THE CYBER SECURITY PUBLIC PRIVATE PARTNERSHIP IN THE NETHERLANDS

An effectiveness study

Marijn van der Loo
Leiden University
s1914855
First reader: dr.J. Reijling
Second reader: dr. S. Boeke

07-08-'17

Abstract

This thesis comprises a study of how the public and private sectors work together to achieve cyber security, done by an effectiveness study of the Dutch cyber security Public-Private Partnership. Multiple theories of effectiveness are merged into a framework to evaluate this partnership. These are projected on the Dutch National Cyber Security Strategy 2, as well as on six interviews conducted with cyber security professionals, mostly active in the private sector. The discrepancies between the analyses of these two sources of data are taken as points of improvement or at least new study. Three main findings can be distinguished according to this study. First, the WOB-law is causing private organizations to be hesitant to share information with the NCSC, the public partner that is dependent on information from the private sector. Second, the cooperation with public organizations like watchdogs should be improved. How these organizations are cooperating influences the cooperation of the NCSC with the private sector, especially in the information exchange. Third, the information that can be provided by non-critical infrastructure cyber security organizations should be more included in the PPP. This thesis ultimately comes to three policy suggestions regarding these three findings which should be studied more in-depth.

Acknowledgements

First, I would like to thank my supervisor dr. Reijling for his guidance and feedback, even when I decided to change subject at the last moment. I would also like to thank my second reader dr. Boeke for his honest suggestion to change the subject to the current one. Furthermore, I would like to thank the respondents that I had the chance to interview, both for agreeing to the interview itself as for thinking with me and suggesting other respondents from their network. In the three months of writing this thesis, I learned a lot about the profession of cyber security, mostly by speaking to the enthusiastic respondents that I interviewed.

Overall, the process of data collection was slow but successful. All respondents were happy to cooperate and were enthusiastic to speak about their profession. Therefore, it was not hard to make them speak freely about things that do not go well in the cooperation with the government. However, many candidates were approached for the interviews that did not have time in their agenda. During the interviews, the questions that were asked were received enthusiastically with mostly elaborate responses, which indicated that the interview questions were mostly relevant. Even so, many answers were somewhat corresponding between respondents, with few contradicting answers. The respondent from the NCSC largely agreed to the points of criticism from the private sector respondents.

Table of Contents

1. Introduction

1.1. Introduction to the subject

> *"This world -- cyberspace -- is a world that we depend on every single day. It's our hardware and our software, our desktops and laptops and cell phones and Blackberries that have become woven into every aspect of our lives. (...) It's also clear that we're not as prepared as we should be, as a government or as a country. In recent years, some progress has been made at the federal level. But just as we failed in the past to invest in our physical infrastructure -- our roads, our bridges and rails -- we've failed to invest in the security of our digital infrastructure" (President Obama, 2009).*

With this remark on the security of the United States (US) cyber infrastructure, Obama both emphasizes the importance of the cyberspace and the necessity to put more effort in securing it. With the development of the cyberspace, there will inevitably be risks to mitigate. In the contemporary age of information, the influence of cyber security has penetrated most parts of society. This means that the security implications are becoming more evident. To counter cyber threats, governments are obliged to establish cyber security strategies to protect their critical infrastructures (Carr, 2016, p.45). However, other than the more traditional 'physical threats' that indicate possible damage to tangible property, the infrastructures most vulnerable to 'cyber threats' are mostly owned by private organizations, Therefore, according to several policymakers, the private sector should take the responsibility for cyber security, as they are in control of the infrastructures (Carr, 2016, p.56). However, when cyber threats threaten to harm the critical infrastructures, they might become threats to national security involving vital provision of a public service. In this case, they become government responsibility as one of the governments core tasks is to safeguard national security. This indicates the essence of the discussion about responsibility of cyber security. On the one hand there is the private sector, mainly concerned with the financial aspects of cyber threat, and on the other hand is the government with its responsibility for the protection of the Dutch cyberspace and its implications for the society. Therefore, it is necessary for the government to closely cooperate with this private sector to ensure the continuation of the operations of these infrastructures (Clinton, 1996, p.1).

1.2. Introduction to the problem

The currently leading approach of protecting national security from the non-traditional threat of cyber to the critical infrastructures, is cooperation between the government and private organizations through the establishment of Public Private Partnerships (PPP) (Carr, 2016, p.43). With this, the information sharing between the public and private world should be improved which would lead to higher levels of Critical Infrastructure Protection (CIP). The concept of the PPP is not new, as it was already established in the 1970s. Although the necessity of cooperation between the government and private organizations is widely accepted nowadays, the functioning of the PPP's is not free of criticism (Dunn Cavelty & Sutter, 2009, p.2). The private sector is considered to be the most appropriate to counter cyber threat, because of the expertise it has in the field of IT and its possession of the largest part of the critical infrastructures. However, it is the government's responsibility to protect the critical infrastructures as disruption would mean threat to national security and the nation to function properly (Gray, 2013, p.155-156). This brings a tension in the cyber security provision that arguably can only be overcome by a mature and sound partnership between public and private sector. It is therefore interesting to provide insights in how this cooperation between government and private companies is taking shape in different countries.

1.3. Introduction to the discussion

Madeline Carr (2016) conducted research on this topic by studying the cyber security PPP in the United Kingdom (UK) and in the United States (US). Her findings mainly encompassed that although partnership is necessary when protecting critical infrastructures that are in private hands, there are some difficulties in the way the partnership works in the UK and the US. Those problems were mostly to be found in the different perception of and motivations for cyber security between the public and the private sector: the government through a national security perception due to the critical infrastructures and the private sector through a profit-driven business perception (Carr, 2016, p.60). These different perceptions do not always align when it comes to policy. Therefore, the shared responsibilities that a PPP suggests was in fact not evident, as the end goal of the partnership was different for the public and the private sectors. Due to the problems that are presented by Carr (2016), it would be interesting to conduct research on the extent to which these findings comply with cyber security PPP's in other countries. Therefore, this thesis will follow the structure for Carr (2016), but with a focus on

the Netherlands and with a newly created theoretical framework with multiple elements of evaluating partnerships. Projecting these elements on the Dutch cyber security PPP can add to the current understanding of the PPP as well as on how it functions in the Netherlands and how it might be improved. As the outcomes of studying cyber giants like the US and the UK like Carr (2016) did may be different than other countries like the Netherlands, this study is useful to gain insights on the relatively new study on the cyber PPP. The choice for the Dutch PPP will be further elaborated on in section 1.6.

1.4. Knowledge gap and relevance

This thesis will not solely aim at the policy side of PPP's in cyber security governance. Instead, this thesis will take a more focused approach, by zooming in on the perception of the PPP by both public and private organizations. Several theories and measurements on the evaluation of partnerships will be used to try and give an answer to the question whether there is a difference in the constituted goals of the PPP's and their actual performance, as perceived by the private organizations. By doing so, this thesis will add to the body of knowledge by making a comparison of the government intentions of the cyber security related PPP and how the private sector perceives it in the Netherlands. This will give an insight on how successful the cyber security PPP is and if this should indeed be considered as the most effective way of governing cyber security. Moreover, it will expose the bottlenecks that the current Dutch cyber security PPP experiences. Few studies have been conducted so far to the perceived effectiveness of the cooperation through PPP regarding cyber security, other than the study of Madeline Carr (2016). Combined with the need for mature cyber security policy due to increased cyber threat all over the world, this study can be a useful contribution.

The societal relevance of this research subject lies in the creation of clarity regarding the governance of cyber security. The PPP is by many considered as the way to go for the critical infrastructure protection by securing the cyberspace, but not without criticism (Dunn Cavelty & Suter, 2009, p.2). Moreover, cyber security is often perceived as a unique security sector (Hansen, 2009, p.1157) and the functioning of the PPP to govern this sector can be questioned. This thesis is therefore aimed to add to the discourse of how the cyber governance through PPP's taking shape by shedding light on the relationship between government and private sector. To do so, this thesis will look at the functioning of the cyber security PPP and

the possible implications of discrepancies in this relationship. The scientific relevance must be sought in the measurement of the effectiveness of the PPP when it comes to non-traditional threats like cyber threats. By doing so, this thesis will contribute to the question whether the PPP is an effective approach in the search for critical infrastructure protection through cyber security. Moreover, this study can be used as a network analysis to find possible weak spots in the 'network' of the Dutch cyber security PPP.

1.5. Case and data selection

The reason for choosing the Netherlands is firstly because of its relatively high percentage of internet users, with 94 percent of households connected to the internet (Nederlands Dagblad, 2016). This indicates that the Netherlands has a mature cyberspace, which makes it an interesting unit of analysis for a cyber related study. Therefore, with the high levels of internet connectedness, it can be expected that the cyberspace influences many infrastructures in the Netherlands. Consequently, this means that there must be a sizable amount of government policy to protect the processes of these infrastructures.

Another reason for studying cyber security in the Netherlands comprises the relatively large amount of bandwidth and for its internationally important role as an internet hub, through which digital attacks can be transited (Cyber Security Beeld Nederland, 2016, p.20). Moreover, the Amsterdam Internet Exchange (AMS-IX), biggest internet node in the world, is based in the Netherlands which emphasizes the importance of the Netherlands as a data hub (Cyber Security Raad, 2017, p.5). This makes the cyberspace in the Netherlands an important critical infrastructure that is worth studying on how it is protected.

The last reason for choosing the Netherlands is the political climate of the Netherlands, which is arguably different than from world powers like the US and the UK, among others when considering the Dutch culture of consensus building through the *polder model* (Clark, 2014, p.29). Therefore, it would be interesting to see how this cooperation between private and public worlds takes shape in the Netherlands. To do so, this thesis will study formal policy documents, more specifically the Dutch National Cyber Security Strategy 2 (NCSS2) in conjunction with relevant actors in the field that are involved in the execution of formal policy. This is done to obtain an understanding of the true role of the PPP as conceived by the government

policymakers and especially by the private parties that are involved. How they evaluate the relationship with the government can have implications for the success of the cooperation.

1.6. Research question

To add to the discussion of cyber security partnership, this thesis will aim to shed light on the effectiveness of the Dutch cyber security related PPP. This on the background of how the PPP's are constituted in the Dutch national cyber strategy, to ultimately see if there are discrepancies on how the Dutch government have planned the PPP to raise cyber security and how it works out in practice. To give an answer to these questions, the following research question will be used in this thesis:

> "How is the cooperation between the government and the private sector regarding cybersecurity through Public Private Partnership as constituted in the National Cyber Security Strategy 2 taking shape and how can possible discrepancies between this strategy and the perception of the private sector be explained?"

With this research question, this study can tell us multiple things about the governance of cyber security. Firstly, this will shed light on how the Public Private Partnership functions in the Netherlands and whether it contributes in an effective manner to the protection of the critical infrastructures that are connected to the Dutch cyberspace. Secondly, it can provide insight in which processes are functioning and which do not, something that can accordingly be transformed into new policy to improve the cooperation.

1.7. Structure of the thesis

To find an answer to the presented research question and therefore contribute to solving the presented problems, this thesis will follow the following structure. First, the theoretical chapter will present an oversight of all existing theories on cyber security, cyber threats, partnerships to overcome these threats and different ways of assessing these partnerships on effectiveness. Then, these different theories will be used to form the theoretical body of this thesis. Hereafter, this theoretical body will be transformed into a methodologic chapter in which the scientific

methods and data will be presented, accompanied by a reflection on these methods. Accordingly, the NCSS2 will be studied through a document analysis, using the analytical framework as constituted in the theoretical chapter. Subsequently, the same analytical framework will be used to make an analysis of the empirical data, collected through the conduction of interviews with cyber security professionals involved in the Dutch cyber security PPP. Thereafter, the findings of the two analyses will be compared to see if there are evident discrepancies. These analyses will therefore contribute to the discussion on what is the best approach on countering cyber threat by looking at to what extend the PPP is the right path for cyber security establishment and how it can be improved by looking at tensions in the partnership. Ultimately, the findings of these analyses will be interpreted in the final chapter, in which also will be reflected on the study. The meaning of the findings and how this may lead to new policy or new studies in the future will be questions that will be answered in this chapter.

2. Theoretical Framework

In this chapter, the relevant concepts and theories will be discussed that are necessary to conduct this study. To begin with, the concepts of cyberspace, critical infrastructure and its protection will be elaborated on to clearly define and determine their governance and their implications. Then, the role of the PPP in cyber security will be discussed: why is the PPP approach desirable and how did it develop? Hereafter, this chapter will continue to elaborate on what characteristics a successful PPP's must have which will lead to the analytical framework that this thesis will use.

2.1. Cyber security

The first concept to discuss is cyberspace, to determine why it should be secured through national security strategies. Cyberspace is the newest domain known to mankind. Besides the traditional land and sea and the more recently added airspace and outer space, cyberspace is the fifth domain that humans can move around in (Kuehl, 2009, p.1). This newest domain can be defined as "Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange information via networked information systems and physical infrastructures" (United States, 2006, p.3).

As Dutch society is embedded with high levels of ICT intensive processes, the cyberspace includes the operations of many of the Dutch infrastructures. As the economy thrives on the interconnectedness caused by the internet, simultaneously it becomes dependent on these operations facilitated by the internet. This makes the ICT important for the critical infrastructures, as it facilitates employment, communication and a crucial driver of socio-economic growth and development (Klimburg, 2012, p.1-2). Based on the predictions made in the Dutch National Cyber Security Framework Manual, five billion people will be connected to the internet and fifty billion objects and devices will be connected in the year 2022. This would have impact on politics, economy, social life and national security of all countries. However, the way these countries choose to protect these infrastructures may differ due to deviating opinions on the economy and security trade-off (Klimburg, 2012, p.4).

Before diving into the study of the cyber security PPP in the Netherlands, it is firstly important to define the objective of this construction, which is establishing cyber security to protect the Dutch critical infrastructures connected to the cyberspace. Therefore, the first

determinations that must be made are based on the traditional trifold of security: security for whom, security from what and security by what means (Carr, 2016, p.50).

2.1.1 Cyber security for whom

Cyber security for whom will normally refer to the security of the state or national security (Hare, 2010, p,15). The state in this case comprises three components. The first component is the security of the individual. As one of the state's responsibilities is to keep its people safe, the interests between the state and its people is considered to be conflated (Carr, 2016, p,50). Therefore, the state needs to secure itself to be able to protect its civilians. There are however exceptions, of which the most prevalent is the tension between security and privacy. This tension encompasses the data gathering to protecting the liberties of society. In other words, appropriate violation of the privacy rights of the individual may be allowed to serve the greater good, being the security and societal freedom (Carr, 2016, p.50).

The second component is the economic impact that cyber threat can pose, as the business sector is essential for the national economy. The success of the business sector is of significant influence of the prosperity of a society and therefore it must be protected. The financial burden of a security breach in the cyber infrastructure may be significant, making it a matter of state security and therefore fit for the national security strategies (Carr, 2016, p.50-51). The third component of state security comprises, after the individual and the economic security, the security of the internet itself. As not only do individuals and businesses use the internet and should be protected through that way, the internet itself faces threats as well. With this, the proper functioning of the internet should be safeguarded whereby it can be used to its fullest by individuals and businesses. In the US for example, the internet was made a 'strategic national asset' (Carr, 2016, p.51) by former president Barack Obama, which made its security from then on, a 'national security priority'. This makes the importance of protecting the internet even bigger; security of the internet does not only mean that the internet itself should be protected, also its users (Carr, 2016, p.51).

When determining for whom cyber security is most important, multiple problems emerge. If it is the individual in a country, the problem arises that sometimes the state is the one that the individual should be protected from, in form of privacy. When the businesses are the referent object, it would be expected that the private sector contributes more to cyber security. Otherwise, cyber security would become a business subsidy. When the internet itself is meant

when regarding cyber security, even more issues may arise when establishing cooperation to create cyber security (Carr, 2016, p.51-52).

