Public-Private Cooperation in Cyber Security

An analysis of the role of the National Cyber Security Centre (NCSC-NL) in public-private cooperation in cyber security

S. van Kalsbeek MSc.
Student number: 2464195
Word count: 23989

February 2020

Master's Dissertation
Crisis and Security Management Program

Supervisors:
Dr. Els de Busser
Dr. Tatiana Tropina

Leiden University
Faculty of Governance and Global Affairs

Universiteit Leiden

"In the long history of humankind (and animal kind, too) those who learned to collaborate and improvise most effectively have prevailed."

— Charles Darwin —

Preface

This research is the final product of my Master in Crisis and Security Management at Leiden University Campus the Hague. This past one year has been somewhat intensive but also satisfying. I have had the opportunity to further increase my knowledge in security and crisis management and broaden my network in this field.

While working in cyber security for several years, choosing my thesis subject was not difficult. However, formulating the research question was a bigger challenge. Consequently, the research question of this study was formulated after many changes. Nonetheless, I am truly happy with the result and hopefully this research will be valuable to the field of public-private cooperation in cyber security.

I would like to thank the NCSC-NL organization for its incredible support in this process. I have been very lucky with the backing and in particular the following persons have been supportive. Mireille, Willemijn, Kees, Rosa, Michael, Ruben and Julia (NCTV). I also wish to thank Liesbeth, Marjolijn, Jacco, Thom and Kevin. Thank you for your contribution to this research and herewith also to public-private cooperation in cyber security in general. Without your input I would not have been able to conduct this research.

My special gratitude goes to my thesis supervisors Dr. de Busser and Dr. Tropina. Thank you, Leiden University, for your support, in particular the CSM study advisors. Thanks to my fellow students.

Moreover, I would also like to thank my friends and family for their support. Especially Carmen, Maarten, Marijn, Sabine, Carlos and all the others. And last, but not least I would like to thank my biggest support in live, Dragan. If I ever lost motivation, you kept me motivated. You are the best supporter ever!

Thank you all for your support!
Saïda van Kalsbeek
The Hague, February 2020

Table of Contents

List of Abbreviations

AIVD – Dutch Intelligence Services
BUZA – Ministry of Foreign Affairs
BZK – Ministry of the Interior and Kingdom Relations
CIP – Critical Infrastructure information Protection
CSA – Cyber Security Alliance
DCC – Defence Cyber Command
DefCERT – Computer Emergency Response Team of the Ministry of Defence
DTC – Digital Trust Center
ECP – Platform for the Information Society
ENISA – The European Union Agency for Cybersecurity
EZK – Ministry of Economic Affairs and Climate Policy
FIRST – Forum of Incident Response Security Teams
GCCS – Global Conference on Cyberspace
ISAC – Information Sharing and Analysis Centre
JSCU – Joint Sigint Cyber Unit
J&V – Ministry of Justice and Security
LDS – National Covering System
MIVD – Dutch Military Intelligence Services
MoD – Ministry of Defence
MSP – Managed Service Provider
NCIRC – NATO Computer Response Capability
NCSA – National Cyber Security Agenda
NCSC-NL – Dutch National Cyber Security Centre
NCTV – National Coordinator for Security and Counterterrorism
NDN – National Detection Network
OCW – The Ministry of Education, Culture and Science
OKTT – Designated Information Clearing House
PPP – Public Private Partnership

List of figures and tables

Abstract

Because of the rapidly increasing cyber-threats the public and private sector in the Netherlands are more and more working together in PPPs in cyber security to meet today's digital challenges. The NCSC-NL is one of the key players in public-private cooperation in the Netherlands and is involved in numerous PPPs. This research analyzes the role of the NCSC-NL in public-private cooperation according to the three roles defined in the model of the Spectrum of Coalition Formation; the director, partner and facilitator role. Eight respondents, four of the NCSC-NL and four external respondents, of four different PPPs were interviewed on their perceptions on the current role of the NCSC-NL and what this role ideally should be.

Main conclusions of this research are that: (1) public-private cooperations in cyber security are rather premature (2) roles in public-private cooperation in cyber security are not yet determined (3) roles in cyber security cooperation are fluid (4) defining roles in the cooperation means at the same time defining if and how organizations work together (5) the NCSC-NL should not or to a very small extent play a director role in public-private cooperation (6) the NCSC-NL should play a strong partner role in public-private cooperation (7) the NCSC-NL should play a facilitator role in public-private cooperation, however limited.

1. Introduction

On September 29, 2019 the Dutch headlines stated, "companies and public organizations vulnerable due to massive security breach" (NOS Nieuws, 2019: para 1). The Dutch government and more than hundreds of the largest companies in the Netherlands were seriously affected by this security breach. Security investigators disclosed that computer network systems had been vulnerable for months and researchers said that this breach was one of the most severe security issues ever seen in history (NOS Nieuws, 2019: para 3). While the vulnerabilities were already known for months, and the Dutch National Cyber Security Centre (NCSC-NL) had issued a notice on the harmful consequences of the breach, a large number of organizations ignored the warning and did not take any adequate measures (NOS Nieuws, 2019: para 3). As a consequence, many organizations in the Netherlands were vulnerable for cyber-attacks for months.

Due to the increasing digitalization, today's societies are more and more depending on information technologies. "From financial systems to trade, travel, health care, education and government, how we operate, survey and control our societies is now tied together through information technology" (Eriksson & Rhinard, 2009: 247). Yet, one of the consequences of the high interdependency of technologies connected is the increasing risk on cyber incidents which can bring along serious consequences for individuals, organizations and society. "Whether instigated by malicious actors or by accident, cyber incidents have the potential to cascade and seriously disrupt the provision of essential public services" (Boeke, 2017: 1). Disruption of community services can consequently have disastrous effects on society. According to Carr "it has implications for national security, the economy, human rights, civil liberties and international legal frameworks" (Carr, 2016: 43). Therefore, to avoid disruption through cyber incidents organizations protect themselves against cyber threats.

Today, keeping information technologies safe is of high concern for organizations and it is stated that "cybersecurity issues are becoming a day-to-day struggle for businesses" (Sobers, 2019: para 1). Most organizations understand the importance of cyber security and take adequate measures to safeguard their IT systems. However, protecting themselves from cyber-threats still remains challenging for many organizations. To meet today's cyber security

challenges, numerous organizations are therefore more and more working together with other organizations. In recent years, one can identify a growing number of collaborations in cyber security between the public and private sector. These collaborations are created to jointly create a more secure digital environment.

In the Netherlands, one of the main organizations involved in cyber security collaboration is the NCSC-NL which was founded in 2012 and is primarily responsible for keeping the Netherlands digital safe (Inspectie Veiligheid en Justitie, 2015: 10). The NCSC-NL is grounded on the principle of public-private cooperation and in this regard, it works closely together with multiple organizations from public and private sector. By collaborating with other organizations, the NCSC-NL aims to meet its mission to contribute to the increasing digital resilience of the Netherlands (NCSC, 2019: para 1). Since the creation of the NCSC-NL, the organization has been involved in a large number of Public-Private Partnerships (PPPs) in cyber security which are an important way for the NCSC-NL to work together and mutually share information with private and public organizations. "By information sharing 'we mean the exchange of a variety of network and information security related information such as risks, vulnerabilities, threats and internal security issues as well as good practice" (ENISA, 2010: 9).

Current collaborations in cyber security in the Netherlands are voluntary and based on trust and equality. "The Dutch institutional cyber landscape closely resembles a participant-governed network connecting public and private partners on a basis of trust and equality" (Boeke, 2017: 6). For this reason, it is important for the NCSC-NL to establish trust with private and public organizations. However, "building trust between public-private, private-private and public-public entities has been considered as one of the biggest challenges of PPP; eventually maintaining the same level of trust seems more challenging" (ENISA, 2017b: 5). Considering the large number of PPPs that the NCSC-NL participates in, it appears that today organizations have sufficient trust in NCSC-NL to work together. However, as in October 2019 the minister of Justice and Safety Grapperhaus said that the government must intervene with organizations that are lacking adequate digital security (Olsthoorn & Jonker, 2019: para 1), this changes the nature of public-private cooperation in cyber security. It is expected that intervention of the government will affect how and if organizations work together with the NCSC-NL.

Consequently, the role of the NCSC-NL might change. This raises the following research question:

'What role (director, partner or facilitator) should the National Cyber Security Centre (NCSC-NL) play in public-private cooperation in cyber security?'

The following three hypotheses are formulated to support the research question:

1. *NCSC-NL should play a director role in public-private cooperation in cyber security*
2. *NCSC-NL should play a partner role in public-private cooperation in cyber security*
3. *NCSC-NL should play a facilitator role in public-private cooperation in cyber security*

The research question will be examined based on the model of the Spectrum of Coalition Formation of Twynstra Gudde which distinguishes three different roles in collaboration; the director, partner and facilitator role. Looking at the current role of the NCSC-NL in PPPs in cyber security, this role is mainly supportive and initiating. However, in case the government gets the legal possibility to intervene with organizations it can be assumed that this role shifts more towards a supervisory role. As a consequence, the willingness of organizations to cooperate with the NCSC-NL can decrease or even end. When this happens, this will have considerable consequences for public-private cooperation in cyber security in the Netherlands.

In recent years, the cyber-threats in the Netherlands have rapidly increased. "Yet, the Netherlands, like many other European countries, faces high levels of cybercrime, industrial espionage, disruption of critical services, and other malicious cyber activities" (Hathaway & Spidalieri, 2017: 4). Private organizations as well as public organizations in the Netherlands are interesting targets for cyber criminals and "hackers are increasingly targeting state governments for their administrative capabilities" (Harkins & English, 2019). Attackers are frequently criminal organizations and foreign governments in search for valued information (Kooistra & Modderkolk, 2015: para 2). Cyber aggressors penetrate into information technology systems to damage the systems or hunt for data. On top of that, the attacks on Dutch digital systems are becoming "more aggressive and insistent" (Rosman, 2019: para 1).

Cyber-attacks can cause serious damage and immense disruptions or even destabilize society. Therefore, most nation states have set up a national cyber security strategy to protect their critical infrastructures. According to Carr "the importance of the internet to national economies makes the business sector a key focus in these strategies" (Carr, 2016: 50). The lack of digital trust can also negatively affect the economy. "If citizens and business owners lack confidence in security, it stands to reason that they may avoid participating in online activities, thereby inhibiting further development opportunities on cyberspace" (ENISA, 2014: 5). Therefore, to avoid chaos and resume continuity in a country and protect the economy digital protection is essential.

"The Netherlands is the digital gateway to Europe and an important data hub" (Ministry of Economic Affairs and Climate Policy, 2018: 16). The country aims to be a significant digital player in the world and creating a safe and secure digital environment is thus extremely important. To meet the cyber challenges of today and in the future, public and private organizations in the Netherlands increasingly consider cyber security as a joint mission and work together. Today, public-private cooperation in cyber security is an important instrument in fighting cyber-threats. The high interdependency of technical systems forces public and private organizations to work together. Public organizations often rely on private cyber security organizations for their skills and knowledge, while private organizations are depending on public organizations like the NCSC-NL creating the laws and setting the standards.

To add knowledge to the field of public-private cooperation in cyber security this research explores the role that the NCSC-NL plays in public-private cooperation in cyber security including four case studies. The results from these case studies will be combined with the theory to come to an advice that can be used to define roles for the NCSC-NL in public-private cooperation in cyber security. With interviews from representatives of public and private organizations, this research explores if there is any discrepancy between how the NCSC-NL perceives its role in public-private cooperation and how outsiders perceive this role. The methodology used of the case studies is further explained in Chapter 3.

This study is structured in the following way. This **first chapter** covers the introduction including the research question and hypotheses. The **second chapter** presents the theoretical

framework. First the meanings of cyber security and public-private cooperation are being defined. Thereafter an overview will be provided of the current Dutch cyber security landscape including most relevant parties. Then public-private cooperation in cyber security in the Netherlands will be explained. Next, the different roles in cooperation are described according to the model of the Spectrum of Coalition Formation of Twynstra Gudde. Afterwards, the knowledge gap and choice of theory are defined. In the **third chapter** the research design of this study is determined including the methodology and the empirical techniques used. **Chapter four,** includes the results of the four case studies. The **fifth chapter** provides an analysis of each case study as well as a general analysis of the current and ideal role of the NCSC-NL. Last, **chapter six,** covers the conclusion of this study including recommendations and the discussion.

2. Theoretical framework

This research fits into the study of security studies and focuses in particular on digital security with an emphasis on collaboration in cyber security between the public and private sector. It investigates the role of the NCSC-NL in public-private cooperation in cyber security. In this chapter, relevant existing theory will be discussed.

2.1 Definition of cyber security

In the literature there are various definitions of cyber security. Cyber security is often confused with other definitions such as information security or computer security. However, information security and computer security merely refer to network and computer processes while cyber security goes a step further. "Cyber security is used to refer to the integrity of our personal privacy online, to the security of our critical infrastructure, to electronic commerce, to military threats and to the protection of intellectual property" (Carr, 2016: 49). According to Carr cyber security can be defined as the protection of cyberspace and its users. Yet, this definition is rather broad. A more detailed definition of cyber security is given by Von Solms. He states that "cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets" (Von Solms & Van Niekerk, 2013: 97). Both definitions describe cyber security in such a way that cyber security includes all aspects of the protection of the cyber environment. Though, the definition of cyber security as suggested by Von Solms & Van Niekerk is leading in this research.

2.2 Definition of public-private cooperation

Public-private cooperation in the Netherlands is not a new phenomenon. "The Netherlands has a long tradition of collaborative relations between partners in the public, private, and civil society sectors, a tradition otherwise known as the 'Rhinelandic model', which characterizes relationships in North-Western Europe" (Koppenjan & De Jong, 2017: 2). However, "the concept of PPP became popular during a wave of de-bureaucratization from the late 1970s onwards" (Dunn-Cavelty et al, 2009: 180). Because many critical infrastructure organizations in the Netherlands are privately owned, public and private sector are frequently working

together. Arrangements made between public and private organizations are often captured in public-private partnerships. "A public – private partnership (PPP) is a long-term agreement/cooperation/collaboration between two or more public and private sectors that has developed through time in many areas" (ENISA, 2017: 7). These agreements are a useful mechanism in public-private cooperation to measure the effectiveness of the collaboration. The aim of this type of collaboration in cyber security is to achieve common goals and create benefit for all parties. According to ENISA there are five main drivers why PPPs are created: economic interests, regulatory requirements, public relations, social interests and new regulations (ENISA, 2017a: 11). Although public and private sector both have their motivations to work together "public-private policy partnerships have in common a shared responsibility for policy that impacts citizens" (Vaillancourt Rosenau, 2012: 12).

2.3 The Dutch cyber security landscape: public and private sector

In the Netherlands, a variety of public and private organizations are involved in protecting the society against cyber threats. However, the Dutch cyber security landscape is rather fragmented.

In the Netherlands, six out of twelve ministries are involved in cyber security matters (Government of The Netherlands, 2019a). The first Ministry is the Ministry of Defence (MoD) responsible for protecting the Netherlands from military cyber threats and external actors. "With a workforce of some 58,000, the Ministry of Defence is one of the biggest employers in the Netherlands" (Government of the Netherlands, 2019b: para 1). This Ministry protects the nation and maintains peace and security in the Netherlands. To protect the digital environment the MoD has established the Defence Cyber Command (DCC). The DCC focuses on three aspects of digital security: Defence, Intelligence and Offense. Defence, includes the protection of military systems against cyber-attacks and espionage. Intelligence focuses on digital internal and external threats. The DCC infiltrates in systems of third parties to collect information on cyber threats. Offense involves attacks of the army, manipulating or eliminating systems of opponents which can be foreign countries as well as (terrorist) organizations or hackers (Ministry of Defence, 2019a: para 2). Since the army is highly depending on information systems, cyber security is extremely important for the MoD. Failure or intrusion of information technology systems must be avoided, and security is therefore key. The Computer Emergency Response Team of the Ministry of Defence (DefCERT) is in charge of cyber security and their

responsibility is to provide reliable information technology systems and to make sure that military missions are not hindered (Ministry of Defence, 2019b: para 2). In its mission, DefCERT closely collaborates with other organizations like the NCSC-NL, the NATO Computer Response Capability (NCIRC), and inside the Forum of Incident Response and Security Teams (FIRST) (Ministry of Defence, 2019b: para 3).

Second Ministry involved is the Ministry of Economic Affairs and Climate Policy (EZK). "The Ministry promotes the Netherlands as a country of enterprise with a strong international competitive position and an eye for sustainability" (Governments of the Netherlands, 2019c: para 1). EZK is responsible for creating a strong and sustainable business climate wherein entrepreneurs can thrive and capitalize economic opportunities. Together with its partners, EZK works to maintain and improve the economic welfare of all Dutch citizens, today and in the future (Rijksoverheid, 2019: para 1). The ministry is focused on national and international collaborations and has an extensive network of cooperation partners. To support entrepreneurs in the digital environment, in 2018 EZK has launched the Digital Trust Center (DTC) to stimulate and facilitate entrepreneurs to independently or jointly work on their digital security (Digital Trust Center, 2018: para 1).

The third Ministry, the Ministry of the Interior and Kingdom Relations (BZK), is responsible for the protection of the democracy. "BZK stands for effective public administration and public authorities that the public can trust" (Government of the Netherlands, 2019d: para 2). Besides, BZK is in charge of the Dutch Intelligence services (AIVD) an important actor in cyber security in the Netherlands. The AIVD works closely together with the Military Intelligence Services (MIVD) and the National Coordinator of Security and Counterterrorism (NCTV) to provide insights to the government and public and private organizations on cyber threats and conceivable digital attacks (AGConnect, 2018: para 3). The close collaboration with MIVD has united in the Joint Sigint Cyber Unit (JSCU). In the JSCU, AIVD and MIVD share manpower and resources in the field of Signals Intelligence and other cyber activities (AIVD, 2019: para 7). JSCY aims to defend the country and the Dutch army from cyber threats.

Fourth Ministry is the Ministry of Foreign Affairs (BUZA) responsible for the coordination of foreign policy. "The Ministry of Foreign Affairs is the channel through which the Dutch

Government communicates with foreign governments and international organisations" (Government of the Netherlands, 2019e: para 1). The Taskforce Cyber of BUZA is responsible for the international strategy of the Dutch government and its mission is to create digital security and freedom worldwide (Nederland Wereldwijd, 2019: para 1). Until now, BUZA has been involved in several international cyber security initiatives in and outside the Netherlands and has hosted for instance the Global Conference on Cyberspace (GCCS) in 2015 (SSC-ICT, 2019: para 1). With the Taskforce Cyber, BUZA uses its international expertise to connect national and international cyber issues.

The fifth Ministry involved in cyber security is the Ministry of Education, Culture and Science (OCW). This Ministry plays an important role in cyber research and education. "Its mission is to ensure that everyone gets a good education and is prepared for responsibility and independence" (Government of the Netherlands, 2019f: para 1).

