Institute for Security & Global Affairs
Leiden University – Faculty of Governance & Global Affairs

Master Thesis Crisis and Security Management

Universiteit Leiden

Cybersecurity through Public-Private Partnership in the Dutch Drinking Water Sector

Author: Tessa Mulders

Master thesis

Program	Master Crisis & Security Management	
Student	Tessa Mulders	
Student Number	S2086190	
Date of admission	28-1-2019	
Subject	Water-ISAC: a PPP for cybersecurity in the Dutch drinking water sector	
Word count	21971 words excluding references, appendices, transcripts, etc.	
	40870 words including references, appendices, transcripts, etc.	
Thesis supervisor	Dr. Vlad Niculescu-Dincă	*Assistant Professor at Leiden University*
Second reader	Dr. E. de Busser	*Assistant Professor at Leiden University*

Foreword

2018 has been a busy year with many new challenges, including the start of this master together with my start at the Departmental Coordination centre for Crisis management of the Ministry of Infrastructure and Water management (DCC-IenW). This combination has allowed me to develop myself, both from an academic and professional point of view, and has led to the delivery of this interesting research. I am glad that I am now able to conclude these 5 years of studying with this result and I feel I am ready for a future full of new challenges and opportunities.

I would like to thank a number of people without whom this study would not have been possible. First, thank you to my supervisor, dr. Vlad Niculescu-Dincă. You have helped me a lot with your good ideas regarding the structure of my thesis, but you also stimulated and encouraged me to take a step more and dive into the matter again and again. Without your help, my thesis would not have had the quality it has now.

Secondly, I would like to thank the three interviewees that helped me gather my data. Without your patience and extensive answers to my questions, I would not have been able to collect the data I have collected now. Thanks to your answers, I was able to provide a decent answer to the research question.

I would also like to thank all my colleagues of the DCC-IenW. You have all helped me throughout the process. Some of you with a periodic review and others with good ideas. You have helped me making use of your networks, which has enabled me to reach out to the right people I needed for my data gathering.

Finally, I would like to thank my family and closest friends. Thank you for your understanding that I was absent a bit more often and sometimes a little stressed. Without your support, I would not have been able to finish two studies within five years.

Tessa Mulders
The Hague, January 28, 2019.

Abstract

The Dutch drinking water sector has experienced ransomware infections and phishing attacks in the office automation environment. This sector is of great importance for public health and for the functioning of society. However, The National Cybersecurity Centre (NCSC) argues that the resilience of Dutch individuals and organisations lags the growth of threats. Based on this problem outline, this research considers t**o what extent the Dutch approach of ensuring cybersecurity in the drinking water sector meets up with the theory of Dunn Cavelty and Suter.** For answering this main question, three sub-questions are answered: (1) *What are the different relevant variants of Public-Private Partnership (PPP) and which one is best suited for this research?* (2) *What is the current Dutch PPP-approach in ensuring cybersecurity in the drinking water sector and what approach is best suited for this research?* And (3) *How does the Water-ISAC relate to the CIP-meta governance approach of Dunn Cavelty and Suter?* The answer to the first sub-question led to the choice for the PPP-theory by Dunn Cavelty and Suter as a framework for this research. Answering sub-question two allowed for a choice for a specific PPP in the Dutch approach: The Water-ISAC was chosen as the subject for this research to further investigate, using the framework of Dunn Cavelty and Suter.

The data necessary for answering sub-question three are gathered through interviews. The analysis of these data is two folded. First, I identified fourteen criteria that Dunn Cavelty and Suter argue that should be met in PPP in CIP. Second, Dunn Cavelty and Suter identified five problems they argue are common in a PPP in CIP. They argue that when applying CIP meta-governance, four of these five problems should be resolved, or at least alleviated. The criteria and presence of problems are compared to the case of the Water-ISAC.

Based on the analysis I performed, the Dutch approach of ensuring cybersecurity in the drinking water sector (Water-ISAC) partly meets up with the theory of Dunn Cavelty and Suter (CIP meta-governance approach). I draw this conclusion since six criteria are not or not completely met by the case. Furthermore, one problem that would be resolved or at least alleviated according to Dunn Cavelty and Suter is still present in the case.

Having applied the theory to the case of the Dutch drinking water sector, allows me to provide two-folded recommendations. Regarding the theory of Dunn Cavelty and Suter, I recommend diving into the aspect of international cooperation. The analysis strongly shows that the

drinking water sector is not concerned with international cooperation, so I advise to reconsider the value of this criterion. I also recommend clarifying the presence of the responsible government agency. Regarding the case of the Dutch approach, I recommend the ISAC-members to clarify who has the responsibility to control and monitor the PPP. This was unclear. The same counts for how the NCSC verifies whether the tasks of the PPP are carried out. Lastly, I recommend the Water-ISAC to consider how the new obligation of reporting incidents to the NCSC under the Wbni impacts the mutual relations of the partners cooperating in the Water-ISAC to prevent changes in trust and willingness to share information.

TABLE OF CONTENTS

List of Abbreviations

AIVD	Algemene Inlichtingen en Veiligheids Dienst (General Intelligence and Security Service)
APT	Advanced Persistent Threat
BAW	Bestuursakkoord Water (Administrative Agreement on Water)
B.V.	Besloten Vennootschap (Private Company)
CERT	Computer Emergency Response Team
CFCS	Centre for Cybersecurity
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CNI	Critical National Infrastructure
CSBN	Cybersecurity Beeld Nederland (Cybersecurity Assessment of the Netherlands)
CSR	Cybersecurity Raad (Cybersecurity Council)
DCC-IenW	Departmental Coordination centre Crisis management of the Ministry of Infrastructure and Water Management
DDoS	Distributed Denial of Service
IAO	Interdepartementaal Afstemmingsoverleg (Interdepartmental Coordination Consultation)
ICCb	Interdepartementale Commissie Crisisbeheersing (Interdepartmental Crisis Management Commission)
ICS	Industrial Control System
ICT	Information and Communication Technology
ILT	Inspectie Leefomgeving en Transport (Human Environment and Transport Inspectorate)
IPO	Interprovinciaal Overleg (Interprovincial Consultation)
IRB	ICT Response Board
ISAC	Information Sharing and Analysing Centre
ISP	Internet Service Provider
MSP	Managed Service Provider
NCSC	National Cybersecurity Centre

NCTV	Nationaal Coordinator Terrorisme en Veiligheid (National Coordinator for Security and Counterterrorism
NDN	National Detection Network
NIS	Network and Information Security
NPM	New Public Management
NRN	National Response Network
N.V.	Naamloze Vennootschap (Limited Liability Company)
PCII	Protected Critical Infrastructure Information
PPP	Public Private Partnership
UK	United Kingdom
UvW	Unie van Waterschappen (Union of Water Boards)
Vewin	Vereniging van Waterbedrijven In Nederland (Association of water companies in the Netherlands)
VNG	Vereniging van Nederlandse Gemeenten (Association of Dutch Municipalities)
Wbni	Wet Beveiliging Netwerk- en Informatiesystemen (Network and Information Systems Protection Act)

1. Introduction

One of the Dutch vital processes, the drinking water sector, has experienced ransomware infections and phishing attacks in the office automation environment[1]. This is not surprising: in 2017, 42% of all handled cyber incidents occurred at a private company[2]. Dutch drinking water companies are, in the end, always owned by a public legal person, being the State, a province, municipality, water board or joint arrangement within the meaning of the Joint Regulations Act[3]. However, in reality, they act as 'normal' companies and they are all registered as Limited Liability Company (Naamloze Vennootshap [N.V.]), foundation or Private Company (Besloten Vennootschap [B.V.]. These numbers are worrying, as the Dutch drinking water supply is of great importance for public health and for the functioning of society. Failure leads to societal dislocation[4], as is stated in the Cybersecurity Assessment of the Netherlands (CSBN) 2017, published by the Dutch National Cybersecurity Centre (NCSC). It provides insight into the interests, threats, resilience and related developments around cybersecurity. The NCSC argues that "digital attacks are used to influence *(the Dutch)* democratic processes" and that "[t]he resilience of *(Dutch)* individuals and organisations lags behind the growth of the threats" [5]. Examples of these threats in the Netherlands are the 2011 DigiNotar hack[6], the large-scale DDoS (Distributed Denial of Service-) attacks that occur frequently[789], the 2017 Not-Petya cyber-attack[10] and WannaCry cyber-attack[11] and the 'cyberwar' between The Netherlands and Russia[12]. That is why this research will consider how public and private partners within the Dutch drinking water sector work together to ensure cybersecurity.

---

[1] Nationaal Coördinator Terrorismebestijding en Veiligheid, "*Cybersecuritybeeld Nederland - CSBN 2017*," The Hague: June 2017, accessed June 14, 2018.
[2] Nationaal Coördinator Terrorismebestijding en Veiligheid, "*Cybersecuritybeeld Nederland - CSBN 2018*," The Hague: June 2018, accessed December 14, 2018.
[3] "Drinkwaterwet." https://wetten.overheid.nl/BWBR0026338/2015-07-01.
[4] NCTV, "*CSBN 2017*".
[5] NCTV, "*CSBN 2017*".
[6] "Vraag en antwoord over DigiNotar," Rijksoverheid, 2011, accessed June 11, 2018, https://www.rijksoverheid.nl/documenten/brochures/2011/09/05/informatie-over-diginotar.
[7] Robin Utrecht, "DDoS-aanvallen op Belastingdienst en DigiD voorbij," (NOS.nl, March 7, 2018).
[8] ANP, "Nieuwe DDoS-aanval op ABN Amro, ING, Rabo en Belastingdienst," (NOS.nl, January 30, 2018).
[9] ANP, "Opnieuw DDoS-aanval op website DigiD," (NOS.nl, August 1, 2018).
[10] Directie Cyber Security, "*Reactie inzake cyberaanval met ransomware en voortgang moties uit Wannacry-debat*," The Hague: 2017, accessed June 15, 2018.
[11] "Belang digitale veiligheid benadrukt," Tweede Kamer der Staten-Generaal, 2017, accessed September 7, 2018, https://www.tweedekamer.nl/kamerstukken/plenaire_verslagen/kamer_in_het_kort/belang-digitale-veiligheid-benadrukt.
[12] ANP, "Minister Bijleveld bevestigt: we zijn in cyberoorlog met de Russen," (NOS.nl, October 14, 2018).

Besides this societal relevance explained above, this research also has an academic relevance. This research contributes to the body of knowledge on how different governments try to protect their sectors from cyber threats. The outcomes of this study into the Dutch approach may, for example, be used in a comparative case study with other countries. Strategies of multiple countries can so be compared to identify similarities and differences, and to identify what strategies lead to what results. Also, insights into best practice, similarities and differences may be identified. This has a link with societal relevance: when best practices, similarities, and differences become clear, countries are enabled to optimise their approach to ensure a better level of cybersecurity in critical infrastructure protection (CIP). To optimise the use of the outcomes of this research, the same structure as Kristan Stoddart used in his research "UK *(United Kingdom)* cybersecurity and critical national infrastructure protection"[13] is applied. By doing so, the outcomes of this research and of the research of Kristan Stoddart may be used in a comparative case study on the differences and similarities in the cyber governance approaches in CIP between the UK and the Netherlands.

Given the problem outline and the societal and academic relevance, I decided to consider how public and private partners within the Dutch drinking water sector work together to ensure cybersecurity.

Research question:

To what extent does the Dutch approach of ensuring cybersecurity in the drinking water sector meet up with the theory of Dunn Cavelty and Suter?

Since the Dutch drinking water sector exists of both public and private partners[14][15][16], I have immersed myself in the theory of Public-Private Partnerships (PPP) for identifying the Dutch approach. Knowing how these public and private partners work together and what differences and/or similarities can be identified, enabled me to propose points of improvement and

[13] Kristan Stoddart, "UK cyber security and critical national infrastructure protection," *International Affairs* 92, no. 5 (2016). https://doi.org/doi:10.1111/1468-2346.12706.
[14] "Bestuur en Governance," Evides, n.d., accessed October 1, 2018, https://www.evides.nl/over-evides/de-organisatie/bestuur-en-aandeelhouders.
[15] "Aandeelhouders," Vitens, n.d., accessed October 1, 2018, https://www.vitens.com/organisatie/bestuur-en-corporate-governance.
[16] "FACTS & FIGURES," Waterbedrijf Groningen, n.d., accessed October 1, 2018, https://waterbedrijfgroningen.nl/organisatie/ons-verhaal/facts-figures/.

additions for the theory as well recommendations regarding the practical situation (Dutch approach).

I do recognise the question 'to what extent' is difficult to answer in qualitative research. However, I show how I have operationalised this concept and how I was able to answer this research question in chapter 3.4 Operationalisation.

1.1 Sub-questions

For answering the main question of this research, the following questions have been answered step by step:

1. What are the different relevant variants of Public-Private Partnership (PPP) and which one is best suited for this research?
2. What is the current Dutch PPP-approach in ensuring cybersecurity in the drinking water sector and what approach is best suited for this research?
3. How does the Water-ISAC relate to the CIP-meta governance approach of Dunn Cavelty and Suter?

As is visible, the research question and sub-questions reveal the knowledge that is gathered and decisions that are taken throughout the process. I decided to incorporate the decisions I took regarding the theory and the specific Dutch approach to make the questions as clear and delineated as possible.

1.2 Reading guide: an outline of the research

The first sub-question is answered by performing a literature review on PPP. Hereafter, the current Dutch approach in ensuring cybersecurity in the drinking water sector (after this: Dutch approach) is identified, which provides the answer to sub-question two. The second part of the research questions whether this current Dutch approach meets the CIP meta-governance approach of Dunn Cavelty and Suter. This makes this an explanatory research, with the research objective being *applying theory*.

The next chapter first positions this research in the body of knowledge. It does so by describing other relevant and related researches. This part also identifies a gap in knowledge and the added value of this research in filling up that gap. Hereafter, all relevant concepts are described and identified. Also, the first sub-question is answered by providing a literature review regarding PPP and determining what PPP is best suited for this research. Further, a consistent theoretical framework to answer the research question is presented. Lastly, sub-question two is answered in this chapter by identifying the Dutch PPP-approach in ensuring

cybersecurity in the drinking water sector and determining what specific approach is best suited for this research.

Chapter three describes the methodological justification and the procedures that are followed to reach a valid answer to the research question. The research design is explained, as well as the case selection, the operationalisation and an outline of the data gathering- and analysis process. Finally, the limitations to this research are outlined.

The chapter that follows contains an accurate report of the results of the data analysis. First, the results of comparing the criteria of Dunn Cavelty and Suter to the interviews are outlined to see how the theory fits the case. Second, I will go into five problems Dunn Cavelty and Suter defined regarding PPP in CIP to see whether these problems are present in the drinking water sector-case.

This paper ends with a conclusion, providing a clear answer to the research question. It also contains a discussion of how the findings relate to current research, of the limitations of the research, and possible avenues for future research. Finally, it concludes with concrete and convincing practical recommendations.

2. Body of knowledge

This chapter first positions this research in the body of knowledge by providing an insight into corresponding researches and identifying a gap in knowledge. It thus points out the added value of this research. Hereafter, the chapter continues with a critical review of existing theoretical and empirical academic literature related to the terms in the research question: a conceptualisation. This includes a part on PPPs, answering sub-question one. Further, a consistent theoretical framework to answer the research question is presented. Finally, sub-question two is answered by providing an overview of the current Dutch approach in ensuring cybersecurity in the drinking water sector. Also, I chose a specific PPP that will be subject to further analysis in this research.

2.1 Position in the body of knowledge

For positioning this research in the body of knowledge and identifying a gap in knowledge, it is necessary to consider corresponding researches and their outcomes. As mentioned before, the first part of the research is based on the structure of the research performed by Stoddart[17]. The reason for this is because there are not many other single case studies into a country's approach to ensuring cybersecurity within a vital infrastructure sector.

In his article, Stoddart first looked at the public and private organisations and mechanisms that have been put in place to try to build cyber-resilience for Critical National Infrastructure (CNI) within the UK. Second, it questions whether these are sufficient to deal with the cyber-related problems the UK faces in protecting its CNI. Stoddart concludes that the UK NCSC is a good step towards improving CNI resilience, but only if it fully connects all relevant stakeholders within government and does not reflect the government's opinion only. Involvement and partnership with the private sector and owner-operators of CNI are crucial elements. He also argues that regulating the reporting of cybersecurity violations to the central government is essential for the protection of CNI. He recommends adopting a Protected Critical Infrastructure Information (PCII-) program. To summarise, all this can only be accomplished with the full agreement of private industry, being owner-operators[18].

[17] Stoddart, "UK cyber security," pp. 1079-1105.
[18] Stoddart, "UK cyber security," p. 1104.

