

Developing trust inside security networks

Researching trust-building inside the Joint-SOC network



Nick de Vries
Crisis and Security Management
S1858483

Eerste lezer:
Tweede lezer:

Jaap Reijling
Dr. Vlad Niculescu-Dinca

Content

Executive summary	4
1.0 Introduction.....	7
1.1. Social discussion.....	8
1.2. Scientific discussion	8
1.3. Research question	10
1.4. Guidance	10
2.0. Theoretical framework.....	11
2.1. Security network governance.....	12
2.1.1. Security networks.....	12
2.1.2. Network governance	13
2.2. Trust	17
2.2.1. An introduction to trust research.....	17
2.2.2. Trust inside (security) networks.....	17
2.2.3. What is trust?	18
2.2.4. The elements of trust.....	20
2.2.5. The three core components of trust.....	20
2.3 Building trust	22
2.4 A dynamic model for building trust.....	24
3.0. Methodology.....	27
3.1. Case Study design.....	27
3.2. Data collection methods.....	28
3.2.1. Desk study.....	28
3.2.2. Interviews.....	28
3.2.3. Document analysis	29
3.3. Data exploitation and assessment	30
3.3.1. Operationalization.....	30
3.4. Interview protocol.....	32
3.5 Coding scheme.....	33
3.6. Reliability and validity.....	34
3.6.1. Reliability.....	34
3.6.2. Validity	34
4.0 Analysis.....	36
4.1 Introducing the Joint-SOC network.....	36
4.1.2. The Joint-SOC Network and its network governance	38

4.1.3. Sharing information inside Cybersecurity networks.....	39
4.1.4. Sub conclusion on governance and the relevance of trust building inside the Joint-Soc network.....	41
4.2. Components of Trust.....	42
4.2.1 Capabilities.....	42
4.2.2. Benevolence.....	43
4.2.3. Integrity.....	44
4.3 The dynamic process of trust-building	45
4.3.1. Screening: The starting point of trust in security networks?	45
4.3.2. Building trust.....	46
4.3.3. Cooperation as starting point	46
4.3.4. Third party relationship: Network closure and structural equivalence	47
4.3.5. The relationship between the trustor and the trustee	49
4.4. Combining all elements of the trust model.....	50
4.5. How is trust build inside security networks?.....	53
5.0. Reflecting, policy recommendations and future research	55
5.1. Reflection.....	55
5.2. Policy recommendations.....	58
5.3. Guidance for future study	59
Literature.....	61
Sources.....	65
Appendix.....	67
Interview protocol.....	68
Respondents	69

Executive summary

Inside security networks information sharing is important and that requires trust. However, building trust inside security networks is underdefined and requires further study. The central question in this research is: *How is trust build inside security networks?* The main purpose of this research is, based on a holistic case-study of the Dutch Joint-SOC network, to provide insights in how trust develops inside a security network, following the works of Lambricht (2010) and Mayer (1995). The security network that is researched in this thesis is the Joint-SOC network. This network consists of three Dutch governmental Security Operations Centers (SOC's) and the Dutch National Cyber Security Center (NCSC-NL). The aim of this network is to improve the cybersecurity of the Dutch government through collaboration. Second, this thesis provides insights inside security network operations and will provide recommendations for security network practitioners.

Trust in this research is described as a dynamic interplay between three components: Capabilities, benevolence and integrity. The dynamic part in this interplay is that there can be different attributions to a construct but there can still be trust. For example, one's capabilities may be ranked low that person or organization is still trusted. This study shows that benevolence and integrity are perceived the most important constructs in this dynamic interplay. Building trust inside networks is portrayed in the model of this thesis as a dynamic process that starts with cooperation. During this cooperation there are several factors that influence whether or not other parties are trusted such as third-party relationships, the relationship between the trustor and the trustee and the frequency of interactions. The main findings of this research are that it requires time and effort to build a trusting relationship and that building trust is strongly dependent on personal contact. During the start of a relationship it is useful to describe which guidelines should be adhered by the network, as it provides a basis for talking about integrity and benevolence. It is also useful to construct a maturity requirement, in order to create a baseline for capabilities. A screening by the Dutch intelligence services seems to be an important part of trust inside the Joint-SOC even though it was outside the initial model of this research. All respondents stated that a screening was a firm basis for trust, which is in line with Whelan (2015) statements on interpersonal trust. This research showed that one's capabilities could be tested before entering a network trough, for example, maturity requirements. Proceeding, this research discovered that trust is about the interplay between capabilities, benevolence and integrity, as indicated by Lambricht et al (2010) and Mayer (1995). Mayer asked himself which construct would be most important in a situation. The analysis of this research states that benevolence and

integrity are the most important constructs. If one's integrity is challenged it is very difficult to be trusted by others (Respondent four, 2018). Another finding is that benevolence is deemed important but does not necessarily have to mean that every party has the same interests. If there is a conflict in interests it should be discussed. The organizations inside the Joint-SOC network accept that other organizations have other interests, but it does not have to damage the trust relationship the parties have with each other (Respondent three, 2018). That is why it is important to create guidelines for cooperation and include this kind of agreements.

This research ends with new material for trust research to explore. It proposes an addition to the model created by Lambricht et al (2010) for trust researchers, to look at trust and use it in a wider variety of networks, or other forms of collaboration. This research also adds to the works of Provan and Kenis (2008), Klijn & Edelenbos (2007) and Whelan (2015). For security network practitioners it shows in what way trust is built in a highly respected network. Building trust inside a security network starts with basic principles that should be adhered by all parties. Personal contact is the most important factor in building trust. When people meet each other and start to work together trust starts to build, in the Joint-SOC network the emphasis lies on the integrity and benevolence of the other parties whether or not trust strengthens.

Four recommendations are suggested. First, network practitioners are advised to write down the basic principles and rules of the network, in order to anticipate on benevolence and integrity issues. Second, organizations participating in a network are suggested that they give concrete attention to the principles of trust: Capabilities, benevolence and integrity. In daily operations these principles play an important role in trusting another but are not discussed on a regular basis. The third recommendation is to arrange '*warm transfers*' when members of a network are succeeded by someone else. Personal relationships are the most important factor in building trust in security networks. When new members of the network are introduced they are trusted quicker because of the transferability of the organizational trust to the new network member. This is complementary to the recommendation of Whelan (2015: p. 42). The final recommendation is to, as a network, frequently interact. Frequent interaction has proven to be important to the trustworthiness of others. The frequency of interactions cannot be grasped in numbers but depends on the situation. The most beneficial form of interaction are network-meetings where people meet in person.

1.0 Introduction

In today's society the concept of security is widely debated, perceived, guaranteed or denied. Modern day headlines are filled with topics concerning security. Security topics traditionally consists of themes such as: Terrorism, warfare, policing and cybersecurity. Different actors across both public and private spheres collaborate to provide '*security*' in these fields. This provision comes with an ordeal. Security itself is a contested concept which means that there is not a consensus about what security entails (Schäfer, 2013: p. 5). Different authors state that absolute security is not achievable, because it requires both the absence of fear and the absence of threats (Schäfer, 2013 & Whelan, 2015 & Zedner, 2009). Security is a field of operations without consensus about how the problem should be solved and through what means. The provision of security is also not easily divided into neat arrangements that will lead to more security and therefore could be classified as a '*wicked problem*' (Whelan, 2015: p. 2). The field of security is also diverse in its problems, it ranges from local crime problems to civil war.

If we state that the provision of security is difficult, how does the government keep society safe? Several authors state that tackling '*wicked problems*' or wildly complex problems requires collaboration (Roberts, 2000 & Krahnemann, 2010 & Whelan 2015). This is also the case in providing security. Security actors, both private and governmental, need to cooperate to achieve a greater sense of security or diminish the threats that target society. Dupont describes these relationships between security actors as '*security networks*' (Dupont, 2004: p. 76). Dupont argues that through the ages governmental organization shifted from hierarchical structures to a form of '*nodal governance*'. In this new form of organization, the government is cooperating with its partner organizations instead of steering them. Dupont introduced the term '*security networks*' as a way of contributing to the literature on public sector networks (Dupont, 2004: p. 77). These security networks could contribute to achieving greater security, may it be objective or subjective security. Whelan argues that security networks are the answer to delivering complex products, however measuring performance of networks is also a complex undertaking on its own (Whelan, 2015).

Security networks are visible in day to day life when encountering a police officer on the street, but also operate in situations with greater complexity. For example, the collaboration between a bank and a police unit to arrest a cyberfraud (Pieters, 2018).

Earlier in this introduction is stated that the field of security is broad. Of central importance to all aspects nowadays is cybersecurity. In this cyberdomain the need for more and better collaboration is consistently stated by researchers, governments and private actors. Public and private parties in the Netherlands created the National Cyber Security Strategy. One of the main points in this strategy is the need for more and better cooperation (NCSS, 2016: p. 2-3). The Cyber Readiness Index portrays the variety of such networks. Examples of such networks are Information Sharing Analysis Centers (ISAC's), the International Watch and Warning Network (IWWN) and the Forum for Incident Response and Security Teams (FIRST) (Hathaway & Spidalieri, 2017: p. 23-25).

1.1. Social discussion

In the last few years cybersecurity has been more important than ever. In modern day society depends on the internet for our healthcare, money, groceries and general well-being. With the comforts from the technological advancements came also remarkable threats. In 2007 Estonia had presumably been attacked by the Russian government (Blank, 2008). In 2015 Ukraine's power grid was turned off during an advanced cyberattack (Zetter, 2016). And it was only a year ago that WannaCry halted the Dutch harbor of Rotterdam (Verschuren, 2017). The Ministry of Justice and Security states in their National Security Agenda of 2018 that cybersecurity is of vital importance for National Security as well as economic advancement (Ministry of Justice and Security, 2018). In order to defend society of the advanced threats of tomorrow it is of vital essence to improve governmental cooperation. In this thesis there will be given a small insight in governmental cooperation on cybersecurity. This can contribute to the strengthening of governmental cooperation and might contribute to protecting society. Inside such cybersecurity networks trust is important, as it provides the grounds to share information. The more trust is present, the better and more sensitive information is shared amongst partner organizations.

1.2. Scientific discussion

A substantial amount of literature exists on the topic of public networks. Governmental steering changed from hierarchal structures to a form of nodal governance or network governance. Kenis and Provan describe networks as: *'Networks, consisting of two or more organizations that consciously agree to coordinate and collaborate with one another, are used to deliver services, address problems and opportunities, transmit information, innovate and acquire needed resources'* (Kenis & Provan, 2006: p. 227). Kenis and Provan argue that networks enhance organizations in their daily operations.

Security networks are often also a form of a public network, because governmental actors work together to deliver complex products such as security. Dupont and Gill have identified the different types of security networks that could be formed. Security networks can be observed on multiple levels; local, national and transnational (Dupont, 2004). Whelan argues that networks can be observed either through structural or relational aspects. Structural aspects include the way a network is governed. Most public administrative research is focused on structural aspects of networks (Whelan, 2015 & Provan & Kenis, 2007). In networks exist also relational aspects which includes the relationship between different organizations in networks and how they behave in daily operations (Whelan, 2015: p. 3). Studying security networks is difficult because such networks are often closed for others. In the Netherlands the different departments of government collaborate with the National Cyber Security Center through the so-called Joint-Security Operation Centers network. The goal of this network is to intensify operational contacts, create a pool of security experts, share incident information and buy security products together (Joint-SOC, 2017). This is done to improve efficiency and effectivity in Security Operation Centers, as stated in the policy of the ministry of Interior and Kingdom Relations (Dutch Central Government, 2016). This ambition is in line with the problems uncovered by the Algemene Rekenkamer. The Algemene Rekenkamer stated that the only ministry that is in control of their ICT is the ministry of Social Works and that many other ministries need to improve their ICT organization (Financieel Dagblad, 2018). According to this research, nine ministries did not have their ICT-defenses in order. In the report is stated that the Tax and Administration Office needs urgent improvement (Hofs, 2017). Therefore, the Joint-SOC network proves as an interesting network to research, as it is situated amidst this field of different interests and would possibly require trust to function properly.

In current security network research there is an emphasis on structural aspects of networks. Whelan argues that more research needs to be conducted on the relational aspects of security networks. In the relational aspects of networks is an important factor: Trust. Trust is often dubbed as the oil that makes networks run smoothly. Whelan, amongst other scholars (Klijn, Edelenbos & Steijn, 2010) puts forth that there has not been conducted enough research on the relational aspects of security networks (Whelan, 2015: p. 43-47).

Trust is an interesting part of public administrative networks. Klijn et al argue that trust is vital in public networks, because trust can be used as a coordinating mechanism. Trust is important in public networks, and in security networks, because the level of uncertainty is high and working on contractual basis is often impossible (Klijn, Edelenbos & Steijn, 2010: p. 2). In addition to the statements by Klijn et al, Provan and Kenis (2008) state that trust is an essential factor in network effectiveness. How can trust be described and used in research? Trust is a concept that is often researched in business administration, economics and political science (Klijn et al, 2010 & Maloy, 2009: p.494). Trust itself serves different meanings, it could be described as a ‘*state of feeling*’, a certain idea that the other will treat you as a partner or even as a ‘*social good*’ (Maloy, 2009: p. 495).

1.3. Research question

This research will look into the security networks in the Dutch public domain of cybersecurity. In cybersecurity it will primarily focus on the relational aspects of building such networks. The following research question will be answered in this project:

In what way does trust develop in the Dutch public Joint-SOC security network?

To answer the research question three sub-questions, need to be answered:

1. What are security networks?
2. What is trust?
3. How does trust develop inside the Joint-SOC network and what can we learn from that?

The goal of this research

This research will provide insights in the way trust develops inside, mainly, public security networks. This research will fill a void that exists about trust in security networks in current security research. Both Whelan as well as Kleijn et al state that more research should be conducted on this topic, both from a public administrative view as a security perception, because there is more to discover about the way trust develops inside networks.

1.4. Guidance

The second chapter will include a theoretical framework that will explore the concept of trust and introduce the core components that will be part of this research. The third chapter describes the procedures and methods used in this research. In the fourth chapter, I will present the principal findings of this research, followed by a conclusion on the analysis. Finally, there will be a short discussion about this current research and propositions for further research on his topic.