The last Ministry that has an essential role in cyber security is the Ministry of Justice and Safety (J&V). "The Ministry of Justice and Security is responsible for maintaining the rule of law in the Netherlands, so that people can live together in freedom, regardless of their life-style or views" (Government of the Netherlands, 2019g: para 1). J&V is in control of a safe and secure society and digital security is an important part. "The Ministry of Security and Justice coordinates national crisis management, although each ministry remains responsible for its own sector and leads when a crisis originates there" (Boeke, 2017: 5). J&V is also responsible for two important organizations tasked with cyber security matters. First is the National Coordinator of Security and Counterterrorism, responsible for policymaking in cyber security. "The National Coordinator for Security and Counterterrorism (NCTV) coordinates the fight against terrorism in the Netherlands" (NCTV, 2019b: para 1). Second is the NCSC-NL which was until 2011 named the Dutch Government Emergency Response Team (GovCert) and used to be part of the NCTV. Though, in 2011 the GovCert changed into the NCSC-NL. "The National Cyber Security Centre (NCSC) is a joint venture between government bodies and business enterprises aimed at forging an integrated approach to cyber security" (NCTV, 2019c: para 4). The NCSC-NL is responsible for the execution of the cyber security policy created by the NCTV. "The centre focuses on developing and offering expertise and advice, supporting and implementing response to threats or incidents and strengthening crisis management" (Government of the Netherlands, 2019h: para 1). As of January 2019, the NCSC-NL became

an independent organization of the Ministry of Justice and Safety, although it still gives account to the NCTV (NCTV, 2019d: para 3).

The NCSC-NL has an important role in the Netherlands in the digital protection of information technology systems of its critical infrastructures and governmental organizations. The organization works closely together with many public and private organizations and has a unique position in cyber security collaboration. One important instrument of the NCSC-NL in cooperation with the public and private sector are Information Sharing and Analysis Centres. "Information Sharing and Analysis Centres (ISACS) are non-profit organizations that provide a central resource for gathering information on cyber threats (in many cases to critical infrastructure) as well as allow two-way sharing of information between the private and the public sector" (ENISA, 2017: 7). ISACS serve as a trusted platform and have an important role in information sharing in cyber security between the public and private sector. "The role of Information Sharing and Analysis Centers is particularly important in creating the necessary trust for sharing information between private and public sector" (ENISA, 2107a: 11).

The first ISACs were founded in the Unites States after the first terrorist attacks on the World Trade Center in 1993 and Oklahoma City in 1995 (ENISA, 2017a: 7). After these attacks the potential for collaboration between the public and private sector became more important for the US government. "One of their recommendations was to establish Information Sharing and Analysis Centres (ISACs), so as to build and strengthen cooperation between public administration and the industry" (ENISA, 2017a: 7). It is proven that the establishment of ISACs in the US and the creation of multiple collaborations between the public and private sector contributed to an increased level of cyber security. "Analysis of twenty years of US experience indicates that ISACs are effective and can scientifically enhance the level of cyber security" (ENISA, 2017a: 7). Following the US, ISACs have also been established in the Netherlands. The first ISAC, the FI-ISAC, was established in 2003 by a group of Dutch banks. In 2016 several public organizations also joined the FI-ISAC (Betaalvereniging Nederland, 2019: para 1). The FI-ISAC has set an example for other sectors in the Netherlands which have now also established their own ISACs.

Thus, most important actors in the public sector in the Netherlands involved in cyber security matters are the MoD, EZK, BZK, BUZA, Ministry of Education, Culture and J&V. Below an overview of the public cyber security landscape in the Netherlands.

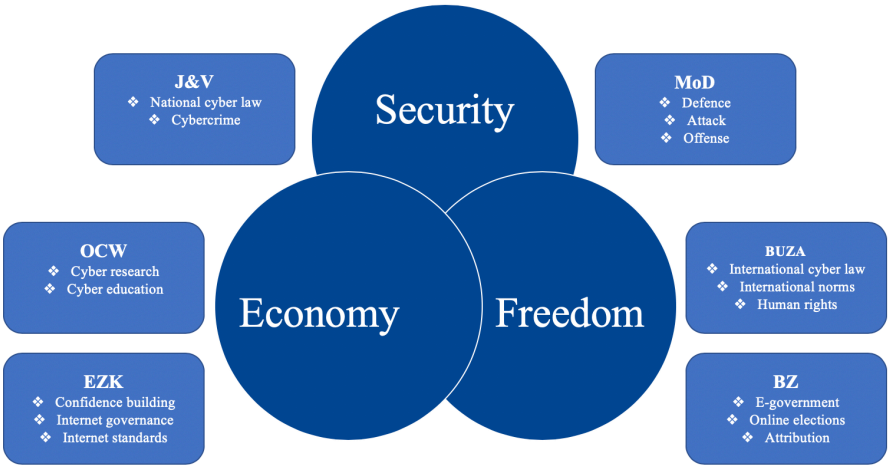


Figure 1 - Key players in cyber security in the public sector in the Netherlands

Next to the public sector, the private sector in the Netherlands also plays an essential role in cyber security. It is estimated that there are nearly 3.500 companies in the Netherlands providing technical and non-technical cyber security solutions. Due to the growing demand for cyber security products and services, the number of solution providers is rapidly increasing. There is a clear categorization between technical and non-technical products and services in cyber security. Below an overview of the division of products and services in the private sector.

Figure 2 - Variety of providers in cyber security in the private sector in the Netherlands

2.4 Public-private cooperation in cyber security in the Netherlands

Until 2011, cyber security was not yet a priority of the Dutch government. However, that changed after the Diginotar case in 2011 when the company got hacked by an Iranian hacker and the digital security of the Dutch government was at stake for more than a month. It is stated that an old website and outdated software was the reason why the hacker could easily enter the IT systems of DigiNotar (Nu.nl, 2012). The consequences of the Diginotar hack could have been enormous and to manage the issue the private sector was called for help. On August 2011, private security company FOX-IT was brought in by DigiNotar to investigate the matter (Prins, 2011: 3). Afterwards the government start realizing that they should take adequate measures to protect the digital safety of the nation and prevent this from happening again.

Due to privatization and deregulation, most critical infrastructures in the Netherlands are owned and operated by private companies. According to Dunn-Cavelty “one of the key challenges for such protection efforts arises from the privatization and deregulation of many parts of the public sector since the 1980s and the globalization processes of the 1990s, which have put a large part of the critical infrastructure in the hands of private enterprise” (Dunn-Cavelty et al, 2009: 179). For this reason, security of critical infrastructures is not solely a task for the public sector anymore. Although “the state is understood to be responsible for the provision of security,

especially national security" (Carr, 2016: 54) it cannot control information technology systems of privately-owned companies. Though, attacks on the systems of national banks, energy companies, airports, or telecom can have tremendous impact on the national security of a country because in today's digitalized world cyber security plays an integral part of the security provision. Consequently, public and private sector in the Netherlands work closely together in the provision of cyber security.

The private sector has several reasons to participate in public-private cooperation. First reason is access to public funds (ENISA, 2017b: 13). PPPs are often (partially) financed by public institutions and participation in a PPP, can financially benefit private organizations. Second reason is the "opportunity to influence national legislation and obligatory standards" (ENISA, 2017b: 13). Working closely together with public organizations means short lines to the government and possibility to influence legislation. Besides, it can also mean easy access to (confidential) knowledge and information. Last reason is that the products and services provided by PPPs are of decent quality guaranteed by the government (ENISA, 2017b: 13).

The reasons for the public sector to join PPPs are rather different. Working with the private sector brings along "better understanding of Critical Infrastructure information Protection (CIP) and industry in general" (ENISA, 2017b: 13). Without public-private cooperation, the public sector has little understanding of the cyber security market. Close collaboration with the private sector increases the available knowledge and information for the public sector. Another reason for the public sector to participate in PPPs is the "possibility to create synergies between different initiative of the private sector" (ENISA, 2017b: 13). As a neutral party the government has the opportunity to bring together private organizations. Last reason is the "access to private actor resources (e.g. valuable experts) which makes it easier to set up standards and good practices" (ENISA, 2017b: 13). The private sector is generally better equipped and has certain expertise and skills that the public sector is in general lacking.

However, there are also numerous reasons why parties are mutually motivated to work together. One important motivation for public as well as private organizations to work together in PPPs is the mutual responsibility to digitally protect the nation. This connects to the motivation "helping to achieve resilience in the cyber ecosystem" (ENISA, 2017b: 13). Additionally,

ENISA states that both sectors join to "sharing knowledge, experiences and good practices" (ENISA, 2017b: 13). The idea is that all parties benefit from the knowledge, experiences and good practices shared in PPPs. Also, information otherwise difficult to get, becomes accessible in PPPs. Another mutual incentive is the network and easy access to reliable contacts in other organizations (ENISA, 2017b: 13). Moreover, the network built in PPPs is extremely valuable for parties. Next motivation is to "increase the trust between public-public, private-private and public-private – PPP allows to meet different people and get to know them; because of that, it allows to have better information and proactive attitude in case of crisis" (ENISA, 2017b: 13). Trust between parties is built inside a protected environment of the PPP.

2.5 Roles in cooperation

Public, private and civil organizations all have their unique visions and values with relevant issues in society (De Jong, 2015: 2). Combining the different visions and values with skills, knowledge and expertise in cooperations can help strengthen the approach to these issues. Coalitions, a group formed of different organizations or people who agree to act together, usually temporarily, to accomplish something (Cambridge dictionary, 2019), are created to jointly achieve common goals. Together parties can achieve more than alone. It is therefore important to form coalitions with other parties. Coalitions are about interaction (interests, values, relations and emotions) and collective meaning (knowledge, creativity, experience and design) (De Jong, 2015: 3). However, working together in coalitions requires certain basics. The National Democratic Institute defined several ingredients of successful coalitions: the coalition must be advantageous for all parties, there must be mutual respect and understanding between the parties, the willingness to compromise and a sense of partnership (NDI, 2004: 1). Lacking one or more of these elements, can influence the coalition.

According to the theory of the Spectrum of Coalition Formation, three different coalitions are distinguished: directive coalitions, collective coalitions and connective coalitions (De Jong, 2015: 3). Different roles adhere to each coalition respectively the director, partner and facilitator role. With different backgrounds each coalition partner has a particular role to play in the cooperation.

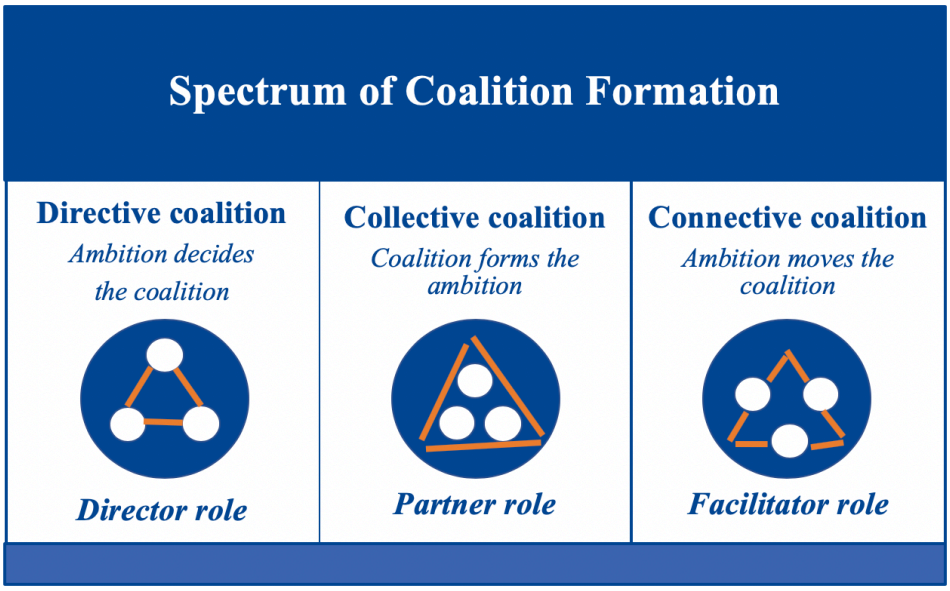


Figure 3 - Spectrum of Coalition Formation based on the model of Twynstra and Gudde

2.5.1 Director role (directive coalition)

In a directive coalition it is usually one or only a few organizations that have a clear ambition that they are willing to realize in coordination with others, from a directing role in an existing arena of stakeholders (De Jong, 2015: 4). In other words, one actor or few actors have an ambition and to perform this ambition collaboration with others is limited. This type of coalition formation is suitable for government interventions or desired by specific organizations and for a large part determined and paid for (De Jong, 2015: 4). Ownership is restricted and only a few parties make the decisions and decide on the direction to realize the ambition. One benefit of this type of coalition is that the directing actor or actors can steer in a structured way which leads to better and faster results than if they would do the same without the forming of a coalition (De Jong, 2015: 4). In this coalition there are clear predominant actors that determine in what way the collaboration is set up and performed. Only one or few parties are in charge and other parties need to follow their lead. Stakeholders will come to a compromise for strategic reasons, without a clear win-win situation or a sustainable solution for the issues (De Jong, 2015: 5). The director role in cooperation is born out of the directive coalition.

2.5.2 Partner role (collective coalition)

The collective coalition is strongly based on the principle of equal partnership. Organizations are partners in a new arena of parties that complement each other, and every party contributes to and benefits from the common ambition in the cooperation (De Jong, 2015: 6). The ambition is created and performed together. In this type of coalition there is a group of organizations that all share the same ambition. An important benefit of this coalition is that participants have an equal sense of ownership and responsibility (De Jong, 2015: 6). As an equal partner each organization gives and takes in the cooperation. In comparison to the directive coalition wherein parties are stakeholders, in the collective coalition the parties are shareholders rather than stakeholders (De Jong, 2015: 6). For governmental parties, however, this type of coalition is rather challenging. Due to its legal powers and responsibilities for the common good, the government is not completely used to work on the basis of equality (De Jong, 2015: 7). In collective coalitions the partner role is assigned to the role in the cooperation.

2.5.3 Facilitator role (connective coalition)

Last coalition is the connective coalition. To feed their own ambition organizations choose to facilitate the collaboration that spontaneously started by the coalition (De Jong, 2015: 8). The initiative to cooperate started with the initiative of one or few organizations but the coalition is open for anyone to join the coalition. There is a flexible ambition and all organizations have the opportunity to bring in ideas or thoughts regarding the ambition. The aim of this type of coalition is to jointly build an initiating network that has serious impact (De Jong, 2015: 8). There is a group of individual organizations that together can create impact where this individually would be difficult. The network is thus constantly changing and growing and built on intrinsically motivation and voluntary services (De Jong, 2015: 9). The coalition as well as the ambition are continuously changing. One of the main challenges in this coalition is the voluntary nature of the collaboration. To solve this issue existing organization can play an assisting role to facilitate the cooperation. Facilitation by these existing organizations can exist of financial support, but also with expertise, capacity, network or media attention (De Jong, 2015: 9). The role in this coalition is therefore determined as the facilitator role.

2.6 Knowledge gap

In the literature on public-private cooperation in cyber security the majority of the studies mainly contain data on how PPPs in cyber security have been created and implemented out of national cyber security strategies, on the motivations of parties to work together and on barriers and incentives of cooperation. Several researches were conducted on public-private mechanisms like PPPs and Information and Analysis Sharing Centres (ISAC) and how these mechanisms have been created and performed. Besides, some scholars have investigated the division of power in cyber security which adds theory to the body of cyber security governance. In the existing literature there is only limited data on the division of roles in public-private cooperation in cyber security, what makes sense since the topic is relatively new. However, considering the increasing importance of cyber security and the fast-growing number of cyber security initiatives it is crucial to further explore public-private cooperation in cyber security and in particular the division of roles in the cooperation. Because public-private cooperation in cyber security has a variety of parties involved it would be useful to capture and formalize the roles in the cooperation. This research specifically focuses on the different roles in cyber security cooperation and herewith adds knowledge to the body of cyber security cooperation.

2.7 Choice of theory

This study is built on the model of Spectrum of Coalition Formation of Twynstra Gudde. This model suggests three types of coalitions in cooperation; the directive coalition, collective coalition and connective coalition. Each coalition has its own role. In the directive coalition this role includes the director role, in the collective coalition it includes the partner role, and in the connective coalition it includes the facilitator role. The model shows how coalitions are formed and allows to classify different roles in cooperation structures and is extremely useful in defining different roles in cooperation. Furthermore, this research includes additional theories. Sub theories used in this research are the theory of Carr on public-private cooperation in national strategies and the theory of Dunn-Cavelty on public-private cooperation in cyber security.

3. Research design

This chapter covers the research design of this study. In the previous chapter, the theoretical framework has been explained. The Spectrum of Coalition Formation is used as the main theory to answer the following research question:

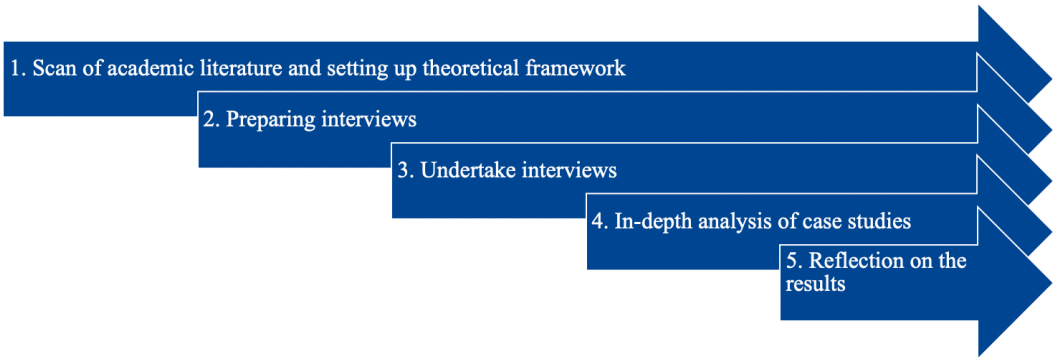
What role (director, partner or facilitator) should the National Cyber Security Centre (NCSC-NL) play in public-private cooperation in cyber security?

The research question is supported by the following three hypotheses:

1. *NCSC-NL should play a director role in public-private cooperation in cyber security*
2. *NCSC-NL should play a partner role in public-private cooperation in cyber security*
3. *NCSC-NL should play a facilitator role in public-private cooperation in cyber security*

The research strategy of this study is based on multiple case study research. Various cases are analyzed and compared to take lessons for the future. An important benefit of the different case studies is that connections can be made between the different cooperations. At the same time, the variety of cases makes it possible to describe and compare different public-private cooperations in cyber security.

The research is divided in five stages: **(one)** scan of academic literature and setting op the theoretical framework, **(two)** preparing interviews, **(three)** undertake interviews, **(four)** in-depth analysis of case studies, **(five)** reflection on the results.



3.1 Methodology

This study is deductive and uses a qualitative methodological approach. Current data forms the basis of the study and additional data will be added to the existing theory. To collect data a combination of three empirical techniques are used.

- **Desk research**

  The data collected through desk research contains useful data for this study. This information is publicly available and contains a variety of documents like policy papers, newspapers, and legislation documents.