Although Stoddart's research is not specifically focussed on PPP, it does touch upon it. He argues that "…CNI is largely owned and operated by private industry…"[19]. He also concludes that "Engagement and partnership with the private sector, and the owner-operators of CNI, are vital to the success of the NCSC and the governments National Cybersecurity Strategy" [20]. This makes choosing Stoddard's structure as the basis for this research, in combination with a theory on PPP, interesting. It enables further research to closely look at the similarities and differences between the Netherlands and the UK and thus adds to the body of knowledge. It might, for example, focus on the question whether the Netherlands focuses more on cooperation with the private sector than the UK does now.

What further stands out is that there are not many other researches that consider a country's approach towards CIP, and certainly not regarding the drinking water sector. Sergei Boeke, for example, looked into crisis management. In his research "First Responder or Last Resort? The role of the Ministry of Defence in national cyber crisis management in four European countries", he investigates the role that the ministry of Defence plays in cyber crisis management in four European countries. The Netherlands was used as a frame of reference. Denmark served as one of the comparative cases, as well as Estonia and the Czech Republic[21]. Boeke argued that because of the blurring of boundaries, the public and private sector, national security and law enforcement are very important. The PPPs this results in are essential to many national cybersecurity strategies, as neither the public or private sector can address the challenges alone[22]. He identifies differences in the national approaches. For example, in Denmark, top-down monitoring should protect government networks. In the Netherlands, however, cyber challenges are countered by different PPPs which are based on equality. Bottom-up initiatives, such as ISACs, compensate the lack of control from above[23]. Boeke concludes that only in Denmark the Ministry of Defence has a prominent place, as its Centre for Cybersecurity (CFCS) provides first response capacity in incident and crisis management. For the Netherlands, Estonia, and the Czech Republic applies that Defence is considered a final way out (*a last resort*), but it is unclear when and under what circumstances these countries can call on their military cyber capacity[24].

---

[19] Stoddart, "UK cyber security," p. 1082.
[20] Stoddart, "UK cyber security," p. 1105.
[21] Sergei Boeke, "*First Responder or Last Resort? The role of the Ministry of Defence in national cyber crisis management in four European countries*," (September 1, 2016), pp. 5-6.
[22] Boeke, "First Responder or Last Resort?," p. 3.
[23] Boeke, "First Responder or Last Resort?," p. 46.
[24] Boeke, "First Responder or Last Resort?," p. 47.

This study by Boeke is interesting as it consists of a comparative case study into cyber approaches as this research does. Also, it shows that in the Netherlands various types of PPPs are active to address cyber challenges. This counts as a justification of sub-question two of this research, in which I identified what type of Dutch PPP is the most suited to focus on.

Further, Boeke does not specifically focus on PPP, even though he touches upon it several times as shown above. In his other study "National cyber crisis management: Different European approaches", he investigates how different models of PPP shape cyber crisis management in the same four European countries[25]. He argues that both the public and private sector are involved in cyber crisis management. The private sector, since it operates the biggest part of national critical infrastructure. The public sector, since it cannot get rid of its own responsibility as the principal security provider. It is a logical result that PPPs are an important part of many national cybersecurity strategies. However, Boeke argues that beyond the benefits of this, there is a divergence of interests in basic definitions and disagreement on who should pay the bill. A logical enhancement of PPPs would then be a *governance approach* that consists of networks of various public and private organisations[26]. This sounds like what Dunn Cavelty and Suter write about the *network approach of governance* theory, an enhancement of the traditional *neoliberal governance* theory. They argue that "less government and more governance" is the key issue of the *neoliberal approach*, which main goal is to enhance efficiency in public administrations by transferring authority from the government to the private sector[27]. However, the goal of CIP should be enhancing *security*, not raising *efficiency*. Because the *network approach of governance* theory is based on the concept of self-regulating networks, the state's core task is not any more to monitor actors that collaborate around this, but more to coordinate and stimulate functional networks consisting of these actors so that they will fulfill the tasks required by the state[28]. I elaborate more on this enhanced form of PPP in 2.2.4 Defining: (the different variants of) Public-Private Partnerships.

The discussion above shows there is not one best approach of ensuring cybersecurity, even though it is such an important activity. Especially ensuring cybersecurity in CIP is under-

[25] Sergei Boeke, "National cyber crisis management: Different European approaches," *Governance* 31, no. 3 (2017). https://doi.org/10.1111/gove.12309.
[26] Boeke, "National cyber crisis management," p. 451.
[27] Myriam Dunn Cavelty and Manuel Suter, "Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection," *International journal of critical infrastructure protection* 2, no. 4 (2009): p. 4. https://doi.org/10.1016/j.ijcip.2009.08.006.
[28] Dunn Cavelty and Suter, "Public-Private Partnerships are no silver bullet," p. 7.

researched, lacking deep (single) case studies for comparative analysis. Stoddart provides a single case study into the UK. However, this is, even though it touches upon it, not focused on PPP or one vital sector. Boeke performed two comparative case studies into four countries. The focus of these studies is, however, more on cyber *crisis management* and not specifically on ensuring cybersecurity in a vital sector. They do focus more on PPP than Stoddart does. Finally, Dunn Cavelty and Suter focus on PPPs in CIP but do not go (deeply) into several cases. The gap in knowledge is therefore identified as that there is **little knowledge on how to ensure cybersecurity in (a) critical infrastructure (sector)**, let alone regarding a sector as specific as the drinking water sector. Conducting a study into the Dutch approach *does* add to this knowledge, is a (small) step towards closing this gap in knowledge and opens avenues for new research.

2.2 Conceptualisation

2.2.1 Defining: Dutch vital infrastructure

As mentioned before, the drinking water sector is one of the Dutch vital processes. In total, there are 26 vital processes. They are subdivided into category A and B. Category A vital processes have greater consequences in case of failure than Category B vital processes. Examples of A-critical processes are *national transport and distribution of electricity*, *gas production, national transport and distribution of gas*, *drinking water supply*, and the *storage, production, and processing of nuclear mat*erials. Examples of B-critical processes are the *regional distribution of electricity*, *internet access, and data traffic* and the *vessel traffic service*[29].

All processes are considered so essential for the Dutch society that failure or disruption leads to serious social disruption and poses a threat to national security. These processes form the Dutch vital infrastructure[30].

In other countries, vital processes or vital infrastructure are often referred to as 'critical infrastructure'[31]. Because of the adoption of the EU Network and Information Security (NIS-) directive in 2016, all EU-member states must identify such operators of essential services.

[29] National Coordinator for Security and Counterterrorism, "*Resilient critical infrastructure*," The Hague: 2018, accessed June 25, 2018.
[30] NCSC, "*Resilient critical infrastructure*".
[31] Stoddart, "UK cyber security," p. 1018.

The NIS-directive comes as part of the EU Cybersecurity strategy. It is the first piece of EU-wide cybersecurity legislation. The goal is to enhance cybersecurity across the EU[32].

In point (4) of article 4 of the NIS-directive, "operators of essential services" is conceptualised as "a public or private entity of a type referred to in Annex II, which meets the criteria laid down in Article 5(2)". Annex II contains the types of entities for the purposes of "operators of essential services". *Drinking water supply and distribution* is also part of this. In the Directive, this is defined as: "suppliers and distributors of water intended for human consumption[33], meaning all water either in its original state or after treatment, intended for drinking, cooking, food preparation or other domestic purposes, regardless of its origin and whether it is supplied from a distribution network, from a tanker, or in bottles or containers, but excluding distributors for whom distribution of water for human consumption is only part of their general activity of distributing other commodities and goods which are not considered essential services[34]". The criteria in Article 5(2) for identifying operators of essential services defines that[35]:

2. "The criteria for the identification of the operators of essential services, as referred to in point (4) of Article 4, shall be as follows:
   a. an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
   b. the provision of that service depends on network and information systems; and
   c. an incident would have significant disruptive effects on the provision of that service".

The Dutch Network and Information Systems Protection Act (Wet Beveiliging Netwerk- en Informatiesystemen [Wbni]) is the translation of the NIS-directive[36]. It defines 'operators of essential services' as "a provider of an essential service as referred to in Article 4 of the NIS-directive, designated pursuant to Article 5, first paragraph, under a"[37]. Regarding the designation of essential services:

1. "The following shall be appointed by general administrative order or by a decision of an administrative authority referred to in that measure

---

[32] "NIS Directive," Enisa, 2018, accessed October 18, 2018, https://www.enisa.europa.eu/topics/nis-directive.
[33] "DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union." https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.
[34] "COUNCIL DIRECTIVE 98/83/EC of 3 November 1998 on the quality of water intended for human consumption." https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31998L0083&from=EN.
[35] "DIRECTIVE (EU) 2016/1148."
[36] Ministerie van Economische Zaken en Klimaat, "*Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) voor Digitale dienstverleners*," The Hague: September 2018, accessed September 15, 2018.
[37] "Regels ter implementatie van richtlijn (EU) 2016/1148 (Wet beveiliging netwerk- en informatiesystemen)." https://www.eerstekamer.nl/behandeling/20181108/publicatie_wet/document3/f=/vkt94dz0rkza.pdf.

a. providers of an essential service or categories of such providers
b. other vital providers or categories of such providers.

2. In the application of the first paragraph, under a, Articles 5 and 6 of the NIS-directive and Annex II of that directive shall be observed"[38].

This shows that the definition of the Dutch governments relies upon what is defined in the NIS-directive and thus that Drinking water supply and distribution, as described earlier, is appointed an operator of an essential service under Dutch law.

As this research is partly inspired by and based on the research of Kristan Stoddart, it is also relevant to know how the UK's critical infrastructure is defined:

"Those facilities, systems, sites and networks [physical and electronic] necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends...There are certain 'critical' elements of national infrastructure that, if lost, would lead to severe economic or social consequences or to loss of life in the UK. These critical elements make up the CNI"[39].

When comparing the definition from the NIS-directive, the Netherlands and the UK, it shows that with different words the same is said. What stands out is that the definition of the NIS-directive is more specified than the UK definition. The definition used by the Dutch government is even more elaborated, as it has divided several important processes into two categories. All those processes are considered critical to the Dutch society.

In essence, all three definitions are the same, emphasising that critical infrastructure regards disruption of certain parts of society which, when disrupted, have a significant negative impact on the society that depends upon them.

Even though this makes for a clear image of what the Dutch vital infrastructure constitutes, the term is defined in different manners within the Netherlands. In their report on Securing Critical Infrastructures in the Netherlands: Towards a National Testbed, The Hague Security Delta[40] argues that Critical Infrastructures (CIs) are "the clockwork that makes modern society tick. CIs are the sectors defined to be of most importance to the functioning of societies"[41]. To this, TNO adds that crucial processes in most critical infrastructures, and in

[38] "Wbni."
[39] Stoddart, "UK cyber security," p. 1081.
[40] The Hague Security Delta, "Securing Critical Infrastructures in The Netherlands: Towards a National Testbed," [The Hague Security Delta.] (2015).
[41] "Securing Critical Infrastructures in The Netherlands: Towards a National Testbed," p. 9.

many other organisations, rely on the correct and undisturbed functioning of Industrial Control Systems (ICS). They monitor and control physical processes. ICS control our critical infrastructures, safety-critical processes, and most production processes. ICS are now everywhere around us, often hiding in everyday functionality. A failure of ICS may both cause critical services to fail and may result in safety risks to people and/or the environment. Therefore, the cybersecurity and resilience of ICS are of utmost importance to society, to utilities and other critical infrastructure operators, and to organisations which use ICS[42].

The definition by the Dutch government is like the one from The Hague Security Delta. However, TNO adds a valuable new element: ICS. This is important, as this research concerns *cyber threats* in critical infrastructure. However, adding ICS to the scope of this research would make it too big and complex to finish the research project on time.

Considering the above, the definition of the NIS-directive applies to this research. Reason for this is because this directive is recent and provides a clear framework for identifying vital infrastructure. The definition is thus:

"All entities that provide services that are essential for the maintenance of critical societal and/or economic activities and of which the provision of that service depends on network and information systems, whereby an incident would have significant disruptive effects on the provision of that service"[43].

2.2.2 Defining: Dutch drinking water sector

Various organisations are entrusted with the care for the Dutch drinking water sector. Drinking water companies, producing and supplying drinking water, and water boards, managing water regionally and treating wastewater, are the most well‑known. Other parties involved in this sector are various government ministries; Rijkswaterstaat (Public Works and Water Management), managing the large bodies of water; provinces, managing groundwater; and municipalities, responsible for the sewer system[44].

The drinking water sector is also defined in the NIS-directive: "suppliers and distributors of water intended for human consumption[45], meaning all water either in its original state or after

[42] Eric Luijf and Bert Jan te Paske, "Cyber Security of Industrial Control Systems," (March 2015).
[43] "DIRECTIVE (EU) 2016/1148," art. 5, par. 2(c).
[44] "Dutch water sector," Vewin, n.d., accessed June 1, 2018, http://www.vewin.nl/english/dutch-water-sector/Paginas/default.aspx.
[45] "DIRECTIVE (EU) 2016/1148," annex II, no. 6.

treatment, intended for drinking, cooking, food preparation or other domestic purposes, regardless of its origin and whether it is supplied from a distribution network, from a tanker, or in bottles or containers[46], but excluding distributors for whom distribution of water for human consumption is only part of their general activity of distributing other commodities and goods which are not considered essential services[47]". This is the definition that applies to this research.

2.2.3 Defining: cybersecurity

Cybersecurity is a widely studied topic. It is mentioned in the earlier discussed NIS-directive, but not defined. To be able to research 'whether the Dutch approach of ensuring cybersecurity in the drinking water sector meets up with the theory of Dunn Cavelty and Suter', it is important to know how the Dutch government defines cybersecurity. The Dutch National Coordinator for Security and Counterterrorism (Nationaal Coördinatiecentrum Terrorismebestrijding en Veiligheid [NCTV]) defines cybersecurity as "the freedom from danger or damage caused by disruption or failure of ICT or by misuse of ICT. The risk or damage due to abuse, disruption or loss can consist of limiting the availability and reliability of the ICT, violation of the confidentiality of information stored in IT or damage to the integrity of that information[48]".

As this research is partly inspired by and based on the research of Kristan Stoddart, it is also relevant to know how the UK defines cybersecurity. In their National Cybersecurity Strategy 2016-2021, cybersecurity refers to "the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, because of failing to follow security procedures[49]".
These two definitions are alike. Given the fact that this research considers the Dutch approach, it makes more sense to choose the definition of the Dutch government instead of the UK government. This is the definition that will be used for this research.

---

[46] "COUNCIL DIRECTIVE 98/83/EC," art. 2, par. 1(a).
[47] "DIRECTIVE (EU) 2016/1148," annex II, no. 6.
[48] "Cybersecurity," Nationaal Coördinator Terrorismebestijding en Veiligheid, n.d., accessed October 2, 2018,
[49] HM Government, "*National Cyber Security Strategy 2016-2022*," last updated September 11, 2017, accessed October 15, 2018.

2.2.4 Defining: (the different variants of) Public-Private Partnerships

When looking at the literature, several definitions regarding PPP can be derived. For example, in their article "Publiek-Private Samenwerking in Nederland: retoriek of bloeiende praktijk?", Klijn and Twist describe it as a "more or less sustainable cooperation between public and private actors in which common products and/or services are developed and in which risk costs and revenues are shared"[50]. They argue that PPPs are often considered good instruments to reach public goals. The main idea is that both public and private actors should do what they are good at. Connecting these qualities should then result in good teamwork. In a PPP, private parties are involved in implementing policy or realising policy products or services. It is assumed that this will lead to better products and more efficiency[51]. The idea is that the added value that can be achieved by this cooperation, would not have come about without that cooperation. How this added value is best achieved, is a contested topic. On the one hand, there are the ideas of *New Public Management* (NPM), which argue that the government should focus more on formulating the policy and leaving the implementation to others, as this would promote the efficiency and effectiveness of government action. On the other hand, there are the ideas of *governance and networks*, emphasising the dependencies of actors (mainly public actors) in realising policy products and that inter-organisational coordination is necessary for realising policy outcomes and services[52].

Klijn and Twist further argue that these different ideas regarding PPP express themselves in different organisational forms of PPP: the concession (or contract) form and the alliance (or partnership) form. In a PPP concession form the design, construction, financing, and managing of a project, are integrated. The added value is achieved in lower transaction costs between the elements, but also in the fact that the private tenderer can create new solutions [53].

In a partnership form, separate activities and subprojects are integrated to create added value. It is thus an organisational cooperation project in which various subprojects are brought together. An added value is achieved because of different projects that can be linked to each other, resulting in synergy, and thus interesting substantive outcomes can be realised[54].

