.H. & M.J.W. van Twist (2007). "Publiek-private samenwerking in Nederland, Overzicht van theorie en praktijk". *M & O: Tijdschrift voor Management en Organisatie*, 3(4). Pp. 156-170
Linder, S.H. (1999). "Coming to terms with the public-private partnership: A grammar of multiple meanings". *American Behavioral Scientist*. 43. Pp. 35-51.
Leukfeldt, E.R. (2018). "De human factor in cyber security: Intreerede dr. Ruger Leukfeldt". Online available at: https://www.dehaagsehogeschool.nl/onderzoek/lectoraten/details/cybersecurity-in-het-mkb#publicaties-en-projecten
Manley, M. (2015). "Cyberspace's Dynamic Duo: Forging a Cybersecurity Public-Private Partnership." *Journal of Strategic Security,* 8(3). Pp. 85-98.
Mayring, P. (2000). "Qualitative Content Analysis". *Forum: Qualitative Social Research*, 1(2), Art. 20.
McQuaid, R.W. (2000). The theory of partnership. Why have partnerships? In: S.P. Osborne (Ed.), *Public-Private Partnerships: Theory and Practice in International Perspective* (pp. 10-35). London: Routledge.
Ministry of Defense (2019). "Russian cyber operation disrupted". Online available at: https://english.defensie.nl/topics/cyber-security/russian-cyber-operation Visited on September 25th, 2019.
Ministry of Security and Justice (2011). "National Cyber Security Strategy (NCSS): Strength through cooperation". Online available at: https://english.nctv.nl/binaries/cyber-security-strategy-uk_tcm32-83648.pdf.
NCTV (2013). "National Cyber Security Strategy 2: From awareness to capability". Online available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf.
NCTV (2017). "Weerbare vitale infrastructuur". Online available at: https://www.nctv.nl/binaries/Factsheet%20Weerbare%20Vitale%20Infrastructuur%20NL%202018_tcm31-234709.pdf.
NCTV (2018a). "National Cyber Security Agenda; A cyber secure Netherlands". Online available at: https://english.ncsc.nl/binaries/ncsc-en/documents/publications/2019/juni/01/national-cyber-security-agenda/National-Cyber-Security-Agenda.pdf.
NCTV (2018b). "Cyber Security Assessment Netherlands 2018". Online available at: https://english.nctv.nl/binaries/CSBN2018_EN_web_tcm32-346655.pdf
NCTV (2019). "Cyber Security Beeld Nederland 2019". Online available at: https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2019/juni/12/cybersecuritybeeld-nederland-2019/CSBN2019.pdf.

Olsthoorn, S. & J. Koot (2017). “Goede cyberbeveiliging te duur voor MKB-er”. *Financieel Dagblad, Ondernemen,* 25 september. Online available at: https://fd.nl/ondernemen/1219873/goede-cyberbeveiliging-te-duur-voor-mkb-er. Visited on September 26, 2019.

Opstelten, I.W. (2011a). Voortgangsbrief Nationale Veiligheid [Government letter]. Online available at: https://zoek.officielebekendmakingen.nl/kst-30821-12.html

Opstelten, I.W. (2011b). Brief regering; Cyber Security - Informatie- en communicatietechnologie (ICT) [Government letter]. Online available at: https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vivpe8gq5hyh Visited at September 26, 2019.

Osborne, S.P. (2000). Public-Private Partnerships: Theory and Practice in International Perspective. London: Routledge.

Politie (2015). “Jaarverslag politie 2015”. Online available at: https://www.rijksoverheid.nl/documenten/jaarverslagen/2016/05/18/nationale-politie-2015

Potter, W.J. & D. Levine-Donnerstein (1999) Rethinking validity and reliability in content analysis, *Journal of Applied Communication Research*, 27(3). Pp. 258-284.

Provan, K. G., & P. Kenis (2007). “Modes of network governance: Structure, management, and Effectiveness”. *Journal of Public Administration Research and Theory*, 18, 229–252.