2.0. Theoretical framework

In this theoretical chapter several important concepts will be discussed. Concepts that need to be explained to grasp the theoretical implications in this research. The first concept that will be elaborated is security networks and in what way they are governed. The notion or concept of ‘*a network*’, however, is quite convoluted – similar to public-private partnerships – and is approached in three different ways (Whelan, 2012). Firstly, the term network can be used as a metaphor to refer to relationships between actors (phrases such as ‘networked society’). Secondly, networks can be a method of analysis. In this approach the network is researched to see in what way the set of actors are connected. As such, the unit of observation are the actors, or nodes, in a particular network and their respective relationships. This is mostly done on a micro-level. Important factors are for example the density and centrality of the specific actor in the network. This approach is also called the “network analytical approach” (Provan & Kenis, 2008, p. 232). Thirdly, networks can be used to refer to a unit of analysis. In this approach the network is analyzed as a particular form of organization. Or the “*network as a form of governance approach*” (Provan & Kenis, 2008, p. 232). These last two approaches are most relevant to this study, as they could be used to characterize and assess the performance of networks.

The second concept that will be explained is trust. Trust is a broad concept that is applicable to many studies. Therefore, the following question will be answered in the first part of the second chapter of this theoretical framework: ‘*What is trust and how does it fit in the research agenda in social sciences?*’ In the second part of the trust chapter, this theoretical framework will analyze theories and models about trust in order to create an analytical framework at the end of this chapter.

2.1. Security network governance

2.1.1. Security networks

As portrayed in the introduction of this thesis the practice of security is diverse. It ranges from local crime prevention to combating terrorism. In public administration such themes will be regarded as '*wicked problems*'. Wicked problems cannot be divided into neat arrangements that can be solved with clear cut measures. In order to tackle these '*wicked security problems*' security organizations have to work together. The collaboration between such security organizations are called '*security networks*' (Whelan, 2017: p. 2). Dupont defines security networks as: '*A set of institutional, organizational, communal or individual agents or nodes that are interconnected to authorize and/or provide security to the benefit of internal or external stakeholders* (Dupont, 2004: p. 78).

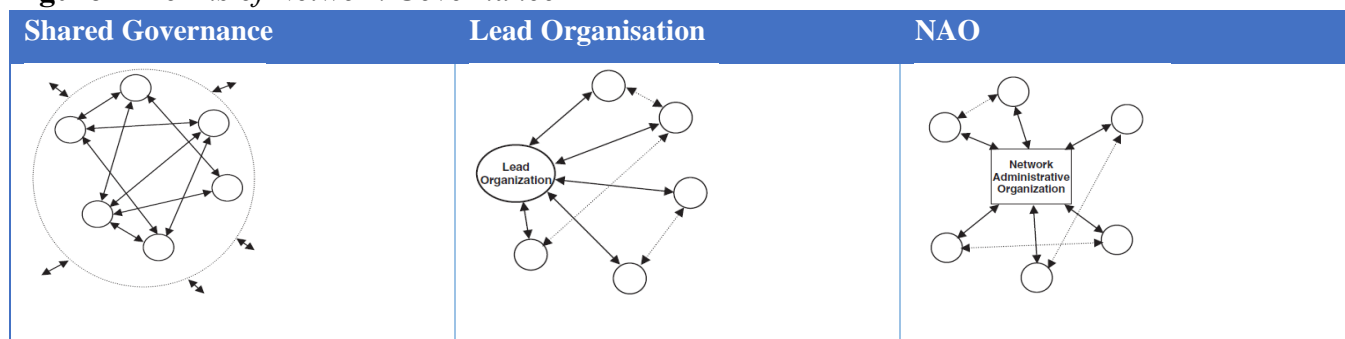
Networks are used to study the way certain actors are networked or focusses on the form of the network itself, in which the network is a unit of analysis. Networks consist of several actors that are linked with one another. Actors in a network can be individuals, organizations or groups. Networks are used as a substitute for hierarchical governance and networks could provide in the flexibility of markets. Networks consists of two properties, structural- and relational properties. Structural properties include topics such as the design of the network, network size and the goal consensus between network members. Relational aspects of networks are based on the relationship between the actors in a network. Relational aspects can be divided into formal- and informal relationships. Especially informal relationships are deemed of great benefit to network performance (Whelan, 2017: p. 3).

Dupont argues that there are four types of security networks; local security networks, institutional security networks, international security networks and virtual security networks. Local security networks are networks where security actors combine resources to tackle local security problems. Institutional security networks are networks formed by several institutions, mostly governmental agencies and the goal of these networks is to optimize efficiency. International security networks depend on international collaboration. Virtual networks are build using innovative technologies (Dupont, 2004: p. 79-82).

2.1.2. Network governance

Whelan states that the relational aspects of security networks need more attention in current research. However, it is necessary to also consider the structural components of such networks, as they play an important role in the operations of such networks. Provan and Kenis (2008), in their theory of network governance, view networks as a variable and analyze different governance forms and the requirements for effectiveness of each form. Additionally, they argue that the management of, and management inside the network plays a huge role in handling the inherent tensions of each network governance form. In their view networks are groups: *“Consisting of three or more legally autonomous organizations that work together to achieve not only their own goals but also a collective goal”* (Provan & Kenis, 2008, p. 231). They define network effectiveness as: *“The attainment of positive network-level outcomes that could not normally be achieved by individual organizational participants acting independently”* (Provan & Kenis, 2008, p. 230). Provan and Kenis (2008) state that network governance forms can also be categorized along two dimensions. This is the extent to which network governance is brokered. One the one hand, networks may be governed solely by the actors that comprise that network. Actors in a network would interact with every other actor in a network to make decisions; resulting in a dense and highly decentralized form. On the other hand, networks may be deeply brokered. In this case the network is governed by one lead actor and the individual actors in the network do not interact as much with each other. In between those extremes is a form of network governance where a single actor controls key governance activities but leaves the rest up to the other actors that comprise the network. An alternate way of this structure is that those key governance activities are divided up to a subset of actors within the network (Provan & Kenis, 2008). A second dimension regarding governance is to what extent a brokered network is governed by internal or external actors. An externally governed network may be voluntary set up or may have been mandated by the government or another party (Provan & Kenis, 2008).

Figure 1. *Forms of Network Governance*



(Provan & Kenis, 2009: p. 447).

This observation leads to the typology of three different network governance forms: shared governance networks, lead organization-governed networks, and Network Administrative Organization (the NAO model) (see figure 1). Each form of governance has its own particular characteristics, structure, and strengths and weaknesses. Additionally, each governance form is faced with particular managerial tensions. These tensions are efficiency vs. inclusiveness, internal vs. external legitimacy, and flexibility vs. stability. How these tensions are managed is critical to network effectiveness, because the network forms inherently lean to a certain side of each tension (Provan & Kenis, 2008).

Shared governance network

A shared governance network is characterized by the fact that it is governed by the members of the network themselves, without any control by a separate entity. The actors that comprise the network make all the decisions themselves and manage network-level activities. While there is no specific actor assigned with administration, these kinds of activities can be designated to a subset of actors within the network. The strengths of this kind of network governance lies in the incorporation and involvement of all participating actors and its speed and adaptability to the needs of the network. Its weakness is its comparative inefficiency. It is a model that is best suited to a network that is comprised of a few number of members that can have face-to-face contacts. Accordingly, shared governance networks favor inclusion, internal legitimacy, and flexibility (Provan & Kenis, 2008; Kenis & Provan, 2009).

Lead organization network

A lead organization-networked governance model is characterized by the fact that all members in the network share at least a common interest in the network, but network-level activities and decisions are made by one actor. This lead actor also takes up the role of administrator and facilitator of the needs of the network. The strengths of this network are its efficiency and legitimacy provided by the one lead actor (in the case it is an organization with ‘gravity’). This is due to the fact that administrative duties are not divided unto all members of the network. The weakness of this network governance model is the fact that the needs and goals of the lead actor may not necessarily be aligned to the needs and goals of the participating actors. Additionally, because the lead actor takes up many of the network-level activities, network members may lose interest and instead only focus on their

own self-interest. The lead organization-networked governance model can be the result of a bottom-up process, but can also have been mandated by another party, such as the government. The tensions of the lead organization-networked governance form favor efficiency, external legitimacy, and stability (Provan & Kenis, 2008; Kenis & Provan, 2009).

Network administrative organization

A Network Administrative Organization (NAO) is a network governance form where a separate administrative entity, such as a governmental or a non-profit organization, is set up to function as a coordinator and manager for network-level activities. However, unlike the case in the lead actor governance model, the administrative entity does not have its own goals or needs. This administrative entity can be set up informally and formally, depending on the need for external or internal legitimacy. The strengths of this model are its legitimacy, tenability and, although to a lesser extent compared to shared governance, its efficiency. Its weaknesses are the fact that members of the network may become too reliant on the administrative entity and could adopt its bureaucratic tendencies. The tensions of the NAO governance form are a bit more balanced but lean more in the favor of efficiency, addresses both sides of legitimacy but in a consecutive method, and favor stability over flexibility (Provan & Kenis, 2008; Kenis & Provan, 2009). Apart from the categorization of network governance structures, an important part of Provan and Kenis' theory (2008) is about the factors of success for networks. Or in other words, how the network can attain positive network-level outcomes (which was already defined as 'the effectiveness of networks'). They state a successful adoption of one of these network governance forms is based on a number of structural and relational key factors.

Success factors governance models

The four key factors for successful adaptation of a certain form of network governance mode are defined by Provan and Kenis (2008) as: (1) trust, (2) number of participants, (3) goal consensus, and (4) network-level competencies. Whereas the key factors number of participants, goal consensus and network level competencies are important, the factor of trust warrants our special attention. Provan and Kenis (2008) state that as trust becomes less densely distributed throughout the network, as the number of participants gets larger, as network goal consensus declines, and as the need for network-level competencies increases, brokered forms of network governance, like lead organization and

NAO are likely to become more effective than shared-governance networks (Provan and Kenis, 2008: p237). The next chapter will explain why trust is an interesting object to research within network research as stated by Provan and Kenis (2008).

2.2. Trust

2.2.1. *An introduction to trust research*

The concept of trust itself is interesting because it is covered in a wide array of sciences. Multiple authors argue that trust is a multi-disciplinary research topic. Trust can be related to different topics such as business innovation, organizational performance and inter-organizational relationships. A few applauded works in trust research are for instance (Fukuyama, 1995) on the basis of trust, Lane and Bachmann on the role of trust in organizational relationships (Lane & Bachmann, 1998) and Kramer and Tyler on trust in organizations (Kramer & Tyler, 1995). Trust research is inherently a study area focused on the individual according to Seppänen. Seppänen calls this ‘*basic trust*’ where for instance relationships between a parent and its children are researched. Trust in such research is about the goodwill of the trusted person. Later also the philosophy school started to investigate the concept of trust. The philosophy school argues that trust is a non-conscious state (Seppänen, 2008: p. 19-21). At a certain moment the scope of research shifted towards organizations and group level. This group level of trust will be examined in this part of the theoretical framework. What theories exist about the building and sustainability of trust?

2.2.2. *Trust inside (security) networks*

The first paragraph of this theoretical inquiry about trust discovers the basic principles of trust. Nooteboom states that trust research itself is confusing and therefore it needs to be distilled what level of trust is discussed; personal, organizational or institutional (Nooteboom, 2006: p. 261). These following paragraphs will look into the usage of trust within networks, inter-organizational relationships or ‘*security networks*’. It should be noted that there is a difference in interpersonal trust, the trust a person has in the counterpart of another organization and inter-organizational trust. Inter-organizational trust is mostly focused on the systems and processes involved in networks (Whelan, 2015: p. 21). Inter-organizational trust is beneficial to network performance according to Klijn and Edelenbos (2007). They pose four arguments why high levels of trust are useful in governance networks. First, high levels of trust could reduce the transaction costs in networks. Second trust could persuade members of the network to invest their resources into the network. Third it is stated in the literature that trust increases knowledge and information-sharing. The fourth argument is that trust leads to more innovation in a network. The research by Klijn and Edelenbos confirmed that these arguments lead to increased network performance (Klijn & Edelenbos, 2010: p. 15). Whelan adds an interesting dimension in this discussion by stating that in security networks interpersonal trust is

more important than inter-organizational trust. This statement is in contradiction with the works of many scholars (Whelan, 2015: p. 42). Whelan states that even though there is a strong institutional trust base, interpersonal and impersonal trust are very important, as stressed by his respondents (Whelan, 2015: p. 46). Is trust then the answer for new coordinating mechanisms that stimulate innovative decision-making? According to most literature and Edelenbos and Klijn it is. Trust as a coordination principle seems promising in settings where the relations between ‘partners’ is horizontal. Without rules and hierarchy another form of steering is needed, and trust can fill that gap. As Edelenbos and Klijn argue: ‘*We cannot organize all uncertainties in life through hierarchical power, direct surveillance or detailed contracts*’ (Edelenbos & Klijn, 2007: p. 27). Goldsmith and Eggers take it one step further and state that trust is: ‘*The bedrock of collaboration. Without it (trust), people will not collaborate or share knowledge*’ (Goldsmith & Eggers, 2004: p. 119). This research will focus on the perceived trustworthiness. The perceived trustworthiness consists of three variables; perceived ability, perceived benevolence and perceived integrity.

2.2.3. *What is trust?*

If trust is a subject in many different research areas, it could also carry different meanings. Lane and Bachman (1998) state that trust is an expectation. Fukuyama argues that trust is the cement of society (1995). Other scholars argue that trust itself is a ‘*container concept*’ that is not different from rules or norms that form society (Edelenbos & Klijn, 2007: p. 29). Edelenbos and Klijn have observed three distinctive properties of trust:

- Trust is inherent to vulnerability. A person trusts the other to avoid opportunistic behavior against him and therefore is vulnerable.
- Trust is linked with risk. In situations with high risk it is argued that trust is necessary for any cooperation.
- Trust comes with expectations. *Trust reduces unpredictability, complexity, and ambiguity in interaction because one can anticipate (some of) the behavior of the other actor* (Edelenbos & Klijn, 2007: p. 29).