---

[50] Erik Hans Klijn and Mark van Twist, "Publiek-Private Samenwerking in Nederland: retoriek of bloeiende praktijk?," (August 2007).
[51] Klijn and Van Twist, "Publiek-Private Samenwerking," p. 1.
[52] Klijn and Van Twist, "Publiek-Private Samenwerking," p. 4.
[53] Klijn and Van Twist, "Publiek-Private Samenwerking," p. 4.
[54] Klijn and Van Twist, "Publiek-Private Samenwerking," p. 4.

The same definition of PPP is used by Van Montfort, van den Brink, Schultz, and Maalsté in their article "Publiek-private samenwerking in maatschappelijke veiligheid: Naar een 'improvisatiemodel'". However, they argue that it is not certain that all the characteristics mentioned in this definition will always be present in practice. They argue that therefore, the definition of PPP as a concept is "not unambiguous and in practice, the definition and delineation often coincide with the specific ambitions from which PPP projects are born"[55].

They further argue that the concession form and the alliance (partnership) form are the models that are used for PPP in practice. According to them, the alliance form is more common and often applied in the security sector. Alliances have a greater variety than the concession form, varying from occasional and more non-committal cooperation to the signing of covenants between partners and the establishment of legal entities. In comparison with the concession form, the alliance form is mainly focused on 'smart collaboration' instead of 'smart procurement'. The relationships between cooperating parties are less based on the hierarchical relationship between customer and contractor and more on horizontal relationships and mutual trust. Goals and methods are therefore not based on the steering and control of one party, although such network collaboration naturally requires coordination[56].

Besides these two models, they add a third dimension which they call the improvisation model[57]. They argue that the first two models will retain their value and be usable in the future. However, they argue that the two models cannot interpret all forms of cooperation between public and private parties. In the present time and partly because of cutbacks, initiatives often arise outside the government, without the government being aware of this. Besides that, security is not always the main goal. To that extent, they argue there is a third direction which has different characteristics than the other two directions: more coincidental, less focused and not dependent on the government[58]. This is not applicable to this research, as the ministry of I&W will remain responsible and the government will be involved as the principal security provider. It is important to keep the government closely involved and that the government is aware of initiatives and cooperation networks.

[55] Cor van Montfort, Gabriel van den Brink, Martin Schulzand Nicole Maalsté, "Publiek-private samenwerking in maatschappelijke veiligheid: Naar een 'improvisatiemodel'," (February 1, 2012).
[56] van Montfort, "Publiek-private samenwerking," pp. 12-16.
[57] van Montfort, "Publiek-private samenwerking," p. 36.
[58] van Montfort, "Publiek-private samenwerking," p. 40.

An often-cited article when it comes to PPP in CIP is *Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection* by Dunn Cavelty and Suter. The specific choice for mentioning this research is because they focus on CIP. The Dutch drinking water sector is classified as critical (or vital) infrastructure, as described in 2.1.1 Defining: Dutch vital infrastructure.

Dunn Cavelty and Suter describe a PPP as "a form of cooperation between the state and the private sector"[59]. They argue that the goal of PPP is to "exploit synergies in the joint innovative use of resources and in the application of management knowledge, with optimal attainment of the goals of all parties involved, where these goals could not be attained to the same extent without the other parties"[60]. To achieve this, they say that the parties involved should have complementary goals and an already existing interdependence of the actors and their goals. Their research shows that the 'traditional' PPP model, coming from *neoliberal governance theory*, is subject to several limitations in the context of CIP. They argue that "less government and more governance" is the key issue of this approach, which main goal is to enhance efficiency in public administrations by transferring authority from the government to the private sector[61]. They claim that the state has no control over whether private companies perform their functions around CIP. PPP is also often difficult due to divergent interests and can only be carried out with selected companies and should be small since the cooperation is based on mutual trust. They argue that the number of PPPs must remain limited since too many would exceed the government's capacities. Thereby, PPPs are not suitable for promoting international cooperation due to the intensive involvement of the government[62].

Countering this, Dunn Cavelty and Suter introduce an approach that does not reduce cooperation between the state and the private sector to direct partnership (as in the case of PPP) but also considers other forms of interaction: the *network approach of governance* theory. They argue that the goal of CIP should be enhancing *security*, instead of raising *efficiency*. Because the *network approach of governance* theory is based on the concept of self-regulating networks, the state's core task is not any more to monitor actors that collaborate around this, but more to coordinate and stimulate functional networks consisting

[59] Dunn Cavelty and Suter, "Public-Private Partnerships are no silver bullet," p. 1.
[60] Dunn Cavelty and Suter, "Public-Private Partnerships are no silver bullet," p. 2.
[61] Dunn Cavelty and Suter, "Public-Private Partnerships are no silver bullet," p. 4.
[62] Dunn Cavelty and Suter, "Public-Private Partnerships are no silver bullet," p. 6.

of these actors so that they will perform the tasks required by the state[63]. The role of the state is redefined by the network approach. Governments no longer contract tasks and monitors implementation, but forms conditions for self-organising networks. The government coordinates and supports existing networks and when existing networks fail or are unable to fulfill the functions they are charged with, the government activates new networks. The network approach thus considers that the state depends on the help of private actors around CIP and at the same time, it defines new forms for government intervention: the activation, stimulation, and coordination of network. This can be described as the organisation of self-organisation or CIP meta-governance[64].

Dunn Cavelty and Suter have developed a road map for CIP meta-governance. First, goals and priorities must be defined and communicated. This is necessary to ensure that the required task is carried out according to the requirements of the government. Secondly, the status quo must be analysed, and it must be determined where action is required. It is important to know what networks already exist and how far they are in fulfilling step 1. They argue that clear, politically founded and applicable definitions are crucial. Hereafter, suitable instruments of meta-governance should be identified. Ideally, the choice of instruments is derived from the differences between the goals and the status quo. However, the choice of the instrument often influences by political processes. The final step of the process is to analyse the efficiency of measures. A government agency checks whether the networks are performing their tasks in such a way that they can achieve the defined goals and priorities[65]. It is visualised in Figure 1.

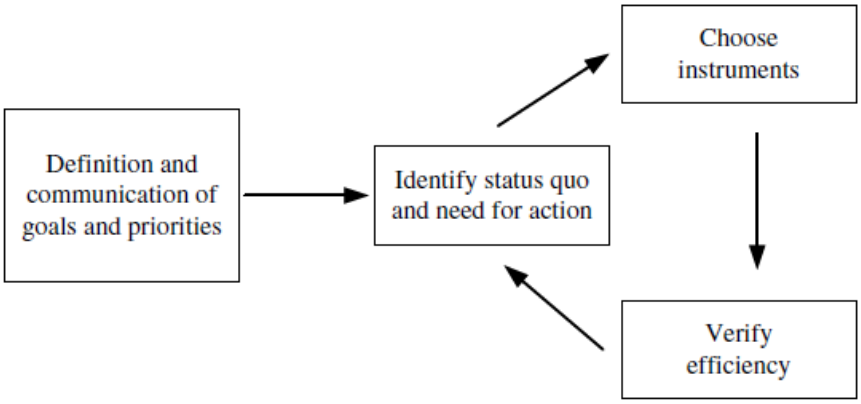

Figure 1: The meta-governance process[66].

[63] Dunn Cavelty and Suter, "Public-Private Partnerships are no silver bullet," p. 7.
[64] Dunn Cavelty and Suter, "Public-Private Partnerships are no silver bullet," p. 7.
[65] Dunn Cavelty and Suter, "Public-Private Partnerships are no silver bullet," p. 7.
[66] Dunn Cavelty and Suter, "Public-Private Partnerships are no silver bullet," p. 7.

As is described, there are many different views regarding PPP. It is a much-debated topic. Thereby comes that PPP in CIP differs from 'regular' PPP, as shows by Dunn Cavelty and Suter, and before by Boeke. In the research question is visible that I chose to use the theory of Dunn Cavelty and Suter for further analysing the Dutch approach. The choice for this theory is because they focus on CIP specifically. This choice is further substantiated in 3.2.1 Theory selection: CIP meta-governance of Dunn Cavelty and Suter.

2.3 Theoretical framework: the road to an answer

This paragraph will shortly go into the theoretical framework I applied to answer the research question. For answering the research question, I made some conclusions based on assumptions of a causal relation. As is further explained in chapter 3.2.1 Theory selection: CIP meta-governance of Dunn Cavelty and Suter, I used the theory of Dunn Cavelty and Suter for this research. Their research also relies upon causal relations which they have or have not established themselves. One of these is that they have identified several **problems** that are common for PPP in CIP, which "can be resolved or at least alleviated"[67] by applying CIP meta-governance. They call this the *network approach*, as explained in the previous chapter. They argue that "If they [*PPP*] are perceived in accordance with the network approach of governance theory, as part of a more diverse toolbox, the result is a liberating step away from the PPP concept, which restricts options, towards a new understanding of the role of the state in this area"[68]. This shows that they assume that *PPP in CIP is successful (X)* when the *network approach (or: CIP meta-governance approach) is applied (Y).* So: Y leads to X.

To test whether this is the case for the Dutch drinking water sector, I have made a division to measure this. I split this causal relation into two parts. The main causal relation is that *the Dutch approach of ensuring cybersecurity in the drinking water sector (after this: Dutch approach) meets up with the theory of Dunn Cavelty and Suter (X)* if *CIP meta-governance is applied (Y).* To see whether CIP meta-governance is applied (Y) I split Y in Z and A.

First, I identified criteria that Dunn Cavelty and Suter require PPP in CIP to meet (see 3.4 Operationalisation). A condition *for (Y) CIP meta-governance is applied* is *that (Z) the case meets most of these criteria.*

---

[67] Dunn Cavelty and Suter, "Public-Private Partnerships are no silver bullet," p. 5.
[68] Dunn Cavelty and Suter, "Public-Private Partnerships are no silver bullet," p. 7, ([PPP] added).

Second, a condition for *(Y) CIP meta-governance is applied* is that *(A) most of the problems identified by Dunn Cavelty and Suter are not present in this case.*

So, if Z (criteria) and A (problems) are met by the case, I can conclude that CIP meta-governance is applied (Y) which leads to the conclusion that (X) the Dutch approach meets up with the theory of Dunn Cavelty and Suter. It is visualised in the scheme below.

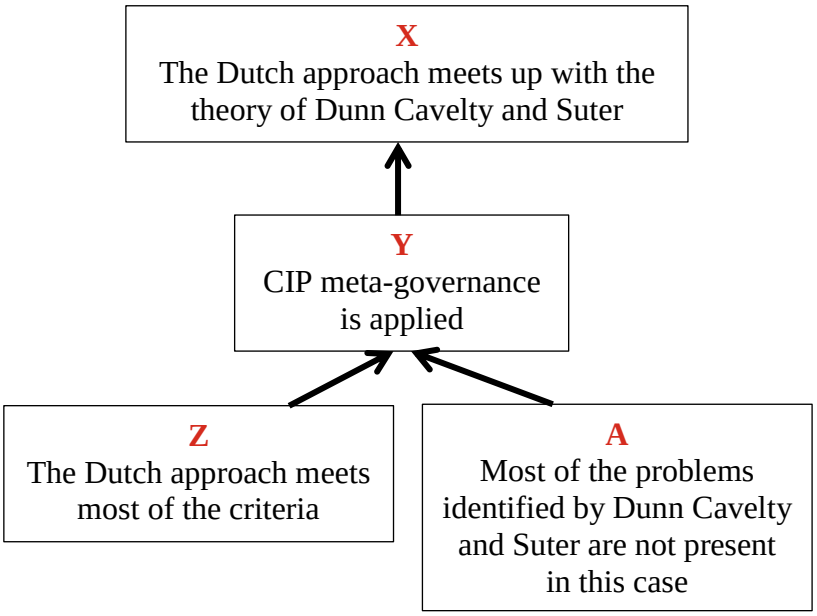

Figure 2: Schematic visualisation of causal relations based on Dunn Cavelty and Suter.

2.4 Overview of PPPs: the current Dutch approach for ensuring cybersecurity

As the NCSC is the central information hub and centre of expertise for cybersecurity in the Netherlands and the drinking water sector is classified as a vital process of the Netherlands, I first looked at what the NCSC has to say regarding PPP.

The NCSC argues that cybersecurity is too comprehensive to be managed by a single sector. ICT structures are interdependent. This, and because cybersecurity affects all sectors of the digital community, makes cooperation between sectors essential. Sharing knowledge is thus very important for, for example, recognising threats. To achieve an adequate response, all partners from different sectors involved must know how and be able to find each other quickly. The NCSC cooperates on a basis of equality and trust. The various partnerships they facilitate and stimulate aim to improve the digital security in the Netherlands[69].

[69] "Cooperation," National Cyber Security Centrum, n.d., accessed October 1, 2018, https://www.ncsc.nl/english/cooperation.

The NCSC cooperates jointly with government and other public parties, with private parties, with professionals in practice, education, and academia and with international partners[70].

The NCSC is committed to PPPs as they argue that intensive cooperation is necessary to keep the Netherlands resilient against cyber threats. Cooperation ensures that the Netherlands is well informed about the opportunities and challenges around cybersecurity. The NCSC focuses in the first place on sectors that are of vital importance to the Dutch society: the so-called vital infrastructure[71].

The NCSC has several core tasks to realise a collaboration platform for public-private parties. These tasks consist of[72]:

1. Organising (public-private) cooperation within the domain cybersecurity. The aim is to strengthen the cooperation by bundling and enriching expertise and experiences within cybersecurity. They do so by, amongst others, maintaining and further developing existing partnerships (including Information Sharing and Analysing Centres [**ISACs**] and **Liaisons**) and fitting cybersecurity into existing structures, networks and processes;
2. Building trust with all stakeholders. As a result, the NCSC is well informed regarding the content about cybersecurity and connected to relevant programs and developments. They do so by, amongst others, remaining in discussion with the stakeholders and considering the interests and managing the expectations and needs of cybersecurity relations.
3. Preparing and coordinating ICT-crisis management throughout the entire crisis management chain. They do so by, amongst others, setting up the Cybersecurity Department of the NCTV for effective combating large ICT-incidents and strengthening the **ICT Response Board** (IRB) quantitatively and qualitatively[73].

From the interviews comes that the drinking water companies talk with each other and with the NCSC in the Water-ISAC[74]. The dossier holder Drinking water of the NCSC stated that the cooperation between drinking water companies and the NCSC is good[75]. From the interviews also comes that the NCSC is mainly facilitating, for example regarding the

[70] NCSC, "Cooperation."
[71] "Publiek-private samenwerking," Nationaal Cyber Security Centrum, n.d., accessed October 1, 2018, https://www.ncsc.nl/samenwerking/publiek-private-samenwerking.html.
[72] NCSC, "Publiek-private samenwerking."
[73] NCSC, "Publiek-private samenwerking."
[74] René van der Helm, interview by Tessa Mulders, November 28, 2018.
[75] Dossier holder Drinking water of the NCSC, interview by Tessa Mulders, December 3, 2018.

secretary-tasks, and is an independent, supportive and expert organisation and especially there for the organisations to help and support them[76].

2.4.1 Explaining: liaisons

The NCSC is connected to liaisons from the public and private parties within the Dutch vital infrastructure. They form the "inner circle" of the cooperation as organised in the NCSC. A cooperation partner can connect to the NCSC with a liaison officer. This liaison officer then acts as a linking-pin and contact point for the NCSC and other cooperation partners. The liaison cooperation consists of trust, common interests, added value, and collaboration[77].

The liaison parties themselves determine the level of commitment of the liaison and the degree to which knowledge and information are shared. The liaison ensures the connection between the organisation and the NCSC and organises the necessary expertise from within the organisation. A strong force of liaison cooperation is to seek connection in quiet times, so that switches can be made faster in times of crisis. In this way, the cooperation is optimally utilised[78].

2.4.2 Explaining: National Detection Network

In the National Detection Network (NDN), national government organisations and vital private organisations cooperate to create a secure digital society.

The NCSC, the General Intelligence and Security Service (Algemene Inlichtingen en Veiligheids Dienst [AIVD]), the Military Intelligence and Security Service [MIVD]) and all affiliated organisations work together in the NDN to make the Netherlands digitally safer. The NDN focuses on sharing threat information with each other to detect cybersecurity risks and hazards more quickly. This allows participants to apply measures to prevent or limit the damage. The NDN manages to simplify knowledge sharing and raises effectiveness. Also, it is a preventive platform: what an incident is with one party, might be a good warning for the other party.