Rijksoverheid (2019). “Cybercrime bestrijden”. Online available at: https://www.rijksoverheid.nl/onderwerpen/cybercrime/cybercriminaliteit-bestrijden. Visited on September 26, 2019.

Success (2019). In: *Cambridge Advanced Learner's Dictionary & Thesaurus*. Online available at: https://dictionary.cambridge.org/dictionary/english/success

Vaillancourt-Rosenau, P. (1999). “The strengths and weaknesses of Public-Private Partnerships”. *American behavioral scientist*, 43. Pp. 10-34.

Van den Berg, B., & E. Keymolen (2017). “Regulating security on the internet: Control versus trust.” *International Review of Law, Computers & Technology*, 31(2), Pp. 188-205.

Van der Steur, G.A. (2015). Naar een veiliger samenleving [Government letter]. Online available at: https://zoek.officielebekendmakingen.nl/kst-29628-514.html#ID-489665-d36e119 Visited at October 11, 2019.

Verhagen, H. (2016). “De economische en maatschappelijke noodzaak van meer cyber security – Nederland digitaal droge voeten”. Online available at: https://www.cybersecurityraad.nl/binaries/Rapport_Verhagen_NED_DEF_tcm107-314468.pdf/

USC Libraries (2019). Organizing your social sciences research papier: limitations of the study. Online available at: https://libguides.usc.edu/writingguide/limitations. Visited on September 13, 2019.

WRR (2019). “Voorbereiden op digitale ontwrichting”. Online available at: https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting.

# 10 Attachments

## 10.1 Attachment 1: Overview of interview respondents

Interview respondents:

**FERM**

| Name | Organization | Job description | Interview date & place |
|---|---|---|---|
| Ramon Domen | DCMR | Information security advisor | 6/8/2019, DCMR office |
| Ward Veltman | Port of Rotterdam | Information & cyber security specialist (program manager FERM) | 13/8/19, Port of Rotterdam office |
| Ineke Nierstrasz | City of Rotterdam | Strategic advisor | 15/8/19 City of Rotterdam office |
| Peter van Loo | Deltalinqs | Security advisor | 14/8/19 Deltalinqs office |
| Peter Duijn | Seaport Police | Innovation advisor | 29/8/19 City of Rotterdam office |
| Rene de Vries | Port of Rotterdam | Port cyber resilience officer / harbor master | 20/8/19 Port of Rotterdam office |

**CYSSEC**

| Name | Organization | Job description | Interview date & place |
|---|---|---|---|
| Fokko Dijksterhuis | CYSSEC | Project lead CYSSEC | 23/9/19 Schiphol Group office |
| Laura Andeweg | CYSSEC | Project member CYSSEC | 23/9/19 Schiphol Group office |

**LMIO**

| Name | Organization | Job description | Interview date & place |
|---|---|---|---|
| Jesse van der Putten | Public prosecutor's office | Public prosecutor cybercrime dedicated to LMIO | 21/8/19 Court district Noord Holland |
| Gijs van der Linden | National police | Team leader LMIO | 11/9/19 Police Alkmaar |
| Tom Wagemans | Considerati | Legal representative of Marktplaats | 20/9/19 Considerati office |

**ECTF**

| Name | Organization | Job description | Interview date & place |
|---|---|---|---|
| Caroline Sander | National Police Team High Tech Crime | Team leader ECTF | 29/8/19 Police Driebergen |