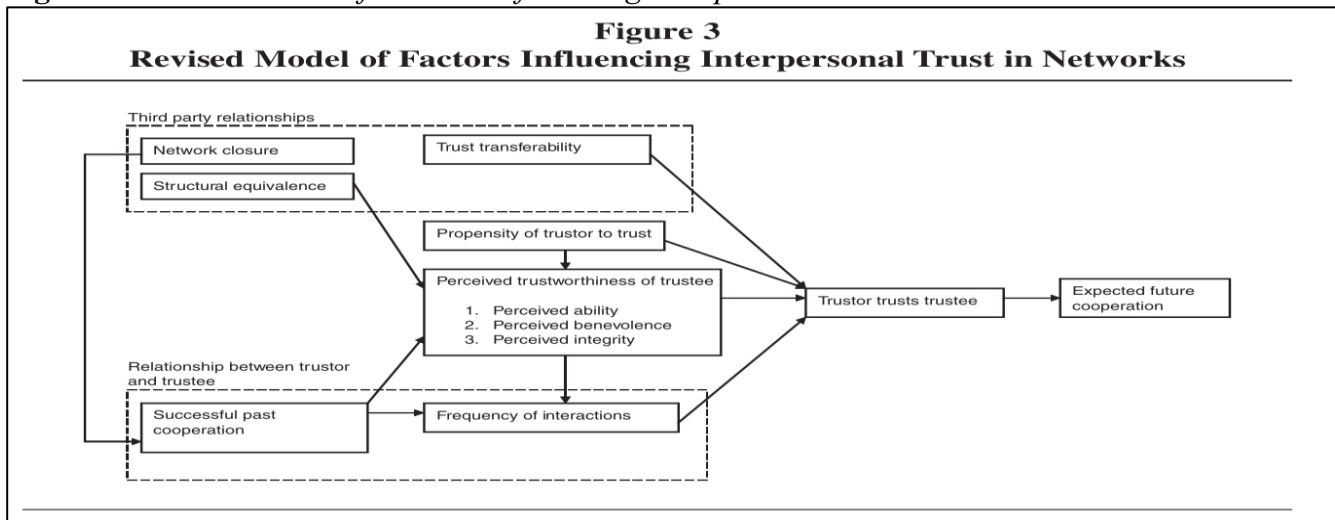
Earlier stated properties are part of trust. It is useful to come with a clear definition of trust as part of this research. With the earlier properties in mind Edelenbos and Klijn created a definition on trust and it goes as follows: ‘*A stable positive expectation that actor A has (or predicts he has) of the intentions and motives of actor B in refraining from opportunistic behavior, even if the opportunity*

arises (Klijn et al, 2010: p. 4). The literature argues that trust therefore facilitates in taking risky decisions. Second characteristic of trust is that there is a need for interdependence. Rousseau argues that trust will only be fulfilled when one party is dependent on another party (Rousseau, 1995: p. 395). It is therefore important to remark that trust is not the equal to cooperation. Mayer argues that cooperation does not necessarily include risk and therefore is not the same as trust (Mayer, 1995: p. 712). Without trust it is said that cooperation is unlikely to occur (Klijn et al, 2010: p. 4). While Klijn and Edelenbos, and with them many other scholars for instance Gargiulo & Ertug, argue that trust is a beneficial control mechanism, others debate that too much trust can also have potential drawback effects (Gargiulo & Ertug, 2006: p. 173-174). Van de Ven and Smith Ring their views are in line with the work of Klijn and Edelenbos and argue that the core components of trust are: *'Willingness to accept vulnerability, positive expectations regarding the intentions or actions of others'* (Van de Ven & Smith Ring, 2006: p. 147). Whelan debates that trust could best be described according to Rousseau's definition: *'A psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another'* (Whelan, 2015: p. 20). Whelan argues that this definition of trust requires the presence of risk and interdependence. Trust could be described as a rational choice or a relational approach (Whelan, 2015: p. 20).

2.2.4. The elements of trust

The previous chapter consists of a digest of trust research. From this literature analysis two characteristics of trust are observed; *risk and interdependence*. The question, what is trust? still stands after the previous chapter. The following part of this thesis will describe the model on trust created by Lambright, Mischen & Laramée which is the key focus point of this research. This model describes three main components of trust: *Ability, benevolence and integrity*. The model created by Lambright et al is portrayed below.

Figure 3. Revised Model of Factors Influencing Interpersonal Trust in Networks.



(Lambright et al, 2010: p. 78).

Lambright et al created a model whereby: ‘*The trustor is putting herself in a position of vulnerability and taking a risk by placing trust in the trustee* (Lambright et al, 2010: p. 66). In this model the trustor is the person or organization that puts their trust into the trustee, a person or another organization that receives the trust from the trustor. In the next section the model of Lambright will be further explained.

2.2.5. The three core components of trust

Lambright et al state, (2010) that trust research is an important part of different areas of research, such as management studies and psychology. However, trust research in public administration is limited, therefore they created the model pictured above, stating that it is a cross-disciplinary model useful for researching trust-building in networks (Lambright et al, 2010: p. 66).

Lambright et al (2010) argue that there are two main factors that contribute to the trustor trusting the trustee. First there is a certain propensity of a trustor to trust, the propensity to trust is the attitude a

trustor has towards a trustee, that could be of positive or negative nature (Lambright et al, 2010: p. 78). Second there is a certain perceived trustworthiness of the trustee. The model by Lambright et al loans three components from the distinguished work of Mayer. Mayer argues that authors interpret trustworthiness in different ways. Earlier is stated that trust is necessary when risky situations occur, and that trust is important because it is necessary in cases where interdependence exists. Mayer argues that these deliberations about trust make it difficult to research the subject and describes trust as follows: *‘The willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that party* (Mayer, 1995: p. 712). Mayer makes an important distinction and states that trust not necessarily means taking risk but is about the willingness to take risk.

Therefore, Mayer has examined the literature of trustworthiness and derived three main characteristics; Ability, benevolence and integrity. Ability, according to Mayer is: *‘That group of skills, competencies and characteristics that enable a party to have influence within some specific domain* (Mayer, 1995: p. 717). Domains are important in considering one’s ability. Someone could be trusted for doing technical analyses, but not trusted with communicating with important network-partners (Mayer, 1995: p. 717-718). In a Yale study *‘perceived expertise’* was an important characteristic of the trustee. In most research abilities are described in a rather specific notion. Therefore, Mayer uses the construct of ability in a: *‘The task- and situation-specific nature of the construct* (Mayer, 1995: p. 718).

Benevolence is described as: *‘The extent to which a trustee is believed to want to do good to the trustor, aside from an egocentric profit motive’* (Mayer, 1995: p. 718). Benevolence points out that there must be an attachment between a trustor and the trustee. A good example of benevolence is the relationship between a mentor and its student, whereby the mentor wants to teach its student out of goodwill rather than out of self-profit. The main focus in benevolence in trust research is on these kinds of relationships. However, benevolence is more than goodwill and also more than the willingness to lie. According to Mayer benevolence is about the intentions and motives of a trustee. Intentions and motives also go beyond the intentions and motives of the trustee towards the trustor, such as the profit motive of the trustee in general (Mayer, 1995: p. 719). Also

The third construct of trustworthiness is integrity. Integrity is described by Mayer as: *'The trustor's perception that the trustee adheres to a set of principles that the trustor finds acceptable* (Mayer, 1995: p. 719). There could be different reasons why the trustor finds certain principles acceptable such as: *'Consistency of the party's past actions, credible communications about the trustee from other parties, belief that the trustee has a strong sense of justice, and the extent to which the party's actions are congruent with his or her words* (Mayer, 1995: p. 719). However, research showed that for researching trust it is more important to know whether the perceived level of integrity is high or low than to know why that perception is formed. In the literature, the term integrity tends to be used to refer to consistency, fairness and openness. Mayer argues that integrity is an interplay of above characteristics, whereby consistency alone is not enough to assign integrity to another person (Mayer, 1995: p. 720).

2.3 Building trust

The previous chapter displayed the model by Lambright et al and distinguished the different components of trust. These components are essential in the way trust is built inside (security) networks. However, the components of trust itself, ability, benevolence and integrity do not necessarily mean that trust is built. This chapter will draw out a small portion of the literature on trust building and apply it to the model of Lambright et al.

The last section has demonstrated that trustworthiness is about capabilities, benevolence and integrity. It is now necessary to talk about the way Mayer sees the three constructs related to each other. Mayer argues that the three components are interdependent and separable, but not unrelated. Mayer writes that if all three components are ranked as high, a person will probably be regarded as trustworthy. He argues that trustworthiness should be seen as a continuum rather than a matter of being trustworthy or untrustworthy. In addition to that Mayer describes situations where being integer, capable or benevolent alone is not enough to be trusted. For instance, when a manager's integrity is doubted, will he be trusted by his employee's? (Mayer, 1995: p. 721). Mayer argues that whether the manager in this situation is trusted is based on the propensity to trust by the employee. Further investigation is needed in the way these three principles play a role in trustworthiness. Mayer poses an important question: *'How low can some of the three factors be before the employee would not trust the manager? In what situations is each of the three factors most sensitive or critical?* (Mayer, 1995: p. 722). Mayer argues that the propensity to trust and the perceived trustworthiness

generate a certain level of trust. However, it does not mean that if all characteristics of trustworthiness are ranked low or medium there is a low level of trust, it depends on the context in which the interaction takes place and the propensity of both the trustee as well as the trustor to trust (Mayer, 1995: p. 720-722).

Lambright et al argue that if one tries to conduct research on the concept of trust it is not enough to focus on the dyadic relationships inside an existing network. Other factors to consider are the third-party relationships and the relationship between the trustor and the trustee (Lambright et al, 2010: p. 79). Third party influences are made up of three components; network closure, structural equivalence and trust transferability.

- Network closure is: *'The number of third parties who interact with both the trustor and trustee'* (Lambright et al, 2010: p. 68). When there is only a dyadic relationship between the trustor and the trustee, trust will not be spread among others. In a network where there are multiple actors it is possible that third parties derive trust from the successful cooperation of two other parties in the network.

- Structural equivalence is about the way the trustor and the trustee are similarly positioned inside a network and think the same about the other participants. The trustor and the trustee see each other as part of a subgroup and feel that both parties are interdependent. This could also lead to subgroups which does not benefit overall levels of trust inside networks.

- Trust transfer-ability is made up of the amount of parties that trust the trustee and are trusted by the trustor (Lambright et al, 2010: p. 68-69).

The relationship between the trustor and the trustee is important in building trust. These relationships are based on two components; Successful past cooperation and the frequency of interactions. Lambright et al argue that the frequency of interactions has an impact on the development of trust. When two parties interact frequently there is a higher chance of trust development because of the retaliation possibility regarding past cooperation inside the future cooperation. Therefore, Lambright et al argue that the trustor will be more likely to believe the good intentions of the trustee (Lambright et al, 2010: p. 67). These frequent interactions have more impact if both the trustor and the trustee regard them as successful. Therefore, the relationship between the trustor and the trustee also consists of successful past cooperation. If the parties have worked successful in the past they are more likely to interact in the future, developing trust. In addition to successful past cooperation having an impact on the frequency of interactions, Lambright et al conclude that successful past cooperation gives

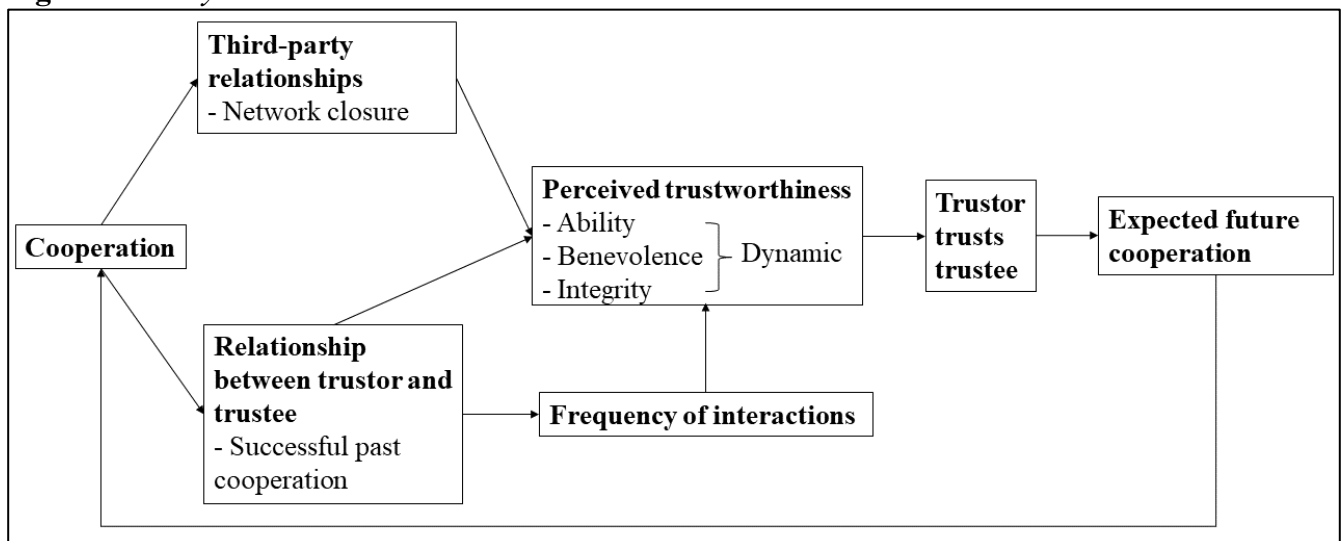
insight in the values and beliefs of the different parties inside a network. Successful past cooperation thus shapes the perceived trustworthiness and, in the end, impacts the trust the parties have in one another.

2.4 A dynamic model for building trust

The previous section described the way the components of trust interact with each other. It also showed that inside inter-organizational collaboration several other constructs influence trust such as third-party relationships and the relationship between the trustor and the trustee. This chapter will alter the model of Lambright et al in order to fit inside the analytical framework of this research.