Within the NDN, the NCSC creates a broad and common picture of the current cyberthreats based on obtained information. The NCSC, the AIVD, and MIVD collect information

---

[76] Interview with René van der Helm.
[77] "Liaisonschap," Nationaal Cyber Security Centrum, n.d., accessed October 2, 2018, https://www.ncsc.nl/samenwerking/liaisonschap.html.
[78] NCSC, "Liaisonschap."

regarding cyber threats and make this information available to the NDN. Organisations that participate in the NDN also provide information (anonymously). In addition, the NDN functions as a platform for participants to meet each other for sharing best practices and working on the analysis of current threats and attacks in a familiar environment[79].

From the interviews comes that the drinking water sector is represented in the NDN. It was mentioned that the NDN is a national service where the members say, "this is what we see coming" (cybercrime-related)[80]. The affiliated parties must filter out what is interesting for them. An NDN thus is more of a technical thing. They send technical messages to each other: "we see something, do you also see something"? The parties send this to the NDN and to the NCSC with the message "What is this?" [81].

2.4.3 Explaining: ICT Response Board

The ICT Response Board (IRB) is a PPP. Boeke describes it as "…a public-private forum that includes representatives from critical infrastructure sectors, telecommunications providers, Internet Service Providers (ISPs), academic researchers, and Computer Emergency Response Team (CERT-) professionals"[82].

During a large-scale ICT crisis or threat, the IRB analyses the situation based on information exchange. Participants of the IRB are ICT-experts from several vital sectors (including telecom / ICT, energy, financial and drinking water) and from government organisations. The representative of the drinking water companies in the IRB has also participated during the interviews performed for this research.

During activation, the composition of the IRB is flexible to be able to respond to the situation. Often, the government services and the ICT-experts of the affected vital sector are involved. The IRB issues advice to the Interdepartmental Coordination Consultation (Inter-departementaal Afstemmingsoverleg [IAO]) or the Interdepartmental Crisis Management Commission (Interdepartementale Commissie Crisisbeheersing [ICCb]), as laid down in the National Crisis Decision-Making Manual[83].

---

[79] "Nationaal Detectie Netwerk," Nationaal Cyber Security Centrum, n.d., accessed October 2, 2018, https://www.ncsc.nl/samenwerking/nationaal-detectie-netwerk.html.
[80] Drinking water companies' representative in the IRB, interview by Tessa Mulders, November 27, 2018.
[81] Interview with IRB-representative.
[82] Boeke, "First Responder or Last Resort?," p. 69.
[83] "ICT Response Board," Nationaal Cyber Security Centrum, n.d., accessed October 3, 2018, https://www.ncsc.nl/samenwerking/ict-response-board.html.

From the interviews comes that the drinking water sector is represented in the IRB, as one of the interviewees is the drinking water companies' representative in the IRB. The interviewees did not mention anything regarding the IRB further on.

2.4.4 Explaining: National Response Network

The National Response Network (NRN) is a partnership aiming to strengthen the joint response to cybersecurity incidents. According to Boeke, the NRN further embodies the public-private approach to (cyber) crisis management[84]. This is done by bundling the forces of different response capacities[85].

The NRN is a joint venture between the NCSC and public-private ICT-response organisations from various sectors. Within the NRN, these organisations can share knowledge and experiences and help each other. The NRN focuses both on organising existing response capacity and on stimulating new response capacity within government and vital sectors. The Information Security Service, the Tax Authority, SURF (an ICT-cooperation organisation for education and research in the Netherlands), the Department of Defence and Rijkswaterstaat form the National Response Network[86].

2.4.5 Explaining: Information Sharing and Analysis Centres (ISAC)

To formulate an appropriate approach to cyber threats and vulnerabilities, various Information Sharing and Analysis Centres (ISACs) have been established. ISACs are PPPs, organised per sector. The participants exchange information and experiences regarding cybersecurity and share analyses about situational awareness sectors. This all mainly happens on a tactical level[87]. In 2011 it was announced that the ISACs in 2012 would be connected to the NCSC[88].

An ISAC comprises various representatives from organisations in a particular sector. Routinely, three different public organisations are also associated: the NCSC, the AIVD and Team High Tech Crime of the National Police. They provide their own substantive expertise regarding cybersecurity[89].

---

[84] Boeke, "First Responder or Last Resort?," p. 16.
[85] "Nationaal Response Netwerk," Nationaal Cyber Security Centrum, n.d., accessed October 3, 2018, https://www.ncsc.nl/samenwerking/nationaal-response-netwerk.html.
[86] NCSC, "Nationaal Response Netwerk."
[87] "ISAC's," Nationaal Cyber Security Centrum, n.d., accessed October 4, 2018, https://www.ncsc.nl/english/cooperation/isacs.html.
[88] CPNI.NL, "Jaarbericht 2011 CPNI.nl," (2011).
[89] NCSC, "ISAC's."

In the Netherlands the following sectors are active: Ports, Airports, Financial Institutions, Water Management, Multinationals, Telecom, Nuclear, Healthcare, Energy, **Drinking Water**[90], Managed Service Provider (MSP), Insurance and the National Government and Pensions. The chairmen of the various ISACs meet up in several sessions every year to discuss the overarching themes with the sector[91].

In his study *National cyber crisis management: Different European approaches*, Sergei Boeke argues that The Dutch network model and consensus culture have facilitated information sharing between the public and private sectors. Companies participate on a voluntary basis and each ISAC sets its own agenda; the NCSC provides secretarial facilities. Representatives of the intelligence sector and the high-tech crime unit of the police frequently attend, though companies sometimes choose to meet without government officials present.

The exchange between the public and private sector offers added value for all participants. Another important added value for all participants is that they build up a permanent network. Participants also know how to find each other outside the ISAC meetings to (informally) exchange knowledge[92].

Each ISAC meets periodically: depending on what the sector wants, varying from two to eight times a year. Participants in an ISAC often play an important role in their own organisation in the field of information security, ICT-security or ICT-policy[93].

Each ISAC is unique and has its own dynamics. They determine their own criteria for participating organisations and their personal representatives. Because specific membership guidelines have been drawn up for each ISAC, the requirements for participation vary per ISAC and per sector. In general, information sharing is the most important function at every ISAC[94].

The NCSC fulfills two roles in an ISAC. First, each ISAC has a substantive NCSC representative. Secondly, the NCSC fulfills the secretariat function within the ISAC. Two different people are appointed for these roles. The secretaries work together with the chairmen

---

[90] On the internet, I found several names for the Water-ISAC. From the interviews comes that it is called a *Water*-ISAC, but in fact, it is only the *drinking* water companies (plus government organisations) coming together. I will use the term Water-ISAC to refer to this specific ISAC.

[91] NCSC, "ISAC's."
[92] NCSC, "ISAC's."
[93] NCSC, "ISAC's."
[94] NCSC, "ISAC's."

and members of the ISACs to link and expand the ISACs. The secretaries ensure the link with the NCSC organisation[95].

The drinking water sector established an ISAC in 2006 based on an American model. In this, ten drinking water companies share information regarding cyber threats, incidents, and best practices. More recently, a 24/7 web portal has been set up for operational and tactical cooperation in the field of cybersecurity, detection, prevention, and response. Through this web portal, companies share real-time cybersecurity threats and incidents[96].

Facilitating the running of the ISAC is a shared responsibility. The NCSC has the role of secretary, thus facilitating the process. The private participants also facilitate the process by periodically organise the meetings. It is thus not the responsibility of just one actor, but it is teamwork[97].

The interviewees provided a lot of data regarding the Water-ISAC and there is a lot of other information available. As is further explained in chapter 3.2.2 Public-private Partnership selection: the Water-ISAC, I, therefore, chose to dive deeper into the Water-ISAC and use it as my research subject.

2.4.6 Explaining: Vewin

Vewin is the Association of water companies in the Netherlands (Vereniging van Waterbedrijven In Nederland). The main task of Vewin is to represent the interests of its members (Dutch drinking water companies) in government-wide, aimed at creating favourable conditions for the continuous production of good drinking water. They argue that collaboration, between companies and with the government, as with the NCSC, is essential for success. By sharing information in a timely manner, incidents can be prevented[98].

Administrative Agreement on Water

In May 2011, the Government, the Association of Dutch Municipalities (Vereniging van Nederlandse Gemeenten [VNG]), the Interprovincial Consultation (Interprovinciaal Overleg [IPO]), the Union of Water Boards (Unie van Waterschappen [UvW]) and Vewin signed the Administrative Agreement on Water (Bestuursakkoord Water [BAW]). The purpose of the

[95] NCSC, "ISAC's."
[96] Vewin, "Waterspiegel," *Digitale veiligheid hoog op de agenda: Cyberdreigingen boven water* (2015).
[97] ENISA, "Information sharing and analysis centres (ISACs): Cooperative models," (Marousai: ENISA, 2018).
[98] Vewin, "Digitale veiligheid."

BAW is to continue providing safety against flooding, good quality of water and enough fresh water[99].

On October 31, 2018, additional agreements on the BAW were presented. This will give the partnership a follow-up. They argue that the increase in cybercrime, espionage, and sabotage requires an integrated approach within the water chain. When systems and processes are disrupted, major consequences can threaten public health, safety, and economy. Therefore, the parties join forces in discovering, researching, learning, and sharing experience around opportunities and threats of the information society, and a joint vision is developed regarding the use and accessibility of data, the required infrastructure, and funding[100].

The results of the interviews show that that Vewin is an important partner within the drinking water sector, but not particularly within the Water-ISAC. They are indirectly represented[101].

2.4.7 Explaining: Dutch Cybersecurity Council

The Cybersecurity Council (Cybersecurity Raad [CSR]) is a national, independent advisory body of the Dutch government and the business community. It is composed of high-level representatives from public and private organisations and the scientific community. The CSR undertakes efforts at the strategic level to support cybersecurity in the Netherlands[102].

The composition of the CSR is related to its objectives, set out in its work program. The Council hopes for the widest possible coverage of the various aspects of the cybersecurity field. The council, therefore, has 18 members based on the 7-7-4 allocation key: seven members from the private sector, seven members from the public sector and four from the scientific community. The CSR has two co-chairs: one on behalf of the public sector and one on behalf of the private sector. The members represent a relevant organisation or sector in the cybersecurity domain and are appointed according to an adopted procedure[103].

---

[99] "Bestuursakkoord Water," Rijksoverheid, n.d., accessed October 5, 2018, https://www.helpdeskwater.nl/onderwerpen/wetgeving-beleid/bestuursakkoord/.
[100] "Actualisering maakt Bestuursakkoord Water toekomstbestendig," Vewin, October 31, 2018, accessed October 6, 2018, http://www.vewin.nl/nieuws/paginas/Actualisering_maakt_Bestuursakkoord_Water_toekomstbestendig_979.aspx?source=%2fstandpunten%2fpaginas%2fCybersecuritywet_158.aspx.
[101] Interview with Dossier holder Drinking water of the NCSC.
[102] "Dutch Cyber Security Council," Cyber Security Raad, n.d., accessed October 6, 2018, https://www.cybersecurityraad.nl/index-english.aspx.
[103] CSR, "Dutch Cyber Security Council."

The CSR's composition (representatives from the public, private and scientific sectors) enables the council to approach priorities, constraints, and opportunities from different angles. The council has three tasks that contribute to achieving its mission[104]:

1. Providing solicited and unsolicited strategic advice on cybersecurity to the Dutch government and the business community;
2. Monitoring trends and new technological developments and, where necessary, translating these into potential measures to reduce the cybersecurity risks and to increase the economic opportunities;
3. Initiating and/or accelerating relevant initiatives in the Netherlands and in the European Union that contribute to raising the level of cybersecurity in the Netherlands[105].

Also, the CSR delivers various types of products. The council draws up advisory documents and guides, individual members conduct boardroom meetings with organisations and businesses, the council commissions researchers to carry out research projects and initiates various activities, such as the Cybersecurity debate and the National Cybersecurity Summer School in 2017[106]. Despite the extensive range of duties and the intensive public-private cooperation, the interviewees did not mention anything regarding the CSR.

[104] CSR, "Dutch Cyber Security Council."
[105] CSR, "Dutch Cyber Security Council."
[106] CSR, "Dutch Cyber Security Council."

3. Methodology

This chapter describes the methodological justification and the procedures that I followed to reach a valid answer to the research question. The research design will be explained, as well as the case selection, the operationalisation and an explanation of how I analysed the data. Finally, the limitations (feasibility, validity and reliability implications) to this research will be explained.

3.1 Methodological justification

As mentioned before, the research is divided into two parts. First, a literature review has been performed for answering sub-question 1 (chapter 2.2.4 Defining: (the different variants of) Public-Private Partnerships). Also, sub-question 2 is answered by performing a content analysis, document analysis, and interviews, providing an overview of the current Dutch approach (chapter 2.4 Overview of PPPs: the current Dutch approach for ensuring cybersecurity). Answering sub-question 3 (how the Water-ISAC meets up with the CIP meta-governance approach of Dunn Cavelty and Suter?) happens in part 2 and is done by applying a PPP-model on the current situation. This enabled me to test whether the current Dutch approach meets up with the CIP meta-governance approach of Dunn Cavelty and Suter.

3.2 Case selection and theory

3.2.1 Case selection: the drinking water sector

The case for this case study is the drinking water sector. This is because it is one of the Dutch vital processes and has experienced ransomware infections and phishing attacks in the office automation environment[107]. The Dutch drinking water supply is of great importance for public health and for the functioning of society. Outage leads to societal dislocation[108]. Thereby, the Ministry of Infrastructure and Water management is responsible for drinking water in the Netherlands. Contacts and security clearance for matters related to this ministry are present since I work at this ministry. This is not the case for other ministries, so speaking to people from other ministries would have been more difficult, complicated and less feasible. Other vital processes (category A) under the responsibility of this ministry are *turning and*

[107] NCTV, "*CSBN 2017*".
[108] NCTV, "*CSBN 2017*".

managing water quantity and the *storage, production, and processing of nuclear material*[109]. For this last process, additional security clearance is a requirement. This is not present, so it is not possible to conduct a single case study into this subject. The process of *turning and managing water quantity* is considered too big for this research project. It includes *closing and opening of vital movable barriers* (including drain locks), *the running of pumping stations that have been designated as vital* and the f*unctioning of the crisis organisation*[110]. In particular, the part regarding the crisis organisation is big and too complex to dive into in this time span.

3.2.2 Public-Private Partnership selection: the Water-ISAC

In the previous chapter, different forms of PPP have been described. These PPPs differ from reactive response units (IRB) to an information- and experience-sharing platform. The form of this research is too small to dive deep into all forms of PPP. I, therefore, conclude that the PPP in the form of an ISAC is the most relevant form of PPP. First, because there is a specific Water-ISAC in which all ten drinking water companies are represented. This is more specific than the other forms of cooperation. These other forms focus on cybersecurity of vital sectors in general where the drinking water sector is one of them, are but not specifically focused on that drinking water sector. The Water-ISAC is focused on the drinking water sector, and since this particular sector is the scope of my research, the Water-ISAC is, therefore, best suited to be further analysed. Also, it turned that there is more information available (online and with the interviewees) regarding the ISAC than there is regarding the NDN, NRN, IRB, and CSR.

3.2.3 Theory selection: CIP meta-governance of Dunn Cavelty and Suter

As mentioned before, the CIP meta-governance approach of Dunn Cavelty and Suter theory is applied to the case to test whether the theory stands in an empirical situation, being the Dutch drinking water sector. The reason for this is because they have thoroughly studied the dynamism that comes with cooperation between public and private partners in protecting critical infrastructure and have developed a road map towards CIP meta-governance. Applying this approach should be a solution to problems that arise from PPP in CIP. Since the Dutch drinking water sector is part of the vital infrastructure, I considered the Dunn Cavelty

---

[109] "Critical Infrastructure (Protection)," National Coordinator for Security and Counterterrorism, n.d., accessed October 6, 2018, https://english.nctv.nl/topics_a_z/critical_infrastructure_protection/index.aspx.
[110] NICC, "*Weerbaarheid van de sector keren en beheren oppervlaktewater tegen uitval van elektriciteit en telecommunicatie*," 2010, accessed October 7, 2018.

and Suter-model the most relevant for applying to the case and so to test how this theory fits the case.

A major disadvantage of this model is that in the Netherlands, ministers always bear the final responsibility for all their policy areas. If something goes wrong outside of their power, but within a policy area of their responsibility, they will have to answer for it. This makes it likely for ministers to be hesitant regarding the Dunn Cavelty and Suter-model because governments have a new role under this meta-governance approach. Instead of distributing tasks and monitoring their fulfillment, governments take on the role of coordinators and stimulators of networks. Governments must ensure that public tasks are met by self-regulating networks and if they are not, they must initiate and fund new networks or incentivise existing networks to achieve these tasks. This indirect control is referred to as organisation of self-organisation" or meta-governance"[111].