## 10.2 Attachment 2: Factors and interview questions

| Factors | Interview questions* |
|---|---|
| General information | Hoe ben je betrokken geraakt bij FERM/CYSSEC/ECTF/LMIO? |
| Goals & interests | **Waarom is FERM/CYSSEC/ECTF/LMIO opgericht?**<br>**Wat is het doel van FERM/CYSSEC/ECTF/LMIO?**<br>Hoe zou je de oprichting van FERM/CYSSEC/ECTF/LMIO beschrijven, hoe is het proces verlopen?<br>**Wat wil jij/jouw organisatie bereiken met FERM/CYSSEC/ECTF/LMIO?**<br>**Hoe wordt binnen FERM/CYSSEC/ECTF/LMIO omgegaan met belangen van verschillende organisaties?** |
| Mutual trust | **Hoe zou je de samenwerking omschrijven?**<br>**Wat zijn volgens jou sterkten en zwakten in de samenwerking binnen FERM/CYSSEC/ECTF/LMIO?**<br>Welke verwachtingen heb je van de leden van de PPPs?<br>**Hoe wordt er binnen FERM/CYSSEC/ECTF/LMIO omgegaan met het delen van gevoelige informatie?**<br>Is de samenwerking echt tussen de partner organisaties of gaat het meer om de personen die betrokken zijn bij FERM/CYSSEC/ECTF/LMIO? |
| Foundation of PPP | **Is de samenwerking geformaliseerd? Zo ja, hoe/waar? Zo nee, waarom niet?** |
| Financial support | **Hoe is de financiering geregeld?**<br>Is er een budget beschikbaar?<br>Zo niet, ervaar je dit als een probleem? |
| Stakeholder support | **Wie zijn er partner in de PPPs?**<br>**Zijn volgens jou alle nodige partners onderdeel van FERM/CYSSEC/ECTF/LMIO? Zo niet, waarom niet?**<br>**Wie mag er wel/niet deelnemen, waarom en hoe wordt dit bepaald?** |
| Roles & responsibilities | **Hoe zou je de rolverdeling binnen FERM/CYSSEC/ECTF/LMIO omschrijven?**<br>Wat is jouw rol binnen FERM/CYSSEC/ECTF/LMIO?<br>**Wie is waar verantwoordelijk voor?** |
| Relationship between partners | **Hoe worden besluiten genomen?**<br>Telt elke stem even zwaar?<br>Levert elke partner een gelijke bijdrage? |
| View on successful collaboration | **Is de samenwerking binnen FERM/CYSSEC/ECTF/LMIO volgens jou succesvol? Zo ja, wat draagt hier aan bij?**<br>Wat zie je als het grootste succes in de samenwerking?<br>**Wat zie je als uitdaging?**<br>**Hoe zie je de toekomst voor je?** |

*Questions in bold are answered by all respondents

## 10.3 Attachment 3: Coding scheme

Note that the keywords are in Dutch because the interview transcripts are in Dutch as well.

| Factor | Score | Keywords |
|---|---|---|
| **Mutual trust** | **High** | Vertrouwen<br>Gezamenlijkheid<br>Hechte band<br>Duurzaam<br>We kunnen op elkaar bouwen<br>We kennen elkaar goed<br>De praktijk heeft zich bewezen<br>Iedereen is bekend<br>Commitment<br>Betrokkenheid |
| | **Low** | Wantrouwen<br>Politiek gedrag<br>Stiekem<br>Er is steeds iemand anders<br>Ze zeggen het wel, maar doen het niet<br>Gebrek aan vertrouwen<br>Er is geen commitment<br>Vraagtekens hebben bij.. |
| **Goals & interests** | **Clear/Shared** | Gedeelde belangen<br>Algemeen belang<br>Hetzelfde doel<br>Collectief<br>Gemeenschappelijk<br>We willen hetzelfde<br>We zitten er hetzelfde in<br>Samenwerken |
| | **Unclear/ Diverging** | Verschillende/andere belangen<br>Eigen belang<br>Tegenstrijdig<br>Dubbelzinnig<br>Eigen doel<br>Ik weet niet waarom de PPPs is opgericht<br>Botsen<br>We zitten er anders in<br>Schuren<br>Uiteenlopen |