2.1.2. Cyber security from what

Threats to national security are often specified as actors like criminals, terrorists, and other states with hostile intentions (Carr, 2016, p.52). When analyzing the threats that can be posed to society, two main fields can be identified. The first is the economy, as briefly touched upon in the previous section. The second is especially important for the scope of this thesis: the critical infrastructures. When the US presented its first cyber security strategy in 2003, president Bush warned for the consequences of a cyber-attack, by saying that such an attack could disrupt economy, national security, and the nations' critical infrastructures. Allegedly, small numbers of hostile hackers with small budgets would be able to disrupt societies by attacking critical infrastructures. Critical infrastructures are, according to this strategic document, infrastructures that when disrupted can cause harm to public health and safety of the concerning country (Dynes, Goetz & Freeman, 2007, p.15). This suggests that given that most critical infrastructures are connected to cyberspace, they may require government regulation when the business objectives do not leave room for adequate protection of society (Dynes et al., 2007, p.16).

As the Dutch National Coordinator for Security and Counterterrorism (NCTV) states, the critical infrastructures in the Netherlands are "Critical processes are processes that could result in severe social disruption in the event of their failure or disruption" (NCTV.nl, 2017c). As for the Dutch society, the NCTV has categorized these processes into A and B, with A processes being bigger in magnitude than B processes. Both categories are based on estimation of potential disruption of three of the following criteria: economic impact, physical consequences, social impact. Category A differs from B that it is also supposed to have a cascading effect on at least two more sectors. Although the ICT/Telecom sector according to the NCTV falls into category B, it is considered to be a critical infrastructure. This means that disruption of any kind may implicate around five billion euro in damage regarding the economic impact, more than a thousand-people dead, seriously injured or chronically ill. It is because of this estimated potential impact that the ICT/Telecom sector is considered a critical infrastructure which means it is government responsibility to protect. This resulted in the first Dutch National Cyber Security Strategy in 2011, followed by a second, revised version in 2013 (EU Cybersecurity Dashboard, 2015).

2.1.3. By what means: Public Private Partnerships

After having set out what needs to be protected and why this is important, this thesis will continue by looking at how cyber security can be established. As concluded in the previous section, critical infrastructures play an important role in the discourse of cyber security. In securing the cyberspace and its critical infrastructures, the leading approach is that public and private parties should cooperate in PPP's. With these constructions, the overarching aim of improvement of information sharing should be encouraged between both sectors (Carr, 2016, p.53-54). Moreover, as the state is responsible for national cyber security (Guitton, 2013, p.23), it must create influence over the critical infrastructures, for reasons discussed in the previous section. And with these infrastructures largely owned by organizations from the private sector (Dynes, 2007, p.16), close cooperation through PPP's seems to be essential for the states wellbeing.

The concept of PPP is not new, as PPP's were used as soon as in 1825 with the creation of the US Erie Canal (Manley, 2015, p.85). Initially, the structure of PPP was mainly used for the construction of major projects like bridges, roads, and water systems (Savas, 2000, p.7). With the idea of a partnership, a middle road was taken in the discussion of nationalization and privatization: it was not either one of the sides, but success should be sought in connecting the two ends (Wettenhall, 2005, p.22). The PPP later also became useful for contracting out of services and the creation of hybrid risk-sharing organizations (Skelcher, 2005, p.347). However, few other areas seem to need a PPP than the cyberspace. Given the fact that the emergence of the cyberspace always has been one of a bottom-up self-governance approach, government legislation had marginal effect, although the critical infrastructures were affected (Kleinwachter, 2003, p.1105). Regardless the rise of the popularity of the approach, the PPP cannot be interpreted as an absolute solution and should be reviewed and criticized. Therefore, several frameworks were being created to evaluate the success of a PPP. Which conditions and characteristics does a partnership has to have to be successful? Moreover, after multiple cyber security breaches in the period of 2000 until 2015, an urge for definition of the structures of PPPs emerged (Manley, 2015, p.85). In this period, multiple conceptions emerged about how a cyber security PPP could be constituted and what characteristics would make them successful. Therefore, several conceptions where developed to evaluate the effectiveness of a PPP. To formulate the conception of what a successful PPP looks like, a brief overview of the PPP will be provided. In this overview, some different conceptions will be discussed, before turning to the Dutch cyber security PPP.

2.2. Constitution and effectiveness of a Public Private Partnership

Now that the establishment of the concept of PPP has been discussed, this section will continue to discuss the elements of a partnership that are of influence when discussing the effectiveness of a PPP. In other words, what elements of a PPP causes it to be successful? Traditionally, the public sector was supposed to be involved with and responsible for public interest, stewardship, and the consideration of solidarity. Moreover, the public sector was accounted with social responsibility and environmental awareness. On the other hand was the private sector, which was involved with the accessing of finance, technological knowledge, managerial efficiency and commercial tendencies. Moreover, the private sector is considered to be more adaptable to change, economic progress, and executing technical tasks. In an ideal partnership, both sectors are supposed to combine their strengths and complement the weaknesses, in order to accomplish the best result possible (Rosenau, 1999, p.11).

As discussed before, partnership between the public and the private sector has been around for some time, but the study of the positive and negative elements of such a partnership is relatively new (Börzel & Risse, 2002, p.1). One of first academic works that has been written about the modern PPP is the article by Stiglitz and Wallstein (1999). In their work, they define the PPP as "a relationship in which each partner is assigned specific responsibilities and given incentives and resources to fulfill those responsibilities" (Stiglitz & Wallstein, 1999, p.57). The ideal partnership is constituted out of parties with the same objectives, but this is no necessity for a partnership to have success. When a partnership only has some common interests, it must have appropriate incentives and accountability among the parties involved. However, although cyber security seems to be a shared wish of private and public world, it is for different reasons. This may not be a problem, but it becomes one when the costs of a cyber security breach become less than preventing one, the profit based private sector will no longer see purpose of cyber security in their business model (Carr, 2016, p.57).

Wettenhall (2003) adds to the idea of cooperation between government and private sector, which is the new way of public management characterizing the liberal democracy. Although some form of participation and cooperation seems to fit the contemporary society, it is important to formalize and make the partnerships concrete. Without doing so, the concept will remain subject to discussion and will be interpreted differently by different parties. However, the fact that the government advocates partnerships by creating "partnerships with society" (Wettenhall, 2003, p.79) seems to be a potentially useful concept but should not remain

vague rhetoric (Wettenhall, 2003, p.78-79). Wettenhall (2003) then continues by distinguishing two types of cooperation: horizontal and vertical. In the first type, decision-making happens through consensus among parties, suggesting equality between the parties involved in the partnership without one single strong party. The second type does have one leading actor, and can therefore be characterized as vertical. This leading actor can make decisions alone without consulting the other parties. A functioning partnership supposedly knows a horizontal structure, wherein all parties have a say (Wettenhall, 2003, p.90). This is in line with the conception of Börzel and Risse (2005). They identify that only two types of successful PPP's exist, both characterized by their non-hierarchical structure. The only distinction that they identify is the way that decision-making takes place: in the first conception, the government uses incentives and bargaining as tools, in the second conception a less manipulative approach is taken. In this latter conception, the partnership is based on soft persuasion like learning and discussion (Börzel & Risse, 2005, p.3). Another change in the conception of the PPP was that, instead of the initial goal of cost reduction, PPP's became an instrument to improve the quality of policy on certain subjects. In other words, the PPP was first conceived as an instrument to cut public spending by working together with the private sector. However, the more recent concept mainly encompassed the creation of effective policy instead of merely economic interests (Klijn, 2009, p.27).

When moving to the critical infrastructure protection, the question is not anymore if the concept of PPP is an asset, but how a PPP is, or should be, structured (Dunn Cavelty & Suter, 2009, p.2). A PPP in critical infrastructure protection is often formal and based on shared goals and interdependence to accomplish these goals. However, different is that in the PPP's discussed before, the overarching goal of the PPP was the creation of cost benefits for the government (Wettenhall, 2003, p.81). When discussing PPP's in critical infrastructure protection however, more focus goes to the sharing of information to enhance security (Dunn Cavelty & Suter, 2009, p.2-3). However, this is not the only variable that determines the success of a partnership.

Having discussed several approaches towards cyber security through partnership between public and private sector, is becomes clear that the existence of the PPP is not in its end form yet. Multiple aspects are subject to discussion and cannot count on consensus among all parties. However, some cooperation seems necessary as the government is responsible to protect the infrastructures and the private sector has the tools to do so (Carr, 2016, 54). However, the discussion about the cyber security PPP often remains in the theoretical details.

Manley (2015) developed a more sophisticated fourfold to assess the effectiveness of a partnership between government and private sector. As addressed upon briefly before, this assessment is based on *trust, clear legal guidance, bottom-up structural approach,* and *community involvement (*Manley, 2016, p.90). These four elements should all be working appropriately to ensure the effective information sharing between government and private sector. Therefore, this will be the basis on which the cyber security PPP in the Netherlands will be assessed. However, these four elements will be complemented with indicators from other theorists that will be useful for this study. The four should not be interpreted as separate categories, as they all build on each other as presented in Figure 1. The elements will be complemented by indicators from other scholars that can be categorized under the according element. In this way, a comprehensive body to assess the effectiveness of the cyber security PPP will be created, including all important works on partnerships created so far.

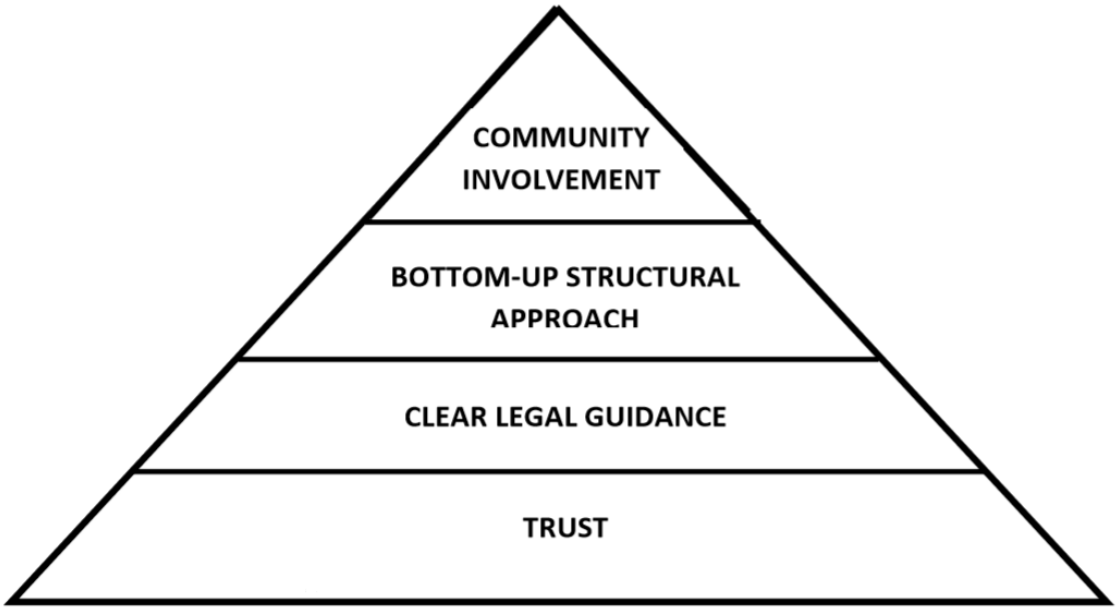

Figure 1: Pyramid of the four elements as described by Manley (2015)

2.2.1. Trust

The rhetoric of trust between the involved parties is essential as it shows confidence in the partnership. With the common goal of the parties as a long-term objective, it is important to establish trust among both private and public organizations. This can happen through transparency, publicly stating the confidence in the partnership, but also through small gestures

to show appreciation and even personal relationships (Manley, 2015, p.90) However, besides these signs of goodwill, there are also some bottlenecks which can trouble the trustworthiness of the relationship and should be overcome. For example, a prevalent issue is the tension between security and privacy that has been discussed before (Carr, 2016, p.50). Private organizations do not share information about their business easily with the government, as this can potentially harm their operations. Sharing this data would require high levels of trust, because the private organization must be certain of the integer handling of this information by the government (Manley, 2015, p.91). It can therefore be said that the relationship and the credibility of the government regarding dealing with information gained by the government through a PPP is essential for the success of the PPP. Moreover, when one or more parties that are involved in the partnership are trying to take the lead in the partnership, this can result in an obstacle in the strive for success of the partnership (Osborne, 2000, p.298). According to Osborne (2000), this does not mean that all parties must be completely equal. It does mean that not one party is clearly striving for the lead, as this may harm the trust of other parties towards the partnership. When one party does so, a situation of 'point-scoring' might occur, which has negative influence on the partnership (Osborne, 2000, p.299). In short, trust building happens through multiple ways, including the elements that will be described in the next sections.

2.2.2. Clear legal guidance

The second element of the assessment of the success of a PPP is the constitution of legal guidance to create effective cooperation. Doing so will create a clear framework of how the cooperation should work and what the parties can expect from each other. These expectations can be formalized through both non-binding collaborative and binding contractual agreements, depending on the nature and objectives of the partnership and with both their strengths and weaknesses (Manley, 2015, p.92). In cyber related PPP's this legislature will comprise how the government trades off its expertise and resources as an incentive for the private parties to stimulate the information sharing. On top of that, which government organizations are responsible for which legislation should be clear for the private sector (Manley, 2015, p.94). The use of incentives only works when the partnership is structured well (Zhang, 2005, p.4). This makes the PPP somewhat of a mixture between collaborative and contractual (Manley, 2015, p.93-94). The government does not order private companies to share their information, but rather incents them to do so by giving trainings and resources in return. The government

can also try to ensure quality of the private sector by setting up minimum requirements or regulations for the projects initiated by the private sector. By doing so, a positive climate is being established in which the private sector knows what the acceptable standards and quality are, which will benefit the partnership (Zhang, 2005, p.4).

Another indicator that somewhat follows out of the latter and is necessary for a successful partnership, is accountability. The notion of accountability can also be categorized under the element of clear legal guidance, as it regards holding parties accountable for their responsibilities. Rosenau (1999) states that accountability mechanisms are essential, as they cause both public and private sector to fulfill their responsibilities towards each other and towards the critical infrastructures they might act in. Other than in the past, now the private sector organizations have the largest part of those critical infrastructures in hands. However, accountability mechanisms are tested when those critical infrastructures are in danger of disruption (Rosenau, 1999, p.19). Therefore, the accountability should be constituted and ensured through clear legal guidance.

Clear legal guidance may come through clear structure of the partnership, but also by using incentives and the clear constitution of partnership goals (Rosenau, 1999, p.21). The most evident reason for the necessity of clear legal guidance to ensure accountability is the role of the government as the last resort. In situations in which critical infrastructure processes face acute danger of disruption with all its consequences for the nation, the public sector becomes the 'last resort' for providing the critical services (Rosenau, 1999, p.20). This means that the government can step in when the dangers becomes apparent and therefore becomes accountable for the critical infrastructures. It is therefore necessary for the public sector to create standards and regulations to assure that the government does not have to step in. This is because the government will be held accountable in the end when critical services disrupt. Clear legal guidance is therefore necessary for governments to ensure that the critical services remain fully operational (Rosenau, 1999, p.19).

2.2.3. Bottom-up approach

The next element of a successful PPP is the existence of a bottom-up approach. As said, when discussing the legal guidance of the PPP, the partnership is not meant as a structure in which the government orders the private organization to do things that are considered by the government as protection of the critical infrastructures. Instead, to achieve success of the PPP, it is important to actively consult all parties involved about the way the partnership is

functioning. Considering the goal of this partnership, which is improved information sharing, it is found to be important that all parties feel like they are on the same level, instead of a hierarchical authoritative system which will lead to hesitation to share information (Manley, 2015, p.95). Moreover, when private organizations are in a bottom-up partnership with the government, they tend to be more resilient for cyber threats as for the autonomy they must have to deal with these threats. This adds to the power-sharing aspect as discussion in the *trust* section. When smaller private organizations must deal with bigger government bodies, they may lose the feeling of empowerment. When maintaining a bottom-up approach and regularly consult even the smallest parties involved, all organizations will feel empowered which will have successful influence on the partnership.

At the same time, when one organization becomes very significant and gains power, the others lose significance and the perceived equality diminishes (Osborne, 2000, p.298). The key to a balanced partnership is to make all parties involved feel equal. In this way, they tend to be more cooperative towards the other parties and the partnership. At the same time, when one party becomes dominant, the voluntary character of the partnership can be harmed which decreases willingness to cooperate. The reason for this might be found in the nature of the human which allegedly prefers the voluntary cooperation, but this is subject for another study (Clark, Stikvoort, Stofbergen, van den Heuvel, 2012, p.28).