3.3 Data gathering

Data have been gathered by performing a literature study, content and document analysis and interviews. The literature study provided insights into the different variants of PPP, while the content and document analysis provided insights into the current Dutch PPP-approach in ensuring cybersecurity in the drinking water sector. These analyses took place before the interviews since they provided answers to sub-questions one and two. However, the results of the analyses were also of use to gain basic knowledge on the topic to be able to have an in-depth conversation with the interviewees for answering sub-question three.
The content and documents I analysed are documents written by civil servants of the Ministry of Infrastructure and Water management and Justice and Security. Most of the content comes from the NCSC and NCTV and concerns public information.

By conducting interviews, I gathered in-depth. I have interviewed four people. The first one is a Policy Coordinator Drinking Water and Water Chain of the Ministry of Infrastructure and Water management; his focus area is cybersecurity related to these subjects. He will further be referred to as expert A. Interviewing expert A was a relevant choice because he has knowledge on many subjects regarding drinking water. I knew he did not have specialized expertise and knowledge on one specific PPP. The aim was thus to collect information regarding the different PPPs related to cybersecurity in the Dutch drinking water sector. In

[111] Dunn Cavelty and Suter, "Public-Private Partnerships are no silver bullet," p. 5.

essence, data gathered from this interview is used to answer sub-question two (described in chapter 2.4 Overview of PPPs: the current Dutch approach for ensuring cybersecurity).

The second interviewee works at the National Cybersecurity Centre (NCSC) and is dossier holder Drinking water. This means she is the main contact point for all Dutch drinking water companies for everything related to cybersecurity. This function also includes the Secretariat of the Water-ISAC. She will further be referred to as **dossier holder Drinking water of the NCSC**. I considered it relevant interviewing her because of my focus on the Water-ISAC. I, therefore, argued that it was a matter of course for me to reach out to the NCSC for an interview. Dr. Sergei Boeke helped me with that: he managed to bring me in contact with her. I argue that I could not have interviewed someone with more relevant expertise than the **dossier holder Drinking water of the NCSC**, since she is always present during the meetings of the Water-ISAC, knows its procedures, the members, the mutual relationships, norms, and values.

Interviewee three wishes to be referred to as **Drinking water companies' representative in the IRB** (see: 2.3.3 Explaining: ICT Response Board). His knowledge is considered relevant, as he has participated in several sessions of the Water-ISAC. Thereby, expert A and René van der Helm (see next section) recommended me to interview him. They argued he has extensive knowledge of many subjects related to cybersecurity in the Dutch drinking water sector.

The last interviewee is my colleague René van der Helm, Program Coordinator / Policy Advisor at the Departmental Coordination Centre Crisis Management of the Ministry of Infrastructure and Water Management (DCC-IenW). His focus is also on cybersecurity-related subjects within the Ministry. His knowledge is considered relevant, because he has knowledge on both the specific PPPs (such as the ISAC), as on what different forms of PPPs exist that are relevant to this research.

The interviews have been conducted in a semi-structured way. This means that starting questions were set, but follow-up questions have been determined during the conversation to stimulate or help the interviewee until they provided sufficient information.

3.4 Operationalisation

In the previous chapter, all important terms have been conceptualised. The next step is defining observable indicators as signs for the presence of the concept(s) that have been

identified through interviews. The third sub-question is answered by performing and analysing these interviews.

For this analysis, it was first important to identify aspects from the Dunn Cavelty and Suter-model, given the causal relation I identified in chapter 2.3 Theoretical framework: the road to an answer: the main causal relation is that *the Dutch approach meets up with the theory of Dunn Cavelty and Suter (X)* if *CIP meta-governance is applied (Y).* To see whether *CIP meta-governance is applied (Y)* I split Y in Z (criteria) and A (problems). Since the authors do not define clear criteria for CIP meta-governance, I have identified themes based on (i.e.) what they write about CIP meta-governance, how it should be organised, what it looks like, how the members behave, et cetera. A condition for *(Y) CIP meta-governance is applied* is that *(Z) the case meets most of these criteria.*

Second, a condition for *(Y) CIP meta-governance is applied* is that *(A) most of the problems identified by Dunn Cavelty and Suter are not present in this case.* So, if Z (criteria) and A (problems) are met by the case, I can conclude that *CIP meta-governance is applied (Y)* which leads to the conclusion that *(X) the Dutch approach meets the theory of Dunn Cavelty and Suter.*

The themes and criteria I identified are listed in Table 1. This table is drawn up together with another CSM student, Thom Spitzen. Thom is conducting research similar to this one. He investigates PPPs in the Dutch energy sector, also classified as vital infrastructure. He uses this case to, as I do, test the theory of Dunn Cavelty and Suter. We cooperated on identifying the criteria for the CIP meta-governance theory Dunn Cavelty and Suter came up with, as the authors have not come up with a clear list of criteria such an approach of CIP governance should meet.

Theme	Criteria	Code
Generalities	A small and relatively homogenous network that involves all actors who will and can contribute to the fulfilment of the public service in their own interest	NET
	Persuasion, negotiations and mutual trust are more important than control and regulation;	PERS
	The network itself has the responsibility to control the PPP	CON
	The PPP / network is self-organising	SELF
	Due to the private actors in the network, the network can more easily reach out to international partners	INT
Members' responsibili-ties	The members fix rules for common actions and determine the responsibilities and commitment of the members	RUL
	The government authorities are represented by the responsible agencies and they do not have a special status or authority;	REPR
	All members are equal	EQUA
	The government takes the role of coordinating and stimulating the network. The government mainly implies coordination and promotion activities.	COO
	The members in the network know each other well and are thus able to assess whether the cooperation is sufficient.	KNOW
	The contribution of the government should be meaningful.	MEAN
Monitoring	The members of the network monitor themselves, since only they have sufficient expertise to check each other;	MONI
Government	The government verifies whether the tasks of the PPP are carried out, but does not check the member directly;	CHE
	The government sets up measures or incentives to obligate or stimulate the participation of the network.	MEAS

Table 1: Operationalisation – themes + criteria for interview Testing Theory

3.5 Data-analysis

As I explained in chapter 2.3 Theoretical framework: the road to an answer, the analysis is two-folded since I established that (1) a condition for *(Y) CIP meta-governance is applied* is that *(Z) the case meets most of these criteria* and that (2) *(A) most of the problems identified by Dunn Cavelty and Suter are not present in this case.*

I analysed the data gathered through the interviews in a systematic manner. I recorded the interviews, so I started with transcribing them. Hereafter, I looked for statements that could be linked to a certain criterion of the table illustrated above. If I found a statement that fit, for

example, the criterion “The PPP / network is self-organising”, I marked this sentence with the same green colour as in the table above and commented why I argue this statement fits the criterion and is thus coded SELF. After doing this to the entire interview, I collected all coded statements in an excel sheet to create an overview of all useful statements. I did so for all three interviews. This allowed me to compare the three interviews when, for example, writing the chapter 4.1.4 The PPP/Network is self-organising. I could switch between the three interviews to see empirical evidence of why the PPP is/is not self-organising. This enabled me to create a well-structured analysis per criterion.

Furthermore, I was able to analyse whether the problems identified by Dunn Cavelty and Suter are present in the case or not, as they are related to several criteria I identified. As I first substantiated whether the case meets the criteria, I was hereafter also able to analyse whether the problems are present or not.

3.6 Limitations

This research design was feasible because I currently work at the ministry that is responsible for the Dutch drinking water sector. The contacts and security clearance necessary to find these people and discuss this subject with them are thus present. This is not the case for other ministries, so speaking to people from other ministries would have been more difficult, complicated and less feasible. Thereby, I made use of the network of my colleagues and professor of Leiden University.

The interviews may pose implications for reliability and feasibility. If another researcher, at another time, would perform this research and thus conduct the same interviews, the results will differ. This means that this researcher will conclude upon a different approach. This is because the interviewees may have switched jobs by then. If they would still be available, they might give other answers as the Dutch approach at that time might *really* be different than it is now. However, it is not the goal of this research to produce answers that are relevant over time. The goal of this research is to produce answers that can be used *now*, for improving the current situation or supplementing to the theory. It goes without saying that the current Dutch approach might change over time, what will make this research irrelevant.

Another factor that could affect the reliability of this research is my choice of interviewees. Due to time limitations, not everyone with knowledge on this subject could be interviewed. I had to select based on contacts and people who are willing to participate. These choices affected the kinds of answers and thus the conclusions. Thereby, the ten drinking water

companies that form the Dutch drinking water sector are located throughout the country. This is a practical obstacle in this research, as I was not able to visit all of them. It is thus to be understood that this research might not be a 100% reflection of the truth, but the truth of a few **experts** on this subject. One can assume that the experts will give relevant, honest and expert answers, however, it still does have reliability implications.

Regarding construct validity, this research is valid. The 'current Dutch approach in ensuring cybersecurity' is operationalised based on the construct as it is defined in theory (see chapter 2.4 Overview of PPPs: the current Dutch approach for ensuring cybersecurity). The content validity of this research is also high, as I systematically worked towards an answer to the question. Assessing the Dutch approach is impossible without determining what exactly this approach is, so this was done as well to ensure content validity.

The internal validity might be an issue in this research, as it is assumed that a certain PPP-approach for cybersecurity leads to a certain level of cybersecurity. Also, the external validity of this research is not high. Each country in the world is responsible for its own critical infrastructure. It goes without saying that the outcomes of the research into the current Dutch approach do not count for Spain or Greece for example. It is also obvious that the outcomes of the second part of the research do not count for other countries either, as it is based on the *Dutch* approach. The outcomes cannot be held to be true for other cases, as each case (country or even sector) is specific with its own approaches, stakeholders and priorities. It is thus also not the goal to strive for results that are generalisable to other cases. This research and its conclusions only consider and apply to the case of the Dutch Water-ISAC, part of the Dutch approach into ensuring cybersecurity in the Dutch drinking water sector. It does not conclude anything regarding a Dutch approach in ensuring cybersecurity in a vital sector in general.

4. Analysis

In this chapter, the results of the data analysis are presented. For this analysis, the transcribed interviews were analysed using the criteria drawn up based on the theory of Dunn Cavelty and Suter (see 3.4 Operationalisation and 3.5 Data-analysis).

The data gathered in 2.4 Overview of PPPs: the current Dutch approach for ensuring cybersecurity provide insights into what the current Dutch approach in ensuring cybersecurity in the drinking water sector comprises (sub-question two). In the next sections, I will elaborate on a specific PPP I have chosen to further investigate and analyse: The Water-ISAC. This concerns the most relevant PPP in the drinking water sector and will show how the Dutch approach of ensuring cybersecurity in the drinking water sector meets up with CIP meta-governance (sub-question three). The reason for the choice for this specific PPP is elaborated on in 3.2.2 Public-Private Partnership selection: the Water-ISAC.

This chapter thus first describes the results from the interviews. Besides data from the interviews, I will also refer to the example membership guidelines from the NCSC[112]. This document provides example membership guidelines for ISACs. The Water-ISAC membership guidelines are confidential, so I am not able to refer to those. However, during the interview with the dossier holder Drinking water of the NCSC, I asked whether the Water-ISAC guidelines are based on the public example membership guidelines. The response was "Yes. In principle, those are the basic membership guidelines. It incorporates per ISAC, including drinking water ISAC, what they consider important when it comes to the members who join the ISAC"[113] . I, therefore, consider the Water-ISAC membership guidelines equal to the public example-version.

After this first part, I will go into several problems Dunn Cavelty and Suter identified in their research. They identified five difficulties that they argue can be resolved or at least alleviated by applying CIP meta-governance, or as they call it: the network approach. Based on the results of the analysis, I will show whether these five problems are present within the Water-ISAC. This allows me to, besides arguing whether the Water-ISAC meets the criteria of Dunn

[113] Interview with Dossier holder Drinking water of the NCSC.

Cavelty and Suter (Z), also argue in how far the ideas of Dunn Calvety and Suter regarding resolving several crucial difficulties are applicable on this case (A).

4.1 Analysing: Criterion versus interviews (and membership guidelines)

4.1.1 A network involving all actors able/willing to fulfill the public service

The first criterion of the CIP meta-governance theory is that the PPP is organised as "a small and relatively homogenous network that involves all actors who will and can contribute to the fulfillment of the public service in their own interest". From the interviews comes that the Water-ISAC can be described and is organised as such a network. First, dossier holder Drinking water of the NCSC stated "… you can describe the ISAC as a network" [114]. To back up this statement, she explained that all ISAC-members know who to call when they want to. She also mentioned that "the network in the ISAC is good"[115] and that there is a mutual exchange of information. Thereby she states that the cooperation between drinking water companies and the NCSC is good, which is crucial for a network. She argued that describing the ISAC-members being "all actors who can contribute to cybersecurity in the drinking water sector" is a good summary of the core[116].

Drinking water companies' representative in the IRB argued that, regarding cyber, the drinking water companies talk with each other and with the NCSC in the Water-ISAC. He thereby argued that, with the drinking water companies, they already form a network to share knowledge, also around cybersecurity[117]. This is interpreted as the Water-ISAC being a network in which all relevant parties are represented. Lastly, René van de Helm (policy advisor at DCC-IenW) argued that the Water-ISAC is indeed network cooperation[118].

Beyond the interviews, the example membership guidelines also confirm that the ISAC can be considered a network that involves all actors who will and can contribute to the fulfillment of the public service in their own interest. Chapter 1 (Task), describes that the ISAC should be "a trusted environment in which information can be shared with those responsible for the

[114] Interview with Dossier holder Drinking water of the NCSC.
[115] Interview with Dossier holder Drinking water of the NCSC.
[116] Interview with Dossier holder Drinking water of the NCSC.
[117] Interview with IRB-representative.
[118] Interview with René van der Helm.

protection of the sector"[119]. This shows that the ISAC is based on the idea that all actors who will and can contribute to the fulfillment of the public service should be represented.

What comes from this analysis is that all three experts view the Water-ISAC as a *network*. This means the Water-ISAC meets the first criterion of the CIP meta-governance theory. What must be mentioned is that the term *network* has not been explained to the interviewees. I assumed that, knowing their level of expertise, the interviewees would know what a *network* comprises. However, the interviewees describing the Water-ISAC as a network does not necessarily mean that they refer to the same. The term *network* is a widely studied topic and can be interpreted in several ways. From the literature on *networks* comes that as a concept, *network* has been highly conducive to theorising phenomena and processes such as globalisation, digital media (internet), speed, symbiosis, and complexity. Dirk de Kerckhove (1996) argued that networks provide higher-order intelligence because of the multiple points of reflection and feedback. They allow a collective learning process that is faster and more far-reaching than the more old-fashioned linear forms of communicating intelligence, which is derived from centralised forms of authorisation and legitimation[120]. This can be related to the Water-ISAC. The presence of all Dutch drinking water companies and the NCSC can be viewed as multiple points of feedback, allowing a collective learning process that is faster and more far-reaching than, for example, the line ministry within its responsibilities being responsible for the essential functioning of society, while transferring authority from the government bureaucracy to the private sector as Dunn Cavelty and Suter argued[121].

4.1.2 Persuasion, negotiations and mutual trust versus control and regulation

The second criterion is that "persuasion, negotiations and mutual trust are more important than control and regulation". The dossier holder Drinking water of the NCSC explained that the network cooperation "…it is more about mutual trust. Control and regulation is really something that fits the line ministry and the regulator"[122]. By saying this, she argues that mutual trust is more important than control and regulation. Drinking water companies' representative in the IRB argued that indeed persuasion, negotiations, and mutual trust are more important than control and regulation and that this is good since "…they are all separate

[119] National Cyber Security Centre, "*Voorbeeld lidmaatschapsrichtlijnen ISAC*," The Hague: n.d., accessed December 10, 2018, chapter 1. Taakstelling (2) Doelstellingen (2.1).
[120] Joost van Loon, "Network," *Theory, Culture & Society* 23, no. 2-3 (2006). https://doi.org/10.1177/0263276406062696.
[121] Dunn Cavelty and Suter, "Public-Private Partnerships are no silver bullet," p. 4.
[122] Interview with Dossier holder Drinking water of the NCSC.

water companies that are all responsible for keeping their own 'world' and their own company safe"[123]. These statements are interpreted as that persuasion, negotiations and mutual trust are more important than control and regulation. Furthermore, from the example membership guidelines the NCSC drafted also comes that trust is an important subject. Regarding trust, the example membership guidelines prescribe in the first chapter (Task) that the ISAC is "intended to facilitate the exchange of information on threats, weak spots, and examples of electronic attacks on members' networks and environments in a confidential and trusted environment"[124]. However, the third interviewee did not mention this point. It is thus not a strong conclusion to make. Another critical point possibly affecting the conclusion is that Jori Pascal Kalkman and Erik J. de Waard (2017) argue that trust and control are viewed as the core aspects for building confidence in network partners and can be viewed as complementary and mutually reinforcing. Also, they argue that trust and control need to be balanced to ensure consistency and flexibility in the collaboration. Their findings suggest that trust and control are complementary and mutually reinforcing[125]. Even though this study relates to disaster response and recovery operations and not PPPs, it contradicts the statement of the NCSC. She argued that trust is very important while control and regulation are more for the line ministry and the regulator[126], who are both not represented in the Water-ISAC because of the impartiality of the NCSC.