| | | |
|---|---|---|
| **Roles & responsibilities** | **Clear** | Duidelijke / heldere rolverdeling<br>Ik weet wat ik moet doen<br>Iedereen weet wat er verwacht wordt<br>Iedereen heeft zijn eigen taak<br>Ik weet waar ik verantwoordelijk voor ben<br>Elke organisatie neemt eigen maatregelen<br>Taken worden verdeeld<br>Het is duidelijk hoe de verhoudingen liggen<br>Verantwoordelijkheden zijn belegd |
| | **Unclear** | Geen rol- of taakverdeling<br>Het is niet duidelijk wie waarvoor verantwoordelijk is<br>Ik weet het niet zeker<br>Onderlinge verhoudingen zijn onduidelijk<br>Ik weet niet wat de anderen doen<br>We doen maar wat<br>Onduidelijkheid<br>Onbepaald<br>Vaag |
| **Stakeholder support** | **High** | De private sector is onderdeel van de PPPs<br>Ik zou niemand toevoegen<br>Alle benodigde partners zijn betrokken<br>(Private) partners zitten aan tafel<br>(Private) partners betalen mee<br>(Private) partners stellen fte's beschikbaar<br>We bepalen samen wat we doen<br>Het is compleet<br>Uitbreiden is niet nodig |
| | **Low** | (Private) partners zitten niet aan tafel<br>De overheid moet het doen<br>(Private) partners hebben andere prioriteiten<br>We weten eigenlijk niet waar behoefte aan is<br>Partijen willen geen moeite doen<br>We krijgen ze niet gemotiveerd om mee te doen<br>De PPPs zou uitgebreid moeten worden<br>(Private) partners ontbreken<br>Niet alle benodigde partijen zijn betrokken |
| **Financial support** | **Available** | Voldoende/genoeg budget beschikbaar<br>Voldoende/genoeg fte's beschikbaar<br>We krijgen subsidie<br>We hebben genoeg geld<br>Financiën zijn geen probleem<br>De locatie wordt gratis beschikbaar gesteld<br>Elke partner stelt iemand beschikbaar |
| | **Unavailable** | Geen/tekort aan budget<br>Geen/tekort aan financiële middelen<br>Tekort aan mensen/fte<br>We doen het er bij<br>Te weinig mensen vrijgemaakt |

| | | |
|---|---|---|
| **Foundation of PPP** | **Formalized** | Geldende wet- en regelgeving<br>Samenwerking is vastgelegd<br>Er is een overeenkomst/contract/convenant<br>Zelfstandige entiteit opgericht<br>Op basis van de wet/artikel<br>Vaste manier van werken<br>Er zijn procesafspraken<br>We hebben ervoor getekend |
| | **Not formalized** | Ad hoc<br>We doen maar wat<br>Onduidelijk wie wat doet<br>Geen procesbeschrijvingen<br>Niks vastgelegd<br>Gewoon zo gegroeid<br>Geen wettelijke/juridische basis<br>Vrijblijvend<br>Geen overeenkomst/contract/convenant |
| **Relationship between partners** | **Equal** | Gelijk<br>Hetzelfde<br>Unaniem<br>Eens<br>Overeenstemming<br>Eerlijk<br>Evenredig<br>Harmonie |
| | **Unequal** | Ongelijk<br>Verschillend<br>Machtsstrijd<br>Wie betaalt, bepaalt<br>Onderscheid<br>Conflict |

## 10.4 Attachment 4: Vacancy 'Financieel specialist ECTF'

**Nationale Politie**
Keywords: Financial crime
Contract type: Permanent employment
Location: Driebergen-Rijsenburg
Education level: Bachelor (EQF 6)
Published on: 16/10/2018
Hours p/wk: 36

**Description:**
Wil jij je financiële kennis en werkervaring inzetten voor het opsporen en bestrijden van cybercrime die de bancaire sector bedreigt? Veel cyberdreigingen worden tegenwoordig vanuit een financieel oogmerk gedaan. Voor de publiek-private samenwerking met de Nederlandse banken zoekt het Team Electronic Crime Task Force (ECTF) van de Landelijke Eenheid een financieel specialist. Ben jij in staat vanuit een financieel oogpunt naar aanvalstechnieken op de vitale financiële infrastructuur te kijken? Kom het bankenteam versterken en sta samen met ons vooraan in de strijd!