Vangen and Huxham (2003: p. 12) created a model for building trust inside inter-organizational collaboration. They argue that trust builds in a cyclical manner. In the beginning of the collaboration there is little trust and it develops over time. The model created by Vangen and Huxham (2003) is out of the scope of this research but their idea of trust developing in a cyclical way is adapted in this research. The model by Lambright et al consists of several constructs that influence trust inside networks as described earlier in the theoretical framework. Below is the adapted model by author of this research portrayed. The model that is displayed below also connects with the works of Provan and Kenis (2008, 2009). As noted earlier, Provan and Kenis state that the key-factors of network governance are trust, number of participants, competencies and goal consensus. This mode zooms in on the aspect of trust. The other key factors also play a part in this model, which will be explained later on. This analytical model therefore also provides a deepening of the works of Provan and Kenis (2008) as the works of Mayer (1995) and Lambright et al (2010).

Figure 2. *Analytical model.*



(Lambright et al, 2010: p. 78, altered by author for analytical purposes, 2018).

Cooperation

Networks that consists of multiple organizations exist because different parties *cooperate* with each other. Cooperation is the starting point of this model, otherwise a network would be nonexistent. When building trust two components play an important part in influencing whether someone is perceived trustworthy or not, third party relationships and the relationship between the trustor and the trustee

Relationship between trustor and trustee

In the model above, is built on the ideas of Lambright et al (2010) that the relationship between the trustor and the trustee consists of successful past cooperation and the frequency of those interactions. Lambright et al (2010) argue that successful past cooperation positively influences the perceived trustworthiness of the trustee and the frequency of the interactions between the parties. The frequency of the interactions is both influenced by past successful cooperation as well as the level of perceived trustworthiness on the trustee. It is an important construct as it directly influences whether parties are trusted or not.

Third party relationships

The other factor influencing the building of trust are third party relationships. Whereby network closure means in what way others in the network interact with the parties that participate with each other and structural equivalence is about the way the trustor and trustee are similarly positioned inside the network. Lambright et al also take trust transferability into account, that is left out in this model because of the limit amount of parties that operate in the network observed in this research and because it is not tightly linked to the main component of this research: Perceived trustworthiness and its main components abilities, benevolence and integrity. Network closure has a strong link with successful cooperation, it is an influence on whether organizations work successfully together. This also connects with the works of Provan and Kenis (2008, 2009), as network closure and third-party relationships are about the number of participants in the network. Provan and Kenis argue that as the number of participants grows, the density of trust changes and thus needs another form of network governance (Provan & Kenis, 2008: p. 237). The second key factor is goal consensus, which could be aligned with the works of Lambright et al, as they state that network closure is also about having the same view (goals) inside the network (Lambright et al, 2010).

Perceived trustworthiness, trust and future cooperation

The most important part of this analytical model is the perceived trustworthiness of the other parties. The perceived trustworthiness has been described earlier in this thesis and consists of the core components of trust: ability, benevolence and integrity. According to this model, high levels of perceived trustworthiness in combination with frequent interaction lead to the trustor trusting the trustee. In this model the propensity of a trustor to trust is omitted. This is because of its deep psychological character which is out of scope in this research, as it focuses on inter-organizational collaboration and not on deep psychology related material. The hypothesis in this research is that trust is generated through core components; Ability, benevolence and integrity. And that trust in the other leads to future cooperation, therefore restarting at the beginning of this model with cooperation. If the cooperation is successful it will have a positive impact on perceived trustworthiness. In this model the perceived trustworthiness is a two-sided dynamical concept. On the one hand because between the three main components there can be interplay, but also because there are external factors that influence whether ones perceived trustworthiness is deemed higher or lower. Additionally, Provan and Kenis argue that the need for network-level competencies depends on the other key factors. Network-level competencies could be part of the abilities necessary for the perceived trustworthiness.

3.0. Methodology

This chapter includes the methodology. In this chapter the used methods are displayed. First, the design of the study will be elaborated. Second, the concept of case-studies and the advantages and disadvantages of case studies method is discussed. Finally, the proposed data-gathering and data-analysis methods will be discussed.

3.1. Case Study design

This research will use a case study design. Case studies are sometimes regarded as the weaker sister in social science, but others point to it as: *'In-depth, qualitative studies of one or a few illustrative cases'* (Berg, 2009: p. 317). The case study is according to Berg an: *'Approach capable of examining simple or complex phenomenon, with units of analysis varying from single individuals to large corporations and businesses; it entails using a variety of lines of cation in its data-gathering segments and can meaningfully make use of and contribute to the application of theory'* (Berg, 2009: p. 317-318). Case studies are also a way to discover and can be a breeding ground for insights and hypotheses (Berg, 2009: p. 329). Case-studies are also very adaptive, which could be useful in this research. It is easier than with other methods to adapt to the situation. Although case studies prove to be very effective in looking at several smaller cases, they also pose some disadvantages. It could for instance be hard for the researcher to gain access to the data, because you have to ask hospitals their weaknesses that they would not throw out on the street so easily. Also, in case studies the external validity remains low. Case-studies are hard to duplicate and have a low generality. Yin argues that it is wise to use case study designs when the stated question is a 'how' question. Questions that are posed with a 'how' statement and questions that involve contemporary situations deserve a case study design. A case study, according to Yin: *'Investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident'* (Yin, 2003: p. 9-13). In this research a phenomenon, trust, is researched in a contemporary setting given a 'how' question.

This research uses a case study design as methodology. The unit of analysis in this case study will be security networks. The unit of observation is the Joint-SOC network. As indicated before, the Joint-SOC network is a security network developed to facilitate better cooperation between *'security operations centers'* (SOC) in the Dutch central government. This network is chosen because it is public security network. In the literature is stated that not enough research has been conducted on

security networks in relation to trust. This group also has been chosen because of its interesting dynamics and dependence of trust on its own performance. This network is also chosen because the researcher is able access this security network and its members. Gaining access to security networks is not easy and therefore this research adds value to the scientific debate about trust. It took this researcher almost a year to gain access to the Joint-SOC network.

3.2. Data collection methods

This study is a single case-study and will work with interviews, documents and a desk study to ensure triangulation of data. In this chapter will be elaborated why these methods are chosen and how they fit in this research.

3.2.1. Desk study

The first step of analysis in this research is performing a desk study. During this desk study considerable literature on trust will be analyzed. Also, there will be research conducted on security networks in general. There are two reasons why this is important for this research. First, it is important because it ensures the researcher is acquainted with the concept of trust. Second it is important to be acquainted with security networks because it is the focus point in this research. The desk study also provides more information on security operation centers (SOC'S). This is both interesting because the network consists of SOC's but also because SOC's are a new phenomenon which are vital in securing the digital infrastructure.

3.2.2. Interviews

Verschuren & Doorewaard argue that case-studies are an intensive study combining observations, interviewing and document analysis (Verschuren & Doorewaard, 2007: p. 163). Interviews are critical in uncovering what respondents find on certain topics. The main focus point of this research is trust inside security networks. Observations about trust could also be shared through surveys, however, trust inside security networks is such a sensitive and confidential topic that this research uses interviews, as they generate more information useful for answering the research question. A downside of using interviews would be that it costs a lot of time to prepare and execute the interviews necessary. However, Verschuren & Doorewaard argue that if one needs to research underlying assumptions or difficult topics interviews provide an excellent starting point (Verschuren &

Doorewaard, 2007: p. 242). This research adds to the existing literature on trust because it's starting point is a qualitative research. Most research on trust consists of quantitative methods. For this research I will interview people that represent the different organizations of the Joint-SOC network. This will include people from the following organizations: SSC-ICT, the Tax and Customs Administration, NCSC and Rijkswaterstaat. This research will only focus on the operational key figures inside this network. This is due to time constraints and the limitations of a master's research but also due to the fact that interviewing these people is almost not achievable. The respondents I approached already stated that normally they do not cooperate with any interview or research due to time constraints and the large number of researchers apprehending them. Interviews are an important tool when researching trust. As trust is often used in personal networks, which are often not written down in formal arrangements. When approaching respondents, a problem that occurred was their available time, especially for the governance board. The interview schedule of this research was planned around June until August, this is proven to be an unfavorable time as most people are on holiday. The relatively few number of respondents is handled by putting extra attention to the literature review and document analysis.

3.2.3. Document analysis

The second form of analysis would be a document analysis. The Joint-SOC network is formed around 2016 and aids to improve cooperation between several 'security operation centers' (SOC) in the Dutch government. Since its foundation the network has been well documented. Interesting information can be found in these documents about the relationships between different organizations in the network. These documents also portray the structural characteristics of the network, even though the structural aspects are not main focus point of this research it is interesting to consider when analyzing all research data. The documents that will be studied are statutory documents, project statements and the 'Joint-SOC best practice guide' in which the cooperation is explained more broadly. In this analysis will be looked at points that could provide evidence for trusting each other during this process, which might add to the data gathered from the interviews. Access to these documents is usually limited to governmental employee's. Therefore, the documents included in this research are limited and the content can only be looked into with permission from the owners of the document.

3.3. Data exploitation and assessment

Interviews and document analysis are the methods used in this thesis. In this chapter of the methodology the conceptual model will be divided into constructs that are operationalized. After the most important concepts are operationalized follows the interview protocol and the coding scheme.

3.3.1. Operationalization

In this chapter several key concepts will be operationalized. First the propensity to trust will be operationalized. Then will trustworthiness be operationalized. Lastly ‘trusting’ will be operationalized

Concept	Indicators	Subindicators	Specifications
Truster: The network member that puts his trust in a trustee			
Trustee: A network member that is trusted by another network member			
Cooperation			
Network closure	To what extent does successful cooperation influence the opinion of others inside the network.	Do all parties follow the cooperation of the others carefully?	
Structural equivalence	To what extent do the parties in the network feel they share the same view on the network.		
Successful cooperation past	Which parties have ‘successfully’ worked together to achieve a common goal in the past	Successful cooperation in this researched is interpreted as the achievement of a common goal, where it is up to the participating organizations to decide whether the outcome has been satisfactory.	
Frequency of interactions	An estimation of the interactions the different parties have on a regular basis	An estimation of the communication between parties. In this research is looked at the physical meeting of the	

		parties. Whereby frequent interactions are described as between 1 or 2 meetings per week. And non-frequent interactions are around 1 or 2 meetings per month, or per two months.	
Perceived trustworthiness: When an individual believes that the other party can be trusted. This can be measured by checking how the trustor perceives the trustee(s) on his or her ability, benevolence and integrity inside the network.	The trustor perceives the trustee as someone with abilities.	The trustor believes that the trustee has skills that have an influence inside the network	Skills considered are: technical skills, relational skills, communicational skills.
		The trustor believes that the trustee has characteristics that have an influence inside the network	Characteristics are reliability and honesty.
	The trustor perceives the trustee as benevolent.	The trustor believes the trustee will handle in the interest of both parties	
		The trustor and trustee have an attachment towards each other	
	The trustor perceives the trustee as integer.	The trustor believes that the trustee adheres to the same principles	
		The trustor finds that the trustee is consistent in his or her actions	
The trustor believes that the trustee is fair in his or her actions.			
Trustor trusting a trustee	The trustor states that he trusts a trustee.	There are high levels of earlier described indicators; ability, benevolence and integrity. And there is a positive propensity to trust.	

		There are frequent interactions between the trustor and the trustee	
Expected future cooperation	Both the trustee and the trustor acknowledge that they will continue to work together and continue their relationship in the future (or start new projects).		

3.4. Interview protocol

This research will use a semi-structured interview. Therefore, there will be an interview protocol consisting of both open and closed questions. Inspiration for this interview protocol is taken from Colquitt et al who measured the same constructs of trust (Colquitt, Scott & LePine, 2007: p. 914).

Protocol:

1. *What is your name and function inside your own organization?*
2. *What would you consider as your function inside the network?*
3. *How would you describe the Joint-SOC network?*
4. *How many interactions do you have with the network?*
5. *What drives you to participate in this network?*
6. *To what extent do you think that trusting each other is necessary in security networks?*
7. *Do you think party X, Y, Z is very capable to perform their actions in this network?*
8. *Do you think party X, Y, Z is known to be successful in their actions in this network?*
9. *Do you think party X, Y, Z are concerned with your welfare?*
10. *Do you think party X, Y, Z would act in your best interest?*
11. *Do you think party X, Y, Z has a strong sense of justice?*
12. *Do you think party X, Y, Z is consistent in his or her actions?*
13. *Could you state with which partners you would like to cooperate in the future?*
14. *To what extent are you satisfied with the operations of the Joint-SOC network?*
15. *Could you indicate with which parties your organization had successful past cooperation?*
16. *In what way does successful cooperation change the opinion of the other network members?*

3.5 Coding scheme

To interpret the answers given during the interview, a coding scheme will be used. The table below consists of the coding scheme.

Construct	Codes	Keywords
1.0 Network closure	1.1. Parties mention successful cooperation between other partners	
2.0 Structural equivalence	2.1. Parties have the same view on the network	
	2.2. Parties do not have the same view on the network	
3.0 Successful past cooperation	3.1. Parties indicate at least one successful past cooperation	
	3.2. Parties do not mention successful past cooperation	
4.0 Frequency of interactions	4.1. The number of meetings the parties have together	
5.0 Perceived Trustworthiness	5.1. Perceived ability	Abilities, Competences Skills, Characteristics
	5.2. Perceived benevolence	Loyalty, openness, caring, receptivity, availability
	5.3. Perceived integrity	Fairness, consistency, promise, fulfillment, reliability, value congruence, discreetness
6.0 Trusting one another	6.1 High levels of perceived trustworthiness and frequent interactions	
	6.2 High levels of perceived trustworthiness and non-frequent interactions	
	6.3 Low levels of perceived trustworthiness and frequent interactions	
	6.4 Low levels of perceived trustworthiness and non-frequent interactions	
7.0 Expected future cooperation	7.1 A statement is made on the continuation of the relationship.	
	7.2 A statement is made on the discontinuity of the relationship.	

8.0 Information about the structural aspects network		
9.0 Other		

3.6. Reliability and validity

This chapter will consist of how the researcher interprets the reliability and validity of this research. The next section will begin with a short introduction on reliability and validity for using these constructs in qualitative research.