4.1.3 The network itself has the responsibility to control the PPP

The third point is that "the network itself has the responsibility to control the PPP". The only interviewee who mentioned this, the dossier holder Drinking water of the NCSC, argued that creating and distributing roles, rules, responsibilities "usually takes place in consultation"[127]. Using the word 'usually' means that this is not always the case. However, it means that 'controlling' in the sense of organising the Water-ISAC is not done by a single party, but that it happens jointly. Also, the NCSC did argue that "as a secretary, you agree with the ISAC which topics will be set on the agenda"[128]. This shows that there is not one particular party who controls the PPP in the sense of controlling the meetings and the points of focus.

---

[123] Interview with IRB-representative.
[124] NCSC, "*Voorbeeld lidmaatschapsrichtlijnen*", chapter 1. Taakstelling (1).
[125] Jori Pascal Kalkman and Erik J. de Waard, "Inter-organizational disaster management projects: Finding the middle way between trust and control," *International Journal of Project Management* 35, no. 5 (July 1, 2017 2017). https://doi.org/https://doi.org/10.1016/j.ijproman.2016.09.013.
[126] Interview with Dossier holder Drinking water of the NCSC.
[127] Interview with Dossier holder Drinking water of the NCSC.
[128] Interview with Dossier holder Drinking water of the NCSC.

In the example membership guidelines is prescribed that "representatives of these organisations must meet the criteria mentioned in Chapter 3" and that "all participants are obliged to comply with the procedures and regulations referred to in Chapter 4 regarding the exchange of information[129]". This shows that the members themselves set up several criteria.

What stands out is that only one interviewee mentions this point. This means that either the interviewees do not exactly know whether the network itself has the responsibility to control the PPP, or that this is not a clear procedure. In both cases, I conclude that it is not clear whether the network itself has the responsibility to control the PPP. It is very much possible that it does since the interviewees did not mention another party (such as the NCSC) who has the clear responsibility to control the PPP. Also, the NCSC did not mention it has this responsibility. The NCSC mainly argued that they have a facilitating, connecting role and task.

4.1.4 The PPP / network is self-organising

The next criterion is that "the PPP / network is self-organising". Reverting to theories regarding this criterion, Dempster (1998 [23]) argues that self-organisation refers to exactly what is suggested: systems that appear to organise themselves without external direction, manipulation, or control[130]. The dossier holder Drinking water of the NCSC argued that each ISAC, so also the Water-ISAC, sets the membership guidelines which "…include what they consider important when it comes to the members who join the ISAC"[131]. Thereby, René van der Helm argued that "the network itself has the responsibility to coordinate the cooperation"[132]. He stressed that by saying that ISACs are completely voluntary: "you can participate, and you cannot participate"[133]. This means that it is up to the parties to decide whether they participate or not and thus that they are self-organising. This also comes from the example membership guidelines: "the establishment of the ISAC is not formalised by a signed legal contract"[134] and "application by an organisation for joining the ISAC is submitted

---

[129] NCSC, "*Voorbeeld lidmaatschapsrichtlijnen*", chapters 3. Criteria for personal representatives and 4. Regulations for information exchange.
[130] Tom de Wolf and Tom Holvoet, "Emergence versus self-organisation: Different concepts but promising when combined," in *Engineering Self-Organising Systems: Methodologies And Applications*, ed. Giovanna Di Marzo Serugendo Sven A. Brueckner, Anthony Karageorgos, Radhika Nagpal (Germany: Springer, 2005), p. 5.
[131] Interview with Dossier holder Drinking water of the NCSC.
[132] Interview with René van der Helm.
[133] Interview with René van der Helm.
[134] NCSC, "*Voorbeeld lidmaatschapsrichtlijnen*", chapter 1. Taakstelling (9).

to the existing members for approval. The members cast their vote; accession is only done by unanimous approval"[135].

These points show strong arguments to argue that the Water-ISAC is a self-organising PPP. Referring to the literature, it shows that the Water-ISAC indeed can organise itself: it is voluntary, yet all relevant parties participate, and the network sets membership guidelines based on what the members consider important.

4.1.5 The presence of private actors stimulates international cooperation

For the fifth criterion, Dunn Cavelty and Suter argue that "due to the private actors in the network, the network can more easily reach out to international partners". The dossier holder Drinking water of the NCSC argued that "at the moment, international connections are not being sought in this way"[136] and that "… there are sectors that are working together more internationally at the moment than the drinking water sector"[137]. This corresponds to what the drinking water companies' representative in the IRB said: "We do not even try at all" and "of course we will not make the connection with the English or with someone else, where the situation is different. We are busy enough with ourselves… to call the Swedes for fun and ask them how they do it there; that has not even occurred to me"[138]. The point is clear: The Water-ISAC does not seek international cooperation, despite the private actors in the network. René van der Helm tries to explain this: "in business, there is a kind of unfamiliarity but also fear of governments". According to him, it "has to do with unfamiliarity" and argued international cooperation is "hard"[139]. Thereby comes that the drinking water sector is nationally oriented. The responsibility of the drinking water companies ends at the land borders. This means that there is no need to cooperate with, for example, neighbouring countries. Cooperating internationally would then only be to exchange best practices, knowledge, and experiences, and not because countries are interdependent. This may be different in another sector, where counties are in contact in day-to-day operations or where there is EU-regulation on that sector specific, as is the case with, for example, aviation.

---

[135] NCSC, "*Voorbeeld lidmaatschapsrichtlijnen*", chapter 2. Criteria membership organisations (3).
[136] Interview with Dossier holder Drinking water of the NCSC.
[137] Interview with Dossier holder Drinking water of the NCSC.
[138] Interview with IRB-representative.
[139] Interview with René van der Helm.

4.1.6 ISAC-members set rules and determine responsibilities and commitment

The next criterion "the members fix rules for common actions and determine the responsibilities and commitment of the members" is linked to 4.1.4 The network is self-organising since some of the statements relate to both self-organisation and setting rules and determining responsibilities and commitment. According to the dossier holder Drinking water of the NCSC "there are preconditions for securing network collaboration"[140]. Regarding 'fix rules', she argued that in the Water-ISAC, the members set up membership guidelines. These guidelines prescribe what the members consider important when it comes to parties joining the ISAC[141]. Also, by saying "yes, they must decide that for themselves" René van der Helm confirmed that the members define roles, rules, and responsibilities regarding the Water-ISAC themselves[142]. Regarding 'common action', the NCSC argued that "as a secretary, you agree with the ISAC which topics will be set on the agenda"[143]. This means that both the NCSC as the drinking water companies are responsible for determining what subjects deserve attention. The drinking water companies' representative in the IRB argued that members are responsible for their own commitment: they vote with their feet. If they are not committed, they will stop coming[144]. Lastly, the fact that there are membership guidelines proofs that the ISAC-members set rules and determine responsibilities themselves. Even though the guidelines are based on an example of the NCSC, they are specified by the members themselves. Also, the example membership guidelines prescribe that "a participating organisation may be requested to withdraw from the ISAC if none of its representatives has attended one or more consecutive meetings"[145]. Thereby, all members must sign an acceptance form in which they declare to understand that if "I or my parent company/organisation do not comply with the membership guidelines, I and/or my parent company/organisation may be denied membership of the ISAC"[146]. This way, Water-ISAC members try to establish commitment and make members realise that there are obligations to the membership. They do set rules and determine responsibilities and commitment.

---

[140] Interview with Dossier holder Drinking water of the NCSC.
[141] Interview with Dossier holder Drinking water of the NCSC.
[142] Interview with René van der Helm.
[143] Interview with Dossier holder Drinking water of the NCSC.
[144] Interview with IRB-representative.
[145] NCSC, "*Voorbeeld lidmaatschapsrichtlijnen*", chapter 3. Criteria for personal representatives (9).
[146] NCSC, "*Voorbeeld lidmaatschapsrichtlijnen*", chapter 7. Acceptance form (2).

4.1.7 Responsible agencies take place and have no special status in the ISAC

The next criterion is that "the government authorities are represented by the responsible agencies and they do not have a special status or authority". Regarding the government authorities being represented, the drinking water companies' representative in the IRB argued that "…we have a Water-ISAC. The NCSC participates in this…we also talk to each other with the NCSC in a Water-ISAC"[147]. These statements confirm this criterion. The dossier holder Drinking water of the NCSC argued that "…other government parties also join in"[148]. 'Also' meaning that, next to the NCSC, other government parties *also* join. She also argued that "from the NCSC it is facilitated in this sense that we deliver a secretary; that is me. In addition, every ISAC has a substantive NSCS-representative"[149]. She also said that "it is more that we are one of the parties at the table", referring to the presence of the NSCS in the Water-ISAC[150]. Referring to 2.4.5 Explaining: Information Sharing and Analysing Centres (ISAC), it was already clear that the NCSC participates in the Water-ISAC: "an ISAC comprises various representatives from organisations in a particular sector. Routinely, three different public organisations are also associated: the NCSC, the AIVD and Team High Tech Crime of the National Police"[151].

However, it is important to know that the NCSC is **not** responsible for drinking water supply in The Netherlands. This is the responsibility of the Ministry of Infrastructure and Water management (I&W)[152]. Thereby comes that the Human Environment and Transport Inspectorate (Inspectie Leefomgeving en Transport [ILT]) has been appointed as supervisor of compliance with the rules for drinking water supply in the Netherlands[153]. Both I&W and ILT do not take place in the Water-ISAC[154]. It can, therefore, be challenged whether one can argue that the responsible government parties actually join the Water-ISAC. The NCSC does take place in the Water-ISAC, but in its turn is not a responsible party in the same sense as I&W and ILT are. NCSCs mission is to contribute to the enhancement of the resilience of Dutch society in the digital domain, and thus to create a secure, open and stable information

[147] Interview with IRB-representative.
[148] Interview with Dossier holder Drinking water of the NCSC.
[149] Interview with Dossier holder Drinking water of the NCSC.
[150] Interview with Dossier holder Drinking water of the NCSC.
[151] NCSC, "ISAC's."
[152] NCTV, "Critical Infrastructure (Protection)."
[153] "Subjects: Drinkingwater," Inspectie Leefomgeving en Transport, n.d., accessed December 23, 2018, https://www.ilent.nl/onderwerpen/drinkwater.
[154] Interview with IRB-representative.

society[155]. However, from November 9, 2018, essential service providers and digital service providers must comply with the Network and Information Systems Act (Wet beveiliging netwerk- en informatiesystemen [Wbni]). Under the Wbni, vital providers and providers of essential services are obliged to report to the NCSC in case of serious incidents. Providers of essential services also report to their sectoral supervisor (ILT for the drinking water sector)[156]. This means that from then on, drinking water companies are obligated to inform the NCSC in case of serious incidents. However, this is something that happens outside the ISAC and does not necessarily affect the cooperation related to the Water-ISAC.

On the other side, the dossier holder Drinking water of the NCSC argued that "if you have the responsible line ministry at the table together with the regulator, then I think it will indeed be a less familiar forum within which information is shared"[157]. From this statement can be concluded that she does not consider it a good idea for the line ministry and the regulator to participate in the ISAC, because the mutual relations then change in a way that will not benefit the confidentiality and therefore the purpose of the ISAC.

It is hard to say whether the government authorities are represented by the responsible agencies. It is clear that the NCSC does take place and that I&W and ILT do not, which is a good thing according to the dossier holder Drinking water of the NCSC; however, I&W and ILT are responsible for drinking water supply and the NCSC is not (directly).
Regarding the government agencies not having a special status, the drinking water companies' representative in the IRB told that everyone is equal and that "the NCSC is not our boss"[158]. The dossier holder Drinking water of the NCSC argued that "the ISAC is from the sector. ISAC is not from NCSC" and "…we are especially there for that organisation to help and support them"[159]. This shows that the NCSC does not have a special status or authority.

[155] "What is the NCSC?," Nationaal Cyber Security Centrum, n.d., accessed December 23, 2018, https://www.ncsc.nl/english/organisation.
[156] "Wet beveiliging netwerk- en informatiesystemen per 9 november van kracht," Nationaal Cyber Security Centrum, n.d., accessed December 23, 2018, https://www.ncsc.nl/actueel/nieuwsberichten/wet-beveiliging-netwerk--en-informatiesystemen-per-9-november-van-kracht.html.
[157] Interview with Dossier holder Drinking water of the NCSC.
[158] Interview with IRB-representative.
[159] Interview with Dossier holder Drinking water of the NCSC.

4.1.8 All members are equal

The next criterion is that all ISAC-members should be equal. The dossier holder Drinking water of the NCSC argued that indeed, "ISAC-members are all equal"[160]. The drinking water companies' representative in the IRB also argued that "everyone is equal. The NSCS is not our boss"[161]. Lastly, René van der Helm responded that "no, all are equal"[162] when asked whether there is one party in such an ISAC that has the most say. This also comes from the example membership guidelines. Regarding the procedure for obtaining membership, it describes that "a proposal submitted is accepted or rejected by the members unanimously. An existing member may only object to the candidate member if he does not meet the criteria set for the membership, as mentioned in chapters 2 and 3"[163]. This means that there is no party that, for example, holds a veto or whose voice is considered more important.

An explanation for this level of equality may be because all drinking water companies have a delimited piece of territory that they provide with drinking water. There is no competition; it will be at most the case that one drinking water company is larger than the other and therefore has a more important role, but that is not apparent from the statements cited above.

What I find strange, is that none of the interviewees mentioned the fact that the NCSC gets another status with the implementation of the Wbni. As explained in the previous paragraph, this translation of the NIS-directive prescribes that the vital providers and providers of essential services are obliged to report to the NCSC in case of serious incidents. Even though this does not directly have anything to do with the ISAC, it does concern the same parties as are represented in the ISAC. This could mean that mutual relationships are about to change when, for example, the drinking water companies have to report an incident to the NCSC for the first time.

4.1.9 The government coordinates and stimulates the network

The ninth criterion is that "the government takes the role of coordinating and stimulating the network. The government mainly implies coordination and promotion activities". From the interview with the dossier holder Drinking water of the NCSC comes that they are "facilitating", for example regarding the secretary-tasks, and "independent, and especially

[160] Interview with Dossier holder Drinking water of the NCSC.
[161] Interview with IRB-representative.
[162] Interview with René van der Helm.
[163] NCSC, "*Voorbeeld lidmaatschapsrichtlijnen*", chapter 3. Criteria for personal representatives (8) De procedure voor verkrijging van het lidmaatschap is als volgt (8.3).

there for that organisations to help and support them"[164]. Thereby comes that the drinking water companies' representative in the IRB believes that the ISACs-network is "set up nationwide by the NCSC"[165], which is considered a coordinating and stimulating activity. Also, he argues that "you just see that the NCSC started to pull the clubs together because they wanted to set it up". He argues that the NCSC "…is simply a government that facilitates that"[166]. This is interpreted as coordination and promotion activities. René van der Helm argues that the NCSC "stimulates". He also mentions that they act "connecting, networking, advisory"[167]. Summarised, all three interviewees argue that the NCSC acts as a coordinating and stimulating party since she initiated the formation of ISACs in The Netherlands and tries to coordinate, stimulate and promote this kind of cooperation. The interviewees show no sign of the NCSC being a regulator or trying to obligate the cooperation; she mainly coordinates, stimulates and promotes. According to the drinking water companies' representative in the IRB that is good, because when the NCSC would start issuing on how it should be done, those water companies would either no longer participate, or sit back and say "well, I did what the NCSC said, and if something goes wrong now, it is their fault"[168].

4.1.10 ISAC-members know each other well and can assess the cooperation

The next criterion is that "the members in the network know each other well and are thus able to assess whether the cooperation is sufficient". The dossier holder Drinking water of the NCSC argued that "they know each other well"[169], referring to the partners in the Water-ISAC. She substantiated this by saying that within the drinking water sector, there are certainly several people "…who have been in the ISAC for years"[170]. Also, she "…do[es] think that the members themselves are able to determine whether the collaboration is useful"[171]. The drinking water companies' representative in the IRB argues that "they know each other. We also know the ISAC-members personally. In that sense, it is a small world where you just know each other by name, call each other, and in that way make the connection"[172]. Regarding being able to assess whether the cooperation is sufficient, he argues

[164] Interview with Dossier holder Drinking water of the NCSC.
[165] Interview with IRB-representative.
[166] Interview with IRB-representative.
[167] Interview with René van der Helm.
[168] Interview with IRB-representative.
[169] Interview with Dossier holder Drinking water of the NCSC.
[170] Interview with Dossier holder Drinking water of the NCSC.
[171] Interview with Dossier holder Drinking water of the NCSC.
[172] Interview with IRB-representative.

that “the members themselves determine whether the ISAC is successful. They vote with their feet. So, if they do not like it, they will not come any more”[173]. That means that if they continue to come, what they do, then “you can only say that they see the value of it”[174]. Summarising, he argued that “the members themselves determine whether the ISAC is successful”.