**Wat ga je doen?**
Als financieel specialist van het Electronic Crime Task Force voer je complexe (financiële) werkzaamheden uit gericht op projectvoorbereiding. Als specialist deel jij continu informatie op het vlak van cybersecurity, onder andere tijdens het wekelijkse werkoverleg met vertegenwoordigers van Nederlandse banken. Jij weet hoe de geldstromen lopen, kent als geen ander de werking van de financiële markt en brengt samenhang tussen de cyberdreigingen met de cashflow. In deze publiek-private samenwerking werk je vanuit bankenperspectief en stel jij in samenwerking met de banken nieuwe werkmethodieken op. Jij doorgrondt nieuwe financiële ontwikkelingen in relatie tot oude geldstromen en koppelt een transactie uiteindelijk weer aan een natuurlijk persoon. Je houdt zicht op de sterke digitale en financiële aspecten die in de modus operandi voorbij komen en daarmee op de cyberdreigingen die banken en de financiële markten bedreigen.

Met jouw financiële expertise en analytische vaardigheden voer je zelfstandig expertisewerkzaamheden uit in het team. Naast het rechercheren op (financiële) informatie pas je ook (nieuwe) methoden en technieken toe om te komen tot bruikbare informatie, voorstellen, aanpak en adviezen. Je bereidt daarmee een opsporingsonderzoek voor en draagt deze warm over aan het Team High Tech Crime of een opsporingsteam in een eenheid. Vanuit jouw onderzoekservaring en inlevingsvermogen ben jij in staat de vertaling te maken, wat de financiële informatie betekent voor het opsporingsonderzoek.
Je ontwikkelt (nieuwe) instrumenten, methoden en technieken en past deze toe. Je weet deze zodanig te formuleren dat deze ook begrijpelijk zijn voor niet-financieel onderlegde personen. Ook coördineer je activiteiten van medewerkers en je coacht collega's binnen jouw expertisegebied. Bij het ECTF ben je flexibel in het invullen van je werkweek binnen kantoortijden. Gedurende onderzoeken kan het wel voorkomen dat je 's avonds en in de weekenden moet werken. Ook kun je ingeroosterd worden voor bereikbaarheidsdienst.

**Waar ga je werken?**
Het ECTF (bankenteam) is een publiek-private samenwerking tussen de Landelijke Eenheid, de ABN AMRO bank, de ING bank, de Rabobank, de SNS bank, ICS (creditcards), de Nederlandse Vereniging van Banken en het Openbaar Ministerie. Het ECTF richt zich sinds 2011 op de bestrijding van digitale criminaliteit die het vertrouwen van de maatschappij in de integriteit van het financiële stelsel aantast.
Jouw werkplek is het ECTF bij het Team High Tech Crime van de Dienst Landelijke Recherche in Driebergen. Het pand ligt dicht langs de A12 en is zowel met openbaar vervoer als met eigen vervoer

uitstekend bereikbaar. Het Team ECTF bestaat uit vijf collega's, te weten een teamleider, financieel specialist, digitaal specialist, tactisch rechercheur en analist.

**Wie ben jij?**
Je bent de ideale kandidaat als je een onderzoekende geest hebt en je financiële kennis en kunde effectief weet in te zetten. Je signaleert kansen, neemt initiatieven en bent alert op trends en ontwikkelingen. Je levert een inhoudelijke bijdrage aan de werkzaamheden binnen het team op basis van een brede kennis van de financiële wereld en meerjarige relevante werkervaring.
Verder verwachten we:

- een hbo-diploma in financieel-economische richting;
- diepgaande financiële kennis;
- brede onderzoekservaring;
- ervaring in publieke en private samenwerkingen;
- affiniteit met digitale criminaliteit (phishing, malware, money mules).

Source: https://securitytalent.nl/jobs-internships/financieel-specialist (visited on October 19, 2019).