3.6.1. Reliability

In quantitative research reliability is about having the opportunity to exactly replicate each research, both of the processes as well as the results. In qualitative research striving to exact replicability is though, if not impossible according to Leung (2015). Stenbacka takes this statement one step further and argues that if a qualitative study is scored by the criterion of reliability, the study itself is no good (Golafshani, 2003: p. 601). Leung proposes argues that some inconsistencies are tolerable in qualitative research and that the main point of reliability in qualitative research is consistency. In this research, consistency is created by following the model portrayed earlier in the analytical chapter. The model is the guideline for this research and should at all times be followed. Leung also states that consistency can be achieved by constantly checking the context and accuracy of the data received with fellow researchers or peers (Leung, 2015). During this research both the authors mentor and other peers contributed to this triangulation, steering back to the correct context. This ensures the reliability, or consistency, of this research.

3.6.2. Validity

Validity is about the appropriateness of the chosen methodology. It can be divided into internal validity and external validity. The internal validity is about how the constructs measure the outcome of the research and to what degree this outcome is warranted. In this research there are models chosen that have a deep theoretical basis, providing a strong starting point. The constructs have been well formed along the extensive literature review and multiple reviews by the supervisor of this study. Benefiting the internal validity is a small focus in a research (Verschuren & Doorewaard, 2007: p.139). In this research the focus point is trust-building. The focus point is as small as possible, given that it is still a subject that is difficult to study. The methodology chosen in this research fits the

research question. As the information is sensitive and rather discussed in person than over e-mail or the telephone, which is also stated by several respondents. Therefore, semi-structured interviews, a document study and desk research are appropriate in the case of the Joint-SOC network. The downside of interviewing members of a security network is that it takes a lot of time to interview them, if possible at all. The external validity is about how the research findings could be generalized or used in other contexts. The external validity in this research is interesting. It could be stated that the external validity is low, because the Joint-SOC network itself is a special network that does not have a lot of similar networks. However, the outcomes of this research could be applied to other networks as it gives an insight in how this research observes trust. This observation can be used in other contexts. In the other context the structural components of the network should be considered.

4.0 Analysis

This part of the thesis will analyze the empirical findings from the document study and the interviews with the respondents. The first chapter of the analysis covers the founding of the network and focuses on the network structural components. The second chapter will look at trust and its main components; Abilities, benevolence and integrity. The third chapter will look at the broader model, its dynamic character and how this influencing building trust.

4.1 Introducing the Joint-SOC network

In 2014 and 2015, The Hague and the Netherlands were the hosts of two important summits. In 2014 the Nuclear Summit took place where 53 countries discussed how nuclear material and weapons could be kept from terrorist's hands (NSS, 2014). In 2015 The Hague hosted the Global Conference on Cyber Space. A conference where leaders, policymakers, experts and other cyber experts: *'Establish internationally agreed 'rules of the road' for behavior in cyberspace and create a more focused and inclusive dialogue between all those with a stake in the internet (governments, civil society and industry) on how to implement them* (GCCS, 2015). International conferences like the GCCS require an immense operation to secure. The Dutch police stated that it was the most complex and extensive operation in their history (Politie Nederland, 2018). Such operations are focused on the physical domain of security but also on the cyberspace. Respondent one, the technical SOC lead of a governmental organization stated that these operations where the main motive to think about governmental cooperation between Security Operation Centers (Respondent one, 2018). The following description describes what a security operation center entails: *'A security operations center (SOC) is a facility that houses an information security team responsible for monitoring and analyzing an organization's security posture on an ongoing basis. The SOC team's goal is to detect, analyze, and respond to Cybersecurity incidents using a combination of technology solutions and a strong set of processes. Security operations centers are typically staffed with security analysts and engineers as well as managers who oversee security operations'* (Lord, 2018). This chapter will shortly describe the Joint-SOC network and will focus on its structural components.

It was around the conferences in 2014 and 2015 that the Tax and Customs Administration, Shared-Service Center ICT and Rijkswaterstaat first worked together on creating a Joint-SOC network. According to the first respondent, a SOC lead at one of these organizations it was a cooperation created by accident. However, it was this first cooperation that proved to be the foundations for a

long-lasting cooperation. Not much later in this time-frame the National Cyber Security Centre joined this collaboration. Since then SSC-ICT, the Tax and Customs Administration, NCSC and Rijkswaterstaat form the core component of the Joint-SOC network (SSC-ICT, 2016). The Joint-SOC could be described as a ‘*Grassroots*’ movement. Whereby it was important that there would be collaboration on all fronts, with as most important target not to re-invent the wheel. Another important aspect of the Joint-SOC network is that there would be no competition. Respondent two, a senior security expert working at the Dutch National Cyber Security Centre stated that there should not be a competition in attracting new staff (Respondent two, 2018). If other parties comply with the accession guidelines of the Joint-SOC they can join the collaboration. Talks are involved with two other parties that are now in the process of joining the Joint-SOC network. The starting point of this network was rather informal.

However, it took a more formal turn later in the collaboration as is described in the Best Practice. In 2016 the minister from the Ministry of the Interior and Kingdom Relations created a new Strategic I-Agenda for the Dutch government. In this I-Agenda strategic decisions regarding topics such as digitizing primary processes, privacy and Cybersecurity are portrayed. The I-Agenda is updated every year. The CIO (Chief Information Officer) creates the I-Agenda in collaboration with the CTO- (Chief Technology Officer) and CIO-councils (Dutch Central Government, 2016, Dutch Central Government, 2008). In the 2016 version of the I-Agenda the Joint-SOC is described as an example of the improvement of operational collaboration, which also has been formalized (Dutch Central Government, 2016: p. 19). Respondent four, a technical SOC lead at a governmental organization, describes how the head of the National Cyber Security Centre, Hans de Vries, presented the Best-Practice signed by all parties to the CIO-Rijk (Respondent 4, 2018). The Joint-SOC network is since then incorporated in the policy of the Ministry of Interior and Kingdom Relations.

The Joint-SOC network consists of a governance board and a more tactical and operational cooperation. The governance board consists of the managers of the respective organizations. The governance board is responsible for the strategy of the Joint-SOC. The governance board in cooperation with the tactical/operational part decides on the future of the cooperation. The governance board also decides on the admission of new members to the network. The other part of Joint-SOC works together to facilitate cooperation and share knowledge and experience. This is done in a two

weekly organized meeting where the state of the present is discussed and where solutions for collective problems are thought out. Important in this collaboration that the person that takes place in these meetings should always be the same representative of the organization involved. This collaboration results in a 'Best Practice', a living document, in which guidelines and helpful tips are portrayed for other governmental SOC's to learn from (Joint-SOC, 2017). The Joint-SOC network could be described as an institutional network as mentioned by Dupont. A security network where several governmental agencies work together to achieve efficiency (Dupont, 2004). Although the Joint-SOC network's ambitions lie beyond efficiency. The ambitions of the Joint-SOC network are to help governmental organizations acquire a SOC with a higher maturity level, benefiting the whole of the Dutch government. As respondent four states: '*I strongly believe in this cooperation, because I think that we only win the cyberwar by working together*' (Respondent four, 2018).

4.1.2. The Joint-SOC Network and its network governance

By the analogy of network governance by Provan and Kenis (2008), the Joint-SOC network could be described as a participant-governed network. This section will explore the structural components of the network and will argue why this network is a participant governed network.

The Joint-SOC Network consists of four parties that share the responsibilities inside the network. This is in line with the argumentation by Provan and Kenis, that shared governance is only possible in networks with limited members. The parties involved are responsible for managing internal relations as managing external relationships, for example the joining of new members to the network. Provan and Kenis (2008) state that in participant-governed networks, there is a need for commitment by all parties in order to achieve the goals of the network. This is also the case in the Joint-SOC network where the ambitions of the network need to be carried out by all respective, in an equal manner, organizations in order to be part of the network (Respondent two, 2018). The National Cyber Security Center has a different role than the other organizations, as it does not have a Security Operation Center. But, this does not change the relation between the other members, as everyone is treated as equal. With the coming of new members, a slight change is seen where new organization the first year are '*aspiring*' members and do not get a seat in the governance board (Respondent four, 2018). The governance board is a form of dealing with external relationships.

It is important to describe the structural components of the network, as it describes why certain aspects of the network are important. The Joint-SOC network could be described as a participant-shared governed network. Provan and Kenis state that when a network is shared: *'It is the collectivity of partners themselves that make all the decisions and manage network activities. Power in the network, at least regarding network-level decisions, is more or less symmetrical, even though there may be differences in organizational size, resource capabilities, and performance'* (Provan & Kenis, 2008: p. 235). This is also the case in the Joint-SOC network, where there are different organizations, all with other sizes, capabilities and performance, that work together to manage the network. In addition to that Provan and Kenis state that: *'In theory, the network acts collectively and no single entity represents the network as a whole'* (Provan & Kenis, 2008: p.235). This is in line with the statement made by respondent four (2018), *'You are not going to find a door with 'Joint-SOC' written on it.*

One of the prerequisites of a participant-shared network to perform well, is a high density of trust in combination with both few participants and a clear goal consensus. The need for a high level of trust is confirmed by the respondents. Therefore, it is interesting to research trust inside a participant-shared governed network.

4.1.3. Sharing information inside Cybersecurity networks

Information sharing is an important component of security networks, especially when intelligence-based organizations are taking part (Whelan, 2015: p. 43). Whelan argues that sharing information is the main activity inside security networks and that *'appropriate'* information sharing is essential to network performance (Whelan, 2015: p. 11). The same holds for cybersecurity networks where sharing information is of vital importance. This is in line with the statements made trust in relation to network performance by Provan and Kenis (2008). All respondents also state that sharing information is the primary reason to build trust. Respondent three, a security network expert working inside the Joint-SOC network, states: *'The better the trust relationship, the more sensitive information can be shared'* (Respondent three, 2018). As one of the respondents argued: *'In collaboration I find it of great importance that I can trust the person I deliver information to'* (Respondent one, 2018). Because sharing information is important the Forum of Incident Response and Security Teams (FIRST), an international group of trusted computer emergency response teams, created the *'Traffic Light Protocol'* (TLP). The TLP was created to: *'Facilitate greater sharing of*

information' and is 'a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colons to indicate expected sharing boundaries to be applied by the recipient(s). TLP only has four colors; any designations not listed in this standard are not considered valid by FIRST (FIRST, 2018). The traffic light protocol knows the following definitions:





TLP: RED = Not for disclosure, restricted to participants only.


TLP: AMBER = Limited disclosure, restricted to participants' organizations.

TLP: GREEN = Limited disclosure, restricted to the community.

TLP: WHITE= Disclosure is not limited (FIRST, 2018).

Figure 4. *The Traffic Light Protocol.*

UNCLASSIFIED		
Protection of Information		
Traffic-Light Protocol (TLP): Originator-controlled classification system developed to encourage greater sharing of sensitive (but unclassified) information with external entities.		
When should it be used?	TLP Color	How may it be shared?
Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	RED 	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting or conversation in which it is originally disclosed.
Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	AMBER 	Recipients may only share TLP: AMBER information with members of their own organization, and only as widely as necessary to act on that information.
Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	GREEN 	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
Sources may use TLP: WHITE when information carries minimal or no risk of misuse, in accordance with applicable rules and procedures for public release.	WHITE 	TLP: WHITE information may be distributed without restriction, subject to copyright controls.


Homeland Security
UNCLASSIFIED
5

(RPC First, Deciphering the Traffic Light Protocol (TLP), 2017).

The TLP should be known when one is trying to research security networks that work with cybersecurity topics because it is the leading principle of sharing information. And sharing information is one of the core components of such security networks as noted by Whelan and stated by the respondents.

4.1.4. Sub conclusion on governance and the relevance of trust building inside the Joint-Soc network

The governance form of the Joint-SOC network could be described as a shared governance form. In this form all parties govern the network by themselves. According to Provan and Kenis (2008) this requires a high level of trust. This makes it interesting to investigate trust building inside the Joint-SOC network for two reasons. First, it could be interesting to check whether a shared-governance network indeed possesses a high level of trust. Second, if there is a high level of trust inside the Joint-SOC network it could be used as an example for other networks. The goal of the Joint-SOC network is to achieve greater efficiency. The network consists of several governmental entities and could therefore be described as institutional network in the works of Dupont (2004). Klijn and Edelenbos (2007) argue that governance networks have four reasons to pay attention to trust. First, they state that transaction costs could be lowered. This is the case in the Joint-SOC network, where resources are shared without using many transaction costs (Respondent one and two, 2018). Second, trust could persuade members of the network to invest resources in the network. This is also the case in the Joint-SOC network and helps the network in achieving its goal. Third and fourth, Klijn and Edelenbos (2007) state that higher levels of trust lead to more information sharing and increasing innovation. Both last points are among the ambitions of the Joint-SOC network (Joint-SOC, 2017). Therefore, trust building inside the Joint-SOC network is important. It is important because high levels of trust are required in the shared-governance model. Trust is also important because it helps the members of the Joint-SOC network in achieving their goals. These goals are important as they could play a role in combatting the problems uncovered by the Algemene Rekenkamer (Financieel Dagblad, 2018).

4.2. Components of Trust

This section will delve into the empirical data to distinguish how trust is build inside the Joint-SOC network. The first chapter will handle the different components of perceived trustworthiness. In this chapters each construct will be individually explored. In the chapter after this exploration the other factors will be considered. In the third and final chapter of this analysis the research question will be answered: *How is trust build inside security networks?*

4.2.1 Capabilities

Capability is about the way certain actors can influence others in the network. It is about competences, characteristics and abilities (Lambright et al, 2010). When talking about characteristics inside security networks respondent two describes it as: *'I believe everyone is a professional here, who all carefully work with the sensitive information at their disposal.'* So, it could be stated that in security networks a capability that is necessary is being careful with sensitive information. In addition to that, respondent two argues that it is necessary that people do not want to know what other people are doing in detail, but do know what their area of interest is, so they can assist in their work with *'need to know information'* (Respondent two, 2018). This is in line with Mayer's statement on capabilities and trust *'to influence in a specific domain'* (Mayer, 1995: p. 717) people do not necessarily need to be capable in everything but need to know about their part of the work. Most information in security networks is shared under the notion that the other party needs to know the information to do its work. Which is in contrast with *'nice to know'* information that is nice to know but does not hold the other from doing his or her work correctly. How to handle information and know how to share information is a core competence of networking members in the field of Cybersecurity. Also taking responsibility for your actions when things go troubled generate trust. These *'competences'* are strongly linked to the integrity of the trustee, as with integrity core components such as discreetness, fairness and promise are important (Lambright et al, 2010). But determining what fair and discreet is, is difficult, to determine such things is the input from all agencies in the network necessary (Respondent two, 2018).