2.2.4. Community involvement

The last element in this fourfold is the involvement of the community in the partnership. As all parties involved represent a community in their participation and strive for cyber security, the PPP must by satisfying for these communities. A deficiency in community support will thus mean that this party will not feel urge to join the partnership (Manley, 2015, p.96). Although the importance of the establishment of greater cyber security is now widely accepted by both private and public organizations and their communities, the question to what cost is still prevalent. Especially the preservation of consumer privacy is still an important emphasis in the participation of private organizations in PPP's. Therefore, it is necessary to keep the community involved and maintain support for the partnership (Manley, 2015, p.97).

Another significant aspect of the establishment of support for a partnership is the societal need for a partnership. In the case of cyber security, it is almost impossible to ensure cyber security for an organization on its own; every organization needs some form of

cooperation as the internet makes nearly every facet of society interconnected (Maughan, 2010, p.29). Moreover, the public sector is responsible to protect the critical infrastructures from disrupting and those critical infrastructures largely being in hands of the private sector, the two sectors appear to be constrained with each other (Manley, 2015, p.96-97). However, hesitations are still prevalent on the private sector side due to the information they have to share with the government (Manley, 2015, p.97). These hesitations of sharing information come from the businesses that the private sector need to ensure. Government requesting this kind of information may harm those businesses, which will in their turn harm the support for the partnership due to possible loss in profit. On the pro side is that PPP's can make critical infrastructure processes like utilities more resistant to pressure coming from the market that may be found unwanted (Gray, 2013, p.154), which may increase the support for participating in the PPP.

2.3. Analytical framework

After discussing the relevant body of knowledge regarding the PPP in cyber security CIP, this thesis will now proceed to the analytical section. To do so, first the analytical framework must be explicated, based on what is discussed in the previous section. To analyze the PPP between Dutch public organizations and the private sector with the aim to raise cyber security, the following sub questions are constituted to answer the main research question:

- How is the Dutch PPP described in the NCSS2 in terms of the required level of trust, legal guidance, bottom-up approach, and community involvement?
- How is the cooperation with the government in the cyber security PPP perceived, in terms of trust, legal guidance, bottom-up approach, and community involvement by the private sector parties that are involved?
- How can possible discrepancies between the NCSS2 and the perception of the private sector be explained?

3. Methodology

In this chapter, the methods that will be used in this thesis will be discussed. This will encompass the design of the study, which data will be used and how it is collected, how this data will be analyzed and finally the reliability and validity of the methods.

3.1. Design of the study

To give insight on the functioning of the cyber security PPP in the Netherlands, a holistic multiple case study will be deployed (Yin, 2003, p.52). This means that cases will be selected in attempt to cover the whole of the cyber security PPP, meaning the sectors with the highest cyber security relevance. The case study is a useful design when studying fields that have not been studied much, which can be said from the cyber security PPP (Kumar, 2011, p.123).

Firstly, for the public sector, the NCSS2 will be analyzed. In this analysis, the strategy will be studied on indications of how the government intended the partnership with the private sector through PPP. This document contains the whole of strategy of the Dutch approach regarding cyber security, when it comes to cooperation with the private sector. Secondly, the perception of this cooperation of the private sector will be studied. This will happen through an analysis wherein six public and private cases will be studied on how they perceive the cooperation with the government on the elements and indicators that are discussed in the previous chapter. This type of research is used to encompass a whole population or country, as the aim of the study is to analyze the Dutch PPP (Gerring, 2004, p.342).

The method that will be used for this study will be a qualitative case study, as this thesis aims for in-depth studying the cooperation between the public and the private world. This will happen through discourse analysis, as the aim of this thesis is to shed light on the perception of all parties that are involved and how this affects the performance of the partnership. More precise, this thesis will use the critical discourse analysis variant, as this includes the meaning of statements made by respondents (Bryman, 2012, p. 536). Discourse analysis is a way to analyze the language used in certain documents to map the social realities behind them (Jackson, 2007, p.396). Therefore, it is valuable to look at how the concerning parties rhetorically mention the participation. This will happen by taking the elements of successful participations as discussed in the theoretical chapter of this thesis. Moreover, possible

discrepancies that will be found will be explained, both by the existing theory and by possible new insights and conclusions. To be able to do so, one must also look at the rhetoric that is being used.

3.2. Data collection

The data that will be used for this thesis will come from different sources. When conducting this kind of analysis, it is important to follow the principle of triangulation. This multiplicity of data will in this case encompass a gathering of policy documents, interviews, and academic literature. This means that empirical data will relate to academic literature, which will then be brought together in an analysis. For this thesis, the empirical data will consist of the *written truth* of a document analysis of policy documents and the *perceived truth* of interviews. This distinction is made to emphasize the two dimensions of the analysis and does only relate to the form of data collection.

For the document analysis, the NCSS2 will be used. This is the second and most recent version of the cyber strategy, which was published in 2013. This strategy is chosen as it is considered to represent the government stance on cyber security in the Netherlands. From this document, a comprehensive picture of the Dutch approach on cyber security can be obtained. This picture will be analyzed through the lens of partnership effectiveness as described in the theoretical chapter of this thesis. In this way, it becomes possible to assess the effectiveness of the partnership with the private sector from the government perspective. This will give insight on how the government generically meant the partnership to function. The Dutch NCSS2 is the particularly appropriate to analyze as it contains the whole of the Dutch strategy on cyber security. Therefore, when the aim of the (sub-)question is to study how the government intends the PPP, the most logical choice is that this document should be the subject of the study.

On the other hand, this thesis will look at how the private sector perceives the partnership. This will happen through a series of interviews in which employees of private sector organizations will be asked questions about the structure and the effectiveness of the partnership. In total, six interviews have been conducted. The respondents are all cyber security professionals, at least somehow working with the government through the PPP. Five respondents are active in the private sector, as their perception is being measured in this study. At least one cyber security professional will be interviewed that has been active in Telecom

sector, the ICT sector, the Financial sector, and the Energy sector. In this way, the sectors that are most influenced by cyber security will be addressed. This will be complemented by one interview with a respondent that has been active at the National Cyber Security Center (NCSC), to add to the *perceived truth* of the analysis of the public side of the PPP. By doing so, a clearer picture can be presented from this public side, especially considering that the NCSS2 stems from 2013.

To collect data from the respondents, interviews are conducted through a semi-structured interview technique. This means that questions will be asked according to an interview protocol, which can be found in the appendix (Appendix A). By asking the respondents the same questions, the differences in the answers can be interpreted as differences in opinion and not as differences in the questions that have been asked. This is important, as all respondents have different backgrounds and different current occupations (Barriball & While, 1994, p.329). In Table 1, an overview of the respondents is provided, together with their (former) occupation. Like in the analysis, the respondents will be numbered one to ten to respect their privacy but still make a clear distinction.

Table 1: Schematic overview of the respondents

Name	**Reference**	**Occupation(s)**
Nicolas Castellon	Respondent 1	Cyber Security Specialist at CGI. Former: FGV and HCSS
Arnaud Thoen	Respondent 2	Cyber Security Officer at Joulz. Former: Eneco
Anonymized	Respondent 3	Cyber Security Entrepreneur. Former: CISO of KPN
Marit Bakker	Respondent 4	Douane Nederland. Former: NCSC
Remco Ruiter	Respondent 5	Liaison Officer Betaalvereniging Nederland.
Stef Liethoff	Respondent 6	CTO at Novaccent

3.3. Data analysis

The empirical data that will be obtained from the strategy and the interviews will be analyzed through a discursive theoretical lens as discussed in the theoretical chapter and as formalized in Table 2. In this way, a picture will be provided on how the PPP is intended to function according to the government and how it is perceived by the private sector. The results from these analyses will be compared. Possible discrepancies that will be found will then be put into perspective of the functioning of PPP's, meaning that they can have implications on both the societal need for a safe cyberspace and on the theoretical concept of PPP.

Measuring the effectiveness of PPP's has always been and will always be relevant as it can expose weak spots of the partnership. When the perception of the private sector differs significantly from the PPP as constituted in the NCSS2, this can have several implications. After identification, new policy can be made according to these weak spots. This can improve the cooperation between public and private sectors and to better functioning critical infrastructure protection, which is a desirable outcome as it means improvement of national security. By speaking to professionals and practitioners of cyber security, clarity can be provided on the question where the biggest problems are in the cooperation between public and private. Discrepancies that will be found in the PPP as described in the NCSS2 might be the cause of these problems. In other words, how does the Dutch cyber security PPP hold against the characteristics of the partnership according to the NCSS2. The findings of the data analysis will be discussed to ultimately say something about the functioning of the PPP when it comes to establishing cyber security for the Dutch society by protecting its critical infrastructures.

The theoretical lens that will be used for the analysis of the data as mention above will be constituted through a coding schedule as presented in Table 2, containing the relevant measurement that are obtained from the theoretical chapter. This will largely comprise the four elements of assessing the effectiveness of PPP's and the relevant indicators. Through discourse analysis of the rhetoric used in both the NCSS2 document and in the interviews with practitioners in the field of cyber security, this thesis will look at to what extend these four elements can be found back in the data received from these two forms of data collection. As for the NCSS2, the elements will be the leading framework of assessment of how the input of the PPP is constituted. By analyzing the rhetoric by using the elements of a successful partnership, it is possible to give insight in how the partnership with the private sector is meant to function.

With the focus on how mutual trust, legal guidance, bottom-up approach, and community involvement is discussed in this strategic document, a comprehensive picture can be created of how the government perceives the partnership through PPP. This will be compared to the private sector perception. By conducting semi-structured interviews with individuals working in the field of either Telecom/ICT infrastructures or in another field that is involved with cyber security, an insight can be given in how the strategic partnership through PPP is perceived by the private sector parties that are involved. By asking questions regarding the four elements of effective partnership, an indication can be given on what elements do not function properly which can be interpreted as strengths weaknesses of the partnership or even the concept of PPP. The result of this analysis can contribute to the broader question of how to govern the new, transnational threat of cyber by using PPP's.

In Table 2, the four elements as mentioned before and as presented in the theoretical chapter are categorized based on the measures of effectiveness of a successful PPP as theoretical chapter. The elements are complemented by the indicators that are most appropriate, according to the theoretical chapter. These indicators will be used for the analysis of both the NCSS2 and the interviews that will be conducted with cyber security professionals. In the analysis, both positive and negative indications of the four elements will be distinguished. Therefore, both the presence and the absence of these four elements with their indicators will be included.

Table 2: Schematic overview of the elements of assessment of the Dutch PPP

Trust	Transparency Personal relationships Power sharing Confidence in the PPP
Clear legal guidance	Formalized expectations/objectives/goals Accountability mechanisms Regulation for standards and quality Use of incentives
Bottom-up approach	Regular consultation of all parties Involvement of participants Perception of equality Voluntary cooperation
Community involvement	Public support Need for the cooperation

3.4. Reliability and validity

Research methods can have possible weaknesses or pitfalls. Therefore, in this section the most important ones will be discussed for the relevant methods. Moreover, this section will discuss how these pitfalls can be marginalized to make this study as useful as possible.

3.4.1. External validity

Besides the useful applications of the multiple case study design, there are some possible limitations and downfalls to this kind of research. First, as only one country will be researched, it can be that the selected unit of analysis of the Netherlands turns out to be a big exception on other countries, regarding developing cyber policies. This can harm the external validity of the study (Yin, 2003). Although this means that the findings may not be generalized in its entirety, it does not mean it cannot add to the academic discourse on the functioning of PPP in cyber security governance (Flyvbjerg, 2006, p.119).

3.4.2. Reliability

Another relevant criterion for this study is reliability. This encompasses to what extend the findings of this study could be repeated, when looking at data collection (Yin, 2003, p.34). For the public document study, this will not be a problem as long as the coding schedule is constructed in a clear way. However, for the interviews it might be more problematic. Therefore, the interview protocol is added in the appendix to make sure that it is clear how the interviews have taken place. The fact that the six interviewees all come from different organizations from the most cyber sensitive sectors (Telecom, ICT, Energy and Financial) requires well-constructed measures, to make sure that the same thing is measures in every case, interview, or document (Yin, 2003, p.34). When the appropriate measures are selected and used for every case, the findings can be compared, which adds to the comprehensiveness of the study and therefore give in-depth knowledge on the cyber security PPP. For this study, the measures that are selected are the four elements as presented in the previous chapter. These will function as indicators of success for the perception of the partnership for every case. The outcome that will be produced by studying all cases in the same way, all four elements can be placed into context and the implications can be discussed.

3.4.3. Internal validity

The internal validity is important to prevent the results from having other causes than the measurable objectives of this study (Yin, 2003. p.34). In other words, is this study really measuring the functioning of the PPP or can the findings be explained by something else? This study can be considered an exploratory without causality involved. However, the internal validity is still important as there might be other (external) influences affecting the results that are found. Therefore, it is necessary to eradicate other explanations that might be evident for statements that are made in both written as *perceived truth*, in this case in the strategy or in interviews. Otherwise, the risk of making incorrect conclusion may be apparent (Yin, 2003, p.36).

3.4.4. Construct validity

As this thesis will conduct six interviews with individuals from different private organizations that are concerned with cyber security, the construct validity must have appropriate attention. The method of discourse analysis is a method with many assumptions and labels, it is open to differences in interpretations. As this is an intrinsic problem to this kind of research, it will be impossible to counter this entirely. However, by carefully constructing the labels and provide them with examples, an accurate indication of how the analysis will be done can be provided (Yin, 2003, p.35). In this way, it should become clear how and why certain constructs are being interpreted as of influence on one of the four elements of assessing a PPP. Therefore, the four elements with its indicators are extensively discussed in the theoretical chapter, both for how they can be recognized and why these elements are picked.

3.4.5. Pitfalls

A possible pitfall in the semi-structured interview can be that as experts on the topic of cyber security will be interviewed, they might not be willing to answer to all question as this might risk a security breach because of confidentiality and privacy. Therefore, the questions that will be asked during the interviews should be carefully constructed to obtain the required information for this study without asking the interviewee to give confidential information. Some respondents will be anonymized upon request, as their answers might have implications on their positions or may have disruptive effects on relations they have in the world of cyber security. Nonetheless, the transcription of the interview will always be provided and their names can be provided upon request.

4. Analysis of the Empirical Findings

4.1. Introduction

This chapter will analyze according to four elements, with the indicators as presented in the methodological chapter, how this partnership is supposed to function and how it really functions using both statements from the NCSS2 and from the interviews. Each time, one or more statements from the NCSS2 will be chosen and discussed how the respondents differ or agree with this statement. This will result in multiple aspects on which the respondents differ from the view presented in the NCSS2 and multiple aspects that the respondents somewhat agree on. By looking at how the government intents the partnership to function and how this works out in practice, something can be said about the effectiveness of the partnership. When many of the elements of a successful partnership as described in the NCSS2 are accordingly perceived by the private sector respondents, this may indicate an effective partnership. However, discrepancies will mean that the partnership does not reach its full potential and leaves room for improvements. Therefore, these discrepancies may be the basis of new policy or at least new future study.

The structure of the analysis will be as follows: all four elements will be discussed in different sections. In every section, first the most important indicators found in the NCSS2 will be presented and discussed according to the coding schedule. Hereafter, these findings will be held against the perception of the respondents to see whether there are major differences that can be distinguished between written and *perceived truth*. All this will be emphasized by the most appropriate statements made in the NCSS2 and by the respondents. It must be said that some indicators may have overlap with each other. When this is the case, the most appropriate indicator will be chosen, but thus not the only appropriate one. Moreover, not all indicators may be addressed in the NCSS2. In these cases, they will be addressed upon in the sub concluding section.

4.2. Trust

Following the structure of the theoretical and methodological chapter, the first element to be discussed in the NCSS2 is the element of trust. It should be said that according to the indicators as constituted in the previous chapter, the notion of trust does not come back often in the

NCSS2. Only one indicator of trust is explicitly mentioned in the strategy, which is the importance of increased transparency. However, the other indicators may have influence on the data sharing process are still relevant to discuss, according to the information provided by the respondents. These indicators will be elaborated on as well, in the context of how they relate to data sharing and what the respondents had to say about these indicators.