René van der Helm argued that the drinking water sector is “a good, organised, close-knit sector”. He believes that “there are a number of pioneers who are well equipped in terms of people, in terms of insight and overview. They will certainly see the importance”. However, he thinks that this does not apply to everyone[175].
Based on the statements of the interviewees, I can conclude that the ISAC-members know each other well and are also able to assess their cooperation.

4.1.11 The contribution of the government should be meaningful

The eleventh criterion is that “The contribution of the government should be meaningful”. The dossier holder Drinking water of the NCSC explained that “there are also ISACs without the NCSC facilitating. This often concerns ISACs within sectors that are not vital. They do not have that information flow, not the secretary of NCSC, no substantive representative”. So, with NCSC present and facilitating, she argues “it is also much more valuable to them”[176]. She believes that “the drinking water sector finds the ISAC very valuable”[177]. The drinking water companies’ representative in the IRB is “very satisfied with how the NSCS facilitates things”. He explains that the parties can be “open and honest” towards the NCSC and say, "we have not arranged this very well" or "that went really wrong". He argued: “I am very positive about the NCSC. I do not know any negative stories”[178]. René van der Helm believes that the cooperation is going well, but that is “because they are not regulators; they are purely connecting, networking, advising and connecting nationally and internationally”[179]. He explains that “the NCSC is a *national* cybersecurity centre. So, they give advice, support and stimulate without having to supervise or enforce laws. Otherwise, that would simply not work”. He explained that they are mainly “facilitating, supportive and expert. They also do

[173] Interview with IRB-representative.
[174] Interview with IRB-representative.
[175] Interview with René van der Helm.
[176] Interview with Dossier holder Drinking water of the NCSC.
[177] Interview with Dossier holder Drinking water of the NCSC.
[178] Interview with IRB-representative.
[179] Interview with René van der Helm.

not have all expertise themselves, but they get that expertise from all the partners who are connected"[180]. All the above statements are very positive regarding the contribution of the government. Based on the statements from the interviewees, I can conclude that they find the contribution of the attached government party (NCSC) meaningful.

4.1.12 The ISAC-members monitor themselves

The next criterion is that "the members of the network monitor themselves since only they have sufficient expertise to check each other". The interviewees were not able to tell a lot about this subject. The dossier holder Drinking water of the NCSC explained that "in principle, they are themselves primarily responsible for that monitoring"[181] with 'they' referring to the other members of the Water-ISAC. She explained that 'if the NCSC can mean something in this by providing information or facilitating something, or if we can contribute in a certain way to the result…which increases resilience, then we can always see what we can do"[182]. René van der Helm argued that "they have to do that themselves. They cán do it themselves; they must see the importance themselves. That is what it is all about"[183].
This is all that the interviewees mentioned regarding this criterion. I can conclude that either the interviewees do not know who is responsible for monitoring, or that this is not a clear and unambiguous agreement.

4.1.13 The government verifies whether the tasks of the PPP are carried out

This criterion requires that "the government verifies whether the tasks of the PPP are carried out but does not check the member directly". The dossier holder Drinking water of the NCSC argued that they "do keep a list of actions performed by ISAC-members", but do not check in the sense of asking "why did you not perform this task/action this yet?"[184] This is the only thing that the interviewees said regarding the government checking on the members. This leads to the conclusion that either the members do not exactly know in what way the NCSC checks on the ISAC-members. However, the fact that they did not mention that the NCSC checks on them accurately, possibly means that the NCSC indeed does not do that. If she did, the interviewees would have noticed this.

---

[180] Interview with René van der Helm.
[181] Interview with Dossier holder Drinking water of the NCSC.
[182] Interview with Dossier holder Drinking water of the NCSC.
[183] Interview with René van der Helm.
[184] Interview with Dossier holder Drinking water of the NCSC.

4.1.14 The government sets up measures/incentives to stimulate participation

The last criterion prescribes that "the government sets up measures or incentives to obligate or stimulate the participation of the network". The dossier holder Drinking water of the NCSC argued that there are also ISACs without the NCSC facilitating them. This often concerns the ISACs of sectors that are not vital. They do not have that information flow, not the secretary from NCSC, and no substantive representative[185]. These are measures the NCSC uses to stimulate the cooperation within an ISAC in a vital sector, such as the drinking water sector. Thereby, the drinking water companies' representative in the IRB argues that the NCSC "does the secretariat, arranges meetings". Also, he argued that "you have to keep pushing it. You must make sure there are meetings; you must make sure there are reports, things like that. It drops if you do not put any energy into it. Then it collapses"[186]. This means that he believes the NCSC pushes it hard enough for everyone to continue to come and participate. Both the interviewees of the NCSC and the IRB thus argue that the NCSC tries to stimulate participation, mainly by facilitating the Water-ISAC as good as possible.

4.2 Analysing: The problems resolved or not?

I can analyse whether the problems identified by Dunn Cavelty and Suter are present in the case or not, as they are related to several criteria I identified. As I substantiated whether the case meets the criteria in the previous chapter, I am also able to analyse whether the problems are present or not.

4.2.1 Problem 1. Monitoring private companies fulfilling functions around CIP

According to Dunn Cavelty and Suter, the first problem is that the state has no way of monitoring whether private companies are fulfilling their functions around CIP. This is considered a problem, because "generating security for citizens is a core task of the state" but is in private hands. The solution of this problem can be found in self-regulation (and self-policing) of the networks. The partners within a network know each other well and are thus able to assess whether the degree of cooperation is sufficient. This does not mean that the government has no monitoring function at all but emphasises a shift from direct monitoring of the owners and operators of CI towards the monitoring of self-regulating networks.

[185] Interview with Dossier holder Drinking water of the NCSC.
[186] Interview with IRB-representative.

This works within the case of the Water-ISAC. The interviewees argued that all ISAC-members know each other well and can determine whether the collaboration is useful. Also, the dossier holder Drinking water of the NCSC argued that the NCSC does check on the members, but not directly. She does keep a list of actions performed but will not force the members to do something[187]. Lastly, the Water-ISAC is self-organising: the members set up membership guidelines by themselves. Doing so, they determine what they find important when it comes to members joining the ISAC. Also, the Water-ISAC is completely voluntary. This means that the members are not forced to participate in the network, but that they decided to do so themselves. They organised this themselves.

4.2.2 Problem 2. PPPs are often difficult due to diverging interests

The second problem is that public-private cooperation is often difficult due to diverging interests. Dunn Cavelty and Suter argue that networks can only be successful if they are based on a sufficiently large common denominator. However, a direct partnership between companies and governmental agencies from the field of security policy is difficult, since they have completely different backgrounds. Dunn Cavelty and Suter argue that the CIP meta-governance resolves this since it prescribes that the government can make a meaningful contribution to the functioning of a network. Also, the actors involved should focus on the common interest and have established mutual trust[188].

The interviewees mentioned that they find the contribution of the NCSC meaningful. The dossier holder Drinking water of the NCSC believes that the drinking water sector finds the ISAC very valuable[189]. The drinking water companies' representative in the IRB is very satisfied with how the NSCS facilitates things. The ISAC-members can be open and honest towards the NCSC[190]. Thirdly, René van der Helm explained that the NCSC is mainly facilitating, supportive and an expert[191]. All three interviewees were positive regarding the contribution of the NCSC. Regarding mutual trust, the dossier holder Drinking water of the NCSC explained that the network cooperation is more about mutual trust. Control and regulation is really something that fits the line ministry and the regulator, who are both not represented within the Water-ISAC. I also believe that the focus on common interests is not a problem within the Water-ISAC. It does not come directly from the interviews, but I noticed a

[187] Interview with Dossier holder Drinking water of the NCSC.
[188] Dunn Cavelty and Suter, "Public-Private Partnerships are no silver bullet."
[189] Interview with Dossier holder Drinking water of the NCSC.
[190] Interview with IRB-representative.
[191] Interview with René van der Helm.

specific drive towards cooperation with the NCSC from the drinking water sector and vice versa. Representatives of drinking water companies in the Water-ISAC are often specialised in IT and ICT. They are not 'just' staff-members with no relation to cybersecurity. They recognise the need for cybersecurity, know what it entails and understand its importance. This makes them a good partner to the NCSC, whose mission is to contribute to the enhancement of the resilience of Dutch society in the digital domain, and thus to create a secure, open and stable information society[192]. They can deliver expertise and a wide network to connect with if necessary. Based on the above, I argue that the problem regarding PPPs being difficult due to diverging interests is not an issue in the Dutch approach.

4.2.3 Problem 3. PPP should consist of selected companies and must be small

The third problem Dunn Cavelty and Suter describe is that a PPP can only be carried out with selected companies and must be small since they are based on mutual trust. The number of PPP must remain limited since an overly large number would exceed the governments' capacities. However, they also argue that this problem of the limited number of possible partners in a PPP is only an issue if one assumes that it is mandatory for the government to work together with private businesses directly. The NCSC has several core tasks to realise a collaboration platform for public-private parties. One of these tasks is organising (public-private) cooperation within the domain cybersecurity. This involves switching between public and private stakeholders. The aim is to strengthen the cooperation by bundling and enriching existing expertise and experience within cybersecurity[193]. This is, amongst others, done by maintaining and further developing existing partnerships (including ISACS, Liaisons). It is the core task of the NCSC to seek public-private cooperation, so in some sense that is 'mandatory'. However, that is not per se a bad thing. It would have been different if it were the line ministry (I&W) who had this task because then I expect it would exceed the governments' capacities. The NCSC, on the other hand, is the forum for creating a collaboration platform in the field of cybersecurity within the vital domain (i.e. drinking water sector). I expect and assume that they are therefore ready for this task. Thereby, the NCSC has appointed dossier holders for all vital sectors in The Netherlands. These dossier holders are responsible for the contacts with one or two sectors. For example, the interviewee of the

[192] NCSC, "Cooperation."
[193] NCSC, "Cooperation."

NCSC is dossier holder of drinking water and another vital sector (not known by me). This division makes the task manageable.

4.2.4 Problem 4. PPPs unsuitable for international cooperation

Dunn Cavelty and Suter argue that due to the intensive involvement of the government, PPPs are not suited for fostering international cooperation. Applying CIP meta-governance allows for the involvement of large corporations that operate critical infrastructures that are frequently well-connected at the international level. Cooperation between experts can, therefore, evolve quite naturally. They give the impartiality of governments as a condition for its success. Although the NCSC can be considered impartial, international cooperation is not a success in this case. The dossier holder Drinking water of the NCSC argued that international connections are not being sought and that there are sectors that are working together more internationally than the drinking water sector[194]. Thereby, the drinking water companies' representative in the IRB said that they do not even try at all[195]. Moreover, it that has not even occurred to him. The point is clear: The Water-ISAC does not seek international cooperation, despite the presence of private actors in the network. I, therefore, conclude that international cooperation is not naturally in the underlying case. However, it is not clear whether that is because of the presence of a public organisation, or because the drinking water sector is less suited for international cooperation because the service 'providing drinking water' is mainly nationally oriented.

4.2.5 Problem 5. Dissonance between the logic of security and the logic of PPP.

The fifth and last problem Dunn Cavelty and Suter describe is that there is a dissonance between the logic of security and the logic of PPP. The core function of the state cannot be outsourced. They thereby argue that this problem cannot be resolved by applying CIP meta-governance. On the contrary, the outsourcing of essential functions in the field of CIP to self-regulating networks that are not subject to government oversight is quite problematic from a security policy point of view. Moreover, the problem of responsibility is further accentuated in this governance, since the state limits itself to the coordination of networks. This is, therefore, a problem that remains. It did not necessarily come up during the interviews, but from experience I gained during the internship at DCC-IenW, I learned that in the end, the minister of the line ministry (I&W in this case) will always be held responsible if something

[194] Interview with Dossier holder Drinking water of the NCSC.
[195] Interview with IRB-representative.

goes terribly wrong. She is ultimately responsible, even though a large part of everything that needs to be done to reach ‘cybersecurity in the drinking water sector’ is arranged together with the NCSC and the (private) drinking water companies.

5. Conclusion

Taking the answers to the three sub-questions into account allows me to answer the research question: *To what extent does the Dutch approach of ensuring cybersecurity in the drinking water sector meet up with the theory of Dunn Cavelty and Suter?* The general conclusion is presented in the first following paragraph. Hereafter, I will shortly go into the answers to the three sub-questions. This chapter also contains a discussion of how the findings relate to current research and will show the limitations of the research and possible avenues for future research.

5.1 Answered: research question

I conclude that the Dutch approach of ensuring cybersecurity in the drinking water sector partly meets up with the theory of Dunn Cavelty and Suter. More specifically, it meets eight of the fourteen criteria (Z) of Dunn Cavelty and Suter. The Dutch approach fails to meet three criteria of the theory. Regarding three other criteria, more research is needed as some parts make me conclude that they do meet up, while other parts make me conclude the opposite. Furthermore, the Dutch approach manages to avoid three out of five problems (A) that Dunn Cavelty and Suter identified and described as common for PPP in CIP. One of the two problems that *are* present in the case, was not expected to be solved in the first place. This means that I am unable to draw an unambiguous conclusion. **The Dutch approach of ensuring cybersecurity in the drinking water sector (Water-ISAC) partly meets up with the theory of Dunn Cavelty and Suter (CIP meta-governance approach). I draw this conclusion since six criteria are not or not completely met by the case. Furthermore, one problem that would be resolved or at least alleviated according to Dunn Cavelty and Suter is still present in the case.**

5.2 Answered: sub-questions

To provide an answer to the research question, three sub-questions have been answered during this research. The answer to sub-question one provided an overview of different variants of PPP relevant to this research, showing that PPP is a much-debated topic. There is not one agreed-on definition and PPP in CIP should, according to Dunn Cavelty and Suter and Boeke, be different from ‘regular’ PPP.

Sub-question two explained the current Dutch approach of ensuring cybersecurity in the drinking water sector. This showed that the NCSC is the main facilitator of PPPs in this field. They are represented in the various PPPs related to ensuring cybersecurity in the Dutch drinking water sector and other vital sectors in general. Their most important partners are the Dutch vital sectors, often consisting of (private) companies. The Water-ISAC turned out to be the PPP-form that fits this research design the most and has thus been the main subject of this research.

Answering the last sub-question provided insights into how the CIP meta-governance approach fits the case of the Water-ISAC. When comparing the criteria derived from the theory of Dunn Cavelty and Suter to the results of the interviews, it appeared that eight criteria of this theory fit the case. These are the following criteria:

1. A small and relatively homogenous network that involves all actors who will and can contribute to the fulfillment of the public service in their own interest;
4. The PPP / network is self-organising;
6. The members fix rules for common actions and determine the responsibilities and commitment of the members;
8. All members are equal;
9. The government takes the role of coordinating and stimulating the network. The government mainly implies coordination and promotion activities;
10. The members in the network know each other well and are thus able to assess whether the cooperation is sufficient;
11. The contribution of the government should be meaningful;
14. The government sets up measures or incentives to obligate or stimulate the participation of the network.

However, there are also criteria that do not meet the case. First, regarding the network itself having the responsibility to control the PPP. Only one interviewee mentioned that creating and distributing roles, rules, responsibilities *usually* takes place in consultation. The other interviewees do not mention this point. This means that either the interviewees do not exactly know whether the network itself has the responsibility to control the PPP, or that this is not a clear procedure.

Further, it is not true that due to the private actors in the network, the network can more easily reach out to international partners. The Water-ISAC does not seek international cooperation, despite the private actors in the network.

Lastly, the interviewees were not able to tell a lot about the members of the network monitoring themselves. I can conclude that either the interviewees do not know who is responsible for monitoring, or that this is not a clear and unambiguous agreement.

Now, three criteria have not yet been qualified as ‘met’ or ‘not met’. This is because I argue I was not able to draw an unambiguous conclusion. The first criterion this applies to is that persuasion, negotiations and mutual trust are more important than control and regulation. From the interviews and the example membership guidelines comes that this is indeed the case. However, the third interviewee did not mention this point and the literature I referred to shows that trust and control are considered core aspects for building confidence in network partners and can be viewed as complementary and mutually reinforcing. This contradicts the statement of the NCSC. I am therefore not able to draw an unambiguous conclusion regarding this criterion.