- **Literature review**

  The literature review is an examination of the academic literature used for the theoretical framework in this research. For the literature review a variety of academic papers are used.

- **Semi-structured interviews**

  In this study, semi-structured interviews are used to support the theory. The data collected through the interviews will be analyzed and then linked to the theory.

3.2 Case selection

In the selection of the different case studies the researcher has selected four public-private cooperations in cyber security with NCSC-NL involvement. Criteria used to select these cooperations:

- The PPP in cyber security already exists
- The NCSC-NL works closely together with the collaboration partner in the PPP

From each cooperation one respondent of the NCSC-NL was selected and one respondent of the collaboration partner. Criteria for the respondents are:

- The respondent works for NCSC-NL or the collaboration partner
- The respondent needs to be closely involved in the PPP on the side of the NCSC-NL or the collaboration partner
- The respondent speaks Dutch

Next a longlist of ten potential respondents was created by the researcher whereof eight respondents have committed to the research. The respondents have been approached via the network of the researcher.

3.3 Data collection

The data collected in this study is information obtained by existing data supplemented with data from semi-structured interviews as explained in the methodology to be able to compare and create a variety of data. In total eight interviews are conducted with respondents from four different PPPs. If necessary, more or other stakeholders will be included.

To conduct the semi-structured interviews, a questionnaire is prepared in advance which includes questions to determine the perception of the respondents on the current and ideal role of the NCSC-NL in the particular PPP. Prior to the interview, each respondent is informed on the process and asked for a written permission to record the interview.

3.4 Measurement

The respondents of this research are asked for their perception on the cooperation in the PPP and in particular on the current and ideal role of the NCSC-NL. On a scale of 0 to 10, respondents can express their view on how strong or weak they perceive the current and ideal role of the NCSC-NL in the cooperation. The independent variable are the three defined roles, director, partner and facilitator role. The dependent variable is the cooperation.

3.5 Data Analysis

The researcher uses sound recordings to make the transcriptions. Afterwards the transcripts are converted by the researcher into readable narratives. These narratives are then used to make an analysis and to get insights in the collected data. “Here, analysis is necessary from the start because it is used to direct the next interview and observations” (Corbin et al, 1990: 6). The results are first compared within each case study and then the four case studies are mutually compared. The analysis of the data is based on the main theoretical concept of this study.

3.6 Outcomes

This study aims to track down the different perceptions of respondents on the ideal and the current role of the NCSC-NL in cyber security cooperation. The literature supplemented by the narratives are the basis for the conclusion.

3.7 Limitations

This study contains several limitations which are explained below.

- **Reliability**

  The use of multiple case studies means per definition loss of reproducibility. To reproduce this research, the same cases must be used, however the reality for the cases might be subject to change over time. This can affect the outcomes of the research.

- **Validity**

  The validity of this study has the following limitations:

  - **One researcher**

    Because there is only one researcher involved in this study this affects the impartiality of the research. To increase the validity, it is preferred that the data is analyzed by at least two different researchers. Hereby, the results do not only depend on the interpretations of just one researcher as is the case now.

  - **Limited number of cases**

    A high number of cases is preferable to guarantee the validity. However, the current number of PPPs in cyber security is still limited. Therefore, although the number of cases in this research is rather limited it can be thus considered as sufficient to validate the research. However, increasing the number of cases will also means increasing the validity.

- **Different interpretations**
  Because the respondents have different frames of references, they might have a different interpretation of the questions asked while the questions are the same for all respondents. To avoid this, the respondents are asked to give a score on a scale of 0 to 10.

To increase the internal validity of the research a combination of literature and semi-structured interviews is used.

Other limitations:

- **Restricted timeframe**
  This research was performed in a relatively short time.

- **Limited data**
  Because cyber security and PPPs in cyber security is relatively new, data available on the topic is still limited.

4. Results - Four cases studies

4.1 Cooperation 1: NCSC-NL and Information Sharing and Analysis Centre (ISAC)

Background Energy-ISAC

In the Netherlands, there are numerous Information Sharing and Analysis Centres (ISACs) representing various sectors. One of these ISACs is the Energy-ISAC led by a chair and co-chair coming from one of the participating energy organizations. In the Energy-ISAC representatives from different energy organizations, vital and non-vital organizations, are participating. To join the ISAC, potential members need to sign the membership guidelines. Request for participation will requested of the other members of the ISAC and without any objection of these members potential members are allowed to join the ISAC. Members of the Energy-ISAC are meeting six times per year to share information and mutually exchange knowledge on cyber security related issues. In each ISAC meeting, presentations will be given that are relevant to the sector and information on cyber incidents is mutually shared to learn from each other.

Background NCSC-NL

Currently, the NCSC-NL is involved in 16 different ISACs. One of these ISACs is the Energy-ISAC and within the Energy-ISAC the NCSC-NL is tasked with the role of secretary. The secretary works together with the chair and co-chair of the ISAC in preparing the ISAC meetings and put together the agenda. This role is done by the Energy Account Manager of the NCSC-NL responsible for the interaction between the NCSC-NL and the energy sector. This way, the NCSC-NL tries to keep in close connection with the energy sector. For the sector this is also helpful because of the close connections with the Dutch government. Besides, NCSC-NL also supports in facilitating the meetings. The ISAC meetings are usually hosted by one of the organizations but organized by the NCSC-NL. The NCSC-NL sets the dates for the meetings and sends the meeting invitations to the ISAC members. It also sends the membership guidelines to potential members and supports in administrative tasks.

Introduction respondents

- ***Security Officer at Stedin - Thom Spitzen***

Since 2018 Thom Spitzen works as Security Officer at Stedin where he is responsible for incident management and penetration testing. Without technical background his focus is on the organizational processes of cyber security. Thom has been a member of the Energy-ISAC since June 2019. Working as a Security Officer for Stedin, Thom works closely together with other partners and organizations within the energy sector. An example is ISIDOOR, the national cross-sectoral crisis simulation of the NCSC-NL, where Thom functioned as an important player and as a frontrunner from Netbeheer which is according to Thom also a small cooperation structure to mutually share information. Thom has many contacts in the field and works closely together with the cybercrime team of the Dutch police. Thom participated in this research because he believes that this type of researches is there to help to improve current collaborations.

- ***Coordinator Vital Organizations at NCSC-NL - Mireille Kok***

After working in the private sector and working in the cultural sector, Mireille joined the NCSC-NL in August 2019. Mireille Kok is coordinator for the vital or private organizations of the NCSC-NL. Mireille coordinates a group of eight account managers that are all responsible for one or two sectors. The account managers are representing the NCSC-NL in their particular sector(s) and share the products and services with the sector and are the main point of contact of the NCSC-NL for the sector. Mireille has a focus on collaboration and lot of knowledge in the field of marketing and communication. Mireille believes that this study on the role of the NCSC-NL, helps her and the organization to be more strategic in collaborations. She sees this research as a useful way to examine the current role of the NCSC-NL in recent collaborations and to explore if this role should be different.

Cooperation coalition

Considering the model of Spectrum of Coalition Formation of Twynstra and Gudde and the cooperation between the Energy-ISAC and the NCSC-NL, Thom believes that the current role of the NCSC-NL in this cooperation is mainly the partner role. In his opinion private organizations are facing the cyber incidents and can therefore share information with the NCSC-NL that also receives information in other ways and from sources like the intelligence

services and other European sources. The NCSC-NL shares additional information with private organizations to support them. Thom believes that this way of working is focused on partnering rather than facilitating. He points out that the composition of the coalition is determined prior to the collaboration, due to the fact that most organizations are vital and because of the introduction of the Directive on Network and Information Systems (WBNI). The ambition is already determined. According to Thom, a director role for the NCSC-NL is not desirable because working together on equal levels helps accelerate organizations. Besides, information shared between the organizations is very sensitive and a director role is considered as an obstacle, especially since the NCSC-NL is a governmental organization.

Mireille thinks that the NCSC-NL currently has a strong facilitating role in the Energy-ISAC because it is mainly involved in the administrative organization of the ISAC. However, her concern is that if the NCSC-NL will not take this role, it can be questioned whether the sector and also which organization will take over this role. However, Mireille also sees the role of the NCSC-NL in the ISAC as an essential way to set the agenda and as an important channel to mutually share information with the sector. Thus, she thinks that the NCSC-NL has therefore also, while limited, a director role. Mireille regrets that the ISAC members do not seem to consider the NCSC-NL in the partner role. Concerning the role of the NCSC-NL, Mireille raises the question on how itself the NCSC-NL wants to fill in this role. In her opinion the NCSC-NL did not yet carefully think through its role in the ISACs and the next stage of the collaboration. The NCSC-NL was involved in establishing the ISACs in the Netherlands, but does it still have a relevant role? And if so, what role? She questions whether the ISACs contribute enough to the ambition of the NCSC-NL.

Benefits cooperation

Thom identifies several benefits of this cooperation. First and most important benefit is equality of the organizations. Each collaboration partner benefits from the cooperation. This is also an important incentive for ISAC members to participate. Lacking incentives means that organizations will no longer attend the ISAC meetings. However, Thom believes that it does not matter which role, director or partner role the NCSC-NL has, as most important fact is that organizations benefit from participation in the cooperation. He thinks that as long as organizations get advantage from it, they will show up. Thom states that most important benefit

is mutual information sharing. In addition, Mireille adds some other benefits to this cooperation besides information sharing. She sees the variety of organizations sitting at one table as an important benefit. The NCSC-NL participation in the ISAC is of great importance especially during cyber incidents. ISACs are an easy way to swiftly connect with each other. Besides, it is extremely helpful to know the relevant people inside the organizations. This is especially useful in times of crisis. Yet, Mireille considers the cooperation with the ISACs not only as an easy way to share information, but also as an important way to meet the mutual ambition to keep the Netherlands digital safe.

Disadvantages cooperation

Nevertheless, both respondents also see disadvantages in the cooperation. Mireille thinks that NCSC-NL lacks knowledge about its cooperation partners. She states that the NCSC-NL needs to know better what systems organizations use and how their business models look like. At this moment there is still a lot to gain for the NCSC-NL. Another disadvantage according to Mireille is that facilitating the ISACs is extremely time-consuming for the NCSC-NL and it can be questioned whether the cooperation brings enough advantage. Capacity is limited and the NCSC-NL should make choices in where to spend its time on. In addition, not every ISAC is very efficient and for some ISACs, the meetings are more a tea party. Mireille wonders what the results are of these meetings for the NCSC-NL. What is the NCSC-NL getting out of it? Furthermore, she believes that the ISACs belong to the sector so why should it be the ambition of the NCSC-NL? She states that it might be better to look at the mutual ambition instead of the ambition of the ISAC alone. This way, the NCSC-NL can also increase its partner role and reduce its facilitator role. Thom sees as one of the main disadvantages in this ISAC's cooperation that it is extremely hard to make decisions. Collaboration is based on consensus and for this reason it will cost time to realize things. For instance: The Energy-ISAC tries to set up new directives, but which are hard to finalize. Another difficulty is that participation of organizations is now limited and not every organization can join the coalition. Although, Tom points this out as a disadvantage he also sees this as a benefit because due to this limitation it is said that only organizations with the same interests can join.

Goals and focus cooperation

In the goals of the cooperation both respondents are somewhat aligned. Thom and Mireille believe that information sharing is the most important goal of the cooperation. Another goal is to know each other and meet in person on a regular basis. Additionally, Mireille mentions that another aim is to know what is going on in the sector. The cooperation focuses on cyber security in the energy sector. This is also the main reason why the Energy-ISAC was created. It is a significant way to share developments and exchange political and legal knowledge in our field. Though, Mireille questions if the principal goals, making organizations cyber resilient, can be met through the ISACs. It is helpful to know what happens with other organizations and what you can do as an organization. This information can be used by organizations to make their own organization more cyber resilient. However, Mireille thinks that currently this is not a clear purpose, but an indirect ambition.

Role selection

Considering the three determined roles, director, partner and facilitator, the opinions of both respondents differ. Thom believes that in the current situation the director role is very limited, while Mireille sees more purpose for a stronger director role for the NCSC-NL. According to Mireille, the partner role of the NCSC-NL is currently very limited, but the facilitator role is extremely high. In Thom's opinion the partner role is medium, and he agrees with Mireille that the facilitator role is rather high. In the ideal situation, Thom perceives the director role of the NCSC-NL as very low and the partner role extremely high. He primarily considers the NCSC-NL as a partner. Although Thom also comments that the current facilitator role of the NCSC-NL is very useful because the NCSC-NL is making all the arrangements for the ISAC. For this reason, he gives a high score for the facilitator role. In case the NCSC-NL will not facilitate the ISAC as they do know, he believes that the ISAC should be supported by the cooperation community. But Thom also adds that in this case the ISAC will probably be carried by the Netbeheer group. However, Thom also states that in this situation, The NCSC-NL is not just necessarily part of the ISAC anymore and can then only attend if they have anything relevant to share with the other members. In the ideal situation Mireille desires a much stronger partner role for the NCSC-NL. She prefers not to have a facilitator or director role in this cooperation at all.

Thom works closely together with the NCSC-NL and he considers the NCSC-NL is a real partner. He points out that he and his colleagues connect with the NCSC-NL on a regular basis but suggest that this should be also done with the ISAC more often. Thom continues that the ISAC members have information and the NCSC-NL has information and he believes that this information must be mutually shared. Even more than it happens now. In his opinion, organizations are still a bit reluctant to share information but since all organizations have the same goal, which is making the Netherlands cyber resilient, he strongly believes in a partner role for the NCSC-NL. In case the NCSC-NL will get a mandate for a more supervisory role such as suggested by Minister Grapperhaus, the role of the NCSC-NL will be more a director role. In Thom's opinion, this is not a good development since there already is a supervisory authority in the energy sector. Currently, working together and sharing information in the ISAC is based on mutual trust, but with a supervising organization participating in the ISAC, this mutual trust will most likely stop. Nonetheless, Thom states that a supervisory role is not the same in his opinion as a director role. On the other hand, Mireille thinks that the director role is implicitly fulfilled by the NCSC-NL anyway, because they make the decisions. The partner role is filled in by the NCSC-NL in a very limited way because the ISAC is from the sector and according to Mireille, at this moment the ISAC members do not perceive the NCSC-NL as a full partner.

Concluding, Mireille believes that the current ambitions of the cooperation should be reformulated. What will be the mutual ambition of the ISAC and the NCSC-NL? She states that the collaboration between the NCSC-NL and the ISACs should be restructured. Important is to focus more on an equal cooperation relationship. Another possibility is that the NCSC-NL reduces its capacity in the ISACs. The NCSC-NL should find a way to get more knowledge whilst lowering the capacity. Currently, this is not balanced according to Mireille. Thom concludes by saying that he hopes that the NCSC-NL and the Energy-ISAC will continue to work together in the future. He sees the role of the NCSC-NL in the ISAC as very useful.

4.2 Cooperation 2: NCSC-NL and Digital Trust Center (DTC)

Background Digital Trust Center

In 2018, the Digital Trust Center (DTC) was established by the Dutch Ministry of Economic Affairs and Climate Policy (EZK). The Digital Trust Center supports entrepreneurs in safe digital entrepreneurship (Digital Trust Center, 2019: para 1). The Digital Trust Center is a program of the Ministry of Economic Affairs and Climate Policy that stimulates and facilitates cooperation in cyber security between public and private sector. The program concentrates on the digital resilience of all businesses other than the critical infrastructures. The target group of the DTC exists of 1.8 million companies: from freelancers to big businesses (Digital Trust Center, 2019: para 2). To meet its mission, to prepare entrepreneurs against cyber threats and make them resilient, the DTC promotes and stimulates collaboration between different networks to increase the cyber resilience of entrepreneurs in the Netherlands.

Background NCSC-NL

The NCSC-NL works closely together with the DTC that falls under the responsibility of the Ministry of Economic Affairs and Climate policy (NCSC, 2019: para 3). DTC and the NCSC-NL are important partners in the field of cyber security. The NCSC-NL provides the DTC with important cyber security information to make the target group of DTC digital cyber resilient. "The DTC largely draws on the high-quality expertise of the National Cyber Security Centre (NCSC-NL), part of the Ministry of Justice and Security" (Ministry of Economic Affairs and Climate Policy, 2019). The NCSC-NL has a dedicated account manager responsible for the NCSC-NL and DTC the cooperation.

Introduction respondents

- ***Relation Manager at DTC - Jacco van der Kolk***

  Since April 2018, Jacco van der Kolk works with the DTC as relationship manager after working in sales for many years. Jacco is responsible for maintaining the external relationships for DTC including the collaboration with the NCSC-NL. Jacco participates in this research because he is very curious to what the results will be. According to Jacco, this study fits into the goals of the DTC and can be extremely useful in serving entrepreneurs in The Netherlands.

- ***Account Manager at NCSC-NL - Kees Boerkamp***

  Kees Boerkamp joined the NCSC-NL in February 2019 where he works as a senior advisor responsible for external relationships. His portfolio includes the DTC account as well as some other governmental accounts such as the Ministry of Interior Affairs and External Affair. Kees has a lot of experience in public-private cooperation but mainly on the physical side of safety and security. Kees participates in this research, because he is interested in how people and organizations work together to reach a certain goal. He believes that all parties aim for the same goals, but from different perspectives. It is therefore important to get a clear overview of the different interests and to explore how a win-win situation for all parties can be created.

Cooperation coalition

Considering the three roles of the Spectrum of Coalition Formation, Kees believes that the role of the NCSC-NL in the cooperation between the NCSC-NL and DTC is mainly a partner role. To a lesser extent, he sees the NCSC-NL in the facilitator role. In his opinion the director role is barely present in this cooperation. This applies specifically to this cooperation. In case of the NCSC-NL organization as a whole, Kees thinks that all roles of the Spectrum of Coalition Formation are applicable. According to Kees, in the DTC cooperation the emphasis is clearly on the partner role and in a lesser effect on the facilitator role. He states that the director role should only be deployed in case the national security is at stake and parties have no information on what is really happening. When this occurs, and the government must take measures because of security reasons, the director role is required. But only in this situation.

Jacco on the other hand believes that the current role of the NCSC-NL is a strong director role. However, he also mentions that the cooperation is in an early stage and both parties are still looking what their role is and how they can support each other. Jacco thinks that the three roles as mentioned by the model of Spectrum of Coalition Formation are too far crystallized. Though, he strongly tends to the director role. His argument is that it is not necessarily a choice, but it is the result of a natural process. The intentions of both parties are different, and this affects the cooperation. The different backgrounds of both organizations are an important reason. DTC falls under the Ministry of Economic Affairs and Climate Policy and the NCSC-NL falls under the responsibility of the Ministry of Justice and Safety. The latter is strongly focused on

information and is particularly careful in sharing its information whilst the Ministry of Economic Affairs aims to share its information as much as possible. The discrepancy in organizational motivations makes it extremely difficult to determine and agree what can be actioned and what cannot be actioned and by whom. One should better think this through in this cooperation. In addition, in some cases on the one side the NCSC-NL has also a great willingness to share information whilst on the other side Economic Affairs can be sometimes very careful in sharing information. Finding an optimal solution has been difficult so far.