4.2.1. Transparency

The first statement comprises a mentioning of the transparency between public and private organizations that provide or use cyberspace services: "Transparency is a precondition for strengthening trust between the actors" (NCSS2, 2013, p.20). With this, the government stresses the need for cooperation to accomplish effective information sharing and therefore emphasizes the fact that the PPP is the way to accomplish this. Moreover, this statement shows that the information sharing should be voluntary as it is in advantage of both public and private sector as for the interdependence as just mentioned. Both transparency itself and the emphasis of trust it brings can be interpreted as signs of the government building actual trust with the private sector when cooperating on the topic of cyber security. Therefore, it can be said that the government values transparency among all parties and therefore emphasizes the trust in the cooperation with the private sector through PPP's. When regarding the element of trust by the government, the preparedness to share data with the private sector is an indicator of this element. Naming transparency as a precondition is can be interpreted as a strong statement, as it suggests that without transparency, the establishment of trust cannot fully develop. This makes transparency an essential ingredient for successful partnership.

When turning to the answers of the respondents, is does not seem to be that transparency has developed between public and private parties enough to enable this "strengthening of trust between the actors" (NCSS2, 2013, p.20). A problem in transparency that almost all the respondents addressed in the interviews is the 'Wet Openheid Bestuur' (WOB). This law encompasses that "journalists, but also other people, every citizen in the Netherlands can request information from the government, according to this law" (Respondent 4, translated from Dutch). The respondent continues by adding: "This happens quite often, and this means that companies will hesitant to share information with the NCSC" (Respondent 4, translated from Dutch). This sounds problematic when considering the importance that the government allocates to transparency. This may indicate a negative effect on the partnership by including

the government, as the private sector will always be hesitant to share information even with each other, when the NCSC is involved.

However, the NCSC should not automatically be seen as a representation of the entire government. Respondent 6 makes this distinction between the NCSC and the rest of the government. About being transparent towards the government, he says: "No. Absolutely not. Because of the different interests you have. Look, from our perspective, you never know what the government will do with your information, if you are sharing transparently, what will happen" (Respondent 6, translated from Dutch). This means that he distrusts the government as he does not know what it will do with the information he provides. However, when regarding the NCSC, he has a different stance: "We give pass along transparently what our infrastructure looks like and they pass along transparently which vulnerabilities and threats it has so that we can anticipate. They also give advice and of course they are completely independent" (Respondent 6, translated from Dutch). Especially with this last statement, this respondent stands out. Where several other respondents indicated that the information provided to the NCSC was also suspected to end up at other government instances or other organizations, this respondent seems to be certain of the independence of the NCSC.

4.2.2. Power sharing

Another reason of a lack of transparency is that some private organizations seem hesitant to share information because of the existence of authorities and supervisors. Although these authoritative instances are accepted and found necessary, they can obstruct the NCSC in their functioning. This is because they are both government instances, although they do not actively share information. Respondent 4, former employee of the NCSC states: "I think that the biggest difficulty in the information sharing by the private sector lies in the fact that authorities and supervisors also lie within the public sector. (…) We are far apart from the authorities but we also talk with them, as they are also our partners" (Respondent 4, translated from Dutch). Other respondents notice this hesitation as well. When asked whether private companies hold back information, Respondent 3 said: "Definitely. Absolutely. Especially in those cases that are under supervision and are facing sanctions. Absolutely. There are several reasons for private organizations to withhold information" (Respondent 3, translated from Dutch). The fact that private organizations are afraid of sanctions cannot be a surprise. However, the supervisors that are responsible for the sanctions seem to be in the way of the partnership between the

government, especially NCSC, and the private organizations. Sharing information and being transparent is troubled by the fact that other public instances are constantly looking to hand out sanctions.

A similar troubling aspect is presented by Respondent 5, in which he says "You can imagine that from the private sector, sometimes there is the fear that everything we say or report to the government will eventually be transformed into regulations, and where regulation is, is supervision. Thus, we will get more regulatory pressure" (Respondent 5, translated from Dutch). So, besides being afraid that any information may become public, the fear also exists that everything a private organization shares with the government will turn into more regulations and thus more sanctions. Logically, business-driven organizations will be averse of regulations with accompanying sanctions. This adds to the fact that private organizations are intrinsically hesitant to share information, as Respondent 1 stated: "For example if you were to create a knowledge exchange, a KPN would be very hesitant to exchange to other companies, because that is their 'magic sauce', their formula" (Respondent 1). This shows that when a private company is transparent towards the government through the PPP, the information might end up with the other, competing organizations. Respondent 1 later on puts more emphasis on this problem by stating "The private sector has their own information that are their crown jewels" (Respondent 1). This is in line with the perception of Respondent 6, who also distinguishes the competition as troubling for the cooperation, but thinks the intentions are good:

> "Transparency is difficult because of the commercial interests that are involved. When regarding the general interest, it should happen, as cooperation must happen because you cannot counter the threat alone. But there is yet a big step to take" (Respondent 6, translated from Dutch).

In the light of what the government states in the NCSS2 about the importance of transparency, this is also an important aspect. Not only is the transparency between public and private important, but transparency among private organizations should also be improved. Respondent 5 presents another similar troubling aspect, in which he says

> "You can imagine that from the private sector, sometimes there is the fear that everything we say or report to the government will eventually be transformed into

> regulations, and where regulation is, is supervision. Thus, we will get more regulatory pressure" (Respondent 5, translated from Dutch).

So, besides being afraid of sensitive information becoming public through the WOB and losing any information advantages with respect to competitors, organizations are hesitant to share information because they feel like it could mean more regulatory pressure. At the same time, more sanctions can be expected from supervising authoritative watchdogs, exercising their power. These three aspects are perceived as the most troubling for the transparency that according to the NCSS2 are essential for improvement of the PPP.

4.2.3. Confidence in the PPP

Besides these issues with transparency that are experienced, most respondents did make clear that the intentions are undoubtedly there to be transparent and make the PPP work. As one can expect from the initiator of the partnership, the government emphasizes the confidence in the partnership several times in the NCSS2. Statements like "Together, we can create a secure, free and profitable digital domain" (NCSS2, 2013, p.25) indicate such confidence.

At the same time, private sector organizations want to share their information with the government through the cyber security PPP, as they seem to believe in what they will get in return for it. However, they do not share information at all cost. Good intentions are apparent from the statement: "We try to be as transparent as possible towards each other and subsequently jointly make arrangements on how we can use the shared information and how we can share the information further on" (Respondent 5, translated from Dutch). So, it is not that the PPP is malfunctioning by the lack of will for transparency. However, it is found to be a major difficulty to find a way in between being fully transparent towards all partners and protecting the core business. One aspect that can be of stimulating influence are personal relationships between cyber security professionals of both public and private organizations, as this would improve information sharing. As Respondent 1 states: "It Is really based on personal relationships between the people in a company and the people in government" (Respondent 1). This is a literal example of the personal relationship indicator as presented in the theory. However, this does not stand out in the NCSS2 as something that the government wants to stimulate. When discussing the confidence in the PPP, besides the aspects that will have to be improved, Respondent 6 has the following to say:

> "On the other hand, you have to react based on a certain level of trust. If we can provide good things and our expertise is being acknowledged and the other party can give back information, then it is more important that we can do business with the government in an integer way and I expect an integer attitude back" (Respondent 6, translated from Dutch).

With this, he tries to emphasize that the intention to create a fruitful cooperation is there as long as the government also shows confidence in the partnership. To overcome the hesitation of sharing information to the government, it is important that the government shows confidence by sharing useful information with the private sector. This can be important as it creates preparedness to share data back, as seen in the statements above. About the information stream from the government to the private sector, respondents are somewhat more positive. Through multiple institutional tools, created by public organizations, information and intelligence is being shared to the private sector. One of these tools is the *National Detection Network (NDN).* This is a collaboration in which organizations can share digital dangers and risks that have been noticed in cyberspace. In this way, other organizations can anticipate on these dangers and increase their resilience (NCSC.nl, 2017a). As Respondent 2 states about the NDN:

> "Then you see that the cooperation is going really well, that we report incidents but also how the government makes cyber intelligence available to the critical infrastructures" and "A good example is the NDN. This is a service that the NCSC provides to partners from the critical infrastructures through which it shares cyber intelligence, but can also be used by the critical infrastructures to report back to through the NDN" (Respondent 2, translated from Dutch).

Respondent 3 somewhat agrees, but focusses on the Information Sharing and Analysis Centre (ISAC) of the sector: "this is by all means a very important function for private organizations mutually, and the government shares and retrieves information from the critical infrastructures" (Respondent 3, translated from Dutch). This means, when regarding the transparency which is valued highly by the government according the NCSS2, that the information sharing platforms like the ISAC and the NDN are in fact working, but mostly from the government sharing information side. Sharing information back to the government by the private sector experiences some more trouble.

As shortly addressed upon before, the function of the ISAC must be elaborated on as most respondents perceived this as a positive addition to the PPP. Every sector has its own ISAC, in which multiple public and private organizations from this sector assemble to exchange information and experiences on the topic of cyber security (NCSC.nl, 2017b). This makes it an important instantiation of the PPP, as it contains both the public and the private sector and aims to improve information exchange between and among public and private sector parties affiliated with cyber security.

Respondent 3 states the following about the ISAC and the government role in it:

> "It is undoubtedly a very important function for organizations in the private sector mutually, and the government of course also shares information and retrieves information from the critical sectors. If I must distinguish the most meaningful aspect, it is the coordination of the information sharing within the private sector. Whereas the government fulfills this coordinating role" (Respondent 3, translated from Dutch).

With this statement, although it is a positive one, it becomes clear that the government, according to this respondent, does not have a big part in the information sharing. It is mostly private organizations that share information in the ISAC, and the government has a mere coordinating role. This is not in line with the statement from before, in which the government was named as the major distributer of information through the NDN.

Somewhat the same argument of the government as coordinator is made by Respondent 4 from the NCSC: "The NCSC facilitates this body and we do not preside it. There is a core team in the ISAC that are public partners (…) but they are there as facilitators and with a role of expertise, whereas the rest is in the ISAC for their substantive role" (Respondent 4, translated from Dutch). With this statement, she emphasizes that it is not the government or the NCSC that leads the most important information sharing platform of cyber security intensive sectors, but it is the private organizations themselves. This will be discussed more elaborately later on in the bottom-up approach section, but for the process of information sharing it is meaningful to know. The reason for this is because it tells that the government is important for information sharing, something that most respondents emphasize, but not for actual information sharing. Instead, the role of the government in the information sharing system is a facilitating, substantiating, and coordinating one. It is no surprise than that the government advocates for

more transparency in the NCSS2. However, according to statements of multiple respondents, it is especially the government's involvement that causes an obstruction in transparency.

4.2.4. Concluding Trust

The Trust chapter is mainly based on the question whether and how data is being shared between public and private sector. Therefore, the aspect of transparency is leading in this regard. As the NCSS2 states that improving transparency should be one of the key points to improve the effectiveness of the PPP, in practice transparency experiences several issues. Most respondents spoke out the intention to be transparent. Through platforms like the NDN and the ISAC, the process of information sharing is being improved. However, there were some obstructions in being fully transparent. One of them, mentioned by almost all respondents is the WOB, which allows every citizen to look into government data and through which information shared by private organizations with the government becomes accessible. In this way, private organizations become hesitant to share information with the government as it may end up in the media or with competitors. Somewhat overlapping with this is the existence of other government bodies like the authoritative instances like watchdogs. As they are also government bodies, the private organizations are afraid that partners like the NCSC share information with these watchdogs. This can be interpreted as difficulties in power sharing in the public sector. The division of labor between these government bodies will be elaborated on in the next section.

Overall, the process of establishing trust is ongoing but does not seem to be close to its final stage. All parties want to be transparent, which shows confidence in the PPP. However, there are some issues that are unacceptable for the private sector, as they have their business model as their highest priority. Creating cyber security is important for them, but not to the cost of their business. Although most respondents seem to have confidence in the PPP, progress can still be made with several obstacles to overcome.

4.3. Clear legal guidance

As set out in the methodological chapter, the element of clear legal guidance mainly comes down to the way how the cooperation is formalized: what can organizations expect from each other and what happens when an organization fails to deliver. This may encompass objectives

and goals of the partnership, but also how the government uses incentives to stimulate certain behavior of private sector organizations without having to take authoritative measures and standards, rules, regulations, and best practices. When this happens in a clear way for all parties, it is supposed to have positive influence on the effectiveness of the partnership. All parties then know what they can expect from each other and can anticipate on that. The following statement sums up the notion clear legal guidance:

> "As an expert authority, the NCSC gives advice, both when asked and at its own initiative, when major vulnerabilities are detected or in the event of (imminent) crisis situations. It is then up to the organisations themselves to implement the recommendations, or to be transparent about their reasons for not doing so. This is particularly important when it concerns government bodies, also with respect to the regulatory authorities and/or line ministries" (NCSS2, 2013, p.19).

4.3.1. Formalized expectations, goals, objectives, and accountability mechanisms

The first notice of the clear legal guidance element in the NCSS2 is about how the roles of participating organizations should be formalized. By stressing the importance of "clear allocation of roles" (NCSS, 2013, p.19), the government emphasizes that all parties must know from each other what their role is in the PPP. However, the statement "how these roles relate to one another will become clear in the future" (NCSS, 2013, p.19) can be labelled as negative, as this can be interpreted as vague and unspecified. The government emphasizes the importance of setting out the division of labor, but then continues by stating that this will happen in a later stage. This makes the statement somewhat contradictory, but can still be interpreted as a notion of 'clear legal guidance'.

A little further, the NSCC2 once more emphasizes this division of labor by putting the responsibility to deal with crisis situations by the organizations themselves and even demanding them to provide clarity on which measures were taken and why, or why certain measures were not taken in this situation (NCSS2, 2013, p.19). This division of labor indicates an accountability mechanism in which all involved parties know each other's responsibilities and how these can be uphold. Although some authority can be noticed in this statement, it should not be interpreted this way. The interpretation should be more about the promotion of clear regulatory by giving advice to private sector organizations, which the government actively

wants to exercise. According to the theory, rules and regulations are not negative when they are set out clearly. The government, as national security provider, wants to regulate the cyber security processes to have some control over it. Therefore, the government wants to have set out who does what how and when, as well as what the consequences are when the private sector fails to meet the regulations.

The first problem arises when discussing the role of the NCSC regarding the watchdogs and that instituted to supervise. Although these watchdogs are not usually considered as part of the cyber security PPP (NCTV.nl, 2017), they are involved and they are part of the public sector. Therefore, it must be clear how they are different in their roles from the NCSC and other public instances that are part of the PPP. Respondent 3 describes a possible problematic outcome: "When the NCSC in its entirety associates themselves with the watchdogs, private parties will be less willing to share information" (Respondent 3, translated from Dutch). In this statement, it comes forward that the division of labor between the public organizations from the cyber security PPP and other public parties is not completely clear. At least, private organizations do not know what information is being shared between the public organizations.

On top of that, the respondent from the NCSC said: "At the same time: we are not a watchdog, but we do have a reporting requirement. That is odd, because what happens when you do not report" (Respondent 4, translated from Dutch). Even employees at the public side of the partnership have trouble distinguishing the true division of labor here, as the NCSC exercises a reporting requirement but does not have the ability to sanction. This must create confusion among the private organizations; do you report or not? Especially added by the difficulties with the WOB and the partnership with watchdogs, this becomes a complicated issue. It seems that regarding rules and regulations, the NCSC has not determined its position yet. Private organizations must report incidents but do not face consequences when they refuse to do so. However, when they report, the information can end up in the publicity or at watchdogs which will make them hesitant to do so.

At the same time, the incidents that are reported are the feed of the functioning of the NCSC, as Respondent 4 says: The NCSC is like a treadmill of information which uses input to create output. Because we add a 'sauce' and this sauce encompasses that we can put all pieces of information together for analysis, and ultimately come to operational policy. This is then sent back to the target groups" (Respondent 4, translated from Dutch). In other words, the NCSC functions because of the information and reports they receive from private organizations, but

these are afraid to share this information as it may end up with the media or at the watchdogs, resulting in sanctions. This does not stimulate private organizations to share information, as we saw in the previous chapter about trust. Reporting requirements of the NCSC do not fix this as ignoring them does not have any consequences. Moreover, reporting requirements do not seem to fit in the equal partner that the NCSC wants to be, but they should somehow ensure their input from the private sector to remain functional.