The second criterion this applies to is that the government authorities should be represented by the responsible agencies and they do not have a special status or authority. The NCSC takes place in the Water-ISAC. I&W and ILT do not. However, I&W and ILT are responsible for drinking water supply and the NCSC is not (directly). Regarding the government agencies not having a special status, I conclude that indeed everyone is equal and that the NCSC is there for help and support. This shows that the NCSC does not have a special status or authority. This makes me conclude that the second part of the criterion does fit the case, however, regarding the first part, I am not able to make an unambiguous decision. Also, it is unclear how the status of the NCSC is going to develop given the changes under the Wbni.

The last criterion I am not certain of is that the government verifies whether the tasks of the PPP are carried out but does not check the member directly. I might conclude that the members do not exactly know in what way the NCSC checks on the ISAC-members, as they did not mention it. However, this might also mean that the NCSC indeed does not check the member directly. If she did, the interviewees would have noticed this. The interviewees did not mention anything that allows me to conclude on the monitoring role of the NCSC.

Regarding the five problems Dunn Cavelty and Suter argued can be resolved or at least alleviated by applying CIP meta-governance, I conclude that three of these fit the case. The problems that are indeed not present in the case are (1) the state having no way of monitoring whether private companies are fulfilling their functions in the area of CIP; (2) public-private cooperation is often difficult due to diverging interests; and (3) a PPP can only be carried out with selected companies and must be small, since they are based on mutual trust.

Problem four and five are, in contrary to the first three, not resolved by applying CIP meta-governance. Dunn Cavelty and Suter argue that due to the intensive involvement of the government, PPPs are not suited for fostering international cooperation (problem four) and that this could be resolved by the presence of private actors. However, the Water-ISAC does not seek international cooperation, despite the presence of (a majority of) private actors in the network. Regarding the fifth problem, a dissonance between the logic of security and the logic of PPP, Dunn Cavelty and Suter argued it cannot be resolved by CIP meta-governance. I endorse this conclusion, as the minister of the line ministry (I&W in this case) will always be held responsible if something goes wrong. She is ultimately responsible, even though a large part of everything that needs to be done to reach 'cybersecurity in the drinking water sector' is arranged together with the NCSC and the drinking water companies. This relates to what Boeke described: the public sector cannot get rid of its own responsibility as the **principal security provider** against top-level threats[196].

5.3 Relevance and limitations

The findings show that Dunn Cavelty's form of CIP meta-governance partly fits the case of the Water-ISAC. This research provides knowledge on a single country's national approach to ensuring cybersecurity in a vital sector, specified on one form of PPP. This is something that is not shown before. The findings partly confirm the correctness of the theory, but also show contradictions and discrepancies. Doing so, the findings contribute to the general body of knowledge about achieving cybersecurity in a vital sector.

Regarding possible avenues for further research, the results may be used in a comparative case study between the UK, as this research is based on the structure of Kristan Stoddart. Also, when more data regarding the Dutch approach within other vital sectors would be

[196] Boeke, "National cyber crisis management."

gathered, the results could be compared to the results of the drinking water sector to see whether the theory holds in both cases and thus stronger conclusions could be made.

Before heading to the recommendations, I would like to mention some limitations of this research. A major limitation is that I was able to perform interviews with only four experts. Even though they have provided me with important, useful and many information and despite the fact they are experts and I do not aim to generalise the results, this research would have had a stronger foundation if I would have been able to collect more empirical data. Unfortunately, I was not able to do so. Many details of cybersecurity in a vital sector are classified and/or politically sensitive. Despite the fact I have a security clearance, some details go beyond this. Also, I had to finish this research within a limited time span. The fact that I worked as an intern at DCC-IenW helped me a lot in the sense of a network, direct colleagues with a wide network and an understanding of the matter, but at some times it also caused a distraction. Working at an organisation that is this interesting, excited and appealing to my interests made that I sometimes placed this research in a second place.

5.4 Recommendations

Having applied the theory to the case of the Dutch drinking water sector, allows me to provide two-folded recommendations. Regarding the theory of Dunn Cavelty and Suter, I recommend diving into the aspect of international cooperation. From the analysis strongly comes that the drinking water sector is not concerned with international cooperation. First, I recommend investigating whether international cooperation is truly an added value regarding (PPP in) CIP, as this is most of the time nationally oriented. International cooperation would then only be of use if the overall structures of that other country are like the national situation. Secondly, I recommend investigating what factors contribute to a sector being concerned / not concerned with international cooperation. From the results comes that the presence of private actors not necessarily leads to international cooperation, so the theory is not quite right on this part.

Further, I recommend changing the criteria that “responsible agencies take place and have no special status”. It is good that they should not have a special status; however, ‘responsible agency’ causes confusions. As is visible in the analysis, it appeared that the NCSC is represented in the ISAC and that they are not directly responsible for ensuring drinking water. I&W and ILT are not represented, while they *are* directly responsible for this. I do argue that it is good that the NCSC is represented and I&W and ILT are not since the NCSC is more

independent and has the status of an expert organisation and its presence is considered helpful. I recommend changing this criterion to “agencies responsible for (cyber) CIP take place and have no special status”. This prevents confusion regarding the type of ‘responsibility’.

Regarding the case of the Dutch approach, I recommend the ISAC-members to clarify who has the responsibility to control the PPP. It might even be necessary to fix this in their membership guidelines. Also, I recommend the Water-ISAC to clarify who is responsible for monitoring the network. This prevents it from becoming a platform with many good intentions, but few achievements. Further, I recommend the Water-ISAC to make clear in what way the represented government (NCSC) verifies whether the tasks of the PPP are carried out. This is in line with the previous recommendation. It is not necessary for the NCSC to check the members directly, as they are a self-organising network. However, it is important to have some form of verification to ensure and secure achievements.

Lastly, I recommend the Water-ISAC to consider how the changing status of the NCSC with the adoption of the Wbni impacts the mutual relations of the partners cooperating in the Water-ISAC. Until now, the NCSC was mainly an expert organisation with no intent or rights to impose penalties in case of non-compliance or incidents on side of the private parties. With the adoptions of the Wbni, the drinking water companies are obliged to report incidents to the NCSC, the party with whom they were used to share confidential information with, without any consequences. To prevent changes in trust and willingness to share information, it is important that this change is carefully considered and discussed, what may lead to agreements on how to deal with this new situation.

Bibliography

ANP. "*Minister Bijleveld bevestigt: we zijn in cyberoorlog met de Russen*." NOS.nl, last updated October 14, 2018, accessed December 20, 2018, https://nos.nl/artikel/2254749-minister-bijleveld-bevestigt-we-zijn-in-cyberoorlog-met-de-russen.html.

ANP. "*Nieuwe DDoS-aanval op ABN Amro, ING, Rabo en Belastingdienst*." NOS.nl, last updated January 30, 2018, accessed June 20, 2018, https://nos.nl/artikel/2214537-nieuwe-ddos-aanval-op-abn-amro-ing-rabo-en-belastingdienst.html.

ANP. "*Opnieuw DDoS-aanval op website DigiD*." NOS.nl, last updated August 1, 2018, accessed December 10, 2018, https://nos.nl/artikel/2244113-opnieuw-ddos-aanval-op-website-digid.html.

Boeke, Sergei. "*First Responder or Last Resort? The role of the Ministry of Defence in national cyber crisis management in four European countries*." September 1, 2016.

Boeke, Sergei. "National cyber crisis management: Different European approaches."*Governance* 31, no. 3(2017): 449-464. https://doi.org/10.1111/gove.12309.

CPNI.NL. "*Jaarbericht 2011 CPNI.nl*." Accessed October 4, 2018. http://publications.tno.nl/publication/101354/GXNyHO/2011-CPNI.pdf.

Cyber Security Raad. "*Dutch Cyber Security Council*." n.d., accessed October 6, 2018, https://www.cybersecurityraad.nl/index-english.aspx.

de Wolf, Tom, and Holvoet, Tom. "Emergence versus self-organisation: Different concepts but promising when combined." In *Engineering Self-Organising Systems: Methodologies And Applications*, edited by Giovanna Di Marzo Serugendo Sven A. Brueckner, Anthony Karageorgos, Radhika Nagpal, 1-15. Germany: Springer, 2005.

Directie Cyber Security. *Reactie inzake cyberaanval met ransomware en voortgang moties uit Wannacry-debat*. The Hague, 2017.

Dossier holder Drinking water of the NCSC. Interview for master thesis by Tessa Mulders. *Crisis and Security Management* (December 3, 2018).

Drinking water companies' representative in the IRB. Interview for master thesis by Tessa Mulders. *Crisis and Security Management* (November 27, 2018).

Dunn Cavelty, Myriam, and Suter, Manuel. "Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection." [In en].*International journal of critical infrastructure protection* 2, no. 4(2009): 179 - 187. https://doi.org/10.1016/j.ijcip.2009.08.006.

Eerste Kamer der Staten-Generaal. "*Regels ter implementatie van richtlijn (EU) 2016/1148 (Wet beveiliging netwerk- en informatiesystemen)*." October 17, 2018. https://www.eerstekamer.nl/behandeling/20181108/publicatie_wet/document3/f=/vkt94dz0rkza.pdf.

ENISA. "Information sharing and analysis centres (ISACs): Cooperative models." Marousai: ENISA, 2018.

Enisa. "*NIS Directive*." 2018, accessed October 18, 2018, https://www.enisa.europa.eu/topics/nis-directive.

Evides. "*Bestuur en Governance*." n.d., accessed October 1, 2018, https://www.evides.nl/over-evides/de-organisatie/bestuur-en-aandeelhouders.

HM Government. *National Cyber Security Strategy 2016-2022*, last updated September 11, 2017.

Inspectie Leefomgeving en Transport. "*Subjects: Drinkingwater*." n.d., accessed December 23, 2018, https://www.ilent.nl/onderwerpen/drinkwater.

Jayawardane, Sash, Jackson, Erin, and Larik, Joris. "Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance."*Policy brief* 17(November 2015).

Kalkman, Jori Pascal, and de Waard, Erik J. "Inter-organizational disaster management projects: Finding the middle way between trust and control."*International Journal of Project Management* 35, no. 5(July 1, 20172017): 889-899. https://doi.org/https://doi.org/10.1016/j.ijproman.2016.09.013.

Klijn, Erik Hans, and van Twist, Mark. "Publiek-Private Samenwerking in Nederland: retoriek of bloeiende praktijk?". (August 2007).

Luijf, Eric, and te Paske, Bert Jan. "Cyber Security of Industrial Control Systems." (March 2015): 3-47.

Ministerie van Economische Zaken en Klimaat. *Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) voor Digitale dienstverleners*. The Hague, September 2018.

Nationaal Coördinator Terrorismebestijding en Veiligheid. "*Cybersecurity*." n.d., accessed October 2, 2018.

Nationaal Coördinator Terrorismebestijding en Veiligheid. *Cybersecuritybeeld Nederland - CSBN 2017*. The Hague, June 2017.

Nationaal Coördinator Terrorismebestijding en Veiligheid. *Cybersecuritybeeld Nederland - CSBN 2018*. The Hague, June 2018.

Nationaal Cyber Security Centrum. "*ICT Response Board*." n.d., accessed October 3, 2018, https://www.ncsc.nl/samenwerking/ict-response-board.html.

Nationaal Cyber Security Centrum. "*ISAC's*." n.d., accessed October 4, 2018, https://www.ncsc.nl/english/cooperation/isacs.html.

Nationaal Cyber Security Centrum. "*Liaisonschap*." n.d., accessed October 2, 2018, https://www.ncsc.nl/samenwerking/liaisonschap.html.

Nationaal Cyber Security Centrum. "*Nationaal Detectie Netwerk*." n.d., accessed October 2, 2018, https://www.ncsc.nl/samenwerking/nationaal-detectie-netwerk.html.

Nationaal Cyber Security Centrum. "*Nationaal Response Netwerk*." n.d., accessed October 3, 2018, https://www.ncsc.nl/samenwerking/nationaal-response-netwerk.html.

Nationaal Cyber Security Centrum. "*Publiek-private samenwerking*." n.d., accessed October 1, 2018, https://www.ncsc.nl/samenwerking/publiek-private-samenwerking.html.

Nationaal Cyber Security Centrum. "*Wet beveiliging netwerk- en informatiesystemen per 9 november van kracht*." n.d., accessed December 23, 2018, https://www.ncsc.nl/actueel/nieuwsberichten/wet-beveiliging-netwerk--en-informatiesystemen-per-9-november-van-kracht.html.

Nationaal Cyber Security Centrum. "*What is the NCSC?*", n.d., accessed December 23, 2018, https://www.ncsc.nl/english/organisation.

National Coordinator for Security and Counterterrorism. "*Critical Infrastructure (Protection)*." n.d., accessed October 6, 2018, https://english.nctv.nl/topics_a_z/critical_infrastructure_protection/index.aspx.

National Coordinator for Security and Counterterrorism. "*Critical Infrastructure (Protection)*." n.d., accessed December 23, 2018, https://english.nctv.nl/topics_a_z/critical_infrastructure_protection/index.aspx.

National Coordinator for Security and Counterterrorism. *Resilient critical infrastructure*. The Hague, 2018.

National Cyber Security Centre. *Voorbeeld lidmaatschapsrichtlijnen ISAC*. The Hague, n.d.

National Cyber Security Centrum. "*Cooperation*." n.d., accessed October 1, 2018, https://www.ncsc.nl/english/cooperation.

NICC. *Weerbaarheid van de sector keren en beheren oppervlaktewater tegen uitval van elektriciteit en telecommunicatie*: NICC, 2010.

Official Journal of the European Communities. "*COUNCIL DIRECTIVE 98/83/EC of 3 November 1998 on the quality of water intended for human consumption*." November 3, 1998. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31998L0083&from=EN.

Official Journal of the European Union. "*DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*." July 6, 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

Overheid.nl. "*Drinkwaterwet*." July 1, 2015. https://wetten.overheid.nl/BWBR0026338/2015-07-01.

René van der Helm. Interview for master thesis by Tessa Mulders. *Crisis and Security Management* (November 28, 2018).

Rijksoverheid. "*Bestuursakkoord Water*." n.d., accessed October 5, 2018, https://www.helpdeskwater.nl/onderwerpen/wetgeving-beleid/bestuursakkoord/.

Rijksoverheid. "*Vraag en antwoord over DigiNotar*." 2011, accessed June 11, 2018, https://www.rijksoverheid.nl/documenten/brochures/2011/09/05/informatie-over-diginotar.

Stoddart, Kristan. "UK cyber security and critical national infrastructure protection."*International Affairs* 92, no. 5(2016): 1079-1105. https://doi.org/doi:10.1111/1468-2346.12706.

The Hague Security Delta. "Securing Critical Infrastructures in The Netherlands: Towards a National Testbed." (2015).

Tweede Kamer der Staten-Generaal. "*Belang digitale veiligheid benadrukt*." 2017, accessed September 7, 2018, https://www.tweedekamer.nl/kamerstukken/plenaire_verslagen/kamer_in_het_kort/belang-digitale-veiligheid-benadrukt.

Utrecht, Robin. "*DDoS-aanvallen op Belastingdienst en DigiD voorbij*." NOS.nl, last updated March 7, 2018, accessed, https://nos.nl/artikel/2221096-ddos-aanvallen-op-belastingdienst-en-digid-voorbij.html.

van Loon, Joost. "Network."*Theory, Culture & Society* 23, no. 2-3(2006): 307. https://doi.org/10.1177/0263276406062696.

van Montfort, Cor, van den Brink, Gabriel, Schulz, Martin, and Maalsté, Nicole. "Publiek-private samenwerking in maatschappelijke veiligheid: Naar een ‘improvisatiemodel’." (February 1, 2012).

Vewin. "*Actualisering maakt Bestuursakkoord Water toekomstbestendig*." October 31, 2018, accessed October 6, 2018, http://www.vewin.nl/nieuws/paginas/Actualisering_maakt_Bestuursakkoord_Water_toekomstbestendig_979.aspx?source=%2fstandpunten%2fpaginas%2fCybersecuritywet_158.aspx.

Vewin. "*Dutch water sector*." n.d., accessed June 1, 2018, http://www.vewin.nl/english/dutch-water-sector/Paginas/default.aspx.

Vewin. "*Waterspiegel*." Accessed October 5, 2018.

Vitens. "*Aandeelhouders*." n.d., accessed October 1, 2018, https://www.vitens.com/organisatie/bestuur-en-corporate-governance.

Waterbedrijf Groningen. "*FACTS & FIGURES*." n.d., accessed October 1, 2018, https://waterbedrijfgroningen.nl/organisatie/ons-verhaal/facts-figures/.