Benefits cooperation

Both respondents see several benefits of the cooperation. Kees sees the knowledge and experience of the NCSC-NL as one of the main benefits. The NCSC-NL has much more cyber security knowledge and experience than the DTC. For this reason, it could be more facilitating in the cooperation. Jacco agrees with Kees that the knowledge of the NCSC-NL is important for the DTC. Knowledge and expertise of both parties is combined in this cooperation. Because the government has subsidized the NCSC-NL and DTC to make the Netherlands digital resilient, DTC also happily uses the acquired NCSC-NL knowledge. Another benefit is that in contrast to the NCSC-NL, DTC has direct access to businesses in the private sector. DTC can therefore support the NCSC-NL in approaching these businesses to make all organizations in the Netherland cyber resilient. Also, working together means that a larger group of businesses can be reached. Since the NCSC-NL focuses exclusively on the critical infrastructure and government organizations, working together with DTC offers them the opportunity to reach organizations that they would otherwise not reach. Though, Kees states that in his opinion this must go a step further than it happens now, but 'legalization of society' makes it difficult sometimes to take certain actions. According to Kees, one should take more risks instead of letting legislation being an obstacle. Last benefit in the cooperation is according to Jacco the physical close proximity of both organizations which he sees as truly helpful in the cooperation.

Disadvantages cooperation

Next to the benefits, the respondents also see some disadvantages in the current cooperation. Jacco believes that it is sometimes more a fight rather than a collaboration, but he sees this as one of the risks of cooperation in general. Besides, one of the current shortcomings in the cooperation is that both parties are still in search for their mutual ambitions. DTC's main

mission is to make businesses in the Netherlands safe whilst the NCSC-NL is exclusively focused on critical infrastructures and government. Thus, the target audiences are completely different for both parties. The question is therefore to what extent is cooperation desired or not. Kees underlines the difference in target audiences as a difficulty within this cooperation. Especially on the DTC side, he identifies certain challenges. Kees believes that it is impossible to approach 1,8 million small businesses and freelancers on an individual basis. Consequently, one should seek for cooperation. However, Kees says that on the freelancer side this can be extremely difficult since freelancers are often not united in any kind of cooperation structure. In addition, freelancers have often little focus on security. When only a small group of freelancers gets affected by cyber incidents, this will not immediately affect the country, but in case 25% of these businesses collapse there will be an enormous problem. However, the question today is how to approach this large group of freelancers. Kees also states that DTC is currently primarily focusing on large organizations which are already supported by the government. Yet, small organizations are not yet supported enough. Although Kees sees that the DTC is investing in this issue, they did not find the right solution just yet. However, Kees has no ready solution on how to approach the small organizations, but he believes that DTC should get the opportunity to further develop this.

Goals and focus cooperation

According to Jacco, the goals of this cooperation do not fully align with each other. The aim of the DTC is per definition something that the NCSC-NL is not allowed to do and outside their mandate and vice versa. This complicates things and therefore one cannot speak of shared goals in this cooperation. However, both organizations strive to make businesses in the Netherlands, including critical infrastructures and government, more cyber resilient. For this reason, Jacco believes that the parties really need each other. Organizations from critical infrastructures in de chain are depending on non-critical organizations and vice versa and it cannot be separated from each other. Equality between the partners, and that parties can work together and share information, is the main goal of this cooperation according to Kees. He states that the NCSC-NL should intensify its collaboration with DTC and share more information with so that DTC can directly answer questions they receive from entrepreneurs. However, a lot of this information cannot be directly shared with the target groups. Hitherto, the NCSC-NL can share sensitive information with DTC and DTC can then use this to give an answer to the questions

from its target groups without giving away any secret information. This way, it is easier for DTC to answer questions and create harmony in the market in case of a crisis. Kees underlines this with his own experiences from the physical security sector as an example. In case of a terrorist attack abroad, Kees communicated directly with representatives of 15 sectors to inform them that Dutch organizations were not or not yet targeted. By doing this, a nuance was given of the media reporting. This was extremely important for management of the organizations to reduce the stress levels. Parties should be only informed when really needed or are informed that no action is required.

The focus of the cooperation is on sharing information such as threat information and developing tools for both organizations. In this stage, the NCSC-NL shares information with DTC but DTC is sharing relatively little information with the NCSC-NL. Jacco expects that more threat information will become available when the community becomes alive. The aim is to share information on the longer term. It is interesting for the NCSC-NL and its target audiences, vital organization and government, to receive information from other type of businesses outside their scope. DTC aims to share information with the NSCS-NL just like the NCSC-NL shares information with the DTC now. In addition, Kees states that the cooperation focuses on crisis information, as well as on knowledge development. In case of indications coming from the market that not immediately lead to a crisis, for example ransomware that has been identified with a wide group of organizations, the parties can technically inform each other. Kees believes that the focus should be much more on information sharing and knowledge development than is the case now. Nevertheless, legislation will remain an obstacle.

Role selection

Considering the different roles of the Spectrum of Coalition Formation, and the current role of the NCSC-NL in the cooperation, Jacco believes that at this moment, the NCSC-NL has a strong director role. De partner role is limited, and the facilitator role medium. According to Jacco, in the ideal situation, the director role should be rather limited, and the partner and facilitator role should be strong. Jacco argues that security should not be decided by a governmental organization, but by the organizations. Government should not push the organizations; though, government should provide the right tools for organizations. This means that the government must be a strong partner and that facilities must be made available for entrepreneurs in an easy

way. The NCSC-NL is exclusively tasked with vital and governmental organizations. However, organizations should not notice the difference between the different public organizations and should be able to contact just one government that facilitates and partners.

Kees perceives the current role of the NCSC-NL not as a director role and states that this role is extremely low. He says that although this role is still developing the partner role is high whilst the facilitator role is medium at this moment. Ideally, the director role should be very limited and the partner role incredibly high. The facilitator role should also be high according to Kees. He argues that the director role does not really fit into this cooperation because DTC is also a facilitator for private and non-vital organizations. The NCSC-NL should sometimes put pressure on the communication. The partner role is crucial in this cooperation since it is not only having the right to protect vital and governmental organizations, but also other sectors in Dutch society. For this reason, the NCSC-NL needs the DTC and vice versa. They should work together as partners in realizing the goals. Therefore, the partner role scores extremely high. Kees thinks that the partner role is more important than the facilitator role. Yet, he says that this role should be significant in the cooperation.

Furthermore, Jacco believes that at this moment the DTC as well as the NCSC-NL focus too much on what is decided by the DTC. The government is supposed to take a frontrunner role, and not just tell other organizations what to do. For example, the statements of Minister Grapperhaus in the media, that the government needs to put more pressure on organizations on how to do it. This will definitely not work, because entrepreneurs will not accept this. They know exactly what to do. Government should therefore clarify its partner and facilitator role more. Currently, this is not happening enough. Kees also mentions that the DTC is officially a program of three years and this should be made structural. The question is on how to structure the cooperation and where to accommodate the DTC. Though, Kees is not so sure yet what the best way is to do this. He argues that for the NCSC-NL to stay decisive, it should not be too big. However, on the other side, to serve all sectors in society direct access to the target groups is needed. This will be made possible via the DTC, but is it then necessary to, for example, accommodate the DTC with the NCSC-NL network? As the NCSC-NL it is maybe not always needed to have all organizations under one roof to meet the goals, but it is definitely compulsory for a decent partnership.

4.3 Cooperation 3: NCSC-NL and Cyberveilig Nederland (CVN)

Background Cyberveilig Nederland

The interest group Cyberveilig Nederland was established in June 2018 and represents cyber security businesses in the Netherlands. CVN aims to increase the digital resilience of the Netherlands and to grow the quality and transparency inside the cyber security sector. CVN targets cyber security service providers and has currently around 50 members. CVN has three important principles: (1) creating transparency and quality in the market (2) show the world that cyber security is not only a risk but also an opportunity (3) look after interests of the cyber security sector towards stakeholders like the government, academia and politics (Cyberveilig Nederland, 2019: para 1).

Background NCSC-NL

NCSC-NL works together with CVN which is an important source for NCSC-NL to mutually share information with cyber security providers. Currently, CVN is involved in two key programs of NCSC-NL, the National Covering System (LDS) and designated clearing house (OKTT). LDS was set up to develop a national system of partnerships in cyber security wherein cyber security information can be shared between public and private parties in a broader and more effective and efficient way to strengthen the position of these parties (Nationaal Coordinator Terrorismebestrijding en Veiligheid, 2019: para 6). OKTTs are essential information nodes that have an essential role in sharing cyber security information between different networks.

Introduction respondents

- ***Policy Advisor at Cyberveilig Nederland - Liesbeth Holterman***

  Liesbeth Holterman is working in the cyber security field for many years. She has a strong cyber security and governmental background and worked for different interest groups on the topic of cyber security. Liesbeth is now policy advisor with CVN and focuses on public-private partnerships in cyber security. Liesbeth enjoys participating in this research because she believes that public-private cooperation in cyber security is often seen as the holy grail, but nobody knows exactly how this holy grail looks like and where to find it. Liesbeth thinks that public-private cooperation is frequently understood as the solution for digital resilience, but she believes that in most cooperations it is at

the end one of the two that steers the cooperation. Therefore, it is never really a full public-private cooperation.

- ***Product Manager Threat Analysis at NCSC-NL - Michael Meijerink***
  Michael Meijerink works for NCSC-NL as a Product Manager for threat products. He works for NCSC-NL since 2012 and has had several jobs within the organization. Michael started as a Coordinator Monitoring and Response, before working as a Program Manager for the National Detection Network (NDN) and Deputy Head of the department. He enjoys participating in this research because he is active in public-private cooperation and one of the initiators of the NDN report of Twynstra & Gudde. He enjoys learning how the cooperation between NCSC-NL and its partners can be further shaped. Michael argues that one part of cyber security exists of the technical side, but to be successful much more is needed such as legal and administration. Collaboration goes much further. Michael believes that diversity in cyber security is essential.

Cooperation coalition

In the cooperation between CVN and the NCSC-NL, Michael says that he sees collaboration with CVN as two-folded. Firstly, NCSC-NL works with the foundation CVN and secondly with the members of CVN. The interaction with both is different. Michael states that the interests of the NCSC-NL are to create an effect with the members of CVN and to do so, it is inevitable to work together with the organization CVN. According to Michael it is important that NCSC-NL makes a clear decision on how to set up the cooperation. He believes that the current cooperation is based on equality and mutual interests. Besides, CVN has a strong interest to look after the interests of her members. The NCSC-NL has an interest in sharing information. Since the cooperation between the NCSC-NL and CVN is still in development, Michael finds it hard to dedicate one of the defined roles to the current cooperation. However, the facilitator role is leading according to Michael. The director is the weakest role. Yet, due to certain developments like the creation of a model on how to manage the content, he expects that if this model will be excepted by the CVN members, the director role will be more shifted towards the partner role. Though, CVN and NCSC-NL will then still be the steersman in the cooperation which can be considered more directive.

Michael claims that due to new legislation CVN is appointed by the NCSC-NL as Designated Information Clearing House (OKTT). He argues that this is a relevant push. Michael is already working with several cyber security providers since 2012 to explore how to give substance to this cooperation. Nevertheless, legal obstacles have always been a burden in sharing information. Besides, the NCSC-NL is not allowed to give benefit to one organization above the other. For the NCSC-NL, working with CVN is an efficient way to interact with a variety of organizations without excluding any of the parties. At the same time, this is exactly the reason why the choice has been made for this type of cooperation. It is difficult for the NCSC-NL to manage single private organizations. Besides, setting up all technical infrastructures is impossible for the NCSC-NL. Therefore, working with private organizations gives the NCSC-NL the possibility to work together with other organizations in serving its target groups. Together, a shared proposition can be created that is interesting for the total private sector. CVN is serving as a middleman for the NCSC-NL to the private sector.

According to Liesbeth the role of the NCSC-NL should depend on the topic. An example provided by Liesbeth is on NDN where SOC service providers serve the vital organizations with network monitoring. In this case it is more a director role. Only a limited group of members can participate due to well-defined requirements. Liesbeth states that equality is needed because in this case it is clear which information NDN has and how private organizations can use this information. Thus, this is based on equality within a framework of requirements that still need to be determined by the NCSC-NL. For instance: what exactly are the requirements for SOC service providers to join the NDN network? Though, with the National Covering System (LDS), the role of the NCSC-NL is more focused on the facilitator or partner role. Therefore, the role of the NCSC-NL is depending on the cooperation within the cooperation. However, Liesbeth believes that all roles are connected to each other and her expectation is that in a few years the roles are even more interconnected. Liesbeth looks at CVN as a collective, because this means that any party in the cooperation is equal. However, in reality it is often a combination between a collective and connective coalition. Liesbeth argues that some members are only a member for the branding to put their logo on the website. Luckily this are only a few members and most members are very willing to contribute to the digital resilience of the Netherlands. Also, one member is more active than the other member or one party has more resources than the other.

It is much easier for larger organizations to provide input than for smaller organizations. For this reason, it is often a combination.

Benefits cooperation

Liesbeth identifies two main benefits of this coalition. First benefit is that Liesbeth and her colleague receive a lot of input from the CVN members and there is therefore no need to invent everything by themselves. Liesbeth and her colleague are provided with valuable information that they can use to take position and defend the cyber security sector and show how proactive the sector is. Second benefit is that the members of CVN are a good representation of the sector and this is an essential benefit for collective and connective coalitions. CVN has members with different backgrounds and it also depends on the maturity level. Some members are active, and others are passive, but you also don't want to only have extremely active members because this makes it then difficult to act. Most things start at a directive level and move then into a collective or connective coalition.

Michael sees as an important benefit that this cooperation saves a lot of money for both parties. Besides, it helps increasing the quality and it gives body to the goals of the NCSC-NL. It indirectly also gives body to public-private cooperation. He argues that one speaks a lot about public-private cooperation, but it is not made concrete. The private sector repeatedly said that it wants to do more, and their motivation is shared interests but also the fact that they can work together with a trusted third party like the NCSC-NL. This gives them a certain stature and the opportunity to receive information that most parties might already have, but it is at the same time also an essential way for them to test the information. For CVN it is of interest that cooperation with the NCSC-NL means working together with a trusted partner which at the same time supports CVN's organizational interests. The NCSC-NL is mostly seen as an important cyber security partner in the Netherlands in and it is hard to ignore the NCSC-NL. The NCSC-NL has certain content, knowledge and information that other organizations are lacking. Besides, it works on innovation and research. There are therefore still loads of opportunities within this cooperation. Yet, it remains important to identify the added value of the NCSC-NL.

Disadvantages cooperation

Michael also identifies difficulties in the cooperation. For example, the competition between parties since not all managed security providers (MSPs) are member of CVN. Besides, Michael states that wrong expectations from both sides are an important shortcoming in this cooperation. It must be clear what parties can offer. What can they offer and what can they not offer? This is important for the NCSC-NL to not overestimate the providers. It might be possible that organizations have only a small footprint with little impact. On the other hand, the expectations of organizations might be that the NCSC-NL is a flexible and dynamic organization that can achieve a lot in a short term, but reality could be totally different. Moreover, organizations might expect to earn money on something or that the NCSC-NL will pay, but NCSC-NL usually does not do that. And vice versa, the NCSC-NL might expect that managed security providers are covering all costs, but this is also not always realistic.

Liesbeth sees as an important disadvantage that the public-private partnership landscape is still facing inadequate maturity levels, across the board, and it is not yet always clear which information is relevant or not relevant. How can the right action perspectives be provided? What type of information should be shared? And how should this information be shared? It is all still in an early stage. For instance: it is not even known yet if IP addresses can be mutually shared since this is part of personal data and herewith falls under the General Data Protection Regulation (GDPR). But what if a new piece of malware is found that can be traced? Is it then possible? This is what Liesbeth means with information sharing. How can information be shared without, in case of the NCSC-NL, tracing the source or without disclosing the customers? All parties are looking for a solution to this question. Parties are willing to share information, but due to legal frameworks it is difficult to do so.

Goals and focus cooperation

This cooperation has according to Michael three important goals. First goal is to identify which of the MSPs of CVN do have customers that fall within the scope of the NCSC-NL. And to find out in what way the NCSC-NL can make sure that threat information is received by the target audiences and vice versa. The NCSC-NL expects herein to have a facilitator role. Second goal, although more on the long term, is to identify what information MSPs collect from their customers and which of this information can be shared with the NCSC-NL to provide NCSC-

NL with a wider picture of things happening. Third goal, at the same time more related to the maturity level of the cooperation, is to partner in more ways. In this case visions on cyber security today and in the future can be mutually shared. Question now is how these visions can be assembled to create a mutual threat analysis valuable for all parties. Additionally, it is a way to explore which party is good at what and this way each party can be positioned as good as possible. The aim of the NCSC-NL is to approach the parties on a higher level, and in Michaels' opinion MSPs are very professional, which however in reality might not always be the case. For this reason, the NCSC-NL works with these parties on a certain level. For example, if MSPs without SOC services are inspired by this cooperation and include certain services in their business model. Current members can come up with their own proposition that at the same time can be interesting for not-customers. For instance: if Gasunie is not yet serviced by a MSP because of the high costs, it is because of this possible to collectively find a solution that makes it interesting for everyone. This way all businesses have the chance to come to a desired level of cyber security.

Liesbeth indicates that most important ambition of the cooperation is to strive after a cyber resilient Netherlands. She states that the cyber security sector has a lot of knowledge and skills that they are willing to use in favor of society. On a daily basis, cyber security parties are already working on cyber security issues and thus know what is going well and what is not going well. The sector wants to use the NCSC-NL mainly to test their findings and vice versa. Are the same patterns and threats identified by both parties? Are these also seen by the cyber security sector that service many non-vital organizations outside the scope of the NCSC-NL. Thus, one of the most important goals of this cooperation is information sharing. But information sharing with a strong assessing character. It is not a matter of throwing information over the fence, but to mutually share opinions and visions. Is the same picture recognized by the parties? It is actually an essential way to start the dialogue.

Michael thinks that this cooperation mainly focuses on which members of CVN have customers that are part of the target audiences of the NCSC-NL and what they offer. Do they facilitate information that goes back and forth? To make this possible, the NCSC-NL has developed technical solutions such as links to SIEM and MISSP. This way technical obstacles are being reduced. The NCSC-NL has done a successful pilot and can use this as a selling argument to

MSPs to motivate them to join. The focus is primarily on information sharing and less on networking, because at this moment it concerns mainly individual relationships via CVN. MSPs are not yet appointed as OKTTs. There is a legal way in which a target audience gives instructions to the MSP, but it is still necessary to sign legal documents before sharing information with CVN. The NCSC-NL is not yet allowed to share information with MSPs, but in case the MSP is facilitating the target audience, after their permission it is possible. Thus, there is a lot of legal work involved. Working with CVN means that the NCSC-NL can maintain individual relationships, but this way the NCSC-NL can service them at once. Though, Michael states that to name this a network approach, is however the next step. Now, the focus is on short communication lines and to mutually share technical solutions. This is the first step and the next step is to explore how the cooperation can be further shaped. However, this process is still in progress.