4.3.2. Regulations and standards

As the government must protect the critical infrastructures of the Netherlands, it may be necessary to set up a set up regulations and standards to ensure continuity. The governments states in the NCSS2 that: "If required, the government also acts in a controlling manner, which may include determining regulations and standards, for instance for the vital sectors" (NCSS2, 2013, p.19). This provides the opportunity to take more influence when a certain sector does not seem to be mature enough to do it for itself. However, as seen in the theoretical chapter, the regulations must be clear to have positive influence on the sector. A major task of the government regarding clear legal guidance is the implementation of the actual standard requirements for cyber security practices (NCSS2, 2013, p.23:25:26.). These are developed through risk analysis by the government. The outcomes of these analyses will be used for standard security requirements that are expected to be implemented by the private sector security practitioners. In a cooperation like this, the government seems to take the role of coordinator of risks and with this steer private sector companies towards certain behavior. In other words, the government does the research and transform the outcomes into best practices which it shares with the private sector. Somewhat the same goes for the management of privacy standards.

The government approach seems to embrace the relationship in which the government sets minimum requirements in the same way as happens with physical products, which did not happen yet (NCSS2, 2013, p.25). With this, the government sets out the ambitious plan to try and control the digital world like it controls the physical world through security measures. To do so, the government digital service provision should function as an example of how the private sector should constitute their security provision. This can be labelled as a somewhat vague statement. The government points at a problem which does not exist in the physical world. Then, it proposes no clear solution other than that there should be basic requirements

based on how the government itself secures its services, which are also not unquestionably secure. Therefore, although the government rightfully addresses a problem and proposes a solution, it remains to vague and does not sound like a useful policy requirement for the private sector to implement. Attempting to give the right example when securing digital processes does not seem to be extensive enough for the security impact of privacy insecurities. A somewhat better solution is presented further on, when the NCSS2 proposes to assemble with the private sector to create both 'security by design' and 'privacy by design' (NCSS2, 2013, p.25). With this, standards and requirements will be set up through consultation of the private sector, an example of the bottom-up approach that will be discussed more in depth in a later section of this chapter. The point to be made here is that this seems to be a more appropriate way that standards and requirements should become into existence and not by vague notions of 'setting the example'. Setting the example and demanding the private sector to copy this policy can even be interpreted as an authoritative measure instead of the equality between parties that a successful PPP should be based on.

The rules, standards and regulations of the PPP as set up by the government are mentioned several times by the respondents, both positively and negatively. Moreover, the standards that are being put out do not seem to be clear for the private sector. As Respondent 3 states: "the government will very seldom provide clear norms. The law is often very abstract with vague description, with statements as 'appropriate measures' and others. Those are far from clear and concrete" (Respondent 3, translated from Dutch). Respondent 5 implicitly joins this issue, by stating "for as far as the government itself knows it, it is clear for me" (Respondent 5, translated from Dutch). With this, the respondent wants to make a positive point, being that he understands the government. However, his statement has some scornful tone in it, by implicitly suggesting that sometimes the government itself does not really know what it is doing with its legal guidance. Respondent 2 does not complain about the unclear or vague regulations, but does question whether the regulations are helpful:

> "If the government was not there, there would be total anarchy. However, to the question whether the government helps or is an obstruction, I would not be able to answer this instant. But this is also because this conversation is recorded" (Respondent 2, translated from Dutch).

Especially because of this last addition, we can conclude that in fact the government's role is sometimes more an obstruction than a helpful tool. Respondent 2 further on emphasizes his wish for self-regulation:

> "Besides, self-regulation is more convenient than being regulated. Then we are talking about another role, that of the ACM. Stedin and Joulz wants to be self-regulated and not being ordered lots of things from the government" (Respondent 2, translated from Dutch).

This indicates initially the negative aspect of regulatory instances who are watching over the shoulders of private organizations and putting out sanctions. As the theory states, regulation is perceived as more negative when forced upon (Manley, 2015, p.94) and apparently the presence of the watchdogs to maintain the regulations is a negative aspect for this respondent. However, the fact that self-regulation cannot work can also indicate that the government does net set clear requirements for private organizations to function as benchmark for self-regulation. Regulations are acceptable, but complying to these rules should preferably happen through self-regulation instead of the use of hard sanctions. Having a watchdog from the public sector giving out sanctions does not seem to help when trying to make the partnership function. This is however not in line with what Respondent 3 has to say about the watchdogs:

> "If you look at 2016 and a part of 2017, they have had a total of eight to nine thousand alerts, with zero sanctions. Zero. If you want to be taken seriously, there must have been one situation in eighteen months of which you thought 'this is out of line'" (Respondent 3, translated from Dutch).

This respondent suggests that it is not the sanctions that bother private organizations the most, but the indecisiveness of the watchdogs. There are rules and regulations with accompanying sanctions, but they mostly exist on paper, according to this respondent. So, although self-regulation is preferred, the promise of handing out sanctions inconsequently is even worse. Sanctions are not popular, but when the rules are clear, private organizations can adapt to it. But with the watchdogs threatening with sanctions but not acting accordingly, a situation of unclearness emerges. Added with the fact that respondents sometimes question whether the government knows what it wants makes this a troubling situation for the PPP. This makes the authority of the watchdogs more questionable, as their behavior is perceived as weakly substantiated, inconsequent, and based on wrong regulations.

Besides the problem of unclear regulations and the issues with sanctioning, there is also some regulation that is simply not accepted by private organizations. A respondent provides one example, in remark to digital information sharing which was considered insecure by the government:

> "and then they will block things and say 'you cannot do this according to our policy, otherwise you will be punished. However, the businesses will not accept this and go their own way. They will find other ways to do it, because we need it for the business process, to share information. That is what our business is built on and how we make money" (Respondent 6, translated from Dutch).

This indicates that sometimes regulations from the government are just not realistic. The government should be considerate when it implies regulations, even when they aim of security is obvious. When regulations become too strict, it may harm the business activity, as this respondent indicates. This will be an outcome that is beyond the aim of the government, which emphasizes the importance of involving the private sector by the constitution of the regulations. Moreover, this statement is in line with the theory of Manley (2015), in which he states that forced upon regulations will cause private organizations to turn to evasive tactics instead of voluntarily sharing information with the government (Manley, 2015, p.94).

In sum, the use of regulations is perceived as unclear, which makes the role of the watchdogs look negative. The watchdogs are threatening to sanction according to regulations that seem to be unclear for both themselves as the private organizations. Maybe this is the reason that actual sanctions are not often been given. However, this still gives the watchdogs an negative kind of authoritative position.

4.3.3. Use of incentives

The next notion of clear legal guidance regards the use of incentives in form of stimulating awareness, education, and innovation (NCSS2, 2013, p.20). This can be interpreted as clear legal guidance as the government as initiator of the partnership is responsible for these sorts of incentives to enhance the implementation of best practices, in this case through raising awareness, providing education, and share and stimulate innovation. Using these incentives, the government abstains from taking an authoritative stance by not force the private sector

organizations to act in a certain way but rather stimulate good behavior. Therefore, this is a clear example of the government promoting certain behavior in the PPP, which is allegedly one of the main aspects that the PPP is designed for.

When turning to the respondents, the general tendency is to value the NCSC as a relatively useful partner in the field of expertise. As Respondent 2 states:

> "I think we have plenty of contact with the government and the NCSC and they know what they can expect from us. And we know what we can expect from them. For example, to create awareness at our board, the intelligence service has brought them a visit to tell what is happening in the Netherlands" (Respondent 2, translated from Dutch).

This indicates the role of NCSC both as a database of expertise and as coordinator of contact with other public organizations like the intelligence services. This statement is somewhat emphasized by the same respondent later: "It is valuable when somebody stands up and tells us and our higher management whether we do enough or whether we should do more on the topic of cyber security. (…) It is great that this kind of awareness is being created from the government and that they are open to help" (Respondent 2, translated from Dutch). This respondent mainly emphasizes the importance of creating awareness by the NCSC, which is in line with the notion in the NCSS2.

Respondent 1 also stresses this need for awareness: "there is a common goal which is to create awareness, to create more impact in securing for example the Netherlands and its critical infrastructures and data" (Respondent 1). The fact that this respondent sees an important task for the NCSC in the creation of awareness might indicate that this is one of the most important roles of the public sector in the PPP. This fits in the learning and incenting role that the NCSS2 presents, and is also backed by the respondent from the NCSC: "The business world has of course a different primary goal" (Respondent 4, translated from Dutch). The primary goal of the private sector is profit, that's why public organizations like the NCSC are necessary to create awareness for cyber security in a big picture.

The role of the NCSC might be found valuable by most respondents, there is also an indication that only the NCSC is not enough. While what the NCSC does might be useful, there should be more guidance on a higher, strategic level. According to Respondent 6, the security of the digital domain should have more attention: "On the operational level, there is the NCSC,

a great initiative, by which a large part of the critical infrastructures is being monitored. But this is only a small fraction. It should be on the political agenda" (Respondent 6, translated from Dutch). With this, he indicates that only analyzing threats is not sufficient, the discussion should be much broader. As he later specifies: "More attention, more giving direction. That would be pleasant. And acknowledging that we are experiencing a digital transformation" (Respondent 6, translated from Dutch). With this, he states that only the implications of the NCSC are too small, that it should be taken to the national politics. Moreover, the digital world should even have a specialized ministry, as this respondent later concludes.

In the light of the use of incentives as described in the NCSS2, this respondent believes that the appropriate awareness, education, and innovation can only be accomplished by installing a nation level public instance, like a ministry. What the NCSC does might be good, it is not extensive enough, which at least indicates that there is space to enlarge the public sectors role in the PPP. However, this suggests that there needs to be a new public organization besides the NCSC with its expertise and the watchdogs with their regulations. This new public organization would then be responsible for a nationwide awareness stimulation, but also possibly shed light on the difficulties in the relationship between the NCSC and the watchdogs by giving direction.

4.3.4. Concluding clear legal guidance

In sum, several notions of clear legal guidance can be found in the NCSS2. By the creation of the document, the government took the position of coordination between organizations involved with cyber security. Not only does the government sets out how the cooperation would look like according to the public perception, it also studies best practices security and produce accompanying standards and requirements to protect the critical infrastructures without controlling these infrastructures entirely. This seems to be the appropriate position to take given that the private sector mostly owns those critical infrastructures. Clear legal guidance seems to be an important element of assessing the effectiveness of the PPP as it is one of the most powerful tools the government has, to influence the world of cyber security. However, the government should beware of becoming too vague in its intentions. When lacking concrete legal guidance like "how these roles relate to one another will become clear in the future" (NCSS, 2013, p.19), the private sector might lose faith in the government guidance as it lacks

concreteness. The goals and objectives should be clear of both public and private sector to create the most effective partnership.

In practice, the role of the NCSC in the PPP experiences some serious issues when working together with the private sector. First, the NCSC tries to be an equal partner that provides expertise and best practices regulations for private organizations that are dealing with cyber security. It does so by creating awareness, organizing information exchange between private organizations and processing data that it receives from private organizations. Most respondents do feel like the partnership with the NCSC is one of equals. However, its division of labor and partnership with the watchdogs and at the same time their dependency on information from the private sector results in tension. The NCSC therefore should not start to force private organizations by setting up and sanction based on regulations, as this is not their role but the role of the watchdogs. Best practices are helpful, but self-regulation is preferred. When taking a more authoritative position like the NCSC does with the reporting requirements is not the solution as this mixes up the division of labor. The information sharing should happen based on trust, as seen in the previous section. The existence of watchdogs is not contested by the respondents, but the regulations they function on should be clearer for both themselves as for the private sector.

When addressing the incentives that the NCSC uses, respondents are more satisfied. Especially the awareness it presents is to the satisfaction of most respondents. As set out in the NCSS2, the role of the NCSC as a distributor of knowledge and expertise is valued by some respondents, but also found insignificant by others. So, the incenting and teaching role of the government as presented in the NCSS2 is found helpful, but not essential. The awareness creating role seems to be more important.

4.4. Bottom-up approach

A sound bottom-up approach is the third element of a successful PPP, which encompasses broadly the regular consultation of the private sector and the equal basis of the partnership. Indicators of the bottom-up approach are therefore consultation and involvement of all parties involved, equality perception and voluntary cooperation. When all this is not present in the partnership, there would be too much authority at one side of the cooperation which would be

harmful for the effectiveness. In this case, it would be a hierarchical constitution and not much of a partnership.

4.4.1. Involvement of all parties

The element that first draws attention is a statement on the introductory page: "About 130 parties, including public and private parties, knowledge institutions and social organisations, were involved in the drafting of this new cyber security strategy" (NCSS2, 2013, p.3). The fact that the NCSS2 is written in cooperation with multiple parties of the private sector shows that the government has thought of involving the private sector by including it in the process of writing the NCSS2. Involving the private sector during the process of creating a strategy can be interpreted as a bottom-up approach. Moreover, this shows that the PPP on cyber security is perceived as a partnership between equals, which is also a characteristic of the bottom-up approach element. Letting the private sector in in the process of policy creation shows equality among the parties, which creates more involvement and therefore increases the chance of the PPP being successful, according to the theoretical framework as discussed in previous chapters.

That the government acknowledges the need for cooperation with private sector in its responsibility to protect the critical infrastructures has already been discussed in previous sections. However, this section will actively study how this involvement is being perceived by the respondents. The first notion of the government involving the private sector comes from Respondent 5:

> "I notice the effort they take to engage in dialogue, and to look at what really happens and not just to throw in regulation. They will rather try to connect and listen to parties, and only use regulation where necessary" (Respondent 5, translated from Dutch).

With this remark, the respondent wants to make clear that he feels that the government bases its regulation on consultation of the private sector, which fits in the bottom-up approach involvement of private parties. In other words, he perceives the regulations that are set up, are rightfully set up because they have emerged from bottom-up involvement.

A significant platform for involving all parties are the ISAC's. At these meetings, the government has three seats for its expertise, but does not chair the meeting nor does it determine the agenda. As Respondent 4 explicates:

> "The NCSC facilitates this body and we do not chair it. There is a core team of public partners in the ISAC's, the Team High Tech Crime (THTC), the General Intelligence and Security Service (AIVD) and the NCSC. Those are the core partners but are there to facilitate and with a role of expertise. The rest has a substantive role. The chairman is always someone from the sector" (Respondent 4, translated from Dutch).

This, coming from a former NCSC employee, is logically in line with the NCSS2 statement of stimulating involvement as she can be seen as a representative from the NCSC policy. Like the NCSS2 statement on involving all parties of the private sector in the discussion, this respondent also emphasizes the non-authoritative position of the government in platforms like these.

Most private sector respondents mentioned the ISAC's and all of those were positive about the initiative. This is evidenced by statements like: "If you look at an important information sharing platform for us, the ISAC. The financial ISAC is properly big. The government supports that" (Respondent 5, translated from Dutch). This statement shows that although the ISAC is important and the government takes place in it, it does not lead it, but merely support. The respondent from the Energy sector also values the role of the government in the Energy ISAC: "I consider the NSCS as a useful factor, with some side notes. Especially the coordination of the critical sectors, so within the ISAC's of the NCSC is exceptionally useful" (Respondent 2, translated from Dutch). With this, he emphasizes the role of the NSCS as coordinator within the Energy ISAC. Thus, it can be concluded that the ISAC construction is a helpful addition to the sector and the role of the government is according to the bottom-up principle as described in both the theory of this study and the involvement of private parties as described in the NCSS2.

Besides the functionality of the ISAC as a platform to engage parties of every sector with each other to share information, there are also some negative notions in the involvement indicator of bottom-up approach. As most of the respondents are or used to be active in a private organization active in a critical infrastructure, they indicate that they are satisfied with the ISAC and the government role in it. However, a downside has also been mentioned. This downside comprises the role of private organizations that are not directly part of the critical infrastructure services. As Respondent 2 noticed: "When we were part of Eneco and therefore not part of the Energy ISAC, I rare to never had contact with the government". This shows that when a company is ought to be not crucial for the critical infrastructures, the willingness to participate diminishes immediately. Although the cyber security PPP is in the first place designed for the

critical infrastructure protection, it seems, according to the bottom-up approach, a missed chance to ignore other parties. This is backed by the answers of respondents that are not or not anymore active in an organization within the critical infrastructures, like the one above.