Considering the Joint-SOC collaboration they believe that all parties can perform their duties, duties in the Joint-SOC network could be described as the duties that are necessary in day to day operations, such as providing feedback, working together during the Joint-SOC meetings, delivering threat information or collaborate in project groups. Therefore, network-level competencies as described by

Provan and Kenis (2008) are only needed on a low level. As both respondent one and two remark that organizations need a certain maturity level to meet the ascension guidelines in the first place. Since the organizations must meet the requirements the others believe that they possess the capabilities necessary to collaborate with the others. Trust in one's capabilities therefore might be generated through ascension guidelines for a security network. In the Best Practice is written down which guidelines need to be followed to join the network (Joint-SOC, 2017). Therefore, it could be stated that inside the Joint-SOC network the capabilities of the parties are an important part of trusting another. As it is the starting point for joining the network in the first place (Joint-SOC, 2017). When the trust is started to be being build, respondent four states that it is necessary to hold on to the *paperwork* and other formal policies such as screening (Respondent four, 2018). The guidelines consist of the basic principles that should be adhered by a SOC wishing to join the Joint-SOC network. These basis for the principles of the Best Practice can be found in the works of Schniagl and Schoon from Noordbeek (Schniagl & Schoon, 2014).

4.2.2. Benevolence

The second construct of trust is benevolence, *the extent to which a trustee is believed to want to do good to the trustor, aside from an egocentric profit motive* (Mayer, 1995: p. 718). In what way do the parties perceive benevolence in general and specific for the Joint-SOC network. First of all, the parties see benevolence as the interplay of interests. There are different interests in synergy in the Joint-SOC network. The governance board have their interest in the strategy of the network. The operational/tactical part of the network strives to certain achievements. And the different organizations all have their own goals and interests (Respondent one, 2018). This interplay of interests could be in opposition with the values of benevolence. However, in the Joint-SOC network respondent one and two state that the different interests do not clash with each other. All parties recognize that all organization have their own interest, because every organization has its own goals and beliefs. This is an interesting statement as it states that both the organization can have a goal as the network can have a goal. It is important to have all network members aligned towards the network goal, therefore creating goal consensus as described by Provan and Kenis (2008). However, the answer to these issues, according to respondent two, is to be open about where your organization stands. This is in line with one of the keywords of benevolence which is openness. Openness, according to the respondents, itself is requiring a high level of trust and could be difficult for

networks do not possess high levels of trust. Inside the Joint-SOC network there is room for such thoughts, which could benefit overall levels of trust.

Another important part of benevolence is the availability of another. Respondent four states that building trust requires effort. This part of the effort is appearing at meetings because of the importance of face to face contact between members of a network. Respondent four described a network that became bigger and bigger whereby not all members had seen each other face to face. Respondent four lost his trust in this network for a moment and demanded the availability of all members during the meetings, which then was written down in the membership guidelines (Respondent four, 2018). In the Joint-SOC network coming to the two-weekly meetings is also very important, it shows that the person or organization is willing to put effort in the trust relationship with the other parties involved.

4.2.3. Integrity

The third construct of trust is integrity: *'The trustor's perception that the trustee adheres to a set of principles that the trustor finds acceptable'* (Mayer, 1995: p. 719). Certain keywords that match with integrity are discreetness, promise, fairness and consistency. Earlier in this research discreetness is discussed. It is closely linked to a capability. However, the other components of integrity are also important. In the Joint-SOC collaboration it is important that information is not shared unnecessarily. All parties also believe that the others will follow the rules about sharing information and therefore *'integrity'* is both important and also guaranteed in the *'Set of principles that the trustor(s) find acceptable'*. Such principles are common inside security networks, especially the networks that handle cybersecurity topics. Therefore, the TLP protocol is also introduced. Inside the Joint-SOC network and other security networks are certain guiding principles that set the baseline regarding what is appropriate and what is not appropriate. This is in line with the works of McFall (1987) who argues that both the adherence to and acceptability of the principles define personal integrity. But when the trustee's principles are not deemed good enough by the trustor it does not guarantee integrity (Mayer, 1995: p. 719). Both respondent one and two argue that integrity is the most important aspect of the perceived trustworthiness as portrayed by Lambright et al (2010). Respondent one argues that one's capabilities or benevolence can be negative due to outside events. These events such as busyness or limited capacity, can decrease the way a trustee is perceived. However, respondent one argues that these issues are not as important as integrity (Respondent one, 2018).

Integrity and discreetness is also deemed the most important by respondent four. The respondent describes that: *'If I share something with you under TLP: RED and I hear it from someone else who obtained the information from you, it is game over'* The exact outcome of this breach of trust on the relationship depends on the way the *'offender'* handles the situation (Respondent four, 2018). It is important in the trust relationship how someone that breaks the rules treats his fellow network members. If the person does this in a respectful manner it could be that there is only a small amount of damage on the trust-relationship.

4.3 The dynamic process of trust-building

4.3.1. Screening: The starting point of trust in security networks?

As the previous chapters explained capabilities, benevolence and integrity are important aspects of whether someone is trusted or not. But first it is necessary to highlight another important condition for trust which is not included in the earlier model. A security clearance is a more impersonal form of trust that comes from institutional-based trust. As Whelan stated in his article: *'The requirements specifying that an individual in this field needs to obtain a security clearance to receive information at a particular level should, in theory, mean that the individual can be trusted. In fact, it could be argued that no stronger foundations of impersonal trust exist in any network than those in the field of national security because of these processes'* (Whelan, 2015: p. 42). Starting point of trust for all respondents in this research was the fact that his or her managers, colleagues or network partners have been screened by the Dutch intelligence services. As the first respondent states quite earlier in the interview: *'First of all I trust people because of their screening or other paperwork'* (Respondent 1, 2018). Whelan states these forms of *'impersonal'* trust can be important in security networks. That is also the case in the Joint-SOC network. As respondent two puts it: *'Inside the Joint-SOC collaboration you have to work with sensitive information. It could be sensitive by its technical character or because it is incident-related. When such information comes into play you do not want to talk about trust and trustworthiness. I know that inside the organizations we work with the trust is safeguarded because the people who handle the information are all screened by the Dutch intelligence services'* (Respondent 2, 2018). The screening of the Dutch intelligence services could be seen as a starting point for trusting others in security networks in the Netherlands. Others forms of screening also apply here but in the Joint-SOC network a screening by the Dutch intelligence services is standard. Whelan adds to this that with a screening: *'You can be confident that someone*

who is cleared to a certain level has been independently audited to be able to have that information. And you can have trust in that (Whelan, 2015: p. 43). In addition to the screening other formal paperwork also benefits (or starts) the trust relationship inside security network. In the case of the Joint-SOC network the membership guidelines are also an institutional form of control. The Joint-SOC network is not the only security network that uses this mechanism, as it is also used in the Rijks-ISAC (Information Sharing and Analysis Center) (Dutch NCSC, 2016, Respondent three, 2018). In addition to that Whelan argues: *'That no stronger foundations of impersonal trust exist in any network than those in the Field of national security because of these processes'* (Whelan 2015: p. 42).

4.3.2. *Building trust*

This chapter will demonstrate how trust is build inside security networks, along the model portrayed in the analytical chapter. This section will analyze the Joint-SOC network and look if the propositions made in the analytical chapter are valid. The model itself is presented here again for practical reasons.

4.3.3. *Cooperation as starting point*

Starting point for the model is cooperation. Starting collaboration with the idea of improving trust is not always an efficient process according to Provan and Kenis (2008: p. 242-243). Building trust through cooperation requires inclusion of all parties involved, therefore taking a toll on their time and other resources. As most authors have stated, trust is about risk and *interdependence* (Mayer, 1995, Klijn et al, 2007, Lambright et al, 2010). There is a need for some form of inter-dependency. In collaboration these inter-dependencies are present. In the case of the Joint-SOC network there is an interdependence present, it is the dependence on the other to secure the IT-infrastructure of the Dutch government. This is the formal approving of the network as it is grounded in the policy of the Ministry of Interior and Kingdom Relations. The beginning of the Joint-SOC network started with the cooperation described earlier in this thesis at the conferences held in the Hague (Respondent four, 2018, Dutch Central Government 2016). Both respondent three and four state that there will only be invested in the trust relationship as there is something to achieve with each other. Respondent four feels that this is especially the case when working together with private companies (Respondent 3, 2018, Respondent 4, 2018). The beginning of the cooperation between the parties during this conference was the first step in building a network and building up a level of trust. A commercial party set up the SOC during the first conference in 2015 as witnessed by the Tax and Custom

Administration and SSC-ICT. They then came up with the idea to do it themselves the next year (Respondent four, 2018). However, if you start a collaboration, how do you start building trust? Respondent four states that it is important to start off in an informal setting and use humor when first working together: *'It is a different situation when everyone takes a seat in a three-piece suit and his or her pencil perfectly aligned with the notepad, I believe it is better to take place in an informal setting where you interrupt the session to have a coffee break and have a chat at the coffee corner'* (Respondent four, 2018). This adds to the statement made by all respondents that in order to trust someone you have to meet him or her face to face. This is an interesting statement as most work in Cybersecurity involves computing, e-mail or chatting. Building trust in security network collaborations starts with meeting each other and looking in the eyes of the person in front of you. Whelan (2015) creates a distinction between *'positional-trust'* and *'relational-trust.'* Whelan describes relational trust as follows: *'You have to work on your relationships. You have to make sure that when someone moves from a position that you know who is taking over, that you go and make contact; you can email people, you can talk to them on the phone, but nothing replaces looking them in the eyes and forming a personal relationship'* (Whelan, 2015: p. 41-42). The statements made by the respondents in this research confirm the statement made by Whelan (2015).

4.3.4. Third party relationship: Network closure and structural equivalence

The next step in the model is that, in a network, there are third party relationships and that there is a relationship between the trustor and the trustee. First, we take a look at the third-party relationships in the Joint-SOC network. According to the model third party relationships are comprised of network closure and structural equivalence. Network closure is about the other parties in the network and how they influence the relationship of the other parties working together. In the Joint-SOC network a lot of work is done together, however there are also projects done with different subgroups or in dyadic relationships. The parties inside the Joint-SOC network know each other well enough that these collaborations do not seem to influence the trust inside the network. However, the collaborations by the Joint-SOC network do have an impact on the broader network of Cybersecurity concerned organizations. Respondent three described it as follows: *'Other organizations know that if you take part in the Joint-SOC network, you have reached a high maturity as a SOC. Therefore, other organizations would like to join the network'* (Respondent three, 2018). From 19 July another organization, DICTU from the Ministry of Economic Affairs, takes part in the Joint-SOC network as aspiring-member (Respondent four, 2018). The network-closure might not be of major importance

inside the Joint-SOC network itself, but the reputation and successful actions of the Joint-SOC spread towards other governmental institutions. This could reassure the parties inside the Joint-SOC network that they are doing a good job and thus positively influence the level of trust the parties have in another. Interesting note is that if someone new, from an organization already in the network, joins he or she derives a certain amount of trust because she comes from an organization that is trusted (Respondent three, 2018). However, the person that is chosen to join the network should not be a new member of the organization it is working for, as he or she does not have learned the organization well enough to gain the same amount of trust (Respondent four, 2018).

Second, we take a look at structural equivalence. Structural equivalence means if the parties inside the network have the same view on the network. According to respondent two the parties inside the Joint-SOC network have the same view on the network. Respondent two also argues that there are differences in the standpoints from the organizations. However, the respondent believes that such behavior is necessary in networks, because not every organization can perfectly fit in the beliefs of other organizations. It is also beneficiary to the structural equivalence of the network that all members of the network have the same function inside their own organizations, with exception for the NCSC as they are not a formal SOC but a CERT (Respondent two, 2018, Respondent three, 2018). According to the theory, structural equivalence can also lead to subgroups inside networks, which undermines trust (Lambright et al, 2010: p. 68). This is not the case in the Joint-SOC network where all parties have the same view on the network and feel that the organizations are matched evenly. This could change however when more parties are joining the network. As these four organizations are the founding fathers of the network, it could be in the future that newer parties are treated differently. There are no current indications that this might be the case. For the members of the Joint-SOC network closure was not an important indicator for trusting another organization, as the network itself currently is rather small. Structural equivalence could be argued to be of importance as the ascension guidelines also demand a view that is related to the organizations already inside the network. Respondent four describes that an aspiring-member has a period of one year to fulfill its ambitions. After the initial year his performance is assessed, the governance board decides whether or not the party is allowed to join the network (Respondent four, 2018). This is an interesting way to influence the structural equivalence of the network.

4.3.5. *The relationship between the trustor and the trustee*

Next to third party relationships there is a certain relationship between the trustor and the trustee. According to Lambright et al (2010) this relationship is formed by the past interactions between the parties involved. Successful past cooperation leads to a higher frequency of current interactions and has a positive impact on whether a person or organization is trusted or not. In the case of the Joint-SOC network it could be observed that the initial cooperation was deemed successful. After that period the parties started to work together on a more frequent basis. As the section in this research about capabilities showed there is a lot of successful past cooperation in the Joint-SOC network. In addition to that there is also a high frequency of interactions, as respondent two notes that there is a meeting every two weeks and that they see each other on a more regular basis, depending on the situation at that time. Provan and Kenis (2008) argue that participant-shared networks are only effective when there is a lot of personal contact (Provan and Kenis, 2008: p. 234). Respondent four states that the amount of times they interact is also dependent on the situation. If times are busy and threats are imminent there are more interactions than if its *silly season*. The respondent argues that when something is going on they usually contact each other directly through a chat channel (Respondent four, 2018). Inside the Joint-SOC network there are many successful cooperation's to discover. They, for example, worked on the implementation of the VERIS framework for identifying incidents and sharing incident information (Best practice, 2017: p. 43, Respondent two & four, 2018, VERIS, 2018). Another fruitful collaboration is the DDoS tests organized by the Tax and Customs Administration each year. Where all parties come together to learn about the mitigation of Distributed Denial of Service Attacks (KPN, 2018 & Respondent four, 2018). Previous cases are examples of larger projects that are executed by the parties of the Joint-SOC. But they also work together on a looser basis. The SOC's of Rijkswaterstaat and the Tax and Custom Administration work together on different incident cases, whereby the expertise of the organizations is used to help each other (Respondent four, 2018). Whelan (2015) argues that personal trust is dependent on frequent interactions over time. This seems to also be the case in the Joint-SOC network. There are a lot of interactions which contribute to the personal trust inside the network.