Liesbeth points out that the focus of this cooperation between CVN and the NCSC-NL is amongst other things to work together in the NDN program and bringing parties together. The overall focus is on collaboration, networking and information sharing on strategical, tactical and operational level. For example, looking at the members of CVN, it is just a small group of organizations that have a business model that includes threat intel. A majority of the organizations, around 98%, do not make any money on threat intel. At the moment, pieces of this intel are not being used to create the bigger picture. It is now only being used to implement intel in the own services of the organizations. For instance: how SOCs are being set up or how penetration tests are being done. To make money out of it, it is essential that analysts value the information and create useful and traceable information. Since the NCSC-NL seems to find this rather complicated, what is however understandable within a public-private cooperation because it is not allowed for government to create any business advantages. Within PPPs the NCSC-NL is therefore somewhat reserved, but they must look into what parties are planning to do with the information. Is it to improve their services or to set up a new business model? In case of the latter, then it is indeed inevitable to recalibrate the cooperation. But it is guaranteed that most organizations use the information to improve their services. The intel is currently shared based on individual connections and not in a structured way. Some members of CVN are willing to share information, but it is hard for them on an individual basis to get back

information. Contrariwise, for parties with a governmental background, it is easier to find the right entrance.

Role selection

Considering the role of the NCSC-NL, Michael argues that in particular the partner role should be strong. He believes that the current relationship is based on equality, however not total equality. The NCSC-NL puts forward its interests as much as possible, but at the same time the cooperation is also initiated by the NCSC-NL. CVN can withdraw from the cooperation at any time and for this reason he sees a limited facilitator role for the NCSC-NL. Nevertheless, because the NCSC-NL also facilitates the cooperation Michael gives a medium score to the facilitator role. He also believes that the facilitator role will further grow in the future. The partner role will remain the same, but this is hard to predict. It depends on the number of CVN members, because the role depends on the size of the partner. Michael surely sees a close connection between the facilitator and partner role. Concerning the director role, Michael thinks that this role is relatively low. However, he also sees a link between the partner role and the director role. The NCSC-NL has a more leading role and the ambition of the NCSC-NL decides how the cooperation looks like. In case CVN will become an official OKKT, this might as a consequence change the role which will then be more a director role. The NCSC-NL is in charge to decide if something is legal or not. Michael thinks that the current roles will not extremely change because there is enough flexibility for the NCSC-NL to bring in its interests. At the same time, the NCSC-NL is dependent on managed security providers, and therefore it should not overestimate its own role. The director role might increase, because of the shift to OKTT and other programs might further intertwine. As a consequence, the director role of the NCSC-NL will then increase.

Classifying roles is not a matter of one size fits all according to Liesbeth. Each cooperation requires another role. In her opinion, the NCSC-NL should have a more directive role looking at the responsibilities of the government concerning cyber security issues. In the NDN cooperation between the NCSC-NL and CVN, Liesbeth sees a combination of a director and partner role. She believes that the requirements imposed to SOC providers to participate in the NDN network should come from the NCSC-NL. Liesbeth expects that these requirements set by the NCSC-NL will be much clearer than it is the case today, and that it will be clear what is

expected from providers. Nevertheless, the NCSC-NL should do this in dialogue with CVN and its members. This is then a clear example of a combination between a director and partner role. Liesbeth also points out that the NCSC-NL should not claim that organizations must have at least 300fte's to participate in NDN, because then only organizations like KPN and Fox-IT can participate. The director and partner role should therefore be both high. It is an equal role.

The facilitator role should be much lower. Although, at this moment the facilitator role is very high. In case NCSC-NL sets clear requirements, this role could be much lower than it is now. Liesbeth states that it is obvious that the NCSC-NL finds its current role very complicated. This is clearly visible. The NCSC-NL seems to struggle with questions such as should get mad on the Ministry of Infrastructure and Water Management that they are working on self-driving cars without keeping in mind the cyber security aspect and without consulting the NCSC-NL. Or should they only provide an advice since they an advice organization. Liesbeth states that cooperation with former minister Dijkhoff was more focus on collaboration. Present minister Grapperhaus, strongly focuses on legislation. The approach of Dijkhoff was more a partner approach whilst Grapperhaus has more directive approach. Though, since many organizations still not take any responsibility, the approach of Grapperhaus is understandable but maybe not the right way. Legislation, in particular in the Netherlands is often not necessarily the answer. Liesbeth indicates that the NCSC-NL should be more creative. For instance: look into other instruments such as financial incentives. Lower the tax on cyber security products and services for a year or two to reduce financial obstacles for organizations. Today, it is all about legislation, while this takes extremely long and the government itself is not always the best example either. When the tax office states that they can only meet the GDPR directive in 2020, organizations that must comply to ISO27001 might also think whatever government. And they are right.

Liesbeth also argues that when all frameworks are clear, the NCSC-NL should move more into a facilitator role to point out to vital organizations the importance of cyber security. That is at the same time a role for CVN that should inform its members on the possibilities in case a managed security provider is supplier to a vital organization. What are the requirements and how can organization meet these requirements? The role of the NCSC-NL and CVN as well will in this case then be more facilitating. Next the director and partner role will reduce, depending on the developments. For instance: in case Kaspersky meets all the requirements,

and CVN and the NCSC-NL are only in a facilitating role, does this then mean that it was not adequately thought through? In this case, it can move to the other side. Liesbeth concludes therefore that the role should depend on the type of cooperation and the stage of the cooperation. Michael points out that the NCSC-NL is already working for five years with other parties, of which one year with CVN. To be successful in this cooperation, he believes that time is extremely important. It requires a deliberated choice meaning enough time, capacity and energy. Currently, in this cooperation the NCSC-NL leans strongly on external hires. The question is when these hires leave, is the NCSC-NL then still be able to uphold this cooperation? Michael believes that at this moment this is not yet the case. In creating partnerships, it is therefore key to think beforehand think through the cooperation. What is expected? If the cooperation is set up this way, is continuation of this cooperation secured? In the past this did not always went quite right. Michael states that a partnership is not a matter of signing a contract and that is it. Partnership are nor concrete nor tangible and it is easier said than done. Signing a contract or MOU is not yet a collaboration it is just the start. In Michaels opinion, the NCSC-NL has too little experience in external cooperation. Michael believes that the NCSC-NL has a strong legal mentality, sign a contract and it is then binding which is in his opinion not cooperating. In addition, he says that one must have a clear vision on which partnerships are relevant and which are not relevant. Michael acknowledges that some of the current partnerships started based on the opportunities he identified and not so much on deliberated plan. It is possible that the NCSC-NL should also participate in other partnerships or set up its own partnerships. Vision and in particular the lack of vision is still a point of attention.

4.4 Cooperation 4: NCSC-NL and Cyber Security Alliance (CSA)

Background Cyber Security Alliance

The Cyber Security Alliance is the platform for public-private cooperation for a digital resilience nation and its mission is to strive to a digital resilient nation (Cyber Security Alliantie, 2019: para 1). The CSA is originated from the NCSA agenda which was created by the National Coordinator for Security and Counterterrorism. The organization was founded in 2018 and currently more than 100 public and private organizations take part in the CSA. Participants are coming from private and public sector and are involved in short-term projects to achieve tangible results and to get insights. The organization aims to increase the network which contributes to the mutual mission.

Background NCSC-NL

As of the start of CSA in 2018, NCSC-NL is one of the main participators of the CSA. The NCSC-NL has one of its political advisors dedicated to the cooperation with the CSA which strongly looks after the interests of the organization. Within the Cyber Security Alliance framework, the NCSC-NL works together with numerous partners from public and private sector in several cyber security projects. The role of the NCSC-NL in the cooperation with CSA is primarily on the execution of cyber security tasks and the organization is not involved in any policymaking in any way.

Introduction respondents

- ***Coordinating Policy Advisor at NCSC-NL - Rosa Gompen-Van Zijl Jansen***
  Rosa Gompen-Van Zijl Jansen works as a political advisor for the NCSC-NL and has a strong background in international relations and politics. Before she worked as an analyst in the field of non-Islamic extremism and terrorism. Rosa is responsible for all strategic and political issues within the NCSC-NL. She focuses on political processes and partnerships and strategy. Rosa has been involved in the CSA cooperation from the beginning where she was part of the NCSA strategy team. Rosa participates in this study because she would like to contribute to the concept design of coalitions. At the same time, she is curious to the results and in specific to the external image of the NCSC-NL in cooperations. Does the NCSC-NL need to adjust its ideas? Or act in a different way? Rosa considers this study as a good way to learn from the current situation.

- ***Deputy Director at ECP - Marjolijn Bonthuis-Krijger***

  Marjolijn Bonthuis-Krijger is Deputy Director of the Platform for the Information Society (ECP) and co-responsible for all security related issues, including cyber security. This independent organization is fully grounded on public-private cooperation and supports public and private organizations in working together in the information society. With ECP, Marjolijn offers a neutral table where public and private parties van meet and make arrangements. ECP is the main facilitator of the CSA cooperation. Marjolijn participates in this research because she believes that ECP has a lot of knowledge on public-private cooperation and she looks forward to the outcomes, because this way they can learn from the results.

Cooperation coalition

Rosa starts of by emphasizing that the CSA has no director role at all. She believes that the director role conflicts with any public-private cooperation. A collaboration should per definition mean that parties work together, and it is difficult to impose anything without a certain status or formality. Rosa thinks that the CSA cooperation is therefore more a collective or connective coalition. A collective coalition because it is in particular about joining forces to achieve the goals set in cyber security which is useful for the entire society. The principle focus is on collaboration. Though, there is also a network focus, but mainly to stimulate cooperation between the public and the private sector and to share lessons learned on threat intel, risks and other challenges that are collected. Together, solutions are discussed, and guidelines are created for parties that are for example less mature in cyber security than larger organizations or the government. Partnerships support in achieving things. Besides, an extensive network is created to enable organizations to easily connect to each other, learn from each other, and work together in different ways.

According to Marjolijn CSA is currently in transition, because the basis first mainly focused on cooperation, existing of stimulating organizations to collectively come up with proposals that can be rapidly executed and spread quickly. Now, it is believed by all participants that the network is most important thing. Therefore, in this transition the focus will shift more towards the importance of the network. The strengths from the network and the strengths of the people that are sitting at the table are used to do so. This will be the starting point to search for

connections instead of demanding that parties should come up with a finalized proposal with a price tag on it that they can rapidly execute. The network is key, and this network is at the same time asked to share their knowledge to their ability so that topics can be proposed to mutually work on.

Benefits cooperation

Marjolijn believes that one important benefit of the cooperation is that parties can easily find each other. She thinks that this way organizations can easier share each other's knowledge and visions. Besides, it makes it easier to bring the different interests to the table and assess if the needs are individual needs of organizations or carried more widely. So, it is necessary to work together on a particular topic. An example are simulations and assessments, a hot topic that all organizations are working on, but maybe only on an individual basis in their own organization and their own network. To make things visible and motivate parties to join. The question is how these parties can be connected and share the lessons learned. There are lots of initiatives and how can these initiatives come together and reach the organizations that need them. Hereby, it is not necessary to invent the wheel over and over again.

In Rosa's opinion an important benefit of this cooperation is that the participating parties are extremely motivated. It is clearly a mutual expectation that organizations are pro-active, and cooperative in sharing results with other parties. In the cooperation it is clear that parties are really interested and willing to spend time and insights and work together to create a digital resilient country. And in particular, because public and private are working together, there is a large variety in insights involved. By assembling these insights one can achieve a lot more. More visions give better insights. In addition, the public and private sector have different interests which are in this way now also coming together. This is important, especially since the aim is to create outcomes for the whole country and that it is useful for anyone. It is then essential to include and compare all of these interests instead of just a few.

Disadvantages cooperation

However, the collaboration with CSA has also some disadvantages according to Rosa. First, since the cooperation is not formalized, it has no formal power, everything depends on the motivation of the parties. Many organizations have signed for the CSA initiative, but at this

moment it is only a small group of key advisors, around 25, that put most effort into the cooperation. Though, this is still enough to sit back and relax while looking at others to raise their hand. For example, in case an organization has less experience they might look at other parties to clear the job. This could be a risk for the cooperation. Another risk is, although the focus is on results in partnerships and projects, it is easy to end up without anything happening. Thus, you can get lost in infinite talking without achieving anything. Questions can be unresolved like; what do we exactly want to do? Do we do this ourselves or do we invite other parties? And if the project is already running, in case of stagnation, it is not possible to enforce anything or any results. There is always a risk of the lack of commitment, but at this moment this is definitely not the case. The current group of key advisors is extremely active. Also, there is another subgroup within this group that in a smaller context reflects on the strategy and how to execute things. However, there are currently some suggestions to change this. Yet, again, there is a lot of commitment.

Marjolijn states that time is one of the biggest disadvantages of public-private partnerships. There are many cyber security initiatives and as such it is therefore difficult to show added value. It is important to showcase why we do something. Thus, it is important to be aware of what can be done and what cannot be done. There are loads of initiatives, also with the NCSC-NL for example the DTC. One can identify some initiative fatigue and for this reason it is important that parties participating in this cooperation can explore together what can be done and who is in charge. Because if it would really have been weariness, parties would not have joined. It is a unique network that helps identifying important topics in cyber security. Another disadvantage mentioned by Marjolijn is that some parties are very active, and others lean backwards. Cooperation forces parties to take action, because organizations can otherwise hide within the network. CSA will therefore try to operate inside. Also, the extent of the network can be a disadvantage. How do you organize such a network? Which roles do parties have? But Marjolijn believes that every disadvantage also has its benefits. It can be really diffuse. The aim is to involve all organizations, because this will help to get broader insights instead of just a small group. But parties should also have their freedom. As long as parties are involved, that is the most important thing. And it is useful to hear from both, public and private, what the issues are and what type of solutions organizations have to these issues. This applies to public and private, but also to public and public cooperation. Last, it is also a matter sometimes of how

clear or unclear the roles are divided and where does it stop. The interests of EZK is another interest of the NCSC-NL what makes it sometimes complicated. Where does one organization starts and where does the other starts? Correspondingly, BZK is now also entering the field and starts all over again. It is all about different interests like economic interests. The CSA cooperation creates the opportunity to create something together.

Goals and focus cooperation

Most important objective of the cooperation in Rosa's opinion is to adhere to the goals of the NCSA agenda. She argues that the motivation to set up the CSA was to achieve these goals through public-private cooperation. At the same time, Rosa says that this also narrows down the scope. For instance: one of the topics that was suggested by the NCSC-NL on existing threats, and current problems. It would also be interesting to look at non-existing threats that can be detected through the NCSC-NL Cyberkompas. From a prevention point of view, it would be interesting to create projects on this topic and support organizations to protect themselves against cyber threats in advance. This way, the scope of the CSA will become much broader than the NCSA agenda. Looking at the output of the Alliance, it is all about creating tangible and concrete results that are useful for all organizations in the Netherlands. The majority of the small business have to do all these things themselves and might not have adequate resources to hire cyber security experts or do not understand the cyber security terminologies. Support can be in the form of guidelines or for example the cyber security dictionary that was generated. This dictionary has been created with around 50 or 60 organizations from the Netherlands that jointly debated on the terminologies and corresponding meanings. This is a concrete and tangible result. But it can also be guidelines or a roadmap on how to become cyber resilient. In the cooperation the focus is mainly on information sharing and one of the projects even has information sharing as an outcome. It is a way to learn from each other. Moreover, the focus is on networking for example organization partner events are organized for participating organizations. Interesting speakers and topics are part of these events as well as the possibility to network. Altogether, the main goal is to achieve the mutual mission set. Collaboration and networking our ways to do this.

Marjolijn claims that the cooperation focuses on collaboration, information sharing and knowledge exchange. All parties contribute to a more digital resilient Netherlands. However,

the suggested topics by the network and the needs of the organizations, are sometimes somewhat different. The aim is to filter some of these important topics that have potential to succeed. Topics are detracted from the NCSA agenda and other related reports such as the WWR report by the Scientific Council for Government Policy. The topics suggested by the organizations are usually assessed by these documents. Both, the public sector and private sector, have the opportunity to suggest topics. In general, most topics are relating back to these documents and it is clear that the majority of the organizations support these documents what is actually a great conclusion according to Marjolijn. The NCSA has obviously obtained this position what she thinks is great. Over the last years, the private sector commented a lot on the fact that the government wants to decide, but here it is made sure that this is not the case. And when the private sector then suggests using the NCSA agenda as a starting point, this is a good position.

Role selection

Concerning the suggested role by the Spectrum of Coalition Formation, Rosa states that she does not see a director role for the NCSC-NL in this collaboration. Although, Rosa is as advisor for the NCSC-NL involved in a small facilitating group, which she indicates as a special position, Rosa argues that her role is definitely not a director role. She is not able to enforce anything and for this reason Rosa gives a low score to the director role. However, on behalf of the NCSC-NL she tries to steer the organization as much as possible. The partner role is the main role of the NCSC-NL and Rosa gives an extremely high score to this role. The facilitator role is more focused on projects and the NCSC-NL made the decision not just to participate or take an active role in all projects per definition, because this does not fits into their capacity or connects to their network in such a way that the NCSC-NL can deploy unlimited sources in these projects. Yet, they are in anyway willing to use their network for example to recruit new parties. Consequently, the facilitator role has a medium score, not because of organizing meetings or writing the minutes of the meetings. Rosa argues that the facilitator role should be focused on the content and the network and not in the sense of administrative support. However, in the ideal situation, the facilitator role should be limited. Since NCSA is an initiative of NCTV, they are in charge. Although, Rosa believes that the role of NCTV should not be a director role either. In her opinion, this role works counterproductive. In case the government will pro-actively lead in a director role for specific outcomes of public-private partnerships,

parties will probably drop out. It should be a joint result. For this reason, the director role scores very low. The partner role scores extremely high and the facilitator role medium. Rosa states that the current role of the NCSC-NL is balanced, and she tries to involve the NCSC-NL where it should be involved. Rosa claims that she can make the right decisions for the NCSC-NL where to join and where not to join. She works together a lot with experts that provide her with the right information and give her advice on which projects to invest or not.

Marjolijn states that the current role of the NCSC-NL is a very constructive one and different roles can be observed. She thinks that the NCSC-NL has above all a partner role. But with a note, that it is also desirable that the NCSC-NL takes the lead on certain topics. Since the NCSC-NL is part of the core team of CSA, the partner role should be extremely high. The director role in this case will be more a managing role. This is way less, so the director role is really low. The facilitator role is medium high because Marjolijn thinks that the NCSC-NL fulfills this role. Ideally, the director role will be very low whilst the partner role should be high. The facilitator role should be medium. Marjolijn says that it is hard to define who should play which role. The division of roles between the NCTV and the NCSC-NL is sometimes already challenging, this should be clearer than it is now. The partner role is the most important role for the NCSC-NL. In the ideal situation the facilitator role should be high as well because the NCSC-NL should take a leading role in certain topics. Marjolijn states that over the last years, the NCSC-NL has grown into its role and it is a good role in her opinion. This is not how it started off and in the beginning the role of the NCSC-NL was limited. Marjolijn believes that NCSC-NL still has serious issues with its role and she personally believes that the NCSC-NL wants to be involved in everything on the one hand but on the other hand they do not have any time. It seemed like they want to be in the director role, but at the same time do not want to be in the director role. Before the mentality was that a project was initiated by the NCTV and they had to do the work. Today, this mentality has totally changed. This could be because of the people or maybe because of the fact that the organization is more settled. Marjolijn enjoys the NCSC-NL role like how it is today, and she believes that this role is rather an important one. She also adds that it is important to have the right people aboard. Besides, it is important to create a good network structure which is broadly supported. Otherwise, it will be very complicated. Currently, the NCSC-NL has also contributed to some topics what shows its involvement which is really crucial. It is not the director role that is preferable in this

cooperation, but the partner role. And once in a while maybe the leading role. That is what the network appreciates.