Other respondents had the following to say about partaking in ISAC or other ways of involvement with the government: “But on the other hand, it would help the NCSC as we would also be able to share our ‘threat intel’ with them” (Respondent 6, translated from Dutch). With this, he suggests that as a ‘third party’ cyber security specialist, he feels excluded from the conversation although his information about threats can be equally important for protecting the Dutch digital world. However, because he is not directly distributing critical infrastructure services, the NCSC and with that the government does not seem to be interested to cooperate. Respondent 1, also active as a third-party specialist has remarked something similar: “The speakers of those conferences are like I said before, the usual suspects always” (Respondent 1). By this, he means that at cyber security events like the One Conference in 2017, only the same few organizations are invited to the table, which are the direct critical infrastructure organizations. Again, it makes sense that these organizations have the focus, but according to the bottom-up approach and the promise made in the NCSS2 to include ‘the private world’, it seems to be a missed opportunity not to actively engage the companies that arguably have the most cyber security knowledge. In the end, every cyber security professional works for the security of the cyberspace of the Netherlands.

4.4.2. Perception of equality

Furthermore, in the introduction the emphasis lies also on the fact that this strategy has been created together with the private sector. With the statement “Together, we can create a secure, free and profitable digital domain” (NCSS2, 2013, p.3), a serious attempt is being made to emphasize the equality in the partnership by underscoring the bottom-up approach. By stating “the government is taking the lead with this new strategy and will publish annual reports about the progress made” (NCSS2, 2013, p.3), it does make clear that the government is the initiator of the partnership, but this does not mean that equality cannot exist.

However, a more authoritative position is also being taken in the NCSS2. In the statement “existing sectoral regulatory authorities will have to widen their scope, if they have not already done so, to also include cyber security, in which overlap should be prevented”

(NCSS, 2013, p.19), the government implies that it does not have hesitations to take authoritative measures by installing and expanding authorities enabled to control private sector organizations on how they comply to the regulations that are set. As discussed in the previous section, setting up clear regulations is considered as a positive element in a partnership, as they may function as security levels that should be achieved. This makes regulations useful, as private sector organizations have a clear body of regulations to aim for. However, the implication that there will be authorities to check whether the private organizations actually achieve these standards changes this, as it then would deny equality between the private and public organizations. Moreover, it does not show trust between the organizations, and a successful partnership is based on trust without having to monitor every regulation. The installation of authoritative bodies to audit private organizations is not beneficial to the bottom-up approach that is necessary for a successful PPP.

When looking to this in the light of the answers provided by the respondents, there are some agreements as well as some discrepancies. When asked, nearly all respondents valued the cooperation with the NCSC as one of equals. Respondent 5 has the following to say about the cooperation: "It is for both sides a meaningful cooperation with reciprocity in it, which always has been very relevant. So, in the end it is a good cooperation" (Respondent 5, translated from Dutch). Especially the notion of 'reciprocity' indicates a perception of equality between the NCSC and this particular private organization. Respondent 3 agrees by stating that "Regarding coordination and cooperation, the NCSC takes an equal position, yes" (Respondent 3, translated from Dutch). This emphasizes the role of coordinating between private parties of the NCSC, for instance at the ISAC's, added by the fact that the NCSC does so by taking a position of equals. With this, it most likely wants to prevent itself from negatively influencing the cooperation by taking an authoritative stance. This also appears from the statement "on the topic of cyber security, we really go hand in hand. That is the feeling that I have, that we are here to improve one another" (Respondent 2, translated from Dutch). This indicates that the cooperation between the NCSC and the private organizations in the concerning ISAC are operating on the same level, as equals.

However, there is also another sound that must be discussed when looking at the cooperation between government and the private world. As mentioned before, there are government instances that are troubling the equal cooperation which seems to discredit the notion of 'partnership' between public and private. When discussing the PPP, Respondent 3 is of opinion that "I see that the meaningful contribution mainly is focused on mandatory

regulations, increasing personal data and cyber security related legislation" (Respondent 3, translated from Dutch). By this, the respondent sets out that the government is pressuring the private sector with oppressing regulation, which is different than the previous statements from the respondents about the cooperation with the NCSC. This is again evidence of the fact that the cooperation with the NCSC and the cooperation with the rest of the public sector organizations differs significantly. Where the cooperation with the NCSC is perceived as one of equals, the cooperation with most other government instances, is not.

As discussed in the clear legal guidance section, regulations are not necessarily a negative influence, if they are clearly constituted. However, the authoritative instances of the public sector are not perceived this way. Respondent 3 has the following to say about the authoritative watchdogs: "The ACM, the telecom agency and the authority personal data, those are the three most important ones, and they do take an authoritative stance. On the verge of being annoying" (Respondent 3, translated from Dutch). This is another emphasis of the regulatory pressure that have been discussed by the watchdogs. As said, regulations are widely perceived as a necessity, but it should happen based on equality as described by the bottom-up approach of successful partnership. As Respondent 3 continues: "From independent, unaffected monitoring. Which is nothing wrong with in itself, but you have to have the knowledge and expertise to do the right things" (Respondent 3, translated from Dutch). This means that this respondent perceives the watchdogs not only as authoritative, but also perceives a lack of legitimacy and expertise. This argument is, different than the argument made in the clear legal guidance section where it comprised lack of clarity, based on a lack of bottom-up constitution of the regulations. The regulations would have had more legitimacy among private organizations when they were included in the constitutional process.

In other words, it might not be the authority itself that is problematic, but rather the fact that private organizations do not feel like the authoritative instances are doing the right thing and setting up the right regulations. This could also explain the desire to be self-regulated, as can be interpreted from statements like

> "With this, we want to stay ahead of parties like the ACM, because when they say what we have to do, we can answer by saying 'we are already doing this'. We are already doing it better then you prescribe. In this way, we can stay ahead of regulations and remain able to set up our own priorities" (Respondent 2, translated from Dutch).

This statement implicitly states that the regulations that are received from the watchdogs are being contested by implementing own, self-regulated standards. This suggests that the regulations of the watchdogs are not valued as appropriate. The existence of the watchdogs and other authorities is not contested, but their functioning is perceived by most respondents as compelling. In short, it is not the fact that there are authorities that make regulations, but rather that the authorities that make them lack legitimacy, expertise, and are too compelling.

4.4.3. Voluntary cooperation

This third indicator of bottom-up approach can be recognized in the statement about the emphasis of mutual dependency. This appears from the statement:

> "The Netherlands is working to realise an active participation of citizens, businesses and government in the digital domain in the context of an ever-increasing mutual dependence between these actors and a complex environment in which a balance between security, freedom and social-economic benefits is constantly pursued" (NCSS, 2013, p.20)

With this, the need for inclusion of the private sector is being emphasized which can be interpreted as bottom-up approach, as it contains both an implicit notion of equality and regular consultation and getting together between public and private sector. This is necessary because the government acknowledges in this statement that it also relies on the private sector and that it cannot alone guarantee cyber security.

The respondents that have been interviewed seem to somewhat agree with this statement. One example is "I would like to say that companies do have a positive intention to share as much as they can" (Respondent 1). With this, the respondent tries to emphasize the willingness to cooperate with the government. This implicitly means that he is voluntarily in this partnership, since the most important goal of the partnership is information sharing. Moreover, he believes that other companies are also voluntarily cooperating and want to share as much as possible. This can indicate that he recognizes the mutual dependency between public sector and private sector as also mentioned in the NCSS2. In a somewhat different way, this is also addressed by in the statement

> "Filling in the big picture together. This means that we have to cooperate and crossing borders. For the government, of course this will be easier, they do not have a commercial interest, but private organizations have their own interest, they need to achieve results. But we also have to see that there is a societal interest, it is not only about profit" (Respondent 6, translated from Dutch).

This seems to be a summary of the whole partnership between public and private sector, with its biggest challenge included. Both sectors have interest in working together. However, they have different main interests: the public sector strives for securing the society whereas the private sector's interest is profit. However, despite these differences, both the NCSS2 and the respondent indicate that they are willing to cooperate with each other. In the end, the common interest is securing the cyberspace, as evidences by the statement:

> "As for the communal assessment of security the 'Nederland BV', I think you should be able to use all the information that is available. But the NDN is only for the critical infrastructures. When you see it going wrong somewhere else, sorry, I see it is going wrong but I cannot inform you. In this case I think, the ethics are touched upon. That is difficult for me" (Respondent 2, translated from Dutch).

Although the complaint of the rigidness of the critical infrastructure can be attributed to the chapter about involvement of all parties, his statement contains an urge to emphasize the communal interest of securing the Dutch cyberspace. This means that although the main interest of the private sector is profit, there is also an urge to keep the cyberspace secure, regardless their own primal interests. With this, the wish for fruitful cooperation is once more stressed. This can be interpreted as an indicator of voluntary cooperation.

4.4.4. Concluding Bottom-up Approach

On a concluding note, the bottom-up approach element is clearly represented in the NCSS2. The government has the intention to show that it needs the private sector in the battle for cyber security and is willing to cooperate with private organizations on an equal basis. Although a minor notion of authority is being used when discussing standards and regulations, the majority of the statements seem to imply a partnership based on mutual dependency and equality instead of top-down government measures. Based on this, the government seems to have thought-out

what kind of communication makes a partnership successful and according to the NCSS2, it is willing to abide to this.

In practice, there seems to be a distinction to make in the evaluation of bottom-up approach elements perceived by the private sector. Based on the statements that have been analyzed, it leaves little doubt that the partnership with the NCSC is mostly one in which the bottom-up approach is being uphold. Two of three main elements, perception of equality and voluntary cooperation are perceived positively. However, there are is a lack in involvement of all parties. When summarizing the positive findings, it is safe to say that the platforms like the ISAC's and the NDN are valuable contributions to the partnership with the NCSC. These platforms accredit a place at the table to share information between private critical infrastructure organizations and the government, which seems to function well. However, private organizations that are related to cyber security but are not directly involved with critical infrastructures seem to be ignored. They do not get invitations which seems to be a missed chance, as they might be able to contribute valuable information. Moreover, when looking at the promise of the government to include 'the private world', it seems to be only the private world within the critical infrastructures that is being included.

When looking at the perception of equality, there is also a distinction in the perception of the private sector. Where the government seems to be equal, it succeeds to do so regarding the NCSC. This government instance is coordinating the information sharing process and does not take a hierarchical stance in the partnership. Overall, the private sector instances perceive the NCSC as supposed to according to the NCSS2. However, when including other government instances like authorities and watchdogs, a troubling cooperation comes to surface. Not only is the cooperation with the watchdogs perceived as troubled, it also has influence on the work of the NCSC. The position of the watchdogs becomes negatively authoritative as they implement regulations which the private sector does not seem to agree with and does not seem to be able to self-regulate. The watchdogs are not open for suggestions and the regulation is often perceived as wrong, different from the position the NCSC takes.

The last bottom-up approach indicator is the voluntary cooperation of the involved parties. All parties, both public and private, seem to be aware of the interest they have in participating in a PPP. Even the authoritative watchdogs seem to be perceived as necessary by the private sector organizations, although they do not perceive their functioning in the same way. Overall, both public and private sector seem to be aware of the mutual dependency

between the two sectors and the necessity for a cooperation. The greater goal of securing the Dutch cyberspace is something that is also apparent in the private sector, despite their primal goal of profit. So, the problem of the cooperation should not be searched for whether private organisations are participating in the cooperation, but how it is filled in. Private party organizations are willing to share information with the public sector as much as they can and are aware of the necessity to do so. However, the regulations must be clear to become legitimate, as also discussed in the previous chapter and should be focused on self-regulation to make the partnership as effective as possible.

4.5. Community involvement

4.5.1. Introduction community involvement

The last element that the NCSS2 will be analyzed on it the involvement of a community. As elaborated on in both the theoretical and methodological chapters, community involvement is important as it shows that there is a sustainable support for the partnership. When there is a lack of support, the partnership will be less likely to sustain. As described in the theoretical chapter of this thesis, when all organizations support the PPP by publicly expressing support, the PPP will be more likely to be successful. Where in the previous section, the mutual dependency has already been discussed briefly, this chapter will more elaborately discuss the greater need for cooperation between public and private. In this way, the necessity for a partnership will be emphasized by considering whether the PPP is the solution, regardless of how it is functioning. When the PPP is perceived by both parties as the long-term solution, the community involvement is high as both sides support the partnership.

4.5.2. Public support

The first notion of community involvement that can be found in the NCSS2 is the statement "in order to be able to continue to respond to these threats, the Netherlands plans to further strengthen and extend their alliances with public and private parties" (NCSS2, 2013, p.3). In this statement, an implicit notion of believe in the long-term solution of the PPP can be found. By stating that the Netherlands wants to tighten the cooperation between private and public sector, the support from the community is emphasized. This can be interpreted as the whole of

public organizations that support the cooperation with the private sector in the field of cyber security. This also comes back in the statement "Increasing the Netherlands' digital resilience cannot be achieved by the government alone, as the ICT infrastructure itself and knowledge about this infrastructure is largely in the hands of national and international private parties" (NCSS2, 2013, p.13). Again, the need to involve the private sector is being stressed, as those are the organizations that control the infrastructures. Moreover, by explicitly saying that the government cannot do it alone, the need for partnership becomes even bigger and so does the support from the government side.

Another example of the need for a partnership comes forward in the respondent representing the NCSC:

> "The critical infrastructure's protection is in hands of the government but the execution lies for a certain percentage in the hands of the private organizations. So, the government is dependent on them. And they are in turn dependent on the government because they must comply to the regulations" (Respondent 4, translated from Dutch).

With this, she emphasizes, as stated in the NCSC, that the dependency goes both ways: the private sector has the infrastructures in control and the government has the responsibility to protect the Dutch society.

Other respondents join in with this argument for the necessity of the PPP of cyber security: "The fact that the cooperation is going on for several years means that we need each other. If we did not profit from it, the cooperation would not be this good" (Respondent 5, translated from Dutch). This is a more general statement about the cooperation, but nonetheless shows that private cyber security practitioners have accepted the fact that private and public needs each other. The same respondent continues by stating: "What we need is the coordinating role of the government" (Respondent 5, translated from Dutch), which is somewhat similar of the comment of Respondent 1: "Do you understand this balance where one has the mandate and the other has the expertise" (Respondent 1). These two statements contain some notion of division of labor in which both parties have a fixed role to play: the public sector has the mandate and the oversight to coordinate, where the private has the expertise and the information. As this division of labor is fixed, both sectors are destined to work together.

4.5.3. Need for cooperation

When discussing the element of community involvement, one of the indicators is the necessity of the partnership. By emphasizing that both public and private are dependent from each other, this necessity is stressed explicitly. The NCSS2 starts by summing up every group or community that allegedly benefits from the partnership. Something similar does the statement "A joint effort made by all parties involved is required, in which each of the parties is expected to take own responsibility" (NCSS, 2013, p.26) contain, with more focus on the individual parties. However, the importance of working together is once more being emphasized which according to the theory can be interpreted as evidence of support from the community that is being represented. A somewhat similar statement is made:

> "The dependencies in the digital domain are also expressed in the chain of producers, providers and clients. These mutual dependencies will have to be discussed by the chain partners to conclude joint agreements about minimum requirements, interoperability and reliable information-sharing" (NCSS2, 2013, p.20).

This need for cooperation is also stressed by the respondents:

> "A company like Shell cannot say 'we will go on without electricity for five minutes'. When that happens, we face the consequences for months and the economy is impacted significantly. I cannot think of a process from which electricity is not a part of" (Respondent 2, translated from Dutch).

This respondent, active within the Energy sector, stresses with this comment that when a private organization like Shell suffers from a cyber-attack that puts down electricity, the whole country will feel the consequences. Therefore, he explicitly makes clear that securing the cyberspace is a matter of both public and private sector and requires cooperation. This is the level of support that means high community involvement, as it implies that the necessity for the partnership is so significant, everyone involved with cyber security would support it. Respondent 6 calls for even more support from the government side: "We need each other. If it appears on the political agenda and it is being stimulated from the highest level, I think it can get even higher on the agenda" (Respondent 6, translated from Dutch). By stating he wants to have even more support from the highest political levels, he emphasizes that he perceives the cooperation should be a political priority, which implicitly shows support from his side. Therefore, this can be interpreted as support from the private sector side.