Respondent one argues that it also is beneficiary to both be inside an organization as well as being part of the Joint-SOC network. As it provides a way that can be used to discuss things. This might be beneficial to the perceived trustworthiness of the other organization as this could be about ability, benevolence or integrity (Respondent one, 2018). In the case of the researched network successful

past cooperation also directly influences whether the other organization is trusted or not. As respondent two puts it: *'In the basis everyone is granted with my trust. The trust I have in another person or organization can grow. That depends on how my relationship with the other develops and how I observe how things are handled'* (Respondent two, 2018). Respondent two argues that these kinds of observations are a reason for trusting someone and thus sharing information with other parties. Respondent two, also states that trust can be diminished in this way. It could be stated that *unsuccessful* past cooperation has a negative influence on the perceived trustworthiness. This could be because the trustor ranks the capability, benevolence or integrity different than earlier in the cooperation. Respondent two also states that unsuccessful cooperation not necessarily lead to negative implications if they handle it *'correctly'*.

4.4. Combining all elements of the trust model

So far, we have distinguished that successful cooperation, frequency of the interactions and third-party relationships have an impact on the perceived trustworthiness of a person or organization. Each variable has a different impact on the perceived trustworthiness and also influences the different components of the perceived trustworthiness. The network closure as described in the model plays a small role in this network because it is only a small network, the parties know quite well what the others are doing, because they closely work together. Successful past cooperation is an important aspect that affects the perceived trustworthiness. The respondents state that their opinion of whether someone is integer, has the capabilities or is benevolent is depending on the others act when working together. In the case of the Joint-SOC network it could be stated that the perceived trustworthiness of all parties is deemed high. The respondents state that they trust the other parties. The parties state that they trust each other but also indicate that they rank the others high in their capabilities, as benevolent partners and as parties who uphold a high standard of integrity, in addition to the security clearance by the Dutch intelligence services. The interplay of the different components of perceived trustworthiness is important. Because it is stated that the components are ranked differently. Inside the Joint-SOC network it is important to define what is *'carefully'* handling work. This is linked with all the components of trust. It is important to define what is appropriate and what is not, this goes beyond capabilities and also treats benevolence and integrity. Most important in handling things well inside security networks is being integer with information distributed to you.

The three components of trust, capabilities, benevolence and integrity are related to each other as Mayer (1995) describes. And this is where the dynamics of trust take place inside the currently explored model. As Mayer notes: *'In what situations is each of the three factors most sensitive or critical?'* (Mayer, 1995: p. 722). In this analysis we have noticed that the levels of perceived trustworthiness are high ranked by the members of the network. It is also seen that the interactions are, considering the busyness of around that time itself, is at a high level. The capabilities of the members of the Joint-SOC network are described as good, which also becomes clear when other governmental organizations adhere capability as a principal part of the Joint-SOC network (Respondent three, 2018). The respondents state that they find integrity the most important part of trust. Respondent three describes that being introduced to a network: *'Is not necessarily about your knowledge of the topic or the network, but about meeting people face to face'* (Respondent three, 2018). Following the words of respondent four who states that after the integrity of a person is questioned it is: *'Game over.'* After such a situation it is hard to regain the trust of a person or organization. We could state that in the Joint-SOC network there is a certain level of capability required to join, but the most important aspect of trusting the other then is the persons integrity or benevolence. Respondent one puts it as follows: *'In collaboration I find it of great importance that I can trust someone with certain information. If this information comes back to me from someone else, it heavily damages the trust relationship'* (Respondent one, 2018). Respondent one is clear on which constructs are the most important as he states that: *'I find integrity the most important in people, more important than my interests being served or the capabilities of another'* (Respondent one, 2018). As all three respondents state that there should not be a conflict of values. All three respondents sketch a situation where a private motive might conflict with the values of the public parties in cooperating (Respondents one, two & four, 2018). In the interplay between the components of trust inside this security network, benevolence and integrity are deemed as the most important. The constructs benevolence and integrity are also laid out in both the best practice as stated by respondent four. An example of such a guideline that involves integrity is that the members of the Joint-SOC meeting must be internal governmental officers. This could indicate that otherwise there might be a clash in interests or it could mean that private officers are not attributed the same values as a government official. Even though capabilities do not seem to be the most important construct for the network members it should be noted that it requires a high level of capabilities to join this network in the first place. To join this network, an organization has to comply with the Best Practice

for SOC's and be an aspiring member for at least a year. There is a certain baseline for capabilities that exists otherwise an organization is not allowed to join the network, and this plays a role in trusting the other's capabilities, because it is '*independently*' measured beforehand. This is also necessary due to the way the network is governed. The Joint-SOC network is governed by all parties themselves. In order to steer this network all parties should be autonomous and able to make decisions on the directions of the network. One of the keywords considering benevolence is availability. The three respondents from the Joint-SOC network state that they would like to see availability in different construct or even outside the scope of trust. All respondents state that availability is not necessarily related to trust as they understand that different organizational goals might not be in line with the goals of the network (Respondent one, two & four ,2018). Therefore, they argue that it is possible that someone is not able to deliver resources to the network from time to time. It could be argued that liability or availability is less important than other keywords of benevolence. Availability in terms of showing up at meetings on the other hand is deemed quite important, as face to face contact is vital to trust-building.

The last part of the model states that if one trusts the other(s) they cooperate in the future. In the case of the Joint-SOC model is clearly visible that they will work together in the future. All respondents state that they will work together in the future, because they are satisfied with the outcomes of the current network and they strongly believe such a network is necessary. Not only are the parties willing to work together, they are also letting in new partners to help them learn how to be more effective as a security operations center (Respondent four, 2018, van Gernerden, 2018: p. 22). If the components of the overall model are analyzed it could be stated that inside the Joint-SOC network there is a high level of trust. This trust enables the parties to cooperate in the future. The parties state that they trust each other and will cooperate in the future, therefore starting the model back from the beginning with new cooperation. It could be argued that this new cooperation starts with a higher level of initial trust then when you start a new collaboration. However, as respondent one, two and three state, the amount of trust you have in someone could change. The next cooperation will prove if the trust relationship will be stronger than the last time cooperation took place. This is depending on the successful cooperation directly influencing perceived trustworthiness.

4.5. How is trust build inside security networks?

This chapter will more explicitly answer the research question of this thesis. How is trust build inside security networks? Earlier is stated that building trust begins with cooperating. This cooperation should be a situation where both parties see the opportunity to achieve something, otherwise a cooperation is not necessary (Respondent four, 2018). This is also in line with the definition of a network Provan and Kenis (2008) who state that a network is: *“Consisting of three or more legally autonomous organizations that work together to achieve not only their own goals but also a collective goal”* (Provan & Kenis, 2008, p. 231) Investing in a trusting relationship takes time and money. In the early stage of this cooperation an informal approach generates the most trust. As Whelan (2015) also puts forward is that informal contact in general is beneficial to trust-building inside security networks. However, if a network plans on a long-lasting cooperation it is useful to start off the collaboration with some kind of statutory document in which the membership guidelines are written down. Examples of these can be found in both the Joint-SOC network as well as the ISAC’s (Best practice, 2017 & Dutch NCSC, 2016). In the case of the Joint-SOC network a screening by the Dutch intelligence services is also a perquisite, this does not necessarily have to be the case in other networks. That largely depends on the information that is being distributed in such networks.

When the cooperation starts it is important to generate successful cooperation, as they provide a ground for trust, and in providing network closure. Together with successful cooperation it is important to strive for a high, but not unnecessarily high, frequency of interactions. In the Joint-SOC network it is important that all parties find each other easily. Finding another easily becomes easier when the frequency of the interactions in general is higher. Furthermore, it is important that all parties have the same view on the network. This is also the case in the Joint-SOC network, even though sometimes not all parties have the same interests. When a clash of interests occurs, it is important to be open about it, this openness improves the perceived trustworthiness component benevolence. Another important factor to consider is the integrity of the network members. This can be formally written down in membership guidelines and recommendations but should also be propagated by the network members. These rules should be in line with how the members of the network would like to see for instance new members. The statements above both agree and contradict the work of Whelan (2015) who states that inter-personal trust is more important than organizational trust. This research puts forward that interpersonal trust is indeed important inside security networks as they provide the breeding ground for trust with high frequency of interactions. On the contrary it is noted that to build

this breeding ground for trust, there needs to be a certain baseline in capabilities as well as other guiding principles that are adhered by the network.

In the cooperation it is observed that all three components of trust come into play, the one more important than the other. In the Joint-SOC case became clear that integrity and benevolence are the most important aspects of trust. Whereby, integrity is the most vital part of cooperation. Without the right principles of integrity, a person or organization will not be trusted in this security network. There is an interplay between the components leading to whether one is trusted or not. The value attributed to each of these components come from how a person or an organization operates during the cooperation with the others. Building trust in security networks is about the way one handles information gained from another party. If a party is damaging the trust the other by leaking this information, it's perceived trustworthiness quickly diminishes (Respondent four, 2018). When we look back at the question posed by Mayer (1995) *'How low can some of the three factors be before the employee would not trust the manager? In what situations is each of the three factors most sensitive or critical?* It could be stated that the capabilities and benevolence can be low, but integrity should remain high at all times. The dynamics between these three components could vary in different situations. For a long lasting cooperation that requires sensitive, sometimes secret, information to be shared, this combination of the constructs is needed.

5.0. Reflecting, policy recommendations and future research

This chapter will briefly reflect on this research. This section will reflect on the choices that have been made during this research, it will provide recommendations for future policy and sketch a new direction for further trust studies.

5.1. Reflection

This research is focused on a governmental cooperation, more explicit the cooperation between governments in the security sphere. This was an explicit choice in the setup of this research. Most current research is focused on public-private partnerships. At the beginning of this research there was a wider scope. The research tried to find an answer on two questions. First, how trust is build inside security networks? Second, how does trust benefit network overall performance? Answering both these questions proved to be too ambitious for this thesis program. It was still important to touch the structural components of security networks and that is why the work of Provan and Kenis (2008) brought forward. The work of Provan and Kenis describes why trust is important in governance networks and provides a basis for researching trust in such networks. This research was particularly interested in how governmental organizations work together in defending the Netherlands from Cyberattacks and what role trust plays in this collaboration. This research also found bits of information on how this cooperation developed and how it functions. During the interviews became clear that the public-private partnerships are important. Further study could explore whether the model used in this research is also applicable to the private sector, or a combination of both the public and private sector. Furthermore, this research provided a lot of information about how the Dutch government tries to arrange its information security. The governmental information security is a remarkable landscape with a lot of interests and organizations.

During this research three members of the Joint-SOC network and a security network practitioner from the Dutch National Cyber Security Center were interviewed. The statements made in this research are therefore not applicable to every security network that exists. However, it was hard to find access to this network and all relevant people inside the network have been interviewed. It could be interesting to also interview people from the governance board. It was already difficult to find entrance to the operational members; the governance board was not reachable for the author during this research. To make more concrete statements on building trust inside security networks there should be research conducted on more networks to see what differences and similarities exist. In this

thesis it is seen that the constructs of trust indeed are part of security networks, but not always as explicit as stated in the literature. The model used in this research provided a basis for researching trust. Trust is a concept that is different for everyone. When a respondent or person says that he or she trusts someone they have their own idea about what trusting someone is and how trust is achieved. Most respondents that were interviewed did not think about what trust means concretely. At first, this research tried to cover every aspect of the model in the interviews. Further, in the study became clear that better answers were given when asking the respondents how they see or feel things about the different components of trust. The model that was created took a while before it was good. It took a lot of time to rearrange all constructs in a way that they benefitted the research, where valid and feasible. Earlier in the process of this research tried to conduct research on both network effectiveness as the building of trust. In the end this deemed to be not feasible as it requires an even more complex model to be analyzed. To argue why trust is still important in security networks the works of Provan and Kenis are used. The model used in this research contributed to the author's view on trust and helped perceive reality through the different constructs in the model.

In the methodological chapter is stated that documents will be analyzed as a way of triangulation of the data. This proved to be very hard in the case of the Joint-SOC network, as the only available source was the best practice. Most information is not written down in separate documents and if it is it is not for publication. This research showed that gaining access to a security network is difficult. It is also important to note that a certain amount of trust is required by the members of a security network to talk with a researcher. Future researchers could use the model of this research to learn more about trust, using it to gain access to security networks and provide in more trust research. When conducted a new research it should be considered that the months June to August are not favorable months to interview government officials, as most of them are on holiday or very busy. In addition to that, this research is conducted on government officials on a more operational or tactical level. It could be interesting to see if the outcomes of this research are the same from a more strategic or management level view. As mentioned before this research started of with a wide scope and a lot of information was added to the theoretical framework of this research. After a broad literature- and empirical study it became clear that it was too broad. In order to clearly explain what is covered in a research study it is necessary to exclude '*nice to know*' information from '*need to know*'.

Concluding, this research shows that researching trust in security networks is interesting, because trust and security network both have many dimensions. The Dutch central government security structure proves to be a dynamic field with different organizations and high importance. This high importance comes forward in the policy created by the ministry of Interior and Kingdom Relations (2016). The closed nature of security networks and the high importance of such networks require a model that is focused on a particular problem or subject. Researching trust provided a small but interesting scope, as trust plays a large role in security collaboration. Trust could be the mechanism that makes security networks effective, as also stated by Whelan (2015), Klijn & Edelenbos (2007) and Provan and Kenis (2008). This research mostly reaffirmed statements made by those authors. But it provided insights in what constructs are deemed more important. This could contribute to generating more trust inside governance- and security networks.