Concluding, Rosa says that one of the reasons of the close involvement of the NCSC-NL in the CSA is not only because of the NCSA Agenda, but also because of the next steps in policymaking. Realizing that policy is important in the execution. One of the most important reasons to participate is to be closely involved and that the goals are closely relating to the fields wherein the NCSC-NL operates. One of the most important motivations of the NCSC-NL is that they have a lot of insights into all the initiatives and activities that are happening in the cyber security field and to point out where the opportunities are in the cooperation. Thus, it is to look after its own goals and aims to identify the blind spots and to organize initiatives. This way, topics handled by the NCSC-NL that are identified as opportunity can still be executed whilst the NCSC-NL can also steer a bit. Then the role of the NCSC-NL tends to be more a director role. But Rosa clearly states that that is not the case in this cooperation.

Marjolijn underlines the importance of the broader picture. With a broader picture it is easier to understand things and take the next steps. Once in a while, it might be hard because it might not fit into the vision of an organization or in what an organization aims in a cooperation, but this is a growing process. At this moment, the process is going into the right direction. There is a clearer structure also within the organization. And people are important. Public-private cooperation depends on people. Do people get it, and do people understand it? The right person should be on the right place. It costs time. Always more time than you would like.

5. Analysis – Choices of roles

In the previous chapter, four case studies have been described wherein respondents of the NCSC-NL and external respondents expressed their view on the current and ideal role of the NCSC-NL in public-private cooperation in cyber security. In this research the three roles as defined; the director, partner and facilitator role were specifically applied to the NCSC-NL. In the interviews with the respondents the role categorization as suggested by the model of the Spectrum of Coalition Formation of Twynstra and Gudde as described in chapter 2 was recognizable. The majority of the respondents could assign at least one or more of the roles to the NCSC-NL. In this chapter the data of these interviews is analyzed in-depth.

First, within each cooperation both respondents, one of the NCSC-NL and one external respondent, assigned current and ideal roles in the particular cooperation to the NCSC-NL. The respondents were asked per role to indicate with a number between 0 and 10 how strong or weak they believe the role of the NCSC-NL is now and how this ideally should be in the cooperation. The choices in roles made by the respondents have then been described and mutually compared between both respondents within the particular cooperation.

After assigning current and ideal roles to the NCSC-NL per cooperation, the four cooperations are compared to determine the overall perception of all respondents on the role of the NCSC-NL. With on the one side, the perception of all NCSC-NL respondents and on the other side the perception of the external respondents. Here, there is no good or bad and a high or low score is not necessarily better or worse. It only provides insights in the different choices made by the NCSC-NL respondents and the external respondents.

5.1 Analysis roles per cooperation

In this first subchapter three roles; the director, partner and facilitator role will be explored per cooperation. A short summary is given per cooperation on how both respondents experience the current role of the NCSC-NL and how they ideally see this role.

5.1.1 Analysis cooperation 1: NCSC-NL and ISAC

In the cooperation between the NCSC-NL and the Energy-ISAC there is a clear discrepancy in the perception of both respondents. Thom (ISAC) sees the cooperation more as a collective coalition while Mireille (NCSC-NL) thinks that it is more a connective or directive coalition. As one of the main benefits of the cooperation Thom mentions the equality between the partners in the coalition. Though, Mireille does not share the same feeling of equality and instead mentions the mutual information sharing and easy way to swiftly connect with other parties as an important benefit and the variety of organizations gathered together at one place. As disadvantage of this cooperation Mireille mentions the lack of knowledge of the NCSC-NL on its collaboration partners, and that facilitating ISACs are extremely time-consuming while capacity is limited. Besides, she thinks that ISACs are not always as efficient and the ambition of the ISACs are not necessarily the ambition of the NCSC-NL. Thom also mentions that it is extremely hard to make decisions and access to the cooperation is restricted. However, both respondents agree on the common goals of the cooperation which are information sharing and building a network. Mireille also adds another goal specifically for the NCSC-NL which is to know what is going on in the markets. In assigning roles to the NCSC-NL, Thom gives the current director role a 2 while Mireille gives a 6. Looking at the partner role this is completely the opposite. Whereas Mireille gives a 3, Thom sees the partner role with a 6 slightly higher in the current cooperation. The facilitator role, however, both respondents give this role a 9 in the current situation as illustrated in the figure below.

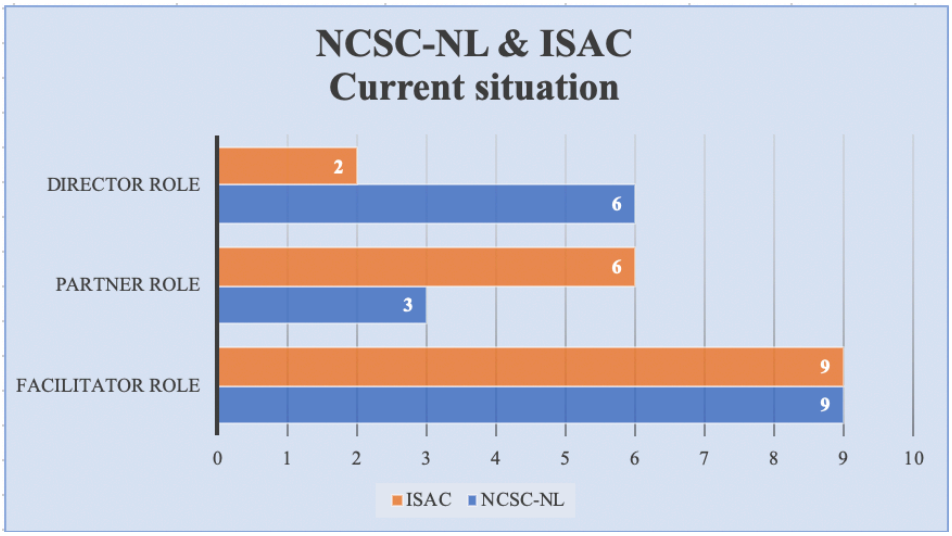


Figure 4 - Current role NCSC-NL in the cooperation with the ISACs

In the ideal situation, Mireille and Thom both agree that in this cooperation the director role should be very weak (respectively 0 and 1) for the NCSC-NL. Besides, according to both respondents the partner role should be very strong. Thom gives a score of 10 and Mireille a score of 8 to the partner role. Yet, looking to the ideal facilitator role the respondents totally not agree. Whereas Thom believes that the facilitator role of the NCSC-NL should be very strong with a score of 8, Mireille believes that the ideal facilitator role should get a score of 0.

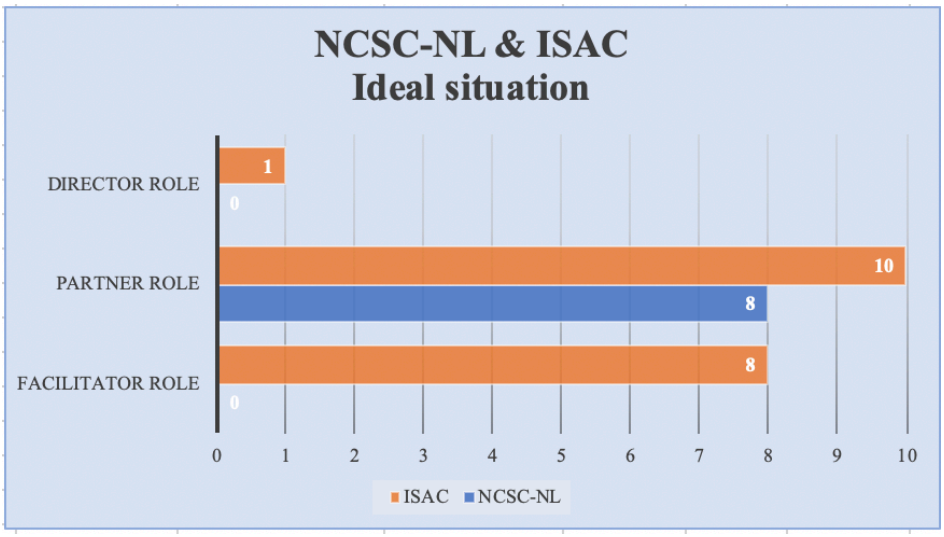


Figure 5 - Ideal role NCSC-NL in the cooperation with the ISACs

Comparing the current situation and the ideal situation in the cooperation between the NCSC-NL and the ISAC the perceptions of both respondents are rather dissimilar. Thom perceives the current director role as limited, but Mireille believes that this role is strong. However, in the ideal situation she thinks that the NCSC-NL should not play a director role at all. Thom agrees with Mireille that in the ideal situation the director role should be extremely weak. Considering the partner role, in the current situation Thom sees this role as medium, but Mireille sees this role as weak. However, both respondents do agree that in the ideal situation the partner role should be very strong. The last role, the facilitator role, is considered by both respondents as extremely strong in the current situation. However, Thom believes that this role should also be strong in the ideal situation, but Mireille does not agree and prefers to completely eliminate the facilitator role in the ideal situation. Concluding, the perception of roles in the cooperation between the NCSC-NL and the ISAC is rather fragmentated.

Table 1 - Summary analysis cooperation NCSC-NL and Information Sharing and Analysis Centre

	THOM	MIREILLE
Coalition	Collective coalition	Connective coalition Directive coalition
Benefits	Equality in cooperation	Information sharing Variety of different organizations at one place Easy way to swiftly connect with each other
Disadvantages	It is hard to make decisions Not every organization is allowed to join	NCSC-NL lacks knowledge on its collaboration partners Facilitating ISAC is extremely time-consuming while capacity of NCSC-NL is limited The ambition of the ISACs are not necessarily the ambition of NCSC-NL
Goals and focus	Information sharing Creating network	Information sharing Creating network To be informed on what is going on in the sector
Current role	Director role: Limited Partner role: Medium High Facilitator role: Extremely High	Director role: High Partner role: Limited Facilitator role: Extremely High
Ideal role	Director role: Very Low Partner role: Extremely High Facilitator role: Very High	Director role: Extremely Low Partner role: Very High Facilitator role: Extremely Low

5.1.2 Analysis cooperation 2: NCSC-NL and DTC

In the cooperation between the NCSC-NL and DTC, Jacco (DTC) sees the coalition more as a directive coalition, whilst Kees (NCSC-NL) thinks that the coalition in this cooperation is more a collective coalition. Both respondents agree that the experience of the NCSC-NL and the direct access of DTC to a large group of businesses from the private sector are true benefits of the cooperation. As important disadvantages of the cooperation, Jacco mentions that he perceives the cooperation sometimes more as a fight rather than collaboration. Also, both organizations are still in search for the mutual ambition in the cooperation which is today still lacking. Kees believes that the differences in target audiences and that the DTC is extremely focused on large companies are important disadvantages of this cooperation. Although, both respondents consider information sharing as one of the main goals of the cooperation, Kees and Jacco also mention goals apart from each other. Jacco sees the pursuit to a more digital resilient country as one of the main goals, whereas Kees is more focused on creating equality between

partners and that organizations can work together and develop knowledge. Considering the current and ideal role of the NCSC-NL in the cooperation differences in perceptions are clearly visible, in particular in the current situation. Jacco believes that the NCSC-NL has a very strong director role (8), whilst Kees thinks that the NCSC-NL has an extremely weak director role (0,5). Moreover, Jacco gives a low score to the current partner role (2) but Kees sees this role as much higher (7). Nonetheless, both respondents agree on a low facilitator role for the NCSC-NL (5).

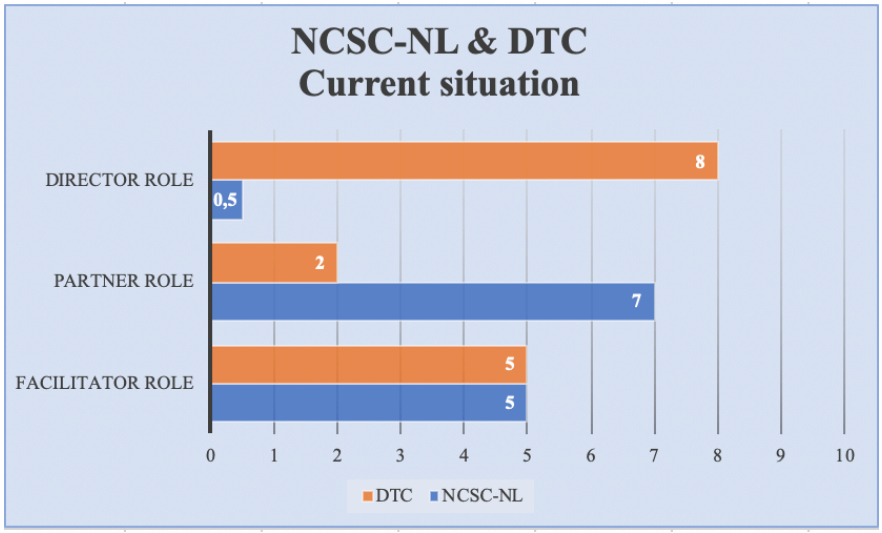


Figure 6 - Current role NCSC-NL in the cooperation with DTC

In the ideal situation both respondents assign a very weak director role to the NCSC-NL in this cooperation (Jacco 2/ Kees 1). For the partner role Jacco gives an 8 and Kees a 9. Herewith both respondents seem to agree that the partner role of the NCSC-NL in this cooperation should be strong in the ideal situation. Moreover, the facilitator role also gets a somewhat similar score from both respondents which agree that this role should be strong (Jacco 8/ Kees 7).

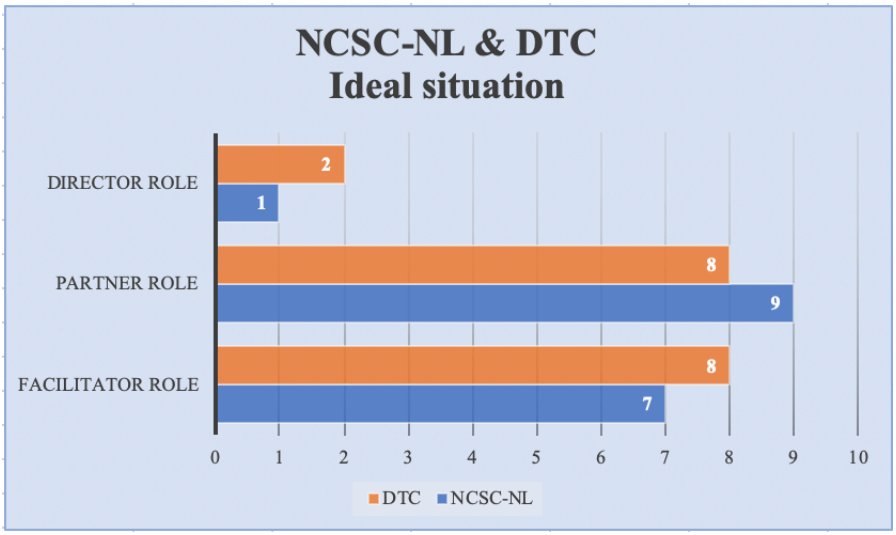


Figure 7 - Ideal role NCSC-NL in the cooperation with DTC

Looking at the current situation and the ideal situation, there is a clear discrepancy in the current situation between the perceptions of roles. Respondents do not always share the same vision on the roles. However, in the ideal situation the perceptions of the respondents are coming much closer together. Although the perceptions of roles in the current situation are different, the respondents find each other in the ideal situation. Both agree that the director role should be weak whereas the partner and facilitator role should be strong.

Table 2 - Summary analysis cooperation NCSC-NL and Digital Trust Centre

	JACCO	KEES
Coalition	Directive coalition	Collective coalition Connective coalition
Benefits	Knowledge and experience of NCSC-NL Access to a large group of businesses in private sector Physical close proximity	Knowledge and experience of NCSC-NL Access to a large group of businesses in private sector
Disadvantages	Collaboration can be sometimes more a fight than collaboration Both parties are still in search for a mutual ambition	Differences in target audiences DTC has an extreme focus on large companies
Goals and focus	To strive to make businesses in the Netherlands more cyber resilient Information sharing	Create equality between partners Parties can work together and mutually share (crisis) information Knowledge development
Current role	Director role: Very High Partner role: Very Low Facilitator role: Low	Director role: Extremely Low Partner role: Medium High Facilitator role: Low
Ideal role	Director role: Very Low Partner role: Very High Facilitator role: Very High	Director role: Extremely Low Partner role: Extremely High Facilitator role: High

5.1.3 Analysis cooperation 3: NCSC-NL and CVN

In cooperation three, the respondents both agree that inside the cooperation there are also sub cooperations which might require their own coalition. Therefore, Liesbeth (CVN) allocates all three coalitions to this cooperation. Though, Michael (NCSC-NL) sees the connective coalition as leading. Both respondents have totally different thoughts on the benefits of the cooperation. Liesbeth sees the input of the CVN members as an important benefit and the fact that these members are a good representation of the sector. Michael, however, states that this cooperation saves a lot of money for both parties and it helps increasing the quality. It also helps to give body to the goals of the NCSC-NL according to Michael. Besides, he mentions that the NCSC-NL has certain content, knowledge and information that other parties in the cooperation can strongly benefit from. Moreover, both respondents identify different advantages of the

cooperation. Michael mentions the competition between organizations and the risk that parties bare the wrong expectations towards each other and what they are able to do. In contrast, Liesbeth sees the inadequate maturity levels in the public-private landscape as an important disadvantage as well as the dominant legal frameworks. In addition, both respondents have other perceptions of the goals of the cooperation. Liesbeth mentions goals like striving after a cyber resilient country, information sharing, collaboration and networking, but in Michael's opinion, most important goals for the NCSC-NL are to identify which MSPs serve customers that fall within the scope of NCSC-NL, what information MSPs collect from their customers and how to partner in more ways. In regard to the current and ideal role of the NCSC-NL, there are clear differences in perceptions of the respondents. Although both respondents give a low score to the current director role (3), they do not agree on the current partner role. Michael perceives this role as medium strong (7), whereas Liesbeth perceives this role as weak (3). In the current situation the perceptions on the facilitator role come closer together (Liesbeth 8/ Michael 6).