Besides these multiple of positive statements regarding the need for partnership to create support by community involvement, some respondents were less positive about the cooperation. Especially the need for a government part in the PPP is questioned by some respondents. The first doubt has been presented by Respondent 5:

> "The private sector can to a large extent carry their own weight and has its own form of organization. The very rich are in the Information Security Forum and in Gartner and the smaller ones are in the Platform Information Security and other clubs in which they reside. (…) If the government would back out today, the system would not collapse" (Respondent 3, translated from Dutch).

With this, the respondent wants to emphasize that the private sector can also organize itself and does not necessarily need the coordination of the government. This can be interpreted as a negative indicator, as this respondent believes that the private sector could survive without the public sector, and thus questioning the need for the cooperation. The same goes for the statement "So are they holding us back, no. But is there more potential, yes" (Respondent 1), suggesting that the government does not really contribute to the success of the partnership. This respondent does not negatively experience the government's role in the partnership, but does not see a big addition to it as well. This indicates a more insignificant role of the government, also implying that the private sector would be able to manage without the government's partnership. However, this is not a widely shared opinion among the respondents.

4.5.4. Concluding community involvement

To end with, the involvement of community does not come back often in the NCSS2. However, the notions that have been discussed do show a wide support among government instances regarding the partnership with the private sector. According to the NCSS2, partnership is supposed to be the solution when countering cyber threat. The private sector is somewhat more divided, but mostly agrees with the support for the PPP. Most respondents agree with the government in the support for the partnership, but some seem to think that the private sector would maintain when it would not partner up with the government. The proponents of the partnership mainly bring arguments to the table that indicate the mutual dependency in the protection of critical infrastructures that are connected to the Dutch cyberspace. Where the public sector has the responsibility to protect the cyberspace and with this the critical

infrastructures, the private sector has the most tools to do so. This paves the way for partnership, according to the NCSS2 and several private sector respondents.

Overall, the partnership is valued as necessary and helpful, but leaves room for improvement. The support from the community seems to be large enough to continue with the PPP approach. The indications of mutual dependency and interwovenness of public and private are sufficiently apparent to make such a conclusion. This indicates that there are no big discrepancies between the public and private sector when it comes to community involvement.

4.6. Conclusions

4.6.1. General remarks

The analysis of this document should be interpreted as a study to create a picture of how the government has meant the partnership. In other words, the partnership written on paper, the *written truth*. When turning to the *perceived truth*, there are some notable discrepancies found, but also elements that are perceived in the same way as the government meant it when writing the NCSS2 in 2013. These discrepancies will be discussed in the next section, when the main and sub research questions will be answered, using the sub conclusions of the four elements as discussed above.

4.6.2. The written truth of the NCSS2

To answer the research question of this thesis, this section will use the empirical findings to find answers to the sub questions. These answers together will form the answer to the main research question. The first sub question that must be answered contains the *written truth* of the cyber security PPP; *How is the Dutch PPP described in the National Cyber Security Strategy 2 in terms of the required level of trust, legal guidance, bottom-up approach, and community involvement?* To answer this question, the most important findings will be presented from the analysis of the NCSS2.

When discussing the four elements of a successful partnership as described as presented in the theoretical chapter of this thesis and as included in this sub question, it can be firstly concluded that it seems that the creators of the NCSS2 took notice of the elements that make

partnerships successful. All four aspects are represented, with the clear legal guidance and bottom-up approach as the two most represented elements. This means that when the NCSS2 was constructed, the government carefully deliberated on how the partnership should function for it to become a success. Although some notion has been found of the government promoting an authoritative role for itself or one of its bodies, overall it seems that the partnership is supposed to be one between equal parties. The government perceives the partnership mainly as one based on standard requirements and self-regulation, which leaves room for private organizations to take their own responsibilities when it comes to cyber security.

It should be noted, however, that the government has the organizing role in the partnership, which can explain their enthusiasm in the partnership. However, the NCSS2 seems to be well thought of considering the four elements of a successful partnership. Although not all elements are evenly represented in the NCSS2, the rhetoric that has been used makes clear that the creators of this policy document carefully constructed the different dimensions of partnership with the private sector. For example, community involvement does not come back often in the NCSS2. Nonetheless, at the occasions that the element of community involvement is recognized, it shows that the government does believe in the PPP as a solution to tackle cyber threat.

When looking at the four elements of an effective partnership individually as the *written truth* of the NCSS2, the most notable finding is that although all four elements can be found to some extend in the strategy, some are more represented than others. This can indicate that the government does not give enough attention to some elements. This might be because the government set priority for the different elements, but this study aims to see whether this is a right choice or that the government should have an extra focus on some aspects in the new cyber security strategy that is coming up in the upcoming years. One of the elements that has not been found often in the NCSS2 is the trust element. Although the importance of being transparent is emphasized in the strategy, it seems somewhat to lack in clear plans to enhance the information sharing coming from the private sector. One possible measures to lower the threshold is to stimulate voluntary information sharing, whereas this happens now mostly through regulatory pressure.

For the legal guidance element, the biggest challenge that presented itself in the findings of this study is the formal relationship between the NCSC and other public instances like watchdogs. Were the theory states that authority has negative influence on the partnership, it might become acceptable when the regulations are set out clearly. In the NCSS2, the emphasis

lies on the allocations of government and private roles. For the government side, this means that it should be clear which public instance is responsible for what and which accountability mechanisms are in function. When this happens through consultation of the private sector, legitimate regulation will appear. However, although the government stresses the fact that the allocation of roles must be clear, it remains unspecified in how this allocation is constituted, with several public instances making regulations and do or does not sanction.

The element of bottom-up approach has arguably the focus of the government. In the NCSS2, the involvement and equality among public and private parties is addressed at multiple occasions. The NCSS2 is even constituted with direct input from the private sector organizations that are involved with the critical infrastructure protection. Moreover, the language used in the strategy shows that the government actively tries to present the involvement towards the outside world, by emphasizing the notion of 'together'. The constitution of the ISAC's seems to be one of the key measures to organize the involvement of the private sector. Although the equality is being stressed several times, the government notes that it still has the lead in the organization of the PPP.

The last element that has been studied in the NCSS2 is the community involvement, that is the support that the PPP can count on. In short, from the government perspective, the PPP seems to have full support. The government shows its faith in the PPP as a solution for cyber security. It is not being emphasized often, but the relevant statements make the support for this solution obvious.

4.6.3. The perceived truth of the respondents

To give an answer to the question *How is the cooperation with the government in the cyber security PPP perceived, in terms of trust, legal guidance, bottom-up approach, and community involvement by the private sector parties that are involved,* this thesis interviewed six cyber security professionals that have been active in the four most cyber intensive sectors, and one representing the NCSC. Again, the retrieved empirical data was analyzed according to the four elements of successful partnership. On the contrary to the analysis of the NCSS2, this has given insight to the *perceived truth* of the functioning of the Dutch cyber security PPP.

The first element to discuss is the element of trust between the partners that are involved. In the perception of the respondents, three main indicators of trust have been distinguished. The

first and most important one is the transparency among participating organizations towards each other and the government. The intention for private organizations to be transparent is undoubtedly there, but in practice they experience difficulties. Two of the biggest difficulties that have been found are the relationship of the NCSC with the watchdogs. This makes private organizations hesitant as they are unsure what will happen with the information. Somewhat similar happens in the second difficulty found, which encompasses the profit driven nature of private organization. Sharing data is the intention, but their competitive position does not allow such levels of transparency. The existence of the WOB has influence on both difficulties as this enables external parties to access almost all information shared with the government.

The clear legal guidance as perceived by the respondents mainly comes down to division of labor, regulations and use of incentives. The division of labor with formalized roles in the PPP again is troubled by the cooperation with the watchdogs. As the NCSC respondent said, the NCSC is also collaborating up with the watchdogs and is also implementing regulations, which makes it unclear for the private organizations to know who does what. Although the NCSC can only function with enough information input, regulations seem to be off limit as it endangers the equal relationship. When looking at the government regulations themselves, they are perceived mostly as ambiguous and unclear. Respondents regularly noted that the governments regulations were unclear or not effective. This is complemented by the relational problems between the NCSC and the watchdogs, wherein the one takes the equal position and the other the authoritative, but still have overlap in their functioning, like when it comes to regulatory pressure. One respondent openly questioned whether the government knows what it is doing. Because of this unclear norms and regulations of the government, private organization find it hard to self-regulate since they do not have clear guidelines. This conclusion is according to the interviews, most respondents did not perceive regulation as negative, as long as it is clear and consequent. Besides the regulations, the output received from the NCSC is valued as useful by most respondents. The expertise and the coordinating role of the NCSC is perceived positively, although some respondents noted that the government could do more. This can either be more political attention or more qualified personal.

The bottom-up approach mainly encompassed the extent to which the public sector included involved the private sector in its policymaking, and how. In the findings, there is again a distinction between the NCSC and the rest of the government, especially the watchdogs. For the NCSC goes, the private respondents perceived the partnership mostly as equal, voluntary, and open for input. However, the watchdogs are described as rigid, authoritative, and even

stubborn. This perception can even have negative influence on the partnership with the NCSC as both instances are from the public sector. Therefore, when answering the question about the private perception of the governments' function in the PPP, no unambiguous answer can be given, as there are multiple public instances active that are perceived differently. Another negative notion that has been found is that the public sector focusses only on organizations that are directly active in the critical infrastructure protection. Organizations that do not qualify are not invited to the table, which is a missed chance as they often can contribute useful information.

The last element to conclude when discussing the perception of partnership by the private sector is the community involvement. To what extend the cooperation is necessary and how much support it gets are indicators of effectiveness. When looking at the support of the PPP, the private sector mostly agrees with the NCSS2 that there is a need to cooperate when attempting to secure the Dutch cyberspace. Most respondents, although often critical of the partnership, seem to accept that collaborating with the government can help both sides. Only one respondent had the opinion that the private sector would manage without the governments' influence. Other respondents mostly emphasized that the security of the cyberspace and thus the critical infrastructures is so important, it needs some coordination and arguably regulation from the government. Therefore, it does not lack for support for a PPP, regardless the points of improvements that have been presented. This is also backed by the fact that almost all respondent observed an interdependence between public and private. There may be different main reasons for striving for cyber security, the end goal is the same for both sides: securing the Dutch cyberspace.

4.6.4. Discrepancies

Having presented both *written truth* and *perceived truth* according to the used theory, this section will look at *how possible discrepancies between the NCSS2 and the perception of the private sector can be explained.* Therefore, it will discuss the main differences between public and private regarding the Dutch cyber security PPP. By doing so, this thesis can give an answer to the research question encompassing what the main differences are between the intended partnership by the government and how it works out in practice. The main discrepancies will again be discussing according to the four elements, altogether functioning as an answer to the

main research question of this thesis: *How is the cooperation between the government and the private sector regarding cybersecurity through Public Private Partnership as constituted in the Dutch National Cyber Security Strategy 2 taking shape and how can possible discrepancies between this strategy and the perception of the private sector be explained?"*

For the trust element, the biggest discrepancy lies within the emphasis of transparency. Where the NCSS2 states that transparency should be one of the key points of the PPP, the respondents perceive difficulties mainly in the existence of the WOB and in the roles of the watchdogs in the partnership. Where the WOB creates distrust because of the access to sensitive information it provides for external individuals like journalists, the existence of the watchdogs is reason for hesitation of private organizations as everything they share might turn into sanctions or new regulations. These two aspects are in the way for private organizations to become fully transparent, something that all respondents interviewed for this thesis mentioned as something they intent to be or become. Regardless this intention to be transparent, the business interest is the biggest interest for private organizations. Therefore, the intentions will remain intentions when being fully transparent threatens to have consequences for the business of the organization.

For the clear legal guidance element, two main problems have been distinguished. The first challenge again concerns the relationship between the different public organizations. Where the NCSS2 speaks of clear allocation of roles, this seems to be a problem in practice. The NCSC and the watchdogs are both implementing regulations which makes it for private sector organizations unclear who does what and who is accountable. Moreover, many of the regulations seem to be vague, normative, and ambiguous. These two aspects are cause for the conclusion that the regulations of the government in the Dutch cyber security PPP cannot be classified as 'clear', which means that this is a negative influence on the effectiveness of the partnership. Regulations are not valued as something bad by the respondents of this study, but the government must be more clear, consequent, and decisive when it comes to regulations. Moreover, there should be one organization responsible for the regulations and not several different organizations. In this way, the NCSC can focus on being an equal partner, whereas the watchdogs can take the responsibility to set up regulations and stimulate compliance. This division of labor is not clear enough according to the findings of this study, while the NCSS2 states that this should be evident.

The bottom-up approach is an element that has significant attention of the government when looking at the NCSS2. In the strategy, multiple emphases can be found that concern involvement of the private sector, indicating that the government takes this element seriously. In practice, this can be noticed to some extent, but with some bottlenecks. The involvement and cooperation with the NCSC is mostly valued as useful and valuable. With its role in the ISAC's and in organizing platforms like the NDN, private organizations active in the critical infrastructure protection feel like the NCSC is a helpful and equal partner. However, private organizations that are not directly involved with critical infrastructure protection are barely or not involved at all. This is felt like a deficiency, both by respondents that are active in organizations not involved with critical infrastructure protection, but also by respondents that are. This is a discrepancy as the NCSS2 allegedly addresses the whole private sector, which it does not in practice. The presence of authoritative organizations like watchdogs are not perceived as negative per se, but only become so when the private sector perceives the regulations it implements as wrong, unclear, or unjustified, which happens regularly as discussed in the previous section.

The last element to discuss the discrepancies from is the element of community involvement. The main indicators of community involvement are not found often in the NCSS2, but the statements that have been identified can be distinguished as useful. The overall conclusion can only be that both public and private side agree that some degree of partnership is necessary and desirable. Were the government emphasizes through the NCSS2 that it needs the private sector as the critical infrastructures are mostly owned by the private sector, vice versa does the private sector thrive on the coordinating role and information processing role of the government. In this regard, few discrepancies can be identified. Some respondents valued the role of the government different than others, but embraced the partnership idea when it comes to cyber security in the Netherlands. Only one respondent had the idea that the private sector would manage without the government, but did not specify whether it would be better off without it.

5. Reflection

5.1. General reflections

The aim of this thesis was to study how the effectiveness of the Dutch cyber security PPP and how this could be improved. To do so, the PPP was studied for discrepancies between the intended partnership by the government and the perception of the partnership by the private sector. The findings of this study mainly encompass some of the fields and subjects that are not functioning as they should to create the most effective partnership as possible. Therefore, the findings can have a contribution to both the scientific discourse on how partnerships can be evaluated on effectiveness and to the societal discourse on how the cyberspace of the Netherlands (or any other country) should be secured. By looking at both the public, policymaking side and the private, practical side, a comparison can be made to see whether there is unanimity on the subject. Elements that are malfunctioning can consequently be identified and analyzed to gain knowledge on which of these elements in the partnership should gain more attention. By consulting both public and private sector, a comprehensive assessment can be made of the Dutch cyber security PPP.

Although the five respondents from the private sector all came from different organizations from mostly different sectors, several subjects were addressed by almost all of them. Even the respondent representing the NCSC gave somewhat the same answers when asked how the main elements that have been researched functioned in her perspective. These findings indicate that there are some aspects in the PPP that are not functioning to their potential, regardless from the position of the perceiving organization. This suggests that there must be some truth in it, as the issues that have been addressed are noticed from different sectors and even from recent employees of the NCSC. These discrepancies can be valuable for the creators of the new NCSS, as these may indicate points that ask for special attention.