5.2. Policy recommendations

Researching the Joint-SOC network has provided meaningful insights. Not only in how trust is build inside networks, but also about the way the Dutch government is trying to unify and combat Cyber-attacks. This section will provide policy recommendations for both the Joint-SOC as well as other parties that wish to initiate a security network:

- As described earlier it is useful, and possible, to establish a written base of trust. This could be in the form of membership guidelines or ascension guidelines. In order to minimize conflicting interests, it is wise to, beforehand, determine the basic principles of the network that should be adhered by all current members and new members.
- An earlier observation was that the components of trust are present in the Joint-SOC network. This presence of the components is not always as explicit as mentioned in the literature, nor in the model. For security networks starting up it might be interesting to place the constructs of trust more in the spotlight. Trust is always an important part of collaboration, but it is also not often explicitly discussed. A recommendation would be to discuss these components every once in a while, in order to achieve a higher level of trust.
- The Joint-SOC itself is an example for the rest of the Dutch government. Its challenges lie in the future, where new organizations join the network and old members retire. It is important to maintain the sphere of trust that exists now. Maintaining this sphere of trust can be done by providing in a *'warm transfer'*. A new member of the network should be guided and introduced by the retiring officer, as this enables a more efficient way of creating trust (Respondent three, 2018). This is in line with Whelan's statement regarding interpersonal trust (Whelan, 2015: p. 3). Whelan states that interpersonal trust is more important than inter-organizational trust, therefore it could be useful to place an emphasis on this aspect in transfers.
- In the case of the Joint-SOC network high frequency of interactions is observed. The analytical model of this research states that frequent interactions between network members positively influence the levels of trust inside the network. Therefore, it is recommended that when creating a network, it is important to organize face to face meetings. A good example is provided by respondent four as he describes the O-IRT-O network where people are obliged to join those meetings (Respondent four, 2018).

5.3. Guidance for future study

The reflection mentioned that this research only focused on one security network in the Netherlands. There are certain limitations to this research due to time constraints and access to security networks. The next brief section will explore what future study could be conducted on the topic of trust in security networks.

First, this research concluded with the statement that integrity is the most important component of trust inside governmental security networks, or at least inside the Joint-SOC network, future study could explore if this is the same inside other forms of collaboration, such as public private partnerships. Security networks are generally closed groups and require quite some time to enter, and even more time to research. Therefore, it might be interesting to apply this model to *more* open security networks. An example of a network that could be interesting to research is the earlier named ISAC. There are several ISAC's that have a public-private component. This might provide more information on components such as benevolence, network closure and structural equivalence (Dutch NCSC, 2016). Even though public-private partnerships are often researched, it could be interesting to notice what constructs of trust are more important in such networks. Are capabilities more important than benevolence and integrity? It could also be interesting to test what principles are more important in different networks than security networks, such as networks between hospitals, municipalities or ministries, in order to generate more knowledge about trust in general.

Secondly, this thesis focused only on one network. For future studies it would be interesting to gain knowledge about more security networks in the Dutch government. It could be interesting to discover differences between the security networks. It might also be useful to research a collaboration that is deemed less successful as the Joint-SOC network, as it might tell more about how unsuccessful cooperation then influences the perceived trustworthiness. It might also be interesting to study different kind of security network. The Joint-SOC network could be described as a shared-governance network. It would be interesting to know how trust is built in networks that have a lead organization or a network administrative organization (NAO). Because, a lead organization network or NAO network require a different level of trust but might also differ in what is deemed important in trust.

Third, the thesis from this researcher is mainly focused on the Netherlands. It might be useful to look at governmental security network cooperation in other countries. This is twofold, because it could provide more insight in governmental security networks in other countries and to see if a '*Joint-SOC*' collaboration exists at all in other countries.

Literature

Adler, P.S. (2001). Market, Hierarchy, and Trust: The Knowledge Economy and the Future of Capitalism. *Organization Science*, 12, 215-234.

Blank, S. (2008). Web War I: Is Europe's First Information War a New Kind of War? *Comparative Strategy*, 27, 227-247.

Berg, B.L. (2009). *Qualitative Research Methods: For the Social Sciences*. New York. Allyn & Bacon.

Colquitt, J.A. & Scott, B.A. & LePine, J.A. (2007). Trust, Trustworthiness, and Trust Propensity: A Meta-Analytic Test of Their Unique Relationships with Risk Taking and Job Performance. *Journal of Applied Psychology*, 92, 909-927.

Dupont, B. (2004). Security in the age of networks. *Policing and Society: An International Journal of Research and Policy*, 14, 76-91.

Gargiulo, M. & Ertug, G. (2006). *The Dark Side of Trust*. In: Bachmman, R. & Zaheer, A. (eds). (2006). *Handbook of Trust Research*. Cheltenham, UK: Edward Elgar Publishing Limited

Goldsmith, S. & Eggers, W.D. (2004). *Governing by Network: The New Shape of the Public Sector*. Washington, Brookings Institution's Press.

Hathaway, M. & Spidalieri, F. (2017). *The Netherlands Cyber Readiness At A Glance*. Potomac, Arlington.

Janowicz, M. & Noorderhaven, N. (2006). *Levels of inter-organizational trust: Conceptualization and measurement*. In: Bachmann, R. & Zaheer, A. (eds). (2006). *Handbook of Trust Research*. Cheltenham, UK: Edward Elgar Publishing Limited

Klijn, EH. & Edelenbos, J. (2007). Trust in Complex Decision-Making Networks. *Administration & Society*, 39, 25-50.

Klijn, EH. & Edelenbos, J. & Steijn. (2010). Trust in governance networks; its impact on outcomes. *Administration and Society*, 42, 193-221.

Krahmann, E. (2010). Security Governance and Networks: New Theoretical Perspectives in Transatlantic Security. *Cambridge Review of International Affairs*, 18. 15-30.

Kramer, R.M & T.R. Tyler (eds) (1995). *Trust in Organizations*. Thousand Oaks, CA: Sage.

Lambright, K.T. & Mischen, P.A. & Laramee, C.B. (2010). Building Trust in Public and Nonprofit networks: Personal, Dyadic and Third-Party Influences. *The American Review of Public Administration*, 40. 64-82.

Lane, C. & R. Bachmann (eds) (1998). *Trust Within and Between Organizations. Conceptual Issues and Empirical Applications*. Oxford: Oxford University Press.

Maloy, J.S. (2009). Two concepts of trust. *The Journal of Politics*, 71, 492-505.

Mayer, R.C. (1995). An Integrative Model of Organizational Trust. *Academy of Management Review*, 20, 709-734.

Nooteboom, B. (2006). *Forms, sources and processes of trust*. In: Bachmman, R. & Zaheer, A. (eds). (2006). *Handbook of Trust Research*. Cheltenham, UK: Edward Elgar Publishing Limited

Paganini, P. (2016). *What is a SOC (Security Operations Centre)?*

[<https://securityaffairs.co/wordpress/47631/breaking-news/soc-security-operations-center.html>].

Retrieved on 08-06-2018.

Pieters, J. (2018). *Teen suspected of DDoS attacks on Dutch financial services wanted to prove a point.*

[<https://nltimes.nl/2018/02/07/teen-suspected-DDoS-attacks-dutch-financial-services-wanted-prove-point>]. Retrieved on 25-02-2018.

Provan, K.G. & Kenis, P. (2008) Modes of Network Governance: Structure, Management, and Effectiveness. *Journal of Public Administration Research and Theory*, 18, 229-252

Provan, K.G. & Kenis, P. (2009). Towards an Exogenous Theory of Public Network Performance. *Journal of Public Administration Research and Theory*, 87, 440-456.

Roberts, N. (2000). Wicked problems and network approaches to resolution. *International Public Management Review*. 1, 1-19.

Rousseau, D.M. (1995). Introduction to special topic forum. Not so different after all: A cross discipline view of trust. *Academy of Management Review*. 23, 393-404.

Schäfer, P.J. (2013). Human and Water Security in Israel and Jordan. *Environment, security, development and peace*. 3, 5-18.

Schinagl, S. & Schoon, K.C. (2014). *Security Operations Center (SOC): Modelleren en meten van effectiviteit*. Amsterdam.

Seppänen, R. (2008). *Trust in inter-organizational relationships*.

Van de Ven, A.H. & Smith-Ring, P. (2006). *Relying on trust in cooperative inter-organizational relationships*. In: Bachmman, R. & Zaheer, A. (eds). (2006). *Handbook of Trust Research*. Cheltenham, UK: Edward Elgar Publishing Limited

Vangen, S. & Huxham, C. (2003). Nurturing collaborative relations: Building trust in inter-organizational collaboration. *The Journal of Applied Behavioral Sciences*. 39, 5-31.

Verschuren, P. & Doorewaard, H. (2007). *Het ontwerpen van een onderzoek*. Den Haag. Boom Lemma.

Whelan, C. (2015). Managing Dynamic Public-Sector Networks: Effectiveness, Performance, and a Methodological Framework in the Field of National Security. *International Public Management Journal*. 1-60.

Yin, R.K. (2003). *Case Study Research: Design and Methods*. California, SAGE.

Zaheer, A. & B. McEvily & V. Perrone (1998). Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance. *Organization Science*, 9, 141–59.

Zaheer, A. & B. McEvily. (2006). *Does trust still matter? Research on the role of trust in inter-organizational exchange*. In: Bachmann, R. & Zaheer, A. (eds). (2006). *Handbook of Trust Research*. Cheltenham, UK: Edward Elgar Publishing Limited

Zedner, L. (2009). *Security*. London. Routledge.

Sources

Dutch Central Government. (2008). *CIO stelsel Rijk – inrichting*.

[https://www.earonline.nl/index.php/CIO_stelsel_Rijk_-_inrichting]. Retrieved on 14-07-2018.

Dutch Central Government. (2016). *Rapport Strategische I-agenda Rijksdienst*.

[<https://www.rijksoverheid.nl/documenten/rapporten/2016/12/02/rapport-strategische-i-agenda-rijksdienst>]. Retrieved on 14-07-2018.

Dutch National Cyber Security Center. (2016). *ISAC's*.

[<https://www.ncsc.nl/samenwerking/isacs.html>]. Retrieved on 21-07-2018.

Financieel Dagblad. (2018). *Rijksoverheid loopt vast in ICT-problemen*.

[<https://fd.nl/economie-politiek/1254408/rekenkamer-hekelt-informatiebeveiliging-overheid>]. Retrieved on 26-07-2018.

FIRST. *TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance — Version 1.0*

[<https://www.first.org/tlp/>]. Retrieved on 09-06-2018.

Global Conference on Cyber Space. (2015). *About GCCS*.

[<https://gccs2017.in/>]. Retrieved on 06-06-2018.

Joint-SOC. (2017). *Best Practice*. Den Haag.

KPN. (2018). *Een DDoS attack: wat is het en wat zijn de gevolgen?*

[<https://www.internetservices.nl/blog/DDoS-attack-wat-is-gevolgen/>]. Retrieved on 21-07-2018.

Lord, N. (2018). What is a Security Operations Center (SOC)?

[<https://digitalguardian.com/blog/what-security-operations-center-soc/>]. Retrieved on 18-07-2018.

Ministry of Justice and Security. (2018). *Nederlandse Cybersecurity Agenda*. Den Haag.

Nuclear Security Summit. (2014). *Past-Summits*.

[<http://www.nss2016.org/past-summits/2014/>]. Retrieved on 09-06-2018.

Politie Nederland. *Nuclear Security Summit*

[<https://www.politie.nl/themas/nuclear-security-summit.html>]. Retrieved on 09-06-2018.

RPC First. (2017). *Deciphering The Traffic Light Protocol TLP*.

[<http://rpcfirst.org/2017/09/13/deciphering-the-traffic-light-protocol-tlp/>]. Retrieved on 18-06-2018.

Om een gepaste oplossing te formuleren voor de aanpak van cyberdreigingen en kwetsbaarheden zijn diverse Info

SSC-ICT. (2016). *Samenwerking SSC-ICT en Belastingdienst*.

[<https://www.ssc-ict.nl/actueel/nieuws/2016/samenwerking-ssc-ict-en-belastingdienst.aspx>].

Retrieved on 10-06-2018.

Van Gernerden, J. (2018). *Het SOC als smeerolie voor de IB organisatie*.

[<https://chapter.isc2.nl/app/uploads/2018/04/20180516-Juri%C3%Abn-van-Gernerden.pdf>].

Retrieved on 21-07-2018.

VERIS. (2018). *Veris Overview*

[<http://veriscommunity.net/veris-overview.html>]. Retrieved on 21-07-2018.

Verschuren, E. (2017). *Wereldwijde aanval met ransomware treft ook deel Rotterdamse haven en TNT*

[<https://www.nrc.nl/nieuws/2017/06/27/aanval-met-ransomware-op-containerbedrijf-haven-rotterdam-a1564693>]. Retrieved on 05-04-2018.

Zetter, K. *Inside the Cunning Unprecedented Hack of Ukraine's Power Grid*.

[<https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>].

Retrieved on 05-04-2018.

Appendix

The transcripts of the interviews are distributed to the supervisor of this thesis.

Interview protocol

Protocol:

1. *What is your name and function inside your own organization?*
2. *What would you consider as your function inside the network?*
3. *How would you describe the Joint-SOC network?*
4. *How many interactions do you have with the network?*
5. *What drives you to participate in this network?*
6. *To what extent do you think that trusting each other is necessary in security networks?*
7. *Do you think party X, Y, Z is very capable to perform their actions in this network?*
8. *Do you think party X, Y, Z is known to be successful in their actions in this network?*
9. *Do you think party X, Y, Z are concerned with your welfare?*
10. *Do you think party X, Y, Z would act in your best interest?*
11. *Do you think party X, Y, Z has a strong sense of justice?*
12. *Do you think party X, Y, Z is consistent in his or her actions?*
13. *Could you state with which partners you would like to cooperate in the future?*
14. *To what extent are you satisfied with the operations of the Joint-SOC network?*
15. *Could you indicate with which parties your organization had successful past cooperation?*
16. *In what way does successful cooperation change the opinion of the other network members?*

Respondents

Respondent 1. Technical SOC Lead at the Dutch government.

Respondent 2. Senior Security Specialist at the Dutch National Cyber Security Center

Respondent 3. Security Network expert at the Dutch National Cyber Security Center

Respondent 4. Technical SOC Lead at the Dutch government.