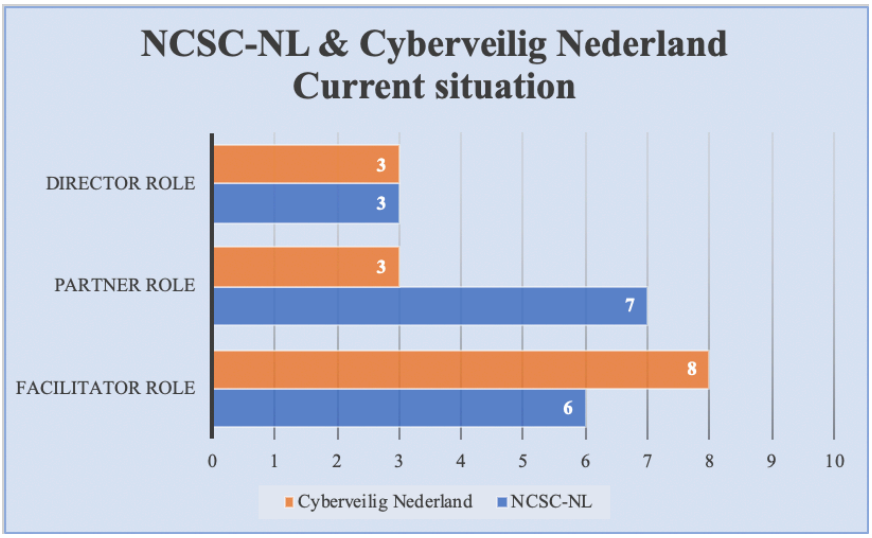


Figure 8 - Current role NCSC-NL in the cooperation with Cyberveilig Nederland

Moreover, in the ideal situation the respondents do not agree on the director role. Liesbeth gives a score of 8 whilst Michael gives a lower score of 5. Considering the partner role in the ideal situation, the respondents meet each other quite closely (respectively 7,5 and 7). Though, the facilitator role shows more inconsistency in the perceptions of the respondents. Whereas Liesbeth perceives this role as weak (3), Michael believes that this role should be strong (8).

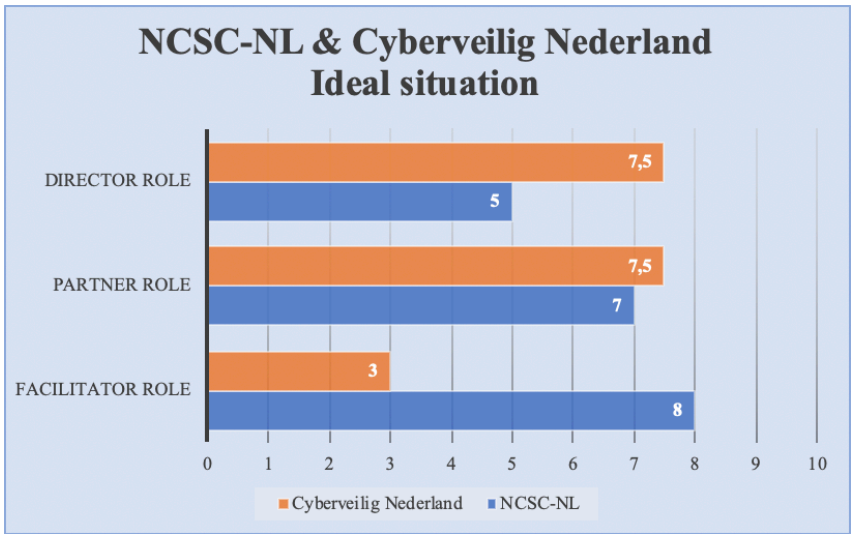


Figure 9 - Ideal role NCSC-NL in the cooperation with Cyberveillig Nederland

Looking at the above, the perceptions of the respondents on the current and ideal situation in this cooperation is not aligned. Both respondents believe that the director role should ideally be stronger than it is now. However, Liesbeth foresees a much stronger director role (7,5) for the NCSC-NL than Michael (5). The partner role is according to Michael in the current situation and the ideal situation alike (7). However, according to Liesbeth in the ideal situation this role should be much stronger (7,5) than is the case in the current situation. She also thinks that the facilitator role should decrease in the ideal situation (from 8 to 3), but meanwhile Michael believes that this role should increase (from 6 to 8). Final, Liesbeth sees opportunity for the NCSC-NL to grow its director and partner role and reduce its facilitator role whereas Michael wishes to increase the facilitator role.

Table 3 - Summary analysis cooperation NCSC-NL and Cyberveilig Nederland

	LIESBETH	MICHAEL
Coalition	Directive coalition Collective coalition Connective coalition	Connective coalition
Benefits	Valuable input from CVN members Good representation of the cyber security sector	Saves a lot of money for both parties Helps increase the quality Gives body to goals of NCSC-NL NCSC-NL has exclusive content, knowledge and information
Disadvantages	Different and inadequate maturity levels in public-private landscape Legal frameworks make things difficult	Competition between CVN members Wrong expectations from both sides
Goals and focus	To strive after a cyber resilient country Information sharing Collaboration Networking	To identify which MSPs, that are member of CVN, serve customers that fall within the scope of NCSC-NL To identify what information MSPs collect from their customers To partner in more ways
Current role	Director role: Low Partner role: Low Facilitator role: High	Director role: Low Partner role: Medium High Facilitator role: Medium
Ideal role	Director role: High Partner role: High Facilitator role: Low	Director role: Medium Low Partner role: Medium High Facilitator role: Very high

5.1.4 Analysis cooperation 4: NCSC-NL and CSA

Rosa (NCSC-NL) and Marjolijn (CSA) agree that this cooperation is a collective coalition, but Rosa adds that it is also a connective coalition. Both respondents mention different benefits of the cooperation. Marjolijn mentions as most important benefit that parties can easily connect and mutually share their knowledge and visions. Besides, the cooperation is helpful in assessing if needs are individual or collective needs. Rosa adds that the participating organizations are extremely motivated and willing to spend time and effort in the cooperation. Also, the cooperation makes it possible to gain a large variety of insights. Furthermore, interests of public and private sector are coming closer together. Nevertheless, Marjolijn perceives the lack of time

is an important disadvantage of the cooperation as well as the extent of the network. It is also sometimes unclear how roles are divided. Besides, due to competing initiatives it is important to clearly show the added value of the cooperation. Moreover, some organizations are very active, whilst others are not. Rosa agrees with the latter. She states that sometimes people look to others to do the job. Another important disadvantage mentioned by Rosa is that the cooperation has no formal power, and thus relies on motivations. There is a serious risk of the lack of commitment and it is easy to end up with nothing happening. As the main goals Marjolijn mentions working together, sharing information and exchanging knowledge. Rosa agrees with information sharing and adds other goals such as adhering to the NCSA Agenda, creating clear and tangible results for all organizations in the Netherlands and networking. Looking at the role of the NCSC-NL in the current and ideal situation, both respondents are rather aligned. In the current situation both respondents give a low score of 3 to the director role. With a score of 9, both respondents also agree on the partner role. The facilitator role is also rather similar (Marjolijn 7,5/ Rosa 7).

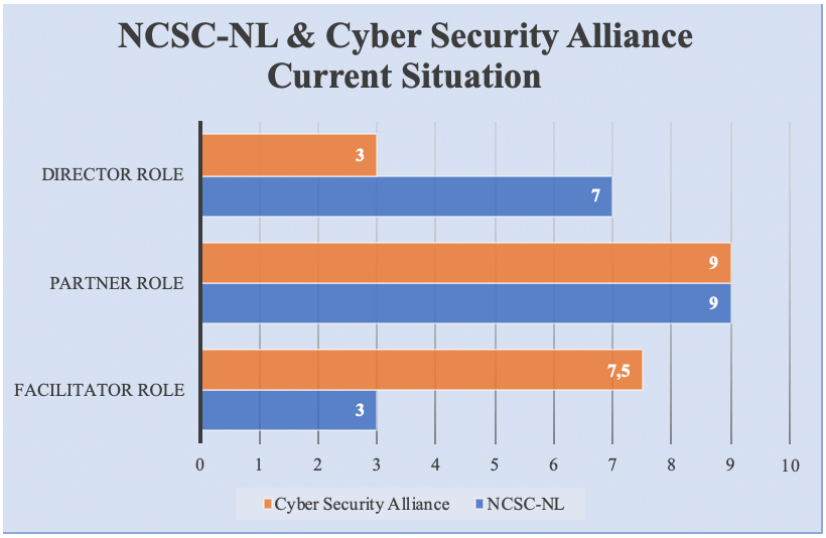


Figure 10 - Current role NCSC-NL in cooperation with Cyber Security Alliance

In the ideal situation the perceptions of the respondents are more diverged. Marjolijn gives a medium score of 6 to the director role, whilst Rosa gives a low score of 3. Though, both agree on a very strong partner role (9). In the ideal situation the facilitator role should be 8 according to Marjolijn and Rosa gives this role a score of 7.

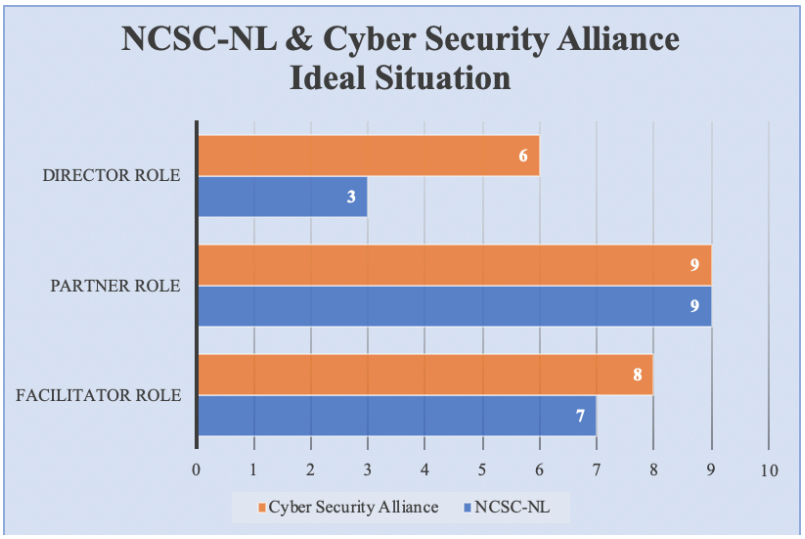


Figure 11 - Ideal role NCSC-NL in cooperation with Cyber Security Alliance

Considering the current and ideal situation in this cooperation according to the respondents, the current and ideal role are somewhat aligned. The main difference is the director role in the ideal situation according to Marjolijn because she believes that this role should be stronger in the ideal situation than is the case today. Finally, the current role of NCSC-NL in this cooperation is almost the ideal role according to the respondents.

Table 4 - Summary analysis cooperation NCSC-NL and Cyber Security Alliance

	MARJOLIJN	ROSA
Coalition	Collective coalition	Collective coalition Connective coalition
Benefits	To easily connect To share knowledge and visions To assess if needs are individual or collective needs	Participating parties are extremely motivated Parties are willing to spend time and efforts Large variety of insights Interests of public and private sector are coming closer together
Disadvantages	Lack of time Important to show added value Some parties are very active, but others are not The extent of the network Sometimes unclear how the roles are being divided	No formal power so depending on motivations People look at others Easy to end up with nothing happening Risk of lack of commitment
Goals and focus	Collaboration Information sharing Knowledge exchange	To adhere to goals of NCSA Agenda Clear and tangible results for all organizations in the Netherlands Information sharing Networking Meet the mutual mission
Current role	Director role: Low Partner role: Extremely High Facilitator role: Medium High	Director role: Low Partner role: Extremely High Facilitator role: Medium High
Ideal role	Director role: Medium Partner role: Extremely High Facilitator role: High	Director role: Low Partner role: Extremely High Facilitator role: Medium High

5.2 Analysis per role

In this part of the analysis, per role a comparison is made between the perception of the NCSC-NL respondent and the external respondent on the role of the NCSC-NL. Afterwards an answer is given on each hypothesis.

5.2.1 Director role NCSC-NL

First role investigated is the director role. All respondents have given a score on a scale of 0 and 10 on how strong or weak they think the current director role is at the moment and how it should be. These scores are shown in the table below.

Table 5 - Average current and ideal DIRECTOR ROLE NCSC-NL

DIRECTOR ROLE				
	CURRENT SITUATION		*IDEAL SITUATION*	
	Outside	**NCSC-NL**	**Outside**	**NCSC-NL**
Cooperation 1: NCSC-NL & ISAC	2	6	1	0
Cooperation 2: NCSC-NL & DTC	8	1,5	2	1
Cooperation 3: NCSC-NL & CVN	3	3	7,5	5
Cooperation 4: NCSC-NL & CSA	3	3	6	3
Average	***4***	***3***	***4***	***2***

Orange = outlier down
Green = outlier upwards

As shown in the table above, the responses of the respondents of the four cooperations on the director role of the NCSC-NL are rather aligned. Most respondents believe that the NCSC-NL should play a weak director role in public-private cooperation. However, there are some outliers visible. Although the majority of the respondents give a low score to the director role in the current cooperation, the DTC respondent considers the director role of the NCSC-NL in the current situation as very strong (8). Also, in cooperation 3 the CVN respondent thinks that in

the ideal situation should be much stronger (7,5) than is the case in the current situation. Meanwhile, the NCSC-NL respondent believes that in the ideal situation the NCSC-NL should not play a director role at all (0). Yet, the overall perception of the respondents is that the NCSC-NL has a weak director role in the current situation and should also play a weak director role in the ideal situation. Herewith the first hypothesis can be answered:

*NCSC-NL **should not** play a director role in public-private cooperation in cyber security*

5.2.1 Partner role NCSC-NL

The second role examined is the partner role. Based on a scale of 0 and 10, per cooperation respondents have given a score on what they think is the partner role of the NCSC-NL in the current situation and what they believe this role should be in the ideal situation. The results are shown in the table below.

Table 6 - Average and current PARTNER ROLE NCSC-NL

PARTNER ROLE				
	CURRENT SITUATION		*IDEAL SITUATION*	
	Outside	**NCSC-NL**	**Outside**	**NCSC-NL**
Cooperation 1: NCSC-NL & ISAC	6	3	10	8
Cooperation 2: NCSC-NL & DTC	2	7	8	9
Cooperation 3: NCSC-NL & CVN	3	7	7,5	7
Cooperation 4: NCSC-NL & CSA	9	9	9	9
Average	***5***	***6,5***	***8,5***	***8***

Orange = outlier down
Green = outlier upwards

In the ideal situation the partner role gets a very high score of all respondents. However, in the current situation this score is, except for cooperation 4, much lower. In the current situation

DTC and CVN give a score of respectively 2 and 3 to the partner role. In contrast to the NCSC-NL that gives itself a 7 in the cooperation with DTC and CVN. In the ideal situation all respondents of cooperation 2 and 3 give a much higher score to the partner role. Looking at cooperation 1, the external respondent believes that the NCSC-NL scores a 6 on the partner role in the current situation while the NCSC-NL respondent gives a score of 3. Though, both respondents give a very high score to the partner role in the ideal situation. Remarkable is that in cooperation 4 both respondents give an extremely high score of 9 in the current and in the ideal situation. Thus, both respondents in this cooperation are rather aligned. Considering these results, all respondents agree that in the current situation the partner role is low and should be much stronger in the ideal situation. Therefore, the second hypothesis can be confirmed.

*NCSC-NL **should** play a partner role in public-private cooperation in cyber security*

5.2.3 Facilitator role NCSC-NL

The last role, the facilitator role, shows some important similarities but also differences as shown in the table below.

Table 7 – Average current and ideal FACILITATOR ROLE NCSC-NL

FACILITATOR ROLE				
	CURRENT SITUATTION		*IDEAL SITUATION*	
	Outside	**NCSC-NL**	**Outside**	**NCSC-NL**
Cooperation 1: NCSC-NL & ISAC	9	9	8	0
Cooperation 2: NCSC-NL & DTC	5	5	8	7
Cooperation 3: NCSC-NL & CVN	8	6	3	8
Cooperation 4: NCSC-NL & CSA	7,5	7	8	7
Average	***7***	***7***	***7***	***5,5***

Orange = outlier down
Green = outlier upwards

Perceptions of the respondents on the facilitator role are rather fragmentated. In cooperation 1, both respondents in the cooperation agree on a very strong (9) facilitator role for the NCSC-NL in the current situation. Although the external respondent also wishes for a strong facilitator role in the ideal situation (8), the NCSC-NL respondent believes that in the ideal situation the NCSC-NL should not play a facilitator role at all (0). The respondents of cooperation 2, both agree that the facilitator role in the current situation is rather weak (5) but should be stronger in the ideal situation (NCSC-NL 7/DTC 8). The third cooperation shows more dissimilarities. Whereas the external respondent thinks that the NCSC-NL has a very strong facilitator role (8) in the current situation, in the ideal situation this should be much weaker (3) according to the respondent. In addition, the NCSC-NL respondent prefers the NCSC-NL to strengthen its facilitator role from 6 in the current situation to 8 in the ideal situation. Last, in cooperation 4 respondents are much more aligned on the facilitator role in the current situation (CSA 7 and NCSC-NL 7,5) and in the ideal situation (8 and 7). Concluding, although the respondents do not agree on the strength of the facilitator role, but except for the NCSC-NL respondent they all agree that the NCSC-NL should play a facilitator role. Hypothesis 3 can therefore be confirmed:

*NCSC-NL **should** play a facilitator role in public-private cooperation in cyber security*

6. Conclusion

The literature and interviews in this research give insights into the research question of this study:

What role (director, partner or facilitator) should the National Cyber Security Centre (NCSC-NL) play in public-private cooperation in cyber security?

6.1 Conclusions

As a consequence of the increasing cyber threats, over the last years a growing number of public-private cooperations can be observed in the Dutch cyber security landscape. One of the key players in cyber security cooperation in the Netherlands is the NCSC-NL. Working together with public and private organizations requires for NCSC-NL to determine its role in public-private cooperation. This research examines the role of the NCSC-NL in the current and ideal situation according to the model of the Spectrum of Coalition Formation of Twynstra Gudde (2019). This model defines three roles; the director, partner and facilitator role. The director role has a more directive approach in the cooperation and one or few organizations have a clear ambition that they are willing to realize in coordination with others. The partner role is focused within a group of organizations that all share one ambition. Last role, the facilitator role is a role wherein the coalition started with the initiative of one or few organizations and is open to anyone interested to join. There is no fixed ambition and participants can bring in their ideas and thoughts on the ambition. Here, the individual organization plays an important role.

In this study the above roles have been applied to four public-private cooperations in cyber security to trace the role of the NCSC-NL in the current and ideal situation. Each case study includes two respondents, one of the NCSC-NL and external respondent. At the start of this research the current role of the NCSC-NL was not yet determined. The main goal of this study was to investigate how the NCSC-NL and its collaboration partners perceive the current role of the NCSC-NL in the cooperation. Then the respondents were asked what they believe that the ideal role for the NCSC-NL should be in public-private cooperation. The main conclusions based on the literature and interviews are as follows.