5.2. Limitations on generalization and applicability

Although the analysis of both the NCSS2 and the interviews with the respondents brought some positive and negative points to the light, there are some limitations that should be addressed. First, although the respondents have been carefully selected to make sure to cover the most cyber intensive sectors, the number of respondents is relatively low. This makes this study hard to generalize, as another person from the same sector can have another opinion. However, this

is not the goal of qualitative discourse analyses nor was it the goal of this study upfront. As the goal of this explorative study was to create an overview of the Dutch PPP, one respondent from these sectors is enough to give an indication of what is functioning and what is malfunctioning. Because the effectiveness of the cyber security PPP has not been studied extensively yet, the explorative study is the most appropriate study, even though it does not lead to generalizable findings. Every empirical study that adds to the study of the cyber security PPP is therefore valuable.

As several respondents mentioned, the sectors may differ from each other when studying them more in depth. Therefore, more research should be done to the sectors individually with multiple respondents per sector to come up with tailor-made policy improvements to enhance the functioning of the PPP per sector. As said, this thesis is aimed to create an overview and can therefore be interpreted as somewhat superficial. Nonetheless, the findings that have been presented can be valuable to determine which part of the PPP requires more in-depth research, as befits explorative studies. Therefore, this study should be interpreted as an addition to the few existing studies on effectiveness of the cyber security PPP and should function as a gateway for new research in the future. The findings of this study should not be interpreted as generalizable facts but are meant to evoke more research to this specific aspect. This is especially useful for the topic of cyber security PPP, as not much study has been done on this subject other that the article of Madeline Carr in 2016.

Finally, there is another significant limitation that must be mentioned could not be influenced during the writing of this thesis. This limitation is the fact that the NCSS2, the main source for the document study of this thesis, was written in the year 2013. Already four years old combined with the rapidly changing world of cyber security, there are undoubtedly aspects that have been discussed that have changed significantly in the conduct of the government policy. To minimalize the differences between how the government has written down their strategy in 2013 and how it is executed now, the respondent of the NCSC has been interviewed. In this way, a more recent representation of the governments policymaking has been given. This concerns just one respondent, but it can be valuable for updating and nuancing the possibly outdated strategy. At the same time, this limitation can also be an emphasis of the relevance of this study. As the new cyber security is currently in the making, this study can add to its constitution as it exposes some difficulties that can and should be overcome in the new strategy, or at least have some special attention of the writers of the new document.

5.3. Contribution of this thesis

5.3.1. Societal contribution

In the contemporary society, cyber is becoming an increasing important term as the connectiveness of society is on the rise. With this increased connectivity, the security implications of the cyberspace also increase. When looking at the recent WannaCry attack on the twelfth of May in this year, over 45.000 attacks were reported in seventy-four different countries (NCSC.nl, 2017c). With attacks of this impact, the importance of a functioning cyber security strategy is once more emphasized. To do so, the cyber security PPP must be evaluated regularly to discover weak spots in the effectiveness. This study tried to do so, with several main findings that indicate elements that are worth improving or at least more study. Therefore, combined with the fact states above that not much study is done on this subject, this study can be useful in securing the Netherlands against threats such as WannaCry. By improving the effectiveness of the Dutch cyber security PPP, the Netherlands can become more secure by becoming more resilient against threats. As the findings of this study proves, there are several improvements to make which means that the cyber security PPP is not functioning at its full potential now. This makes the findings of this study both important and urgent, as weak spots in the PPP may indicate opportunities for hostile parties to penetrate the Dutch cyberspace. In this way, the government can learn from the practice, how their strategy and policy is perceived and consequently take these findings into account when designing a new strategy.

5.3.2. Scientific contribution

When discussing the effectiveness of a PPP, there is some more literature to consider than when focusing on the cyber security PPP specifically. However, as the topic of cyber security is relatively new, it is interesting to see how the partnership functions in this new field. Therefore, the findings of this thesis can add to the discourse of measuring effectiveness of partnerships between public and private. The studies of effectiveness of PPP's are mainly limited to theoretical models, like the one of Manley (2015) that was largely used as the foundation of this thesis. These theoretical studies need application of the models that it produces in practice by using empirical data. This is done in this study, as the four elements of Manley (2015), added with some indicators from other effectiveness studies, have been used on a case study containing actual empirical data. Therefore, this thesis adds to the scientific body of knowledge

by using models of determining effectiveness on new security PPP's. The theoretical model that has been used for this thesis, the modified model of Manley (2015) turned out to be suitable for the analysis. This is apparent from the significant number of indicators that have been found in the document study as well as in the interviews.

5.3.4. Policy recommendations

The findings of this thesis suggest several policy recommendations for future strategies, for example for the new NCSS coming out in the upcoming years. However, as this study concerns an exploratory study, the aim of this thesis was rather to evoke new studies than to present direct policy suggestions. Despite this exploratory aim of the study, some main problems have been addressed by almost all respondents which makes it somewhat safe to say that these problems should require certain new policy. For this sake, these policy recommendations will be addressed to the makers of the NCSS3. However, these recommendations should only be interpreted as indications and require more in-depth research before implementation into actual policy.

The first policy recommendation is based on the issue with the law of WOB. This law, which makes it possible for anybody to gain insight in almost every government body, excluding intelligence services. Because this law is also applicable on the NCSC, the private sector organizations are hesitant to share information with the NCSC as this information basically becomes public. It is therefore not that private organizations do not trust the government with the information, it is the public access to it that concerns them. This should be addressed in the new strategy, for example by providing the NCSC exclusion on the WOB like intelligence services also have. Transparency of government bodies is an important asset for a democratic society, but examples should be made to make sure that these organizations function properly. As the NCSC only exists because of the feed information it gets from the private sector, it must be a priority to safeguard this feed. Providing public access to this feed by law means it is risked too much to function at its full potential.

A second policy recommendation can be made regarding the cooperation between organizations from the cyber security PPP and the different watchdogs that are active in the Netherlands. At the moment, it is sometimes unclear which how the public sector is organized. The watchdogs seem to be responsible for development and compliance of regulations, but the NCSC is also developing regulations, although not mandatory. Moreover, the NCSC is also

collaborating with the watchdogs, which makes it unclear for private organizations what information is being exchanged between these public organizations. The influence of watchdogs on the PPP is necessarily perceived as negative by the respondents, but should be more transparent, even as the information exchange with the NCSC. In this way, the private organizations know what the NCSC shares with the watchdogs which might improve the transparency between NCSC and private organizations which will benefit the effectiveness of the PPP.

The third policy recommendation that can be made according to the findings of this thesis encompasses the inclusion of private organizations that are not directly involved with the protection of the critical infrastructures. Although it leaves little doubt that the private organizations that are directly responsible for critical infrastructure protection should be priority, it seems like a missed chance to not include private organizations that are professionalized in cyber security but not directly involved with the protection of the critical infrastructures. Several respondents mentioned this missed opportunity to include the information and expertise of these cyber security practitioners. Organizations that are professionalizing cyber security services in every from can contribute to the overarching goal of securing the Dutch cyberspace. Therefore, all the information available should be included in the formation of new policy and new cyber security mechanisms. In the NCSS3, when the inclusion of the private sector is mentioned for the protection of the critical infrastructures, the whole private sector should be addressed and not only organizations directly involved with critical infrastructures. The information that other cyber security systems can provide is too valuable to be ignored.

5.3.5. Future study

As mentioned before in this chapter, the greater goal of this study was to determine which specific aspects of the cyber security PPP need more study to eliminate discrepancies. Although the respondents gave varied answers, multiple respondents addressed the same aspects. The policy suggestions mentioned above should therefore be studied more specifically before implemented into new policy. According to the findings of this study, future study should be focus on how the NCSC relates to the watchdogs that are active in each sector. Because each sector has their own watchdogs, the NCSC should make clear arrangements with the watchdogs about who does what. To do so, more case studies should be conducted to how these public

instances are currently working together. Moreover, a network analysis should be done to map the public sector organizations active in the field of cyber security. In this way, an overview can be obtained about sector specific partnerships, which should be the basis of new government policy. As the sectors that are cyber related, which is considered to be a growing number, can differ significantly from each other, it might be impossible to come up with uniform policy that fits every sector. This proofs once more that this study should be perceived as an indication for new studies and not for direct policy suggestions.

Bibliography

Barriball, K. L., & While, A. (1994). Collecting Data using a semi-structured interview: a discussion paper. *Journal of advanced nursing*, 19(2), 328-335.

Börzel, T. A., & Risse, T. (2005). Public-Private Partnerships: Effective and legitimate tools of international governance. *Complex sovereignty: Reconstructing political authority in the twenty first century*, 195-216.

Bryman, A. (2012). *Social research methods*. Oxford university press.

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43-62.

Clark, K., Stikvoort, D., Stofbergen, E., & van den Heuvel, E. (2014). A Dutch approach to cybersecurity through participation. *IEEE Security & Privacy*, 12(5), 27-34.

Clinton, W. J. (1996). Executive order 13010-critical infrastructure protection. *Federal Register*, *61*(138), 37347-37350.

Cyber Security Beeld Nederland. (2016). Directie Cyber Security van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

Dunn-Cavelty, M., & Suter, M. (2009). Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection*, *2*(4), 179-187.

Dynes, S., Goetz, E., & Freeman, M. (2007). Cyber security: Are economic incentives adequate?. *Critical Infrastructure Protection*, 15-27.

EU Cybersecurity Dashboard, 2015. Accessed through: http://cybersecurity.bsa.org.

Flyvbjerg, B. (2006). Five misunderstandings about case-study research. *Qualitative inquiry*, *12*(2), 219-245.

Gerring, J. (2004). What is a case study and what is it good for?. *American political science review*, *98*(02), 341-354.

Gray, C. P. (2013). Cyber Utilities Infrastructure and Government Contracting. *Nat'l Sec. & Armed Conflict L. Rev.*, 3, 151.

Guitton, C. (2013). Cyber insecurity as a national threat: overreaction from Germany, France and the UK?. *European Security*, 22(1), 21-35.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, 53(4), 1155-1175.

Hare, F. (2010). The interdependent nature of national cyber security: Motivating private action for a public good. George Mason University.

Jackson, R. (2007). Constructing enemies: 'Islamic terrorism' in political and academic discourse. *Government and Opposition*, *42*(3), 394-426.

Kleinwachter, W. (2002). From self-governance to public-private partnership: The changing role of governments in the management of the internet's core resources. *Loy. LAL Rev.*, *36*, 1103.

Klimburg, A. (2012). National cyber security framework manual. *NATO CCD COE Publication.*

Klijn, E. H. (2009). Public–private partnerships in the Netherlands: Policy, projects and lessons. *Economic Affairs*, *29*(1), 26-32.

Kumar, S., & Phrommathed, P. (2005). *Research methodology* (pp. 43-50). Springer US.

Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. *Cyberpower and national security*, 24-42.

Manley, M. (2015). Cyberspace's Dynamic Duo: Forging a Cybersecurity Public-Private Partnership. *Journal of Strategic Security*, *8*(5), 85-98.

Maughan, D. (2010). The need for a national cybersecurity research and development agenda. *Communications of the ACM*, 53(2), 29-31.

Ministerie van Veiligheid en Justitie, (2013). De Nationale Cyber Security Strategie 2. Van bewust naar bekwaam. Accessed through: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2013/10/28/nationale-cyber-security-strategie-2/rapport-nationale-cybersecurity-strategie-2-2.pdf.

National Cyber Security Centre. (2016). Weerbare vitale infrastructuur. Accessed through: https://www.nctv.nl/binaries/Factsheet%20weerbare%20vitale%20infrastructuur_tcm31-234709.pdf.

NCSC.nl. (2017a). National Detention Network. Accessed through: https://www.ncsc.nl/english/Cooperation/national-detection-network.html

NCSC.nl. (2017b). ISAC's. Accessed through: https://www.ncsc.nl/english/Cooperation/isacs.html

NCSC.nl. (2017c). Grote activiteit van pogingen tot ransomware besmettingen. Accesses through: https://www.ncsc.nl/actueel/nieuwsberichten/toename-van-pogingen-tot-ransomware-infecties.html.

Nederlands Dagblad. (2016). 75-plusser steeds vaker online. Accessed through: https://www.nd.nl/nieuws/actueel/binnenland/75-plusser-steeds-vaker online.2453225.lynkx.

Obama, B. (2009). Remarks by the President on Securing our Nation's Cyber-Infrastructure. *The White House, East Room*. Accessed through: https://www.whitehouse.gov/the press- office/remarks-president-securing-our-nations-cyber-infrastructure.

Osborne, S. (2002). *Public-private partnerships: Theory and practice in international perspective*. Routledge.

Savas, E. S., & Savas, E. S. (2000). *Privatization and public-private partnerships* (p. 4). New York: Chatham House.

Skelcher, C. (2005). *Public-private partnerships* (pp. 347-370). Oxford University Press, New York.

Stiglitz, J. E., & Wallsten, S. J. (1999). Public-private technology partnerships: Promises and pitfalls. *American Behavioral Scientist*, *43*(1), 52-73.

United States. Office of the Chairman of the Joint Chiefs Staff. (2006). *The national military strategy for cyberspace operations.* Department of Defense.

Wettenhall, R. (2003). The rhetoric and reality of public-private partnerships. *Public Organization Review*, *3*(1), 77-107.

Yin, R. K. (2003). Case study research (Vol. 5). *Thousand Oaks, California*.

Zhang, X. (2005). Critical success factors for public–private partnerships in infrastructure development. *Journal of construction engineering and management*, 131(1), 3-14.

Appendix

Interview protocol

At the start of the interview, the respondent was asked for permission to record the interview. After this, they were asked to introduce themselves and include how they relate to the cyber security world and the cooperation with the government.

The following questions were used as a guideline for the interviews. They are provided both in Dutch as in English as one of the respondents did not speak Dutch so the interview was conducted in English. The other five interviews were conducted in Dutch.

The order of the questions was not always the same to benefit the advancement of the interview. Moreover, not all questions were asked as sometimes a question was already answered during another question.

Trust

- How would you broadly describe the cooperation between your company and the government regarding cyber security?
  Hoe zou u de samenwerking of relatie tussen de private sector en de overheid kort willen omschrijven?

- Could you briefly describe the process of information sharing with the government?
  Hoe gaat het proces van informatie delen tussen de private sector en de overheid normaal gesproken?

- How would you evaluate the cooperation between your company and the government? What are tensions/difficulties
  Hoe zou u de samenwerking willen waarderen? Wat zijn moeilijkheden, uitdagingen?

- Do you feel like the cooperation is based on equality?
  Heeft u het idee dat de samenwerking gebaseerd is op gelijkheid tussen uw bedrijf en de overheid?

- Do you feel like both parties are fully transparent towards each other?
  Heeft u het idee dat beide volledig transparant zijn tegenover elkaar? Waarom?

Clear legal guidance

- Is it clear for you what the government expects from your company?
  Is het voor u duidelijk wat de overheid van de private sector verwacht?

- What does your company expect from the government in the cooperation?
  Andersom, wat kan de private sector verwachten van de overheid?

- What would you say are the shared objectives between your company and the government?
  Wat zijn kunt u aanwijzen als gemeenschappelijke doelen van de private sector en de overheid?

- How will these objectives be accomplished?
  Hoe worden deze doelen bewerkstelligd?

- Does the government provide sufficient assets, like knowledge and resources for your company to enhance the ability to create cyber security?
  Vindt u dat de overheid genoeg aanreikt in het bereiken van cyber security, zoals kennis, middelen et cetera?

Bottom-up approach

- How does the communication with the government normally go? Consultations, meetings etc.
  Hoe ziet het contact er normaal gesproken uit tussen u en de overheid?

- How often do you assemble with the government in bilateral or multilateral meetings?
  Hoe vaak komt uw bedrijf bijeen met de overheid in bilaterale of multilaterale ontmoetingen?

- Do you feel that the government is open for suggestions or remarks from the private sector?
  Vindt u dat de overheid genoeg openstaat voor input vanaf de private sector?

- Do you feel like the cooperation with the government is a cooperation between equal parties?
  Heeft u het idee dat de samenwerking gebaseerd is op gelijkheid tussen alle partijen?

- Does your company share all the information available with the government if asked?
  Denkt u dat uw bedrijf alle informatie deelt met de overheid indien gevraagd?

Community involvement

- Do you feel like your company needs the government in establishing cyber security?
  Heeft u het idee dat de private sector de overheid nodig heeft voor cyber security?

- Do you feel like the government holds your company back in providing cyber security?
  Heeft u het idee dat de overheid uw de private sector weleens dwars zit op het gebied van cyber security?