1. **Public-private cooperations in cyber security are rather premature**

   Due to the novelty of PPPs in cyber security, this arena is rather immature. Today, public and private organizations working together in the field of cyber security is relatively new and organizations are therefore still searching for their position in the field. This also goes for the NCSC-NL. The organization is still searching what role to play in the Dutch cyber security landscape and in particular in public-private cooperation.

2. **Roles in public-private cooperation in cyber security are not yet determined**

   At this moment, the role of the NCSC-NL in PPPs in cyber security is not evident and not yet defined. In the interviews with the respondents, it was obvious that the interpretations of the role of the NCSC-NL were dissimilar. Respondents have different perceptions on the current role of the NCSC-NL and were often not aligned on the exact meanings. It is evident that the NCSC-NL organization did not yet carefully think through its role in PPPs.

3. **Roles in cyber security cooperation are fluid**

   Each phase in the cooperation might require a different role for the NCSC-NL and defining roles is therefore not set in stone but an ongoing process. It may depend on the maturity level of organizations or on the phase of the cooperation which role should be played in the cooperation.

4. **Defining roles in the cooperation means at the same time defining if and how organizations work together**

   The role of the NCSC-NL appears to be extremely relevant for the way how public and private organizations work together with the NCSC-NL.

5. **The NCSC-NL should not or to a very small extent play a director role in public-private cooperation**

   According to the respondents in this research, in case the NCSC-NL plays a strong director role in public-private cooperation, this will affect the willingness of organizations to work together with the NCSC-NL. However, in special circumstances, for instance when national security is at stake, the NCSC-NL should play a stronger director role according to the respondents.

6. **The NCSC-NL should play a strong partner role in public-private cooperation**
   The most preferred role, the partner role, appears to be the ideal role for the NCSC-NL according to the respondents. External respondents as well as the NCSC-NL respondents agree that in the responsibility of the NCSC-NL to keep the Netherlands digitally safe the partner role would be most suitable.

7. **The NCSC-NL should play a facilitator role in public-private cooperation, however limited**
   In the interviews the majority of the respondents preferred a facilitator role for the NCSC-NL, but they did not agree on how this role should be performed. Compared to the director and partner role, the facilitator role was much more subject to different interpretations of the respondents.

The conclusion of this study is that the NCSC-NL should focus and further develop its partner role in public-private cooperation in cyber security. According to the respondents of this study this partner role can sometimes also be combined with the facilitator role. Though, the director role is less favorite with the respondents and should be minimalized as much as possible. Based on the data of this research, it can be concluded that the role or roles performed by the NCSC-NL has consequences for how organizations work together with the NCSC-NL in public-private cooperation in cyber security. To collaborate with other organizations in public and private sector it is therefore important for the NCSC-NL to determine its role or roles to meet the expectations. This way, it is evident for organizations what role the NCSC-NL plays and if and how other organizations prefer to work with the NCSC-NL and vice versa. Besides, it is fundamental that the role or roles of the NCSC-NL are continuously evaluated and were needed adjusted throughout the cooperation. By doing so, public-private cooperation in cyber security in the Netherlands can further develop.

6.2 Recommendations

The experiences of the respondents interviewed in this research, are important lessons learned for the role arrangement in existing public-private cooperations in cyber security but also for any future initiatives. To improve its role in public-private cooperation in cyber security, it is therefore recommended for the NCSC-NL that:

1. **The NCSC-NL should clearly define its role or roles**

   To meet the mutual expectations, it is inevitable for the NCSC-NL, prior to the start of the cooperation, think carefully through what role to play in the cooperation.

2. **The NCSC-NL should create a clear strategy on how it aims to cooperate with public and private organizations**

   The NCSC-NL should carefully think through what strategy the organization prefers to perform in the cooperation. Per public-private cooperation a strategy should be created that fits into the overall strategy of the NCSC-NL.

3. **The NCSC-NL should further deepen its partner role in public-private cooperation**

   To bring its current partner role in public-private cooperation to a higher level, the NCSC-NL should focus on how to further improve this partner role.

4. **The NCSC-NL should reduce its director role**

   The director role is not preferred by the respondents and even calls for resistance. Therefore, the organization should minimalize its director role in current and future cooperations. However, in case of emergencies, the director role is preferable.

5. **The NCSC-NL should work on its facilitator role**

   The current understanding of the facilitator role is rather fragmented. Therefore, the NCSC-NL should further explore what this role contains and how it prefers to fill in this role.

6. **Continuous improvement**

   It is recommended that the NCSC-NL evaluates its role or roles on a regular basis.

6.3 Discussion

In this research the current and ideal role for the NCSC-NL have been investigated by analyzing four public-private cooperations in cyber security. Based on the results in this research, it is evident that only assigning roles is not enough. Because public-private cooperation in cyber security is relatively new, there are still many questions on this topic. There are for instance only few standards set yet on cyber security collaboration. Existing cooperations are often created out of opportunities instead of a thoughtful strategy. Therefore, lessons learned from recent experiences in public-private cooperation, can be used to improve future cooperations.

This study has disclosed many questions for further research. First of all, public-private cooperation in cyber security goes through different phases. How can roles be defined and what role should be played in which phase of the cooperation? Also, in cooperation it is not about defining roles only but also to give substance to these roles by all organizations. Therefore, to improve the division of roles in public-private cooperation in cyber security further research is recommended. In the dynamic landscape of cyber security cooperation, additional research could also help to further improve other aspects of public-private cooperation in cyber security. However, for the NCSC-NL in particular, it is suggested to do further research on its role within public-private cooperation. Since the NCSC-NL is one of the key players in the Netherlands, this would definitely contribute to take position for the organization not only in the landscape but also in public-private cooperation in cyber security in general.

Bibliografie

AGConnect. (2018*). BZK zet fors in op cybersecurity en digitale overheid*. AG Connect website Retrieved from: https://www.agconnect.nl/artikel/bzk-zet-fors-op-cybersecurity-en-digitale-overheid

AIVD. (2019). *Over de AIVD.* AIVD website
Retrieved from: https://www.aivd.nl/onderwerpen/over-de-aivd

Betaalvereniging Nederland. (2019). *Publiek-Private Samenwerking.* Betaalvereniging website
Retrieved from: https://www.betaalvereniging.nl/veiligheid/publiek-private-samenwerking/

Boeke, S. (2017). *National cyber crisis management: Different European approaches.* Wiley Governance, p. 1-16

Cambridge Dictionary. (2019). *Coalition.* Cambridge website
Retrieved from: https://dictionary.cambridge.org/dictionary/english/coalition

Carr, M. (2016). *Public-private partnerships in national cyber-security strategies*. International Affairs 92: 1, p. 44-62

Corbin, J., Strauss, A. (1990). *Grounded Theory Research: Procedures, Canons and Evaluative Criteria.* Qualitative Sociology. Vol. 13, No. 1

Cyber Security Alliantie. (2019). *Over de CS Alliantie.* Cyber Security Alliantie website
Retrieved from : https://www.cybersecurityalliantie.nl/over-de-alliantie

Cyberveilig Nederland. (2019). *Brancheorganisatie 'Cyberveilig Nederland' maakt samenleving digitaal weerbaarder.* Cyberveilig Nederland website
Retrieved from: https://cyberveilignederland.nl

De Jong, M. (2015). *Adaptief samenwerken in verschillende coalities.* SomSammag Achtergrond, p. 2-13.
Retrieved from:
https://www.researchgate.net/publication/334785221_ADAPTIEF_SAMENWERKEN_IN_VERSCHILLENDE_COALITIES

Digital Trust Center (DTC). (2018). *Digital Trust Center maakt veilig digitaal ondernemen makkelijker.* Digital Trust Center website
Retrieved from: https://www.digitaltrustcenter.nl/actueel/nieuws/2018/06/08/digital-trust-center-maakt-veilig-digitaal-ondernemen-makkelijker

Digital Trust Center (DTC). (2019). *Over het Digital Trust Center.* Digital Trust Center website
Retrieved from: https://www.digitaltrustcenter.nl/over-het-digital-trust-center

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

Eriksson, J., Rhinard, M. (2009). *The Internal External Security Nexus: Notes on an Emerging Research Agenda.* Cooperation and Conflict 2009; 44, p. 243-267

European Union Agency for Network and Information Security (ENISA). (2010). *Incentives and Challenges for Information Sharing in the Context of Network and Information Security.* ENISA website
Retrieved from: https://www.enisa.europa.eu/publications/incentives-and-barriers-to-information-sharing

European Union Agency for Network and Information Security (ENISA). (2014). *An evaluation Framework for National Cyber Security Strategies.* ENISA website
Retrieved from: https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies

European Union Agency for Network and Information Security (ENISA). (2017a). *Information Sharing and Analysis Centres (ISACs), Cooperative models,* p. 1-51
Retrieved from: https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models

European Union Agency for Network and Information Security (ENISA). (2017b). *Public Private Partnerships – Cooperative models,* p. 1-47
Retrieved from: https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models

Government of the Netherlands. (2019a). *Ministries*. Government website
Retrieved from: https://www.government.nl/ministries

Government of the Netherlands. (2019b). *Ministry of Defence*. Government website
Retrieved from: https://www.government.nl/ministries/ministry-of-defence

Government of the Netherlands. (2019c). *Ministry of Economic Affairs and Climate Policy*. Government website
Retrieved from: https://www.government.nl/ministries/ministry-of-economic-affairs-and-climate-policy

Government of the Netherlands. (2019d). *Ministry of the Interior and Kingdom Relations*. Government website
Retrieved from: https://www.government.nl/ministries/ministry-of-the-interior-and-kingdom-relations

Government of the Netherlands. (2019e). *About the Ministry.* Government website
Retrieved from: https://www.government.nl/ministries/ministry-of-foreign-affairs/about-the-ministry

Government of the Netherlands. (2019f). *Ministry of Education, Culture and Science*. Government website
Retrieved from: https://www.government.nl/ministries/ministry-of-education-culture-and-science

Government of the Netherlands. (2019g). *Ministry of Justice and Security.* Government website
Retrieved from: https://www.government.nl/ministries/ministry-of-justice-and-security

Government of the Netherlands. (2019h). *The National Cyber Security Centre (NCSC) bundles knowledge and expertise.* Government website
Retrieved from: https://www.government.nl/latest/news/2012/01/12/the-national-cyber-security-center-ncsc-bundles-knowledge-and-expertise

Harkins, R., English, E. (2019). *Guarding the Public Sector: Seven Ways State Governments Can Boost Their cybersecurity.* Marsh & McLennan Insights website
Retrieved from: http://www.mmc.com/insights/publications/2018/oct/guarding-the-public-sector--seven-ways-state-governments-can-boo.html

Hathaway, M., Spidalieri, F. (2017). *The Netherlands cyber readiness at a glance.* Potomac Institute for Policy Studies, p. 1-50
Retrieved from:
https://www.thehaguesecuritydelta.com/media/com_hsd/report/139/document/CRI-Netherlands-Profile-PIPS.pdf

Inspectie Justitie en Veiligheid. (2015). *Gebruik van veiligheidsadviezen van het Nationaal Cyber Security Centrum. Thematisch inspectieonderzoek.* The Hague Security Delta website, p. 1-36
Retrieved from:
https://www.thehaguesecuritydelta.com/media/com_hsd/report/52/document/inspectierapport-beveiligingsadviezen-ncsc-webversie.pdf

Kooistra, S., Modderkolk, H. (2015). *Overheid veel vaker doelwit van cyberaanvallen.* De Volkskrant website
Retrieved from: https://www.volkskrant.nl/wetenschap/overheid-veel-vaker-doelwit-van-cyberaanvallen~b3290ec8/

Koppenjan, J., de Jong, M. (2017). *The introduction of public-private partnerships in the Netherlands as a case of institutional bricolage: The evolution of an Anglo-Saxon transplant in a Rhineland context.* Public Administration, p. 1-14

Luiijf, E., Kernkamp, A. (2015). *Sharing Cyber Security Information – Good practice Stemming from the Dutch Public-Private-Participation Approach.* Conference Paper Global Conference on CyberSpace 2015. TNO website
Retrieved from:
https://www.researchgate.net/publication/274635680_Sharing_Cyber_Security_Information

Ministry of Defence. (2019a). *Defensie Cyber Commando*. Ministry of Defence website
Retrieved from: https://www.defensie.nl/onderwerpen/cyber-security/cyber-commando

Ministry of Defence. (2019b). *Defensie Computer Emergency Response Team*. Ministry of Defence website
Retrieved from: https://www.defensie.nl/onderwerpen/cyber-security/defcert

Ministry of Economic Affairs and Climate Policy (2018). *Dutch Digitalisation Strategy, getting the Netherlands ready for the digital future.* Ministry of Economic Affairs and Climate Policy, p. 7-46
Retrieved from: https://www.government.nl/documents/reports/2018/06/01/dutch-digitalisation-strategy

Ministry of Economic Affairs and Climate Policy (2019). *Factsheet Digital Trust Center.* Ministry of Economic Affairs website
Retrieved from: https://www.digitaltrustcenter.nl/sites/default/files/2019-12/Factsheet%20DTC%20English%20version.pdf

National Cyber Security Centre (NCSC). (2019). *Partners van het NCSC*. NCSC website
Retrieved from: https://www.ncsc.nl/over-ncsc/onze-partners

National Coordinator for Security and Counterterrorism (NCTV). (2019a). *Beschermen van een veilig Digitaal Nederland.* NCTV website
Retrieved from: https://www.nctv.nl/themas/cybersecurity

National Coordinator for Security and Counterterrorism (NCTV). (2019b). *Counterterrorism.* NCTV website
Retrieved from: https://english.nctv.nl/themes/counterterrorism

National Coordinator for Security and Counterterrorism (NCTV). (2019c). *Cyber Security*. NCTV website
Retrieved from: https://english.nctv.nl/themes/cyber-security

National Coordinator for Security and Counterterrorism (NCTV). (2019d). *National Cyber Security Centrum.* NCTV website
Retrieved from: https://www.nctv.nl/onderwerpen/nationaal-cyber-security-centrum

National Democratic Institute for International Affairs (NDI). (2004). *Coalition Best Practices. NDI West Bank and Gaza.*
Retrieved from:
https://www.ndi.org/sites/default/files/1811_coalbestpractwestgaza_010104_5.pdf

Nederland Wereldwijd. (2019). *Naast 'techies' ook diplomaten nodig voor een stabiel cyberspace*. Nederland Wereldwijd website
Retrieved from:
https://www.nederlandwereldwijd.nl/actueel/weblogs/weblogberichten/2019/%E2%80%98naast-%E2%80%9Ctechies%E2%80%9D-ook-diplomaten-nodig-voor-een-stabiel-cyberspace%E2%80%99

NOS Nieuws. (2019). *Bedrijven en overheid maandenlang kwetsbaar door groot beveiligingslek.* NOS-website
Retrieved from: https://nos.nl/l/2303667

Nu.nl (2012). *Zwaar verouderde website was oorzaak Diginotarhack,* NU.nl website
Retrieved from: *https://www.nu.nl/internet/2961331/zwaar-verouderde-website-was-oorzaak-diginotar-hack.html*

Olsthoorn, S., Jonker, U. (2019). *Justitie wil ingrijpen bij bedrijven die digitale beveiliging niet op orde hebben*. FD-website
Retrieved from: https://fd.nl/ondernemen/1318504/justitie-wil-ingrijpen-bij-bedrijven-die-digitale-beveiliging-niet-op-orde-hebben

Prins, J.R. (2011). *Interim Report, DigiNotar Certificate Authority breach "Operation Black Tulip"*. Fox-IT report, p. 1-13

Rijksoverheid. (2019*). Missie*. Government website
Retrieved from: https://www.rijksoverheid.nl/ministeries/ministerie-van-economische-zaken-en-klimaat/organisatie

Rosman, C. (2019). *AIVD: Digitale aanvallen op Nederland steeds agressiever.* AD website
Retrieved from: https://www.ad.nl/tech/aivd-digitale-aanvallen-op-nederland-steeds-agressiever~a0b62f6d/

Sobers, R. (2019). *60 Must-Know Cybersecurity Statistics for 2019*. Veronis website
Retrieved from: https://www.varonis.com/blog/cybersecurity-statistics/

SSC-ICT. (2019). *Monitoring Cyberspace*. Ministry of Interior Affairs and Kingdom Relations
Retrieved from: https://www.ssc-ict.nl/onze_dienstverlening/global_conference_cyber_space/index.aspx

Twynstra Gudde. (2019). *Banden bouwen voor digitaal Nederland. Een onderzoek naar de professionalisering van samenwerking rond cybersecurity.* Twynstra Gudde, p. 1-48

Vaillancourt Rosenau, P. (2012). *The Strengths and Weaknesses of Public-Private Policy Partnerships.* University of Texas. Houston. SAGE Publications, p. 10-34

Von Solms, R., van Niekerk, J. (2013). *From information security to cyber security.* Computers & Security 38, ScienceDirect, Elsevier, p. 97-102

Interview guideline

Checklist:

- Introduction of the researcher
- Background of the research: to examine the role of the National Cyber Security Centre (NCSC-NL) in public-private cooperation in cyber security
- The research question: '*What role (director, partner or facilitator) should the National Cyber Security Centre play in public-private cooperation in cyber security?'*
- Procedure: four public-private partnerships in cyber security have been identified with involvement in any form of NCSC-NL, namely: Information Sharing and Analysis Centre (ISAC), Digital Trust Center (DTC), Cyberveilig Nederland and Cyber Security Alliance. From each of these partnerships, one person from NCSC-NL and one person of the partnership will be interviewed.
- The conversation will be recorded. Request for permission.

Introduction

- Can you tell me a bit about yourself? Who are you? What is your background?
- How did you get to this position?
- Why are you participating in this research?

Collaboration

- Considering the model of the Spectrum of Coalition Formation of Twynstra Gudde, in which coalition would you share the current cooperation?
- What is the reason for you to make this choice?
- Which benefits do you identify in this coalition?
- Which disadvantages do you identify in this coalition?
- What are the main goals of this cooperation?
- What is the focus of this cooperation?
- What do you think is the current role of NCSC-NL in this cooperation?
- What do you think should be the ideal role of NCSC-NL in this cooperation?
- Why do you choose this role/ these roles?
- Do you have anything to add?

List of respondents

Name	Position	Organization	Date of Interview
Liesbeth Holterman	Policy Advisor	Cyberveilig Nederland	02-12-2019
Michael Meijerink	Product Manager Threat Analysis	National Cyber Security Centre (NCSC-NL)	06-12-2019
Mireille Kok	Coordinator Vital Organizations	National Cyber Security Centre (NCSC-NL)	06-12-2019
Thom Spitzen	Security Officer	Stedin	06-12-2019
Rosa Gompen-Van Zijl Jansen	Coordinating Policy Advisor	National Cyber Security Centre (NCSC-NL)	09-12-2019
Kees Boerkamp	Account Manager	National Cyber Security Centre (NCSC-NL)	09-12-2019
Jacco van der Kolk	Relation Manager	Digital Trust Center (DTC)	09-12-2019
Marjolijn Bonthuis-Krijger	Deputy Director	Platform for the Information Society (ECP)	10-